Do it OR ELSE!
Exploring the Effectiveness of Deterrence on Employee Compliance with Information Security Policies

Submission Type: Research in Progress

Sal Aurigemma
University of Tulsa
sal@utulsa.edu

Thomas Mattson
University of Richmond
tmattson@richmond.edu

Abstract

Organizations have long relied upon the threat of sanctions to influence employees to follow information security policies. Unfortunately, the belief in the power of deterrence has provided mixed results in both research and in real life. This study explored the impact of sanction effects in an organization with a robust information security program. Findings indicate an employee's perceived sanction severity has a significant impact on their intent to follow ISP guidelines while their perceived certainty of sanction imposition does not, both of which support previous research. However, this paper was unique in that it addressed the impact of punishment experiences on sanction effects and found, somewhat counterintuitively, that those with personal or vicarious punishment experiences were less likely to be influenced by the deterrent effects of sanctions.

Keywords

Information security, deterrence, policy compliance, employee, planned behavior, punishment experiences, sanction certainty, sanction severity.

Introduction

As the global economy becomes ever more interconnected, the threats to our information resources' confidentiality, integrity, and availability are increasing. Information System (IS) information security compromises are estimated to cost the world economy trillions of dollars annually (Calluzzo & Cante, 2004). Organizations generally tend to focus on defending the perimeter of their networks, spending up to 85% of security funding towards these efforts (Gilliland, 2013). However, the insider threat is often considered the weakest link in information security (Mitnick et al., 2002; Zhang, Reithel & Li, 2009).

Insiders are employees (or supporting contractors) with legitimate access to information resources who often understand the organizational mechanisms of information security (Willison & Warkentin, 2013). Two general types of insiders are malicious and non-malicious (Brackney & Anderson, 2004). Whereas malicious employee actions can be labeled as intentional and deviant (sabotage, stealing, espionage, etc.), non-malicious employee actions can range over a continuum of volitional to non-volitional (Crossler, Johnston, Lowry, Hu, Warkentin & Baskerville, 2013) and include a number of characteristics including ignorance, apathy, resistance, and disobedience (Harris & Furnell, 2012). Adapted from criminology literature (Wells, 2005), this study defines non-malicious insiders as employees that potentially may fail to fulfill the requirements of information security policies with counterproductive behavior that may be common and even silently condoned in the workplace. Numerous studies have examined security compromises (such as data breaches) over the past decade and attribute 35% to 60% of incidents to non-malicious employee activities (Richardson, 2011; Ponemon, 2013).
While there are a range of technologies to assist companies in addressing the external threat, the main mechanism to assist non-malicious employees in protecting organizational information resources is the Information Security Policy (ISP) (Panko, 2009; Ernst & Young, 2011). An ISP describes employee roles and responsibilities, addressing specific security issues, in protecting the information resources of their organization (Panko, 2009). Having a sound ISP is mandatory for every major corporate information security framework including PCI DSS, COSO, COBIT-5, and ISO 2700X.

A growing base of IS security research has improved the knowledge of the behavior of non-malicious employees in complying (or not) with ISPs (Barlow, Warkentin, Ormond, Dennis, 2013; Wili & Warkentin, 2013; Crossler et al., 2013). A significant number of studies have focused on the impact of sanctions on employee's intent to follow the ISP, and for good reason. Understanding sanction effects are important because the threat of employee punishment for non-compliance with requirements should be a cornerstone of all ISPs (Diver, 2006). However, the results of ISP compliance-related research on the effectiveness of sanctions is inconclusive (Hu, Xu, Dinev & Ling, 2011; Guo & Yuan, 2012; Barlow et al., 2013). This paper builds upon the work of previous studies by examining the influence of ISP-related punishment experiences on employee sanction risk perceptions. The study is framed to explore the intentions of a sample of non-malicious employees of a large organization against an extensible and recognizable information security threat included in the subject organization’s ISP.

