Information & Computer Security

Deterrence and punishment experience impacts on ISP compliance attitudes
Salvatore Aurigemma, Thomas Mattson,

Deterrence and punishment experience impacts on ISP compliance attitudes

Salvatore Aurigemma
Department of Computer Information Systems, University of Tulsa, Tulsa, Oklahoma, USA, and
Thomas Mattson
Robins School of Business, University of Richmond, Richmond, Virginia, USA

Received 27 November 2016
Revised 2 March 2017
Accepted 3 March 2017

Abstract

Purpose – The paper aims to examine the inconclusive impacts of sanction-related deterrence on employee information security policy (ISP) compliance from the extant literature. It proposes that the disparate findings can be partially explained by two factors: investigating the mediating impact of attitudes on sanction effects instead of directly on behavioral intentions and examining employees with and without previous punishment experiences separately.

Design/methodology/approach – The paper relied upon survey data from 239 employees of a large governmental organization with a robust ISP and security education and training awareness program.

Findings – The paper provides empirical evidence that the rational estimation of sanction effects impacts the cognitive component of attitudes to develop a positive or negative attitude toward performing the ISP directed behavior. Furthermore, this attitudinal effect (created by sanction threats) will be biased depending on whether the employee has experienced, personally or vicariously, any previous punishment for violating the ISP.

Research limitations/implications – Because of the chosen research approach (self-reported survey data) and context (single hierarchical organization and a very specific security threat), the research results may lack generalizability. Therefore, researchers are encouraged to test the proposed propositions further in different organizational and threat contexts.

Practical implications – Organizations should have a thorough understanding of how their employees' perceive sanctions in relationship to their prior experiences before implementing such policies.

Originality/value – The paper addresses previous research calls for examining possible mediation variables for deterrence effects and impacts of punishment experiences on employee ISP compliance.

Keywords Information security, Punishment, Policy compliance, Sanctions, Deterrence

Paper type Research paper

Introduction

Employees and supporting contractors are often considered the weakest link in information security because technical security systems are only as strong as the employees operating them (Mitnick and Simon, 2011; Wall, 2013; Cole, 2015; Shropshire *et al.*, 2010). Due to a variety of human factors such as ignorance, apathy, resistance, naivety, honest mistakes and disobedience, employees knowingly or unknowingly place the organization's information assets at risk (Harris and Furnell, 2012). The main mechanism to assist employees in protecting organizational information resources is the information security policy (ISP) (Smith, 2015)[1]. Yet, simply having a well-documented set of policies and procedures is not, by itself, good enough to deter information security breaches (Safa *et al.*, 2016). Employees

Information & Computer Security
Vol. 25 No. 4, 2017
pp. 421-436

2056-4961
DOI 10.1108/ICS-11-2016-0089

must be adequately trained on the ISPs *and* have the intrinsic and/or extrinsic motivation to abide by the policies and procedures.

One way to motivate or encourage employees to comply with organizational ISPs is the threat of sanctions under the broad umbrella of general deterrence theory (GDT) (D'Arcy *et al.*, 2009). GDT proposes that employees can be discouraged from breaking the rules (i.e. violating the policies in the ISP) through the use of disincentives matched with appropriate sanctions (Wall *et al.*, 2015). In other words, increasing the likelihood of being caught when breaking the rules and having a 'just' punishment should an employee be caught will incentivize an employee to follow the rules (Cheng *et al.*, 2013). Understanding sanction effects are important because the threat of employee punishment for non-compliance with requirements should be (and typically is) a cornerstone of all ISPs (Diver, 2006). For good reason, a significant number of studies have focused on the impact of sanctions on an employee's intent to follow the ISP (D'Arcy *et al.*, 2009; D'Arcy and Herath, 2011; Willison and Warkentin, 2013; Cheng *et al.*, 2013; Hovav and D'Arcy, 2012; Harris and Furnell, 2012).

However, the results from ISP compliance-related research on the effectiveness of sanctions are inconclusive in terms of the direct effect of sanctions on behavioral intentions to follow required or recommended security actions (Hu *et al.*, 2011; Cheng *et al.*, 2013; Guo and Yuan, 2012; Barlow *et al.*, 2013; D'Arcy and Herath, 2011; Liao *et al.*, 2009). The purpose of our paper is to further investigate sanction effects using GDT to help make sense of these mixed empirical results. We argue that the mixed empirical results can be partially explained by two factors:

(1) examining the impact of attitudes as a mediator between sanction effects and ISP behavioral intentions; and

(2) examining the impact of past punishment experiences as a moderating factor.

We argue that the threat of sanctions creates attitude-dependent (as opposed to direct act oriented) information security behaviors because perceived sanction threats create an attitude awareness concerning the impact of complying or not complying with information security policies. Consistent with previous literature (D'Arcy and Herath, 2011; Bulgurcu *et al.*, 2010; Herath and Rao, 2009; Moquin and Wakefield, 2016), we argue that the rational estimation of sanction effects impacts the cognitive component of attitudes to develop a positive or negative attitude toward performing the ISP-directed behavior, which then impacts behavioral intentions to comply with the information security policies.

We further suggest that the positive or negative attitudes created by sanction threats will be biased depending on whether the employee has experienced, personally or vicariously, any previous punishment for violating the security rules and regulations because attitudes are heavily shaped by previous experiences (Harris and Furnell, 2012). We provide empirical support for these conjectures using a survey of employees from a large government organization. We specifically investigate compliance attitudes and behavioral intentions associated with the unauthorized use of flash media (USB drives) because these cheap, convenient and small storage devices have been a security thorn to all types of organizations for years (Silowash and King, 2013; Krombholz *et al.*, 2015).

Theoretical background and research hypotheses

IS behavioral information security research has improved our knowledge of the behavior of non-malicious employees in complying (or not complying) with ISPs using theories such as the theory of planned behavior (TPB), rational choice theory, protection motivation theory, and GDT (Barlow *et al.*, 2013; Crossler *et al.*, 2013). Despite this theoretical diversity, one commonality across many of the studies is the theorized (or assumed) link between

behavioral intentions and actual security related behaviors (Aurigemma, 2013). This means that employees will (on average) act on their intentions to comply or to not comply with an organization's ISPs (Ajzen, 1985). This linkage has become a cornerstone of ISP behavioral compliance research due to the difficulty in gaining access to organizational data related to actual employee non-compliance in this sensitive area (Kotulic and Clark, 2004). The idea of behavioral intentions is derived from the TPB (Ajzen, 1985).

