Are your employees committed to following your Information Security Policies? Let's hope.

Abstract

Faced with a growing range of information security threats in the workplace, organizations rely upon employee compliance with codified information security policies (ISPs) in order to protect corporate information resources. However, employees are widely considered the weakest link in security in that they often fail to follow security requirements and thus jeopardize their organization's specific or overall security posture. This study explores the impact of an employee's affective organizational commitment on their attitude towards and intent to follow general ISP requirements at a United States governmental organization with an established ISP. Utilizing rational choice theory to decompose the attitudinal antecedents of security policy compliance intent, this study found that organizational commitment is, indeed, an important factor impacting an employee's overall attitude towards security behaviors and compliance intent. Additionally, employee perceptions of benefits of complying with security policies were significant contributors to favorable security attitude whereas perceptions of the cost of compliance and non-compliance were not significant contributors to general security attitude.

Keywords

Information security, organizational commitment, policy compliance, employee, planned behavior, rational choice, attitude.

Introduction

The 2013 data breach of stores owned by Target Brands, Inc. received worldwide media coverage. Over 110 million customer records were stolen by cyber-criminals in November – December 2013. While the long-term financial impact of the Target data breach will not be known for some time, Target estimated the security incident cost $148 million just for the second quarter of 2014 (Abrams, 2014). While Target has not released an official report on the circumstances of the data breach, it is believed that the cyber-criminals gained an initial foothold in the company's network by targeting a third-party employee that was using inappropriate malware detection tools (United States Committee on Commerce Science and Transportation, 2014). For Target, and in numerous other security incidents, employees represent a fragile element, which often fails, in the overall security architecture of an organization.

Employees are appealing information security targets because they hold some level of legitimate access to corporate information resources and reside inside of externally-focused protected network boundaries (Panko, 2010). The primary tool organizations use to prepare employees to best protect themselves and organizational information resources is the Information Security Policy (ISP). The ISP, which describes employee roles and responsibilities across a range of

security threats, is seen by many as one of the most critical components of protecting an organization's information resources (Diver, 2006; Karyda, Kiountouzis, & Kokolakis, 2005). In recognition of the inherent importance of employee actions on organizational information security, there has been an increased focus on behavioral information security research over the past 10-15 years (Barlow, Warkentin, Ormond, & Dennis, 2013; Crossler & Bélanger, 2014; Q. Hu, Xu, Dinev, & Ling, 2011; Willison & Warkentin, 2013).

This paper builds off of the theory of planned behavior and rational choice theory to evaluate how an employee's level of organizational commitment impacts their attitude towards general ISP requirements and their intent to comply with the requirements of the ISP. The study is framed to explore the intentions of a sample of employees of a very large organization with a well-established ISP.

Theoretical Background and Hypotheses Development

Theory of Planned Behavior, Behavioral Intent, Attitude, and Rational Choice Theory

There are numerous theoretical frameworks that can be used to examine employee intended behaviors and actions. We chose to use the Theory of Planned Behavior (TPB) in this study for several reasons. The TPB is one of the most widely used theories in examining human behavior (Ajzen, 2001) and it has been used extensively and successfully in ISP compliance-related research (Bulgurcu, Cavusoglu, & Benbasat, 2010; Dinev & Hu, 2007; Q. Hu, Dinev, Hart, & Cooke, 2012; Siponen, Mahmood, & Pahnila, 2014). Additionally, the TPB lends itself well to decomposing distinct antecedents of behavioral intent, allowing researchers to further develop knowledge of behavioral influences while providing more specific factor details that translate to more practical implications of the research (Taylor & Todd, 1995).

The TPB proffers that a person's intention to take an action 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 factors including subjective norms, perceived behavioral control, attitude towards the behavior, and other context-dependent variables (Ajzen, 1991). Subjective norms represents the perceived social pressure an employee feels to perform an action from relevant others, which in the case of this study will be their co-workers. According to the TPB, the greater the perceived social pressure to perform security-related behaviors, the more the employee will intend to comply with the ISP. Perceived behavioral control exists to accommodate the employee's belief in how much they can overcome obstacles impeding their ability to perform the behavior; a higher perceived behavioral control in personally executing ISP behaviors will result in higher intent to comply with the ISP.