**Theoretical Background and Hypotheses Development**

*Theory of Planned Behavior, Behavioral Intent, and Attitude*

Numerous theoretical lenses have been applied to exploring the antecedents of employee behavioral intent to comply with ISPs. One of the most prevalent in ISP compliance research is the Theory of Planned Behavior (Ajzen, 1985). The theory proffers that a person’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, human behavioral intention to perform an action is guided by a number of antecedent factors (subjective norms, attitude towards the behavior, perceived behavioral control, and other context-dependent variables). The linkage between behavioral intent with expected behavior has become a cornerstone of recent ISP behavioral compliance research due to the difficulty in gaining access to organizational data related to actual employee non-compliance in this sensitive area (Crossler et al., 2013). Taylor and Todd (1995) extended the theory by decomposing individual factors in order to more deeply explore these variables as multi-dimensional constructs. By decomposing the antecedents of behavioral intent, the model becomes less parsimonious but more effective in highlighting specific factors that may influence behavior (Taylor & Todd, 1995; Herath and Rao, 2009a). The theory of planned behavior, in its original and decomposed form, has been used successfully and extensively in ISP compliance literature.

The present study is most interested in exploring the sanction effects of the deterrent elements of organizational ISPs on employee behavior. The theory of planned behavior factor most relevant to this exploration is that of Attitude. Attitude towards a particular behavior is a person’s overall evaluation of desirability of implementing a behavior in a particular context. Attitude is influenced by beliefs about the consequences of a behavior and the respective positive and/or negative judgments about the behavior (Ajzen, 2001). Attitude can be one of the strongest predictors of behavioral intent and has been a focus in recent ISP compliance research (Aurigemma, 2013; Bulgurcu, Cavusoglu & Benbasat, 2010; Guo, Yuan, Archer & Connelly, 2011; Herath & Rao, 2009; Pahnila, Siponen & Mahmood, 2007; Zhang, Reithel & Li, 2009). In the context of this study, the more desirable a particular behavior required by the ISP is to an employee, the more likely they intend to follow the behavior. The following core hypothesis (as shown in Figure 1) is posited:

Hypothesis 1: An employee’s attitude toward compliance with the organization’s ISP positively affects intention to comply with the requirements of the ISP.
**General Deterrence Theory**

General Deterrence Theory is prominent in the study of criminology with its roots dating back hundreds of years (Siponen & Vance, 2010). Deterrence theory leans on the effectiveness of formal and objective sanctions to influence a person’s decision to commit or abstain from an unwanted act (Theoharidou, Kokolakis, Karyda & Kiountouzis, 2005). In essence, sanction effects are a negative version of rational choice theory (Simon, 1955) which argues that behavior is determined by balancing costs and benefits of different options. General Deterrence Theory conceptually consists of three components of sanction effects: severity, certainty, and celerity (Gibbs, 1975). Perceived sanction severity and certainty are the most prominent components of the general deterrence theory represented in ISP-related research (D’Arcy & Herath, 2011). Research on these factors in this field have 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 while Bulgurcu et al. (2011) found the opposite. Others (Cheng, Li, Li, Holm & Zhai, 2013; Herath & Rao, 2009; D’Arcy et al., 2008) found perceived sanction severity to have a significant effect on intent while perceived certainty of sanction imposition was not significant. While the purpose of this paper is not to examine the possible causes of these discrepant findings, D’Arcy & Herath (2011) do examine this topic and provide a number of possible causes and recommendations. The approach being taken in this study is to evaluate the two most frequently modeled components of sanction effects (severity and certainty) and address celerity by evaluating sample groups based upon sanction punishment experiences as described below.

![Figure 1 - Research Model and Hypotheses](image)

Following the general deterrence theory, the greater the perceived severity of sanctions for a specific behavior, the more likely individuals are to avoid that behavior. Sanctions address negative outcomes that employees may try to avoid. Thus, the higher the perceived sanction severity for violating actions directed by the ISP, the more favorable the employee’s attitude will be towards fulfilling the ISP behavior.

**Hypothesis 2:** The more severe the perceived sanction for non-compliance with actions directed by the ISP, the more likely an employee will have a favorable feeling about fulfilling the ISP behavior.