The TPB proffers that an individual's intention to take an action, given some actual control over the behavior in question, generally leads to that actual behavior taking place. According to the theory, individual behavioral intentions are determined by personal attitudes, social pressures (subjective norms) and a sense of control (perceived behavioral control) (Ajzen, 1985). The TPB has been used in numerous studies specifically aimed at improving awareness of factors affecting employee compliance intentions with ISPs and other information security behaviors. Of the core TPB constructs, attitude has been consistently found to be one of the strongest predictors of behavioral intent within ISP compliance research (Bulgurcu *et al.*, 2010; Dinev and Hu, 2007; Guo *et al.*, 2011; Hu *et al.*, 2011; Karahanna *et al.*, 1999; Zhang *et al.*, 2009).

Many factors can impact the formation of positive or negative attitudes such as rational decision making processes and past experiences (Bulgurcu *et al.*, 2010; Herath and Rao, 2009; Liao *et al.*, 2009). A component of rational decision making concerning whether to comply with an organizational ISP is an evaluation of the threat of being punished, which falls under the broad umbrella of GDT. GDT is prominent in the study of criminology (i.e. deterring criminal activity related to murders, car thefts and so on) with its roots dating back hundreds of years (Straub, 1990; Siponen and Vance, 2010). GDT leans on the effectiveness of formal sanctions to influence an individual's decision to commit or abstain from an unwanted act (Theoharidou *et al.*, 2005). It conceptually consists of three components of sanction effects:

(1) severity (harshness of the punishment);

(2) certainty (likelihood of getting caught); and

(3) celerity (swiftness of the process) (Gibbs, 1975).

The general idea behind the theory is relatively straightforward. Given equal conditions (i.e. speed (celerity) of the judicial process), the harsher the punishment and the greater the likelihood of being implicated, the less likely a crime will be committed (D'Arcy *et al.*, 2009). In the criminology literature, punishment certainty has consistently been found to have a greater deterrent effect than punishment severity (Nagin and Pogarsky, 2001; Von Hirsch *et al.*, 1999). That is, not being able to get away with the crime reduces criminal activity more than the seriousness of the punishment for getting caught.

Perceived sanction severity and certainty are the most prominent components of the GDT represented in ISP-related research (D'Arcy and Herath, 2011). However, research on these factors in the ISP context has yielded mixed results. For example, Hu *et al.* (2011), Guo *et al.* (2011) and Pahnila *et al.* (2007) found perceived deterrence (defined as a unitary variable) to have no impact on an employee's behavioral intent, whereas Bulgurcu *et al.* (2010) found the opposite. Others (Cheng *et al.*, 2013, Herath and Rao, 2009, D'Arcy *et al.*, 2009) found perceived sanction severity to have a significant effect on intent, whereas perceived certainty of sanction imposition was not significant, which is counter to the general finding in the criminology literature (Nagin and Pogarsky, 2001). Part of this overall lack of consistency in research results may be attributable to not modelling the interaction of sanction severity and probability because different levels of sanction severity may work

better or worse based on different levels of probability of being caught (D'Arcy *et al.*, 2009). In essence, the relationship may not be straight-forward main effects only relationship.

Sanction effects are a negative component of rational choice theory, which argues that behavior is determined by balancing costs and benefits of different options (Simon, 1955). In terms of the GDT, the cost calculation of violating the ISP rules is an additive or multiplicative function of sanction certainty and the associated punishments, whereas the benefit is being able to, possibly, perform a job task more efficiently (albeit with greater information security risks) due to skipping steps in the process (D'Arcy and Herath, 2011). Bulgurcu *et al.* (2010) argue that when individuals rationally determine the costs and benefits of complying or not complying with information security policies, individuals are shaping their attitudes concerning compliance (as opposed to directly impacting their behavioral intentions). This makes logical sense because an attitude toward a particular behavior is an individual's overall evaluation of the desirability of implementing a behavior (Ajzen, 2001). The desirability of implementing a behavior is certainly impacted by the costs and benefits associated with following or not following the rules (Bulgurcu *et al.*, 2010; Workman *et al.*, 2008; Moquin and Wakefield, 2016). Once an individual's attitudes are formed concerning the behavior, he/she will then choose to perform or not perform the action (Liao *et al.*, 2009), which is consistent with the TPB (Ajzen, 2001). Therefore, we propose the following mediating hypothesis:

H1. The impact of sanction effects on ISP behavioral intentions will be mediated by attitudes.

Attitudes are heavily influenced by prior experiences (Safa and Von Solms, 2016; Ajzen, 2001). This poses an interesting issue for employees who have either been punished themselves or know of someone who has previously been punished. If the past punishment experience involved an employee who consistently broke the rules before getting caught (low probability of getting caught) and the punishment was a mere slap on the wrist (low sanction severity), then it would be logical to predict that this employee would develop a negative attitude toward complying with the ISP. If on the other hand, the past experience involved someone who got caught violating the policy the first time that he/she did something wrong (high probability of being caught) and the punishment involved a suspension or a cut in pay (high sanction severity), then it would be logical to predict that this employee would develop a positive attitude toward complying with the ISP. We suggest that employees who have no prior experiences will not be biased based on a lack of prior experiences because they have no direct or indirect knowledge to cognitively bias their attitudes toward compliance. Therefore, we expect that the standard sanction effects reported in the prior literature will be most applicable to them. These effects, however, may be quite different and biased in either a positive or a negative direction based on prior experiences depending on the nature of those prior experiences.