The present study is primarily interested in exploring the impact of employee affective organizational commitment on employee security behaviors. Affective organizational commitment is defined as an employee's identification with, involvement in, and emotional attachment to an organization associated with the perceived costs of supporting organizational goals and interests (Meyer & Allen, 1984; Wiener, 1982). The TPB factor most relevant to this exploration is that of attitude. Attitude toward ISP behaviors is deep rooted in compliance-related beliefs. Attitude toward ISP compliance is "the degree to which the performance of the compliance

behavior is positively valued" (Bulgurcu et al., 2010) (p. 529). 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). 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.

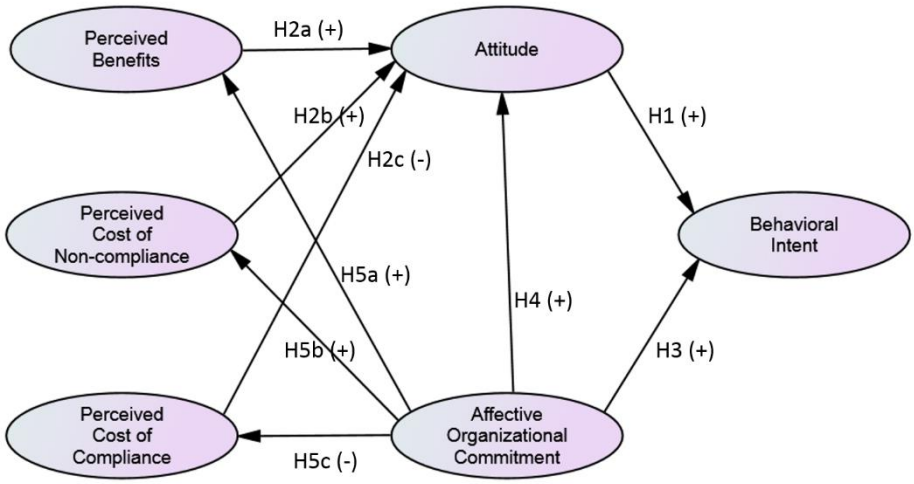

Figure 1 - Research Model and Hypotheses

While it is important to understand the impact of an employee's attitude towards a behavior, treating attitude as a monolithic construct can be limiting as it does not represent any of the variety of dimensions that influence formation of an individual's attitude (Taylor & Todd, 1995). Rational choice theory (RCT) can be used to elucidate the underlying antecedents of an individual's attitude toward compliance with an ISP. RCT indicates that an individual completes a mental calculation of the potential benefits and costs before deciding whether to comply or not comply with the ISP (Vance & Siponen, 2012). Fundamentally, RCT defines the compliance-related beliefs as being composed of (1) perceived benefit of compliance, (2) perceived cost of compliance, and (3) perceived cost of non-compliance (Bulgurcu et al., 2010; Simon, 1955).

The perceived benefit of compliance represents the favorable consequences that are expected as a result of complying with the ISP. For example, if an ISP prohibits the downloading and installing of software from the Internet, employees could (and should) perceive this as a method to reduce the introduction of malware onto the corporate network. The perceived cost of compliance assesses the unfavorable consequences that are expected as a result of complying with the ISP. Keeping with the previous ISP example, the perceived cost of complying with the no-Internet downloads could be large if an employee feels that they need a tool to complete a task that is readily available on the Internet but not on the corporate network. Finally, the perceived cost of

noncompliance represents the expected unfavorable consequences that are expected as a result of noncompliance with the ISP. Not complying with the no-Internet downloads policy may be perceived as not only resulting in sanctions by the organization, but perhaps the introduction of malware that debilitates the corporate network for a period of time. RCT focuses on these consequences of potential courses of action, considering both compliance and noncompliance and costs and benefits. Prior research has also explored response cost and response cost-benefit (included in protection motivation theory) as influences on attitude and behavior in compliance with an ISP (Herath & Rao, 2009; Workman, Bommer, & Straub, 2008). However, the definitions match closely without the finer granularity of variable definitions given by the RCT. Therefore, this research will focus on the RCT constructs.