Numerous criminology studies have shown that the perceived probability of sanction imposition has as strong, if not a stronger, deterrent effect than sanction severity (von Hirsch, Bottoms, Burney & Wikstrom, 1999). The higher the perceived probability of being punished for a behavior, the more favorable an individual’s attitude will be to avoid that behavior and its associated punishment. In the context of ISP compliance, the more likely an employee is to be punished for failing to follow an ISP-directed behavior, the more likely the employee will be to follow the procedures.

**Hypothesis 3:** The more certain an employee feels that they will be punished for non-compliance with actions directed by the ISP, the more likely an employee will have a favorable feeling about properly fulfilling the ISP behavior.
Punishment Experiences and Sanction Celerity

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 Stafford and Warr’s (1993) expansion of general deterrence theory. 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 compliant behavior. Studies in criminology using the Stafford & Warr model provide interesting findings that may well apply to the study of the sanction effects on ISP compliance. For instance, Piquero & Fogarsky (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.

In this study, we examine the effects of sanction celerity through the theoretical lens of punishment experiences. The measure of celerity in this case is dyadic – either the respondent knows of someone (including themselves) that has been punished for failing to follow an ISP requirement or they don’t. This binary representation of sanction celerity is clearly limited, but does address the two ends of the spectrum of sanction imposition: eventually and never.

Research Method

Data for this study were collected using a questionnaire administered to United States Department of Defense (DoD) employees at multiple organizations, all of whom fell under the same overarching information security policy 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 Appendix). The DoD is an interesting research population that consists of over 3.5 million employees with a mixture of military and civilian work force members. All of the employees have at least one thing in common – they all fall under the same general ISP, known as DoD Information Assurance (IAA). Each and every DoD employee, regardless of rank, status or organization, falls under the IAA guidelines and requirements, in addition to any more-restrictive individual command ISPs. All DoD employees are required to complete mandatory information security training annually; failure to complete this training is meticulously tracked and will result in loss of access to DoD IT systems at a minimum.

The specific information security threat examined in this study 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. In a 2009 survey of IT security professionals and executives worldwide, 57% of respondents reported that their top security concern was personal portable storage device misuse (Computer Economics, 2009). Removable flash media (and all other removable media) devices are considered a major potential source of information leakage from organizations and malware injection points, yet approximately one-third of respondent organizations make no attempt to deter such device use. The DoD banned the use of removable flash media and storage devices from all government computers in 2008 following the most significant breach of U.S. 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 U.S. military laptop at a remote base by a non-malicious employee (Lynn, 2010). In 2010, the ban was partially rescinded for special cases and requires a new set of very restrictive compliance requirements. Most DoD organizations currently enforce the total ban on removable flash media.

Primary survey collection was via an online survey tool. A paper version of the questionnaire (identical to the online version) was made available to potential respondents. Fifty paper surveys were collected. Survey email invitations were sent to organization leaders who were then requested to provide the survey to their subordinate employees. A total of 1380 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. 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%.

**Analyses and Results**

Covariance-based structural equation modeling (SEM) procedures using SPSS AMOS was used to analyze the model in this paper. Structural equation modeling techniques are considered an appropriate analysis method when testing or disconfirming explanatory relationships between latent constructs of a theoretically derived, a priori model (Raykov & Marcoulides, 2006; Gefen, Rigdon & Straub, 2011). Prior to conducting SEM analyses, the data were screened for issues that may jeopardize the results, such as minimum sample size, outliers, multicollinearity, non-normality, and missing data (Kline, 2011; Byrne, 2001; Gefen et al., 2000). Measurement item convergent and discriminant validity were addressed during the confirmatory factor analysis (CFA) stage. Common method bias was addressed using the methods described in Podsakoff, MacKenzie & Lee (2003) per the guidance in Gefen et al. (2011).

Covariance-based SEM analysis consists of two parts: a confirmatory factor analysis stage and the structural model analysis (also known as path analysis) stage (Joreskog & Sorbom, 1989; Heck, 1998). The CFA stage assessed the quality / validity of the construct measures. The average variance extracted (AVE) was examined to ensure the individual item reliability and convergent validity of construct items. Measurement item loadings for each construct are shown in Table 1. Measurement item loadings on respective constructs for the large majority were above the recommended minimum value of 0.707 indicating that at least 50 percent of the variance was shared with the construct; however, item values between .40 and .70 are acceptable for inclusion as long as composite reliabilities are above .70 (which they are in all cases) (Chin, 1998). 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 2 provides the factor correlation matrix from the CFA along with the composite reliabilities and AVE. The model fit for the CFA analysis was satisfactory ($\chi^2/df = 2.912; CFI = 0.97; SRMR = 0.04$).