Harris and Furnell (2012) are one of the few studies related to ISP compliance that entertained the role of punishment experiences while evaluating the effect of shaming in the workplace using the Stafford and Warr (1993) expansion of the GDT. The Stafford and Warr (1993) model introduced the deterring effect of punishment experiences (personal and vicarious punishment and avoidance) as having a potentially major influence on compliance behaviors. Studies in criminology using the Stafford and Warr model provide interesting findings that may well apply to the study of the sanction effects in the ISP compliance context. For instance, Piquero and Pogarsky (2002) found that punishment experiences affect behavior by influencing sanction risk perceptions (severity and certainty). Paternoster and Piquero (1995) found that perceived certainty of a sanction was lowest for individuals

with little or no personal and vicarious punishment experience and highest for those with such experiences. Therefore, we propose the following moderating hypothesis relating to prior punishment experiences:

H2. The sanction effect antecedents to attitudes will be moderated by previous punishment experiences.

This hypothesis is not making a directional prediction concerning whether the moderation will be positive or negative because we propose that it depends on the context of the previous experiences. Certain prior experiences might create positive attitudes toward compliance whereas other experiences might create negative attitudes toward compliance. We are simply predicting that the effects of previous experiences will have a differential impact on the strength (and possibly the direction) of the attitudinal antecedents associated with sanction severity and probability. Figure 1 graphically summarizes the research model.

Research design and methods

Data for this study were collected using a questionnaire administered to the US Department of Defense (DoD) employees across multiple departments and work functions, all of whom fell under the same overarching ISP guidance at the time of survey data collection. The survey instrument was derived from empirically validated quantitative scales from related ISP behavioral compliance studies (see Table II). All items were measured reflectively using seven-point Likert scales ranging from (1) strongly disagree to (7) strongly agree. The survey was designed and administered using best practices outlined by Dillman *et al.* (2014) such as instruction wording, question order, participant follow-up and so on. The survey instrument was piloted twice, first with a group of three DoD security management practitioners at different organizations and then with 20 DoD personnel and academics. Each pilot study focused on question clarity and removing ambiguities, resulting in minor changes to the organization, structure and content of the survey instrument.

The DoD is an interesting research population that consists of over 3.5 million military and civilian employees. Despite the large number of employees in the DoD, they all fall under the same general ISP, known as DoD Information Awareness Assurance (IAA). Every DoD employee, regardless of rank, status, organization or work function, falls under the IAA guidelines and requirements, in addition to any more-restrictive individual command ISPs.

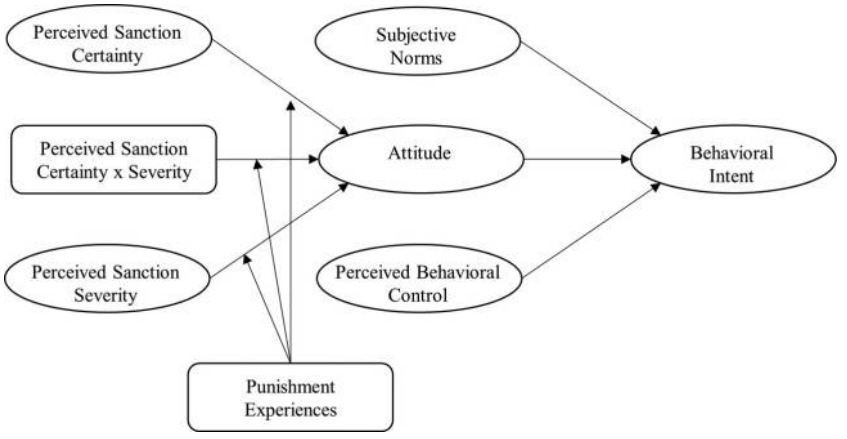

Figure 1.
Research model

All DoD employees are required to complete mandatory information security training annually. Additionally, failure to complete this training is meticulously tracked and results in loss of access to DoD IT systems (at a minimum) (Table I).

The specific information security threat examined in our paper is the use of unauthorized removable flash media (such as thumb drives). These cheap, convenient, small storage devices have been a security bane to all types of organizations for years (Silowash and King, 2013; Krombholz *et al.*, 2015) including being used in ongoing criminal activities (Pearce, 2016). Flash drives are routinely lost or misplaced by well-intentioned employees, which puts the organization's data at a significant risk, and flash drives often contain rootkits, viruses or bot executables that can further put the organization's information resources at risk (Tischer *et al.*, 2016; Williams, 2016). Additionally, organizations such as the DoD have policies and procedures in place to attempt to deter the improper use of flash media, but employees still engage in risky flash drive use practices (Silowash and King, 2013; Krombholz *et al.*, 2015). As such, studying GDT effects with this threat is highly relevant and useful due to the problems associated with deterring improper USB flash media usage.

The DoD banned the use of removable flash media and storage devices from all government computers in 2008 following the most significant breach of US military computers in modern history. The breach was caused by a flash drive, containing malicious code placed by a foreign intelligence agency, being inserted into a network-connected US military laptop at a remote base by a non-malicious employee (Lynn III, 2010). In 2010, the ban was partially rescinded for special cases and requires a new set of very restrictive compliance requirements. Table II shows the roles and responsibilities outlined in the ISP (at the time of the survey) for DoD employees and contractors related to removable flash media.

Our survey was primarily administered via an online survey tool. A paper version of the questionnaire (identical to the online version) was also available to potential respondents. Survey email invitations were sent to organization leaders who were then requested to provide the survey to their subordinate employees. A total of 1,380 DoD employees were provided the opportunity to participate in the survey. Individual survey responses were anonymous for both the organization and individual. In accordance with federal and DoD regulations, survey participation was voluntary and limited demographic data was collected to maintain anonymity. A total of 317 survey responses were collected, 50 of which were paper surveys and the rest were taken online. There were 78 unusable surveys, categorized as such because the survey participants did not complete the survey sufficiently. Therefore, the total useful sample was 239 and the useful survey response rate was 17.3 per cent.

To check for possible response and non-response biases, we ran a series of ANOVAs (1) between groups that finished all sections of the survey and those that did not and (2) between groups that finished the survey before follow-up e-mails were sent and those that finished the survey after follow-up e-mails. Results of the ANOVA analyses showed no statistically significant differences between either sets of groups.