Few studies have specifically explored the impact of the RCT constructs on an employee's attitude towards ISP compliance. Bulgurcu et al. (2010) found that perceived benefit of compliance, perceived cost of compliance, and perceived cost of non-compliance influence attitude towards compliance, and attitude, in turn, influences ISP compliance intention. Additionally, research has examined and found perceived benefits (in terms of time) to influence one's intention to violate an ISP (Vance & Siponen, 2012). We have adopted Bulgurcu et al. (2010)'s conceptualization of RCT components and influence on attitude.

Given the TPB and the RCT, an individual's attitude towards complying with the ISP will be influenced by the three RCT beliefs. Those three beliefs contribute to the employee's attitude as defined in the TPB which then influences behavioral compliance intent (as shown in Figure 1). More specifically, the individual's perceived benefit of compliance will positively influence their attitude towards complying with the ISP such that that the stronger the perceived benefit, the more positive the attitude towards the behavior. An individual's perceived cost of compliance will negatively influence their attitude towards complying with the ISP such that larger the perceived costs associated with following ISP-related behavior, the weaker the employee's attitude will be towards that behavior. Finally, the individual's perceived cost of noncompliance will positively influence their attitude towards the behavior such that the larger the perceived associated costs related to non-compliant behavior, the more likely they are to have a positive attitude towards enacting the behavior. Therefore, we propose the following hypotheses:

> Hypothesis 2a: An increase in an individual's perceived benefit of compliance with ISP-related behaviors will positively influence their attitude towards compliance intent.
>
> Hypothesis 2b: An increase in an individual's perceived cost of compliance with ISP-related behaviors will negatively influence their attitude towards compliance intent.
>
> Hypothesis 2c: An increase in an individual's perceived cost of noncompliance with ISP-related behaviors will positively influence their attitude towards compliance intent.

Affective Organizational Commitment

There is a rich base of organizational behavior research on the concept of organizational commitment. Porter, Steers, Mowday, and Boulian (1974) first defined organizational commitment as a unitary construct that represented the strength of an individual's identification

with and involvement in an organization. A higher commitment from employees is valued by organizations with the belief that higher levels of commitment leads to less negative and more positive behaviors (Mathieu & Zajac, 1990; Mowday, Steers, & Porter, 1979). This general belief in organizational commitment has been supported by research that indicates employees with low levels of commitment perform at minimum levels required for continued employment (Riketta, 2002) and high levels of commitment are reflected in more positive proactive work behaviors (Ng, Feldman, & Lam, 2010).

Meyer and Allen (1991) decomposed organizational commitment into three related yet distinctive forms of commitment: affective, continuance, and normative. Affective commitment refers to an individual's emotional attachment to an organization (through identification and involvement) (Meyer & Allen, 1991). Continuance commitment relates to the perceived costs associated with leaving an organization and normative commitment refers to a perceived obligation to remain with the organization (Meyer, Stanley, Herscovitch, & Topolnytsky, 2002). It has become widely accepted that the Porter et al. (1974) original definition of organizational commitment represents affective commitment (Mowday, 1999). As the purpose of this paper is to explore the impact of employee organizational commitment on performing ISP-related behaviors, as opposed to employee retention (via continuance and normative commitment), we focused on the impact of affective organizational commitment.

Little research has been undertaken to explore the impact of affective organizational commitment on employee ISP behavioral compliance. Stanton, Mastrangelo, Stam, and Jolton (2004) surveyed an international pool of participants in a wide variety of industries with measures of affective organizational commitment and a sample of positive and negative security behaviors. They found that higher organizational commitment generally facilitates the performance of positive security behaviors and inhibits the performance of negative security behaviors, in congruence with the larger community of organizational commitment research. Herath and Rao (2009) sampled employees in 78 organizations in the western New York area and found that affective organizational commitment positively impacted both employee intent to follow ISP requirements as well as the respondents' beliefs in the effectiveness of ISP-related actions. Due to the sample method used, neither of the aforementioned studies included knowledge or the presence of ISPs at the organizations of the participants, which limits the applicability of projecting the findings on organizations that do have established ISPs. To overcome this limitation, we surveyed participants at a single large organization with an established ISP. We understand that by doing so, we are limiting the scope of generalizing the findings of this study to other organizational contexts, but we felt it was more important to evaluate actual employees of organizations that have known codified ISPs.