### Table 1: Confirmatory Factor Analysis Standardized Factor Loadings

<table>
<thead>
<tr>
<th>Latent Construct</th>
<th>Item</th>
<th>Standardized Item Loading</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behavioral Intent</td>
<td>BINT3</td>
<td>0.973</td>
</tr>
<tr>
<td></td>
<td>BINT2</td>
<td>0.981</td>
</tr>
<tr>
<td></td>
<td>BINT1</td>
<td>0.969</td>
</tr>
<tr>
<td>Attitude</td>
<td>ATT3</td>
<td>0.913</td>
</tr>
<tr>
<td></td>
<td>ATT2</td>
<td>0.934</td>
</tr>
<tr>
<td></td>
<td>ATT1</td>
<td>0.961</td>
</tr>
<tr>
<td>Perceived Sanction Severity</td>
<td>SSEV3</td>
<td>0.788</td>
</tr>
<tr>
<td></td>
<td>SSEV2</td>
<td>0.626</td>
</tr>
<tr>
<td></td>
<td>SSEV1</td>
<td>0.762</td>
</tr>
<tr>
<td>Perceived Certainty of Sanction Imposition</td>
<td>SPROB2</td>
<td>0.831</td>
</tr>
<tr>
<td></td>
<td>SPROB1</td>
<td>0.619</td>
</tr>
</tbody>
</table>

N = 239. All items significant at least at p< .0001

Following establishment of the measurement model in the CFA stage, the data were fitted to the hypothesized models and assessed for goodness-of-fit. The assessment of model fit should be based on multiple criteria (Raykov & Marcoulides, 2006; Kline, 2011; Hu & Bentler, 1999; Heck, 1998). First, the Normed Chi-Square, which is the model chi-square coefficient divided by the overall degrees of freedom ($\chi^2/df$), is reported for which values ranging from less than 2.0 (good fit) to 5.0 (acceptable fit) (Kline, 2011) are used to assess evaluation. Kline (2011) recommends, in addition to $\chi^2/df$, reporting one goodness-of-fit and one badness-of-fit metric when assessing overall model fit. The comparative fit index (CFI) is the goodness-of-fit metric reported and measures model fit relative to a null or baseline model; CFI is one of
the most widely used goodness-of-fit indices in information systems SEM-based research (Gefen et al., 2011). Values for CFI above .90 (Marsh, Hau & Wen, 2004) or .95 are recommended (Russell, 2002; Hu & Bentler, 1998). The badness-of-fit metric reported is the standardized root mean square residual (SRMR). A value of .08 or lower is generally considered a good fit (Hu & Bentler, 1999). It is important to note that it is acceptable that not all fit indexes be simultaneously within the above threshold rules of thumb (Gefen et al., 2011).

<table>
<thead>
<tr>
<th>CR</th>
<th>AVE</th>
<th>MSV</th>
<th>ASV</th>
<th>SSEV</th>
<th>ATT</th>
<th>SPROB</th>
<th>BINT</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSEV</td>
<td>0.773</td>
<td>0.534</td>
<td>0.396</td>
<td>0.187</td>
<td>0.731</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATT</td>
<td>0.955</td>
<td>0.876</td>
<td>0.339</td>
<td>0.162</td>
<td>0.310</td>
<td>0.936</td>
<td></td>
</tr>
<tr>
<td>SPROB</td>
<td>0.701</td>
<td>0.541</td>
<td>0.396</td>
<td>0.164</td>
<td>0.629</td>
<td>0.224</td>
<td>0.735</td>
</tr>
<tr>
<td>BINT</td>
<td>0.983</td>
<td>0.949</td>
<td>0.339</td>
<td>0.151</td>
<td>0.265</td>
<td>0.582</td>
<td>0.212</td>
</tr>
</tbody>
</table>