Results

To analyze our survey data, we used covariance-based structural equation modeling (SEM). SEM techniques are considered an appropriate analysis method when testing or disconfirming explanatory relationships between latent constructs of a theoretically derived model (Raykov and Marcoulides, 2006; Gefen *et al.*, 2011), which is the case for our hypotheses. Prior to conducting SEM analyses, we screened the data for issues that may jeopardize the results, such as minimum sample size, outliers, variance inflation factors, multi-collinearity, non-normality and missing data (Kline, 2011, Byrne, 2001; Gefen *et al.*, 2000). We transformed all skewed variables (all latent constructs except perceived sanction

construct	Survey question/measurement item	Item	Factor loading	Source(s)
Behavioral intent	I intend to comply with the removable flash media requirements of the ISP of my organization in the future	BINT1	0.979	Ajzen (1991), Bulgurcu et al. (2010)
	I intend to protect information and technology resources according to the removable flash media requirements of the ISP of my organization in the future	BINT2	0.989	
	I intend to carry out my removable flash media responsibilities prescribed in the ISP of my organization when I use information and technology in the future	BINT3	0.972	
Subjective norms	My peers/colleagues think that I should comply with the removable flash media requirements of the ISP	SNFP	0.901	Taylor and Todd (1995), Herath and Rao (2009)
	My executives think that I should comply with the removable flash media requirements of the ISP	SNFE	0.677	
	My subordinates (or those junior to me) think that I should comply with the removable flash media requirements of the ISP	SNFS	0.848	
Perceived behavioral control	I would be able to follow the ISP for removable flash media threats	PBC1	0.886	Taylor and Todd (1995)
	Following the ISP for removable flash media threats is entirely within my control	PBC2	0.859	
	I have the resources and knowledge and ability to follow the ISP for removable flash media threats	PBC3	0.913	
Attitude	Adopting ISP-related security technologies and practices is important for protecting against removable flash media threats	ATT1	0.966	Herath and Rao (2009)
	Adopting ISP-related security technologies and practices is beneficial for protecting against removable flash media threats	ATT2	0.949	
	Adopting ISP-related security technologies and practices is helpful for protecting against removable flash media threats	ATT3	0.933	
Perceived certainty of sanction	Employees that fail to follow the removable flash media requirements of the ISP would be caught, eventually	PSANCT1	0.768	Herath and Rao (2009)
	The likelihood the organization would discover that an employee failed to follow the removable flash media requirements of the ISP is	PSANCT2	0.824	
Perceived sanction severity	My organization disciplines employees who fail to follow the removable flash media requirements of ISP	SSEV1	0.736	Herath and Rao (2009)
	My organization terminates employees who repeatedly fail to follow the removable flash media requirements of the ISP	SSEV2	0.641	
	If I were caught violating the removable flash media requirements of the ISP, I would be severely punished	SSEV3	0.806	

Notes: $N = 239$; All items significant at least at $p < 0.0001$

Table I.
Survey instrument

Security threat	Security policy requirements
Removable flash media	Use of removable flash media is forbidden except in case of command-directed and documented mission essential tasks per Chairman of the Joint Chiefs of Staff Instruction 6510.01F. If approved, the following conditions must be met: Craft, promulgate and implement risk management policies concerning the use of removable media Restrict use to removable media that are USG-owned and have been purchased or acquired from authorized and trusted sources Encrypt data on removable media using, at a minimum, the Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules Verify that the media contain only the minimum files that are necessary, and that the files are authenticated and scanned so that they are free of malicious software Limit use of removable media to authorized personnel with appropriate training Implement a program to track, account for and safeguard all acquired removable media, as well as to track and audit all data transfers Conduct both scheduled and random inspections to ensure compliance with department/agency promulgated guidance regarding the use of removable media Implement system level software restriction rules to significantly reduce the potential for malicious code execution by removable media

Table II.
ISP requirements for removable flash media

severity) using the inverse transformation as recommended by Kline (2011). We also mean centered the sanction effect variables to test the interaction effect of sanction severity and sanction probability.

We took several steps to mitigate and assess the potential impact of common method bias per the guidance in Gefen *et al.* (2011) and Podsakoff *et al.* (2003). First, we used survey best practices to minimize the possible impact of common method bias. For instance, the survey was administered online (189 responses) and paper-based (50 responses), participation was completely voluntary, respondents were assured anonymity, and the survey instructions stated that there were no right or wrong answers so respondents could answer honestly. Second, we conducted a post-hoc Harman's single-factor test to assess the presence of common method variance, which revealed that no single factor accounted for a majority of the variance. While the results of the above analyses do not completely negate the possibility of common method variance, they do suggest that it is not a major concern in these data.

Covariance based SEM analysis consists of two parts: a confirmatory factor analysis stage and the structural model analysis (also known as path analysis) stage (Heck, 1998). The CFA stage assessed the quality/validity of the construct measures. We examined the average variance extracted (AVE) to ensure the individual item reliability and convergent validity of construct items. The measurement item loadings on respective constructs for the majority of the items were above the recommended minimum value of 0.707, which indicates that at least 50 percent of the variance was shared with the construct (see Table II for factor loadings). However, item values between 0.40 and 0.70 are acceptable for inclusion as long as composite reliabilities are above 0.70 (Chin, 1998), which they are in all cases. The AVE values for all constructs were greater than the minimum recommended value of 0.50, indicating that the items satisfied the convergent validity requirements. Table III displays the factor correlation matrix from the CFA along with the composite reliabilities and AVE. The model fit for the CFA analysis was satisfactory (χ^2/df = 2.693; CFI = 0.956; SRMR = 0.0604).

Following establishment of the measurement model in the CFA stage, we fitted the data to the hypothesized models and assessed each model for goodness-of-fit. We assessed model

fit using multiple criteria (Raykov and Marcoulides, 2006; Kline, 2011). We report the normed chi-square (χ^2/df), comparative fit index (CFI) and the standardized root mean square residual (SRMR) measures of model fit. It is important to note that not all fit statistics have to be within the suggested threshold rules of thumb to have an acceptable model fit (Gefen *et al.*, 2011). All reported CFI values are above the 0.90 (Marsh *et al.*, 2004) or the 0.95 (Hu and Bentler, 1999) recommended thresholds. The badness-of-fit metric reported in our paper is SRMR, which compares the residuals (unexplained variance) to what would be reasonably expected from a well-fitting model. In all of evaluated research models except the proposed model (for those without ISP punishment experiences), the SRMRs are below the common threshold of 0.08 indicating good model fit (Hu and Bentler, 1999). Table IV displays the structural model evaluation results.

The structural path analyses (shown in the bottom half of Table IV) provide interesting results for the proposed and alternate models. The proposed model (using the full sample) shows significant contribution of the three sanction constructs to attitude with a strong SMC of 0.708 (meaning the sanction constructs alone explain 70.8 per cent of the variance in an employee's attitude toward complying with the removable flash media ISP). However, there is no significant direct effect of any of the sanction constructs on behavioral intent, as seen in the results for the alternate model. These results support *H1* (the impact of sanction effects on ISP behavioral intentions will be mediated by attitudes).

Our models indicate that the results when removing the subjects who have not directly or indirectly experienced sanctions for violating the ISP indicate that the directionality and relative magnitude of the sanction effects are quite different (Table V). For those subjects who have not had any prior sanction experiences, the effects are what the GDT would predict. The greatest impact on attitudes toward compliance with flash drive policies and procedures are when the probability of being punished and the severity of the punishments are both high (for the no experiences subjects). However, when we add in the prior experience subjects, this is not the case. In this sample, the greatest attitudes toward compliance are when the probability of getting caught is high but when the sanction severity is relatively low (one standard deviation below the mean in Table V). This means the 48 individuals with prior experiences are skewing the results because the sanction effects are impacting their attitudes differently. This evidence supports our second hypothesis, which predicts a moderating relationship associated with punishment experiences.

There were only 48 subjects in the sample who had prior punishment experiences so we were unable to run a full covariance based SEM model using just those subjects.

Construct	CR	AVE	MSV	ASV	SNORM	ATT	BINT	PBC	SSEV	PSANCT
SNORM	0.853	0.663	0.523	0.307	0.814					
ATT	0.965	0.901	0.423	0.294	0.650	0.949				
BINT	0.986	0.960	0.523	0.287	0.723	0.646	0.980			
PBC	0.917	0.785	0.415	0.256	0.576	0.644	0.590	0.886		
SSEV	0.773	0.534	0.280	0.127	0.373	0.282	0.275	0.242	0.731	
PSANCT	0.776	0.634	0.280	0.147	0.343	0.369	0.268	0.359	0.529	0.796

Notes: SNORM = Subjective Norms; ATT = Attitude; BINT = Behavioral Intent; PBC = Perceived Behavioral Control; SSEV = Perceived Sanction Severity; PSANCT = Perceived Certainty of Sanction; CR = Composite Reliability; AVE = Average Variance Extracted; MSV = Maximum Shared Squared Variance; ASV = Average Shared Squared Variance

Table III.
Validity table with factor correlation matrix

SEM model fit statistics	Proposed model (Full sample)	Proposed model (No punishment experiences)	Alternative model (Full sample)	Alternative model (No punishment experiences)
N	239	191	239	191
χ^2/df	3.123	3.007	2.614	2.18
χ^2	374.807	360.831	300.621	250.655
Df	120	120	115	115
CFI	0.936	0.933	0.954	0.962
Standardized root mean residual (SRMR)	0.0665	0.1511	0.0588	0.0566
Attitude squared multiple correlation (SMC)	0.708	0.231		
Behavioral intent squared multiple correlation (SMC)	0.592	0.595	0.604	0.655
SEM structural path analyses				
Perceived sanction certainty → behavioral intent			NS	NS
Perceived sanction severity → behavioral intent			NS	NS
Probability × severity interaction → behavioral intent			(0.101)*	NS
Attitude → behavioral intent	0.226***	0.3***	0.247***	0.241***
Perceived sanction probability → attitude	2.141***	0.306***		
Perceived sanction severity → attitude	(−1.643)**	0.278**		
Probability × severity interaction → attitude	(−0.536)*	0.179*		
Subjective norms → behavioral intent	0.483***	0.553***	0.469***	0.507***
Perceived behavioral control → behavioral intent	0.165*	0.124 (.077)	0.18**	0.162*

Notes: *$p < 0.05$; **$p < 0.01$; ***$p < 0.001$ NS: Not Significant

Table IV.
SEM Model results

Instead we ran a series of ANOVAs comparing the two groups on a variety of outcomes (Table VI). As seen in Table VI, the only statistically significant differences in the model constructs between the two groups (those with and without punishment experiences) are in the sanction constructs. The group with ISP punishment experiences had significantly higher perceived sanction severity (mean = 5.8472) and sanction probability (mean = 5.9792) compared to the no-punishment experiences group (mean = 4.9127 and mean = 5.3639, respectively). The combination of the results from Tables IV to VI provide strong evidence that there are significant differences in the impact of sanction-derived attitudinal antecedents of the employees sampled based upon whether they have had ISP punishment experiences or not.

Discussion and conclusion

Our study makes three important contributions to the literature. First, we empirically demonstrate that attitudes fully mediate the impact of sanction effects on ISP behavioral intentions. D'Arcy and Herath (2011) suggest that sanction effects might have an indirect effect on ISP compliance behavioral intentions and we provide empirical support and theoretical justification for such an indirect effect. We argue that the threat of sanctions shapes an employee's attitudes, which then influences the employee's behavioral intentions to comply with the ISPs. We suggested that this is the case because the rational estimation of sanction effects acts in a similar manner to a rational estimation of costs and benefits, which has been previously demonstrated to impact the formation of attitudes concerning a variety of IS behaviors including ISP compliance (Bulgurcu *et al.*, 2010; Workman *et al.*, 2008;

Sanction severity	Sanction probability			
	−1 STDEV	Average	+1 STDEV	Difference
All Subjects (n = 239)				
+1 STDEV	−2.32	−1.92	−1.53	0.79
Avg	−0.56	0.00	0.56	1.11
−1 STDEV	1.20	1.92	2.64	1.44
Difference	3.52	3.84	4.17	
No punishment experiences (n = 191)				
+1 STDEV	0.19	0.33	0.46	0.27
Avg	−0.08	0.00	0.08	0.16
−1 STDEV	−0.35	−0.33	−0.30	0.05
Difference	−0.54	−0.65	−0.76	