CR = Composite Reliability  
AVE = Average Variance Extracted  
MSV = Maximum Shared Squared Variance  
ASV = Average Shared Squared Variance  
SSEV = Perceived Sanction Severity  
ATT = Attitude  
SPROB = Perceived Certainty of Sanction  
BINT = Behavioral Intent

Table 2 - Validity Table with Factor Correlation Matrix

The threat of common method bias (Podsakoff et al., 2003; Straub et al., 2004) was addressed. By ensuring anonymity to the respondents, assuring participants that there were no right or wrong answers, requesting that each question be answered as honestly as possible, and providing no incentive for participating in the study (which is actually forbidden by the DoD), the likelihood of bias caused by social desirability or respondent acquiescence is expected to be reduced (Podsakoff et al., 2003). Also, following Podsakoff et al. (2003), common method variance was empirically evaluated using Harman’s single-factor test. All items in factor analysis were simultaneously loaded using Varimax rotation on a single item in SPSS (Dinev & Hu, 2007). No single factor accounted for a majority of the variance.

The structural analysis stage specifies direct and indirect causal relationships among the constructs and the amount of unexplained variance. Path analyses were used to test hypotheses 1 – 3 for three different groups. Group 1 included all survey participants. Group 2 included just those survey participants that reported having punishment experiences (personal or vicarious) related to violations of the organization’s ISP while Group 3 represents those that did not. The results of the structural model evaluation results are shown in Table 3.

<table>
<thead>
<tr>
<th></th>
<th>n</th>
<th>χ²/df</th>
<th>CFI</th>
<th>SRMR</th>
<th>Variance Explained (ATT)</th>
<th>Variance Explained (BINT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group 1</td>
<td>239</td>
<td>2.831</td>
<td>0.970</td>
<td>0.0473</td>
<td>0.10</td>
<td>0.341</td>
</tr>
<tr>
<td>Group 2</td>
<td>48</td>
<td>2.057</td>
<td>0.898</td>
<td>0.0784</td>
<td>0.10</td>
<td>0.070</td>
</tr>
<tr>
<td>Group 3</td>
<td>191</td>
<td>3.119</td>
<td>0.962</td>
<td>0.0603</td>
<td>0.11</td>
<td>0.403</td>
</tr>
</tbody>
</table>

Group 1 = full data set  
Group 2 = population with punishment experiences  
Group 3 = population without punishment experiences

Table 3 - Structural Model Evaluation Results

As shown in Table 3, Group 1 model fit criteria is fairly good as χ²/df is within reasonable limits and both CFI and SRMR are very good. Group 2 also shows a satisfactory fit with the best (lowest) χ²/df of the three groups, but also the worst (lowest) CFI (bordering on the lower acceptable limit) and highest SRMR (but still within acceptable limits). Finally, Group 3 fit is also satisfactory with very good CFI and SRMR and a χ²/df within limits (albeit the highest of the three groups). The proposed research model explained approximately 40% of the variance for employee intention to follow ISP requirements for removable flash media usage for Group 3, 34% for Group 1, but only 7% for Group 2.
Table 4 provides the results of the structural path analysis including the standardized and unstandardized path coefficients, standard errors, and associated p-values. Groups 1 and 3 show very similar results, both supporting H1 (attitude’s positive impact on behavioral intent) and H2 (positive impact of perceived sanction severity on attitude). However, H3 (positive impact of perceived certainty of sanctions on attitude) is not supported in either the Group 1 or Group 3 models. In contrast, Group 2 (those that reported ISP sanction-related punishment experiences) provided the weakest support for H1 (p = 0.075) and did not support either H2 or H3.

| Hypothesis | Group 1 | | | Group 2 | | | Group 3 | | |
|---|---|---|---|---|---|---|---|
| H1 | 0.584** | 0.494** | 0.048 | 0.265 (p=0.075) | 0.349 (p=0.075) | 0.196 | 0.635** | 0.482** | 0.045 |
| H2 | 0.282* | 0.159* | 0.062 | 0.338 | 0.164 | 0.130 | 0.259* | 0.16* | 0.071 |
| H3 | 0.049 | 0.041 | 0.095 | -0.032 | -0.022 | 0.198 | 0.101 | 0.086 | 0.101 |