Table V.
Interaction effect of sanction probability and sanction severity

Analysis	Severity	Probability	Attitude	Perceived behavioral control	Subjective norms	Behavioral intention
Between group ANOVAs						
Mean Square	33.4980	14.5224	0.0278	0.1802	0.5235	0.0377
F	26.9137	12.2293	0.0608	0.4163	0.9864	0.1193
Significance	0.000	0.001	0.806	0.519	0.322	0.730
Descriptive statistics						
Punishment experience						
Mean	5.8472	5.9792	6.5208	6.4236	6.3125	6.6528
N	48	48	48	48	48	48
SD	1.17290	1.13905	0.61466	0.70707	0.69243	0.64854
No punishment experience						
Mean	4.9127	5.3639	6.4939	6.4921	6.4293	6.6841
N	191	191	191	191	191	191
SD	1.10101	1.07718	0.69150	0.64511	0.73714	0.53829
All						
Mean	5.1004	5.4874	6.4993	6.4784	6.4059	6.6778
N	239	239	239	239	239	239
SD	1.17480	1.11514	0.67562	0.65705	0.72847	0.56083

Table VI.
Between group ANOVAs

Taneja *et al.*, 2014). Interestingly, Liao *et al.* (2009) found, counter to our findings, that attitudes did not fully mediate the relationship between sanction effects and behavioral intentions in their study of workplace internet misuse. The different results may be due to flash drive misuse being a different threat context with different workplace risks (either perceived or real) than workplace internet misuse. Having a tangible 'thing' (the flash drive) may make the perceived threat of flash drive misuse greater (relative to a threat involving just digital 0 and 1 s) in the eyes of a typical, non-technical employee, which may amplify the attitudinal mediation effect associated with sanctions.

Second, we demonstrated that sanction effects are different depending on whether an employee has experienced, personally or vicariously, any previous punishment for violating the security rules and regulations because attitudes are heavily shaped by previous experiences (Harris and Furnell, 2012). Without prior experiences, we demonstrated empirically that the sanction effects will have the expected effect (i.e. greater severity and greater probability increases attitudes toward compliance), but those with prior experiences are influenced quite differently. Prior experiences, depending on what those prior experiences are, may change the sign and relative magnitude of the sanction effects. An interesting future line of research can investigate the specific details concerning the prior experiences. Determining which types of prior experiences increase or decrease compliance intentions is an important step in effectively utilizing sanctions to encourage/motivate ISP compliance attitudes and behavioral intentions.

Third, our study results suggest that it is important to test the multiplicative interaction effect of sanction probability and sanction severity in GDT research. Our results reveal that there is a differential effect based on different levels of severity and probability. Simply running a main effect's only model might not reveal the nuanced effects associated with sanction antecedents in the context of ISP compliance research. This suggests that it is important to find the right balance between sanction severity and probability of being caught. Our results reveal that it is not necessarily the best strategy to simply increase perceptions of both for all groups of people. From a practical standpoint, this means that organizations should have a thorough understanding of how their employees' perceive sanctions in relationship to their prior experiences before implementing such policies.

Like all research, our study has several limitations that should be considered when interpreting and extrapolating our results. By design, our study explored a specific organizational context with a robust ISP and security education training awareness (SETA) program. Research has shown that organizations with strong SETA programs positively affect the security awareness of its employees (Chen *et al.*, 2015); employees in organizations with weaker or lacking SETA programs altogether may behave differently for the examined security threat context. Extrapolating results of this study to different types of organizations, cultures and threat contexts should be considered with caution (Lee and Baskerville, 2003; Tsang and Williams, 2012). Particularly in very large organizations such as the one we examined, there are many organizational sub-contexts that may influence employee compliance with ISPs. For example, employees who work regularly with sensitive intellectual property may have significantly different perspectives compared to employees working in job functions that rarely interact with highly sensitive information. Furthermore, we only investigated one particular information security threat (flash drive compliance) and the associated ISP compliance requirements. Other threats that may not be as widely known as this one or may involve more social interactions with colleagues, which may increase or decrease the sanction effects. As such, future research should investigate our proposed relationships in additional organizations with other threat conditions to empirically validate the generalizability of the findings.

Taking into account the limitations discussed above, there are some potential considerations for applying the results of this study outside of the specific information security threat (improper flash media/USB drive use) and organizational context (DoD). Accepting that deterrence and sanction effects have a stronger indirect than direct effect on intended security behaviors allows organizations to focus their SETA efforts on other behavioral factors with more impact on employee security actions. For example, in this study, social influences (subjective norms) was, by far, the strongest and most influential factor of an employee's intention to follow the USB-related ISP guidelines. In this case, tailoring future security education efforts to emphasize the heightened social desirability of following the ISP (and therefore keeping corporate networks and personal information safer) instead of focusing on threats against non-compliance could return a far-greater reward in the form of increased security behavior intentions and actions. Each organization should expend the effort necessary to understand the factors that influence their employees' security behaviors across the spectrum of threats that matter to them. In this study, it is completely rational that the DoD has a firm policy against the use of USB drives except in exceptional circumstances. Other organizations may not have the same concerns about USB drive use, but every organization has a threat profile and security risks that matters to them, and the results of this study can be applicable across a range of potential threats and organization types.

Lastly, the finding that punishment experiences have such a significant impact on employee security behavioral intentions means that a one-size-fits-all approach to security training is likely not optimal, whereas sanction effects have a stronger effect on employees without punishment experiences (such as new employees), taking the same SETA approach with seasoned employees that have witnessed, personally or vicariously, punishments from security policy violations, does not necessarily have the same expected effect on security behaviors. The DoD, for example, does not provide an alternative or tailored general SETA program for its employees; everyone receives the same security training, regardless of their security experiences. It is possible that the DoD, and other organizations, would see improved results from their SETA programs if they tailored their sanction-related messages toward employees with varying levels of punishment experiences.

Note

1. An ISP describes employee roles and responsibilities, addressing specific security issues, in protecting the information resources of their organization (Safa *et al.*, 2016; Theoharidou *et al.*, 2005). Having a sound ISP is mandatory for every major corporate information security framework including PCI DSS, COSO, COBIT-5 and ISO27000.

References

Ajzen, I. (1985), *From Intentions to Actions: A Theory of Planned Behavior*, Springer.

Ajzen, I. (1991), "The theory of planned behavior", *Organizational Behavior and Human Decision Processes*, Vol. 50 No. 2, pp. 179-211.

Ajzen, I. (2001), "Nature and operation of attitudes", *Annual Review of Psychology*, Vol. 52 No. 1, pp. 27-58.

Aurigemma, S. (2013), "A composite framework for behavioral compliance with information security policies", *Journal of Organizational and End User Computing*, Vol. 25 No. 3, p. 20.

Barlow, J.B., Warkentin, M., Ormond, D. and Dennis, A.R. (2013), "Don't make excuses! Discouraging neutralization to reduce IT policy violation", *Computers & Security*, Vol. 39, pp. 145-159.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly*, Vol. 34.

Byrne, B.M. (2001), "Structural equation modeling with AMOS, EQS, and LISREL: comparative approaches to testing for the factorial validity of a measuring instrument", *International Journal of Testing*, Vol. 1 No. 1, pp. 55-86.

Chen, Y., Ramamurthy, K. and Wen, K.-W. (2015), "Impacts of comprehensive information security programs on information security culture", *Journal of Computer Information Systems*, Vol. 55 No. 3, pp. 11-19.

Cheng, L., Li, Y., Li, W., Holm, E. and Zhai, Q. (2013), "Understanding the violation of IS security policy in organizations: an integrated model based on social control and deterrence theory", *Computers & Security*, Vol. 39, pp. 447-459.

Chin, W.W. (1998), "Commentary: issues and opinion on structural equation modeling", *JSTOR*, Vol. 22 No. 1.

Cole, E. (2015), *Insider Threats and the Need for Fast and Directed Response*, SANS Institute.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R. (2013), "Future directions for behavioral information security research", *Computers & Security*, Vol. 32, pp. 90-101.

D'Arcy, J. and Herath, T. (2011), "A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings", *European Journal of Information Systems*, Vol. 20, pp. 643-658.

D'Arcy, J., Hovav, A. and Galletta, D. (2009), "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach", *Information Systems Research*, Vol. 20, pp. 79-98.

Dillman, D.A., Smyth, J.D. and Christian, L.M. (2014), *Internet, Phone, Mail, and Mixed-Mode Surveys: The Tailored Design Method*, John Wiley & Sons.

Dinev, T. and Hu, Q. (2007), "The centrality of awareness in the formation of user behavioral intention toward protective information technologies", *Journal of the Association for Information Systems*, Vol. 8.

Diver, S. (2006), *Information Security Policy – a Development Guide for Large and Small Companies*, SANS Institute.

Gefen, D., Straub, D. and Rigdon, E. (2011), "An update and extension to SEM guidelines for admnistrative and social science research", *MIS Quarterly*, Vol. 35, pp. 3-14.

Gefen, D., Straub, W. and Boudreau, M. (2000), "Structural equation modeling and regression: guidelines for research practice", *Communications of the Association for Information Systems*, Vol. 4.

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

Guo, K.H. and Yuan, Y. (2012), "The effects of multilevel sanctions on information security violations: a mediating model", *Information & Management*, Vol. 49 No. 6, pp. 320-326.

Guo, K.H., Yuan, Y., Archer, N.P. and Connelly, C.E. (2011), "Understanding nonmalicious security violations in the workplace: a composite behavior model", *Journal of Management Information Systems*, Vol. 28 No. 2, pp. 203-236.

Harris, M. and Furnell, S. (2012), "Routes to security compliance: be good or be shamed? ", *Computer Fraud & Security*, Vol. 2012 No. 12, pp. 12-20.

Heck, R.H. (1998), "Factor analysis: exploratory and confirmatory approaches", *Modern Methods for Business Research*, pp. 177-215.

Herath, T. and Rao, H.R. (2009), "Protection motivation and deterrence: a framework for security policy compliance in organisations", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 106-125.

Hovav, A. and D'arcy, J. (2012), "Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the US and South Korea", *Information & Management*, Vol. 49 No. 2, pp. 99-110.

Hu, L. and Bentler, P.M. (1999), "Cutoff criteria for fit indexes in covariance structure analysis: conventional criteria versus new alternatives", *Structural Equation Modeling: A Multidisciplinary Journal*, Vol. 6 No. 1, pp. 1-55.

Hu, Q., Xu, Z., Dinev, T. and Ling, H. (2011), "Does deterrence work in reducing information security policy abuse by employees?", *Communications of the ACM*, Vol. 54 No. 6, pp. 54-60.

Karahanna, E., Straub, D.W. and Chervany, N.L. (1999), "Information technology adoption across time: a cross-sectional comparison of pre-adoption and post-adoption beliefs", *MIS Quarterly*, Vol. 23 No. 2.

Kline, R.B. (2011), *Principles and Practice of Structural Equation Modeling*, Guilford Press, New York, NY.

Kotulic, A.G. and Clark, J.G. (2004), "Why there aren't more information security research studies", *Information & Management*, Vol. 41 No. 5, pp. 597-607.

Krombholz, K., Hobel, H., Huber, M. and Weippl, E. (2015), "Advanced social engineering attacks", *Journal of Information Security and Applications*, Vol. 22, pp. 113-122.

Lee, A.S. and Baskerville, R.L. (2003), "Generalizing generalizability in information systems research", *Information Systems Research*, Vol. 14 No. 3, pp. 221-243.

Liao, Q., Gurung, A., Luo, X. and Li, L. (2009), "Workplace management and employee misuse: does punishment matter?", *Journal of Computer Information Systems*, Vol. 50, pp. 49-59.