* = significant at least at p <.05; ** p<.0001
Model 1 = full data set (n = 239)
Model 2 = population with punishment experiences (n=48)
Model 3 = population without punishment experiences (n=191)

Table 4 - Structural Model Path Coefficients

Discussion, Limitations, Conclusion

The amount of variance explained for Attitude and Behavioral Intent by the model in this study is at or above the 10% rule of thumb generally accepted in order to claim explanatory power (Guo & Yuan, 2012). Compared to other studies that explored both of these constructs in ISP compliance, the amount of variance is considerably lower; that is to be expected. The model in this study focused on evaluating the Attitude component of the theory of planned behavior without addressing the contributions from other behavioral antecedents (such as subjective norms and perceived behavioral control). Likewise, ISP compliance studies (Bulgurcu et al., 2010; Herath & Rao, 2009; Zhang et al., 2009) have identified numerous other factors associated with Attitude derived from protection motivation, rational choice and other supporting theories that were not included in this study.

Results of this study support the findings of other research (Cheng, Li, Li, Holm & Zhai, 2013; Herath & Rao, 2009; D’Arcy et al., 2008) which found perceived sanction severity to have a significant effect on intent while perceived certainty of sanction imposition was not significant. In the organizational context explored in this paper, the higher the perceived severity of the penalty for using unauthorized removable flash media, the more desirable their attitude towards following the requirement to not use such devices, which in turn resulted in a stronger intent to follow the ISP guidance. However, the certainty of being caught and then penalized was not a significant contributor to attitude. It is possible that employees feel that the likelihood of being caught is very low or that they can work around existing mechanisms that prevent the use of such media.

The most interesting results of this study are related to the differences in employees that reported having personal or vicarious punishment experiences related to unauthorized removable flash media usage. There were considerably more employees that reported having no punishment experiences (Group 3), and this significantly influenced the model results for the combined model (Group 1). Previous studies on ISP compliance have not explored this aspect of deterrence theory, and the results of this paper indicate more emphasis Stafford and Warr’s (1993) conceptualization of deterrence is warranted. Specifically, those employees that did report having punishment experiences (Group 2) were not only less concerned with
being caught using unauthorized storage devices, but the severity of sanctions if they were caught was not a significant contributor to either their attitude about the behavior or their intent to follow the ISP guidance. In essence, employees with punishment experiences were seemingly not motivated to comply with ISP rules by the primary control mechanism of most organizations – sanctions. This is counterintuitive and should cause organizations to reflect on the effectiveness of their relative reliance on sanctions.

While this study does not address why employees with punishment experiences are less influenced by sanction effects, criminology research may offer some possible explanations. For example, Piguero & Pogarsky (2002) found that punishment experiences appeared to encourage instead of discouraging future offenses. Explanation for such an “emboldening effect” could be that those with punishment experiences are likely the most committed offenders and, having been caught and punished before (personally or vicariously), they have greater inclination for future non-compliance. Thus, an organization’s past offenders of ISP non-compliance could be pre-disposed by their punishment experiences to not comply in the future. Another possible explanation is related to Sherman’s (1993) work on defiance. In the case of this study, if an employee believes the restriction on the use of removable flash media is unjust, they may be more likely to not comply with the requirements of the ISP in a form of social protest. Related work in neutralization (Siponen & Vance, 2010; Crossler et al., 2013; Barlow et al., 2013) have explored such phenomena, but not in the context of punishment experiences.

There are a number of limitations that should be considered when interpreting the results of this study. By design, this study explored a specific organizational context with a robust ISP and security awareness training program. Extrapolating results of this study to different types of organizations and cultures should be considered with caution. The data collected in this study was cross-sectional and came from a convenience sample of a very small subset of organizations within the greater DoD. Additionally, in very large organizations such as examined in this study, there are many organizational sub-contexts that can significantly influence employee compliance with ISPs. For example, employees that work regularly with sensitive intellectual property may have significantly different perspectives, technologies, and procedures to protect their information resources compared to other employees in work functions that rarely interact with extremely sensitive information or IT infrastructure. Also, only one particular information security threat and ISP requirement was explored in this study. Many of the supporting ISP compliance-related studies referenced in this paper did not focus on a specific organization, security threat, or ISP.