Lynn III, W. (2010), "Defending a new domain", *Foreign Affairs*, Council on Foreign Affairs.

Marsh, H.W., Hau, K.-T. and Wen, Z. (2004), "In search of golden rules: comment on hypothesis-testing approaches to setting cutoff values for fit indexes and dangers in overgeneralizing Hu and Bentler's (1999) findings", *Structural Equation Modeling*, Vol. 11 No. 3, pp. 320-341.

Mitnick, K.D., and Simon, W.L. (2011), *The Art of Deception: Controlling the Human Element of Security*, John Wiley & Sons.

Moquin, R. and Wakefield, R.L. (2016), "The roles of awareness, sanctions, and ethics in software compliance", *Journal of Computer Information Systems*, Vol. 56 No. 3, pp. 261-270.

Nagin, D.S. and Pogarsky, G. (2001), "Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence: theory and evidence", *Criminology*, Vol. 39 No. 4, pp. 865-892.

Pahnila, S., Siponen, M. and Mahmood, A. (2007), "Employees' behavior towards IS security policy compliance", 40th Annual Hawaii International Conference on System Sciences, HICSS, *IEEE*, 156b-156b.

Paternoster, R. and Piquero, A. (1995), "Reconceptualizing deterrence: an empirical test of personal and vicarious experiences", *Journal of Research in Crime and Delinquency*, Vol. 32 No. 3, pp. 251-286.

Pearce, R. (2016), "Vic Police issue warning over USB drive letterbox drops", *ComputerWorld*, IDG.

Piquero, A.R. and Pogarsky, G. (2002), "Beyond Stafford and Warr's reconceptualization of deterrence: personal and vicarious experiences, impulsivity, and offending behavior", *Journal of Research in Crime and Delinquency*, Vol. 39 No. 2, pp. 153-186.

Podsakoff, P.M., Mackenzie, S.B., Lee, J.-Y. and Podsakoff, N.P. (2003), "Common method biases in behavioral research: a critical review of the literature and recommended remedies", *Journal of Applied Psychology*, Vol. 88 No. 5, p. 879

Raykov, T., and Marcoulides, G.A. (2006), *A First Course in Structural Equation Modeling*, Lawrence Erlbaum, Mahwah, NY.

Safa, N.S. and Von Solms, R. (2016), "An information security knowledge sharing model in organizations", *Computers in Human Behavior*, Vol. 57, pp. 442-451.

Safa, N.S., Von Solms, R. and Furnell, S. (2016), "Information security policy compliance model in organizations", *Computers & Security*, Vol. 56, pp. 70-82.

Shropshire, J.D., Warkentin, M. and Johnston, A.C. (2010), "Impact of negative message framing on security adoption", *Journal of Computer Information Systems*, Vol. 51, pp. 41-51.

Silowash, G.J., and King, C. (2013), *Insider Threat Control: Understanding Data Loss Prevention (DLP) and Detection by Correlating Events from Multiple Sources*, Software Engineering Institute, Carnegie Mellon University CERT Program.

Simon, H.A. (1955), "A behavioral model of rational choice", *The Quarterly Journal of Economics*, Vol. 69 No. 1, pp. 99-118.

Siponen, M. and Vance, A. (2010), "Nuetralization: new insights into the problem of employee information systems security policy violations", *MIS Quarterly*, Vol. 34.

Smith, R.E. (2015), *Elementary Information Security*, Jones & Bartlett Publishers.

Stafford, M.C. and Warr, M. (1993), "A reconceptualization of general and specific deterrence", *Journal of Research in Crime and Delinquency*, Vol. 30 No. 2, pp. 123-135.

Straub, D.W. Jr (1990), "Effective IS security: an empirical study", *Information Systems Research*, Vol. 1 No. 3, pp. 255-276.

Taneja, A., Vitrano, J. and Gengo, N.J. (2014), "Rationality-based beliefs affecting individual's attitude and intention to use privacy controls on Facebook: an empirical investigation", *Computers in Human Behavior*, Vol. 38, pp. 159-173.

Taylor, S. and Todd, P.A. (1995), "Understanding information technology usage: a test of competing models", *Information Systems Research*, Vol. 6 No. 2, pp. 144-176.

Theoharidou, M., Kokolakis, S., Karyda, M. and Kiountouzis, E. (2005), "The insider threat to information systems and the effectiveness of ISO17799", *Computers & Security*, Vol. 24 No. 6, pp. 472-484.

Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E. and Bailey, M. 2016. "Users really do plug in USB drives they find", *37th IEEE Symposium on Security and Privacy*, *San Jose, CA*.

Tsang, E.W. and Williams, J.N. (2012), "Generalization and induction: misconceptions, clarifications, and a classification of induction", *MIS Quarterly*, Vol. 36, pp. 729-748.

Von Hirsch, A., Bottoms, A.E., Burney, E. and Wikstrom, P.-O. (1999), *Criminal Deterrence and Sentence Severity: An Analysis of Recent Research*, Hart, Oxford.

Wall, D.S. (2013), "Enemies within: redefining the insider threat in organizational security policy", *Security Journal*, Vol. 26 No. 2, pp. 107-124.

Wall, J.D., Lowry, P.B. and Barlow, J.B. (2015), "Organizational violations of externally governed privacy and security rules: explaining and predicting selective violations under conditions of strain and excess", *Journal of the Association for Information Systems*, Vol. 17, pp. 39-76.

Williams, M. (2016), "Lost thumb drives bedevil US banking agency", *PCWorld, IDG News Service*.

Willison, R. and Warkentin, M. (2013), "Beyond deterrence: an expanded view of employee computer abuse", *MIS Quarterly*, Vol. 37.

Workman, M., Bommer, W.H. and straub, D. (2008), "Security lapses and the omission of information security measures: a threat control model and empirical test", *Computers in Human Behavior*, Vol. 24 No. 6, pp. 2799-2816.

Zhang, J., Reithel, B.J. and Li, H. (2009), "Impact of perceived technical protection on security behaviors", *Information Management & Computer Security*, Vol. 17 No. 4, pp. 330-340.

Corresponding author
Salvatore Aurigemma can be contacted at: sal@utulsa.edu