It is important to note that the sample size for the analyses of punishment experiences was only 48 employees. Minimum sample size for SEM analyses depends on many factors such as size of the model, reliability of the variables, and strength of the relationships among the variables (Heck, 1998). There is no universal agreement on minimum sample size required for SEM analyses. However, many minimum sample size rules of thumb exist to help researchers: 10 times the number of item indicators in the model; 50 + 8 times the number of item indicators in the model; >200 observations (Gefen et al., 2011). Sample size in the current study is 239 usable observations for the Group 1 model and 191 for the Group 3 model, both of which satisfy the majority of sample size rules of thumb. It is acknowledged that the sample size for the Group 2 model is very likely too small to fully trust the results of the SEM analysis for that group. However, the magnitude and scope of the differences between the results associated with Group 2 (those with punishment experiences) and the other groups shows a clear impact from punishment experiences.

In conclusion, organizations have built upon centuries of belief in deterrence theory resulting in the adoption of sanctions as a key mechanism to influence employees to follow ISP guidelines. This study explored the impact of sanction effects in a specific context and found support to previous research that perceived sanction severity does have a significant impact on an employee’s intent to follow ISP guidelines. Also in concurrence with some previous research, this study found that the perceived certainty of sanction imposition on an employee does not have a significant effect on behavioral intent. However, this paper was unique in that it addressed the impact of punishment experiences on sanction effects and found, somewhat counterintuitively, that those with personal or vicarious punishment experiences were less likely to be influenced by the deterrent effects of sanctions. Future research in this area should expand upon the extended deterrence concepts presented by Stafford & Warr (1993) to gain a greater understanding of the
impact of personal and vicarious experiences of both punishment and punishment avoidance on employee intention to follow ISP guidelines.

Appendix - Survey Instrument

<table>
<thead>
<tr>
<th>Variable</th>
<th>Survey Question/Item</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Behavioral Intent</strong></td>
<td>I intend to comply with the removable flash media requirements of the ISP of my organization in the future.</td>
<td>Ajzen (1991), Bulgurcu et al. (2010)</td>
</tr>
<tr>
<td></td>
<td>I intend to protect information and technology resources according to the removable flash media requirements of the ISP of my organization in the future.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td><strong>Attitude</strong></td>
<td>Adopting ISP-related security technologies and practices is important for protecting against removable flash media threats.</td>
<td>Herath &amp; Rao (2009a), Peace et al. (2003), Riemenschneider et al. (2003)</td>
</tr>
<tr>
<td></td>
<td>Adopting ISP-related security technologies and practices is beneficial for protecting against removable flash media threats.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Adopting ISP-related security technologies and practices is helpful for protecting against removable flash media threats.</td>
<td></td>
</tr>
<tr>
<td><strong>Perceived Sanction Severity</strong></td>
<td>My organization disciplines employees who fail to follow the removable flash media requirements of ISP.</td>
<td>Herath &amp; Rao (2009a), Peace et al. (2003), Knapp et al. (2005)</td>
</tr>
<tr>
<td></td>
<td>My organization terminates employees who repeatedly fail to follow the removable flash media requirements of the ISP.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If I were caught violating the removable flash media requirements of the ISP, I would be severely punished.</td>
<td></td>
</tr>
<tr>
<td><strong>Perceived Certainty of Sanction Imposition</strong></td>
<td>Employees that fail to follow the removable flash media requirements of the ISP would be caught, eventually.</td>
<td>Herath &amp; Rao (2009a), Peace et al. (2003), Knapp et al. (2005)</td>
</tr>
<tr>
<td></td>
<td>The likelihood the organization would discover that an employee failed to follow the removable flash media requirements of the ISP is:</td>
<td></td>
</tr>
</tbody>
</table>

References


Lynn III, W. 2010. "Defending a New Domain,").