Meta-analysis studies of organizational commitment (Mathieu & Zajac, 1990; Meyer et al., 2002) found that affective commitment had the strongest and most favorable correlations with organization-relevant behaviors and outcomes. Affective organizational commitment has also been identified in the literature as attitudinal commitment (O'Driscoll, 1987; Williams & Anderson, 1991). .

As the results of the extant literature in organizational commitment that examines affective organizational commitment as both a proxy for and as a component of attitude, we examine the direct impact of affective organizational commitment on both attitude and individual behavior with the following hypotheses:

> Hypothesis 3: An increase in an individual's affective organizational commitment will positively influence their ISP-related behavioral compliance intent.
>
> Hypothesis 4: An increase in an individual's affective organizational commitment will positively influence their attitude towards an ISP-related behavior.

As discussed above, the model we propose (shown in Figure 1) decomposes attitude using rational choice theory into three contributing factors: perceived benefits, perceived cost of compliance, and perceived cost of non-compliance. In the context of this study, we would expect an employee with a higher level of affective organizational commitment to feel closer aligned with the beliefs of the organization to include a greater perception of the benefits of complying with the ISP, a decrease in the perceived costs of complying with the ISP, and an increased perceived cost of non-compliance. Given that affective organizational commitment is expected to positively impact employee attitudes about security behaviors, we hypothesize:

> Hypothesis 5a: An increase in an individual's affective organizational commitment will positively influence their perceived benefit of compliance with ISP-related behaviors.
>
> Hypothesis 5b: An increase in an individual's affective organizational commitment will decrease (negatively influence) their perceived cost of compliance with ISP-related behaviors.
>
> Hypothesis 5c: An increase in an individual's affective organizational commitment will positively influence their perceived cost of noncompliance with ISP-related behaviors.

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 and organizational commitment studies (see Table 1). The DoD consists of over 3.5 million military personnel and civilian employees. All DoD employees, including contract personnel, fall under the same general ISP, known at the time as DoD Information Awareness Assurance (IAA). Every DoD employee, regardless of rank, status or organization, falls under the IAA guidelines and requirements, in addition to any additional potentially 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, which often precludes many personnel from their daily work. In order to best compare the results of our study to the majority of ISP compliance-related research, our proposed model focuses on employee general ISP compliance

instead of any specific threat; we realize that this decision is limiting and we discuss that later in the paper.

Variable	Survey Question/Item	Item	Mean	STD	Factor Loading	Source(s)
Behavioral Intent (BINT)	I intend to comply with the general requirements of the ISP of my organization in the future.	BINT1	6.660	0.484	0.949	Ajzen (1991), Bulgurcu et al. (2010), Herath & Rao (2009)
	I intend to protect information and technology resources according to the general requirements of the ISP of my organzation in the future.	BINT2	6.599	0.495	0.969	
	I intend to carry out my general responsibilities prescribed in the ISP of my organization when I use information and technology in the future.	BINT3	6.622	0.479	0.991	
Attitude (ATT)	Adopting ISP-related security technologies and practices is important for protecting against information security threats in general.	ATT1	6.592	0.502	0.934	Ajzen (1991), Bulgurcu et al. (2010), Herath & Rao (2009)
	Adopting ISP-related security technologies and practices is beneficial for protecting against information security threats in general.	ATT2	6.606	0.508	0.947	
	Adopting ISP-related security technologies and practices is helpful for protecting against information security threats in general.	ATT3	6.620	0.496	0.894	
Affective Organizational Commitment (ORCOM)	I am willing to put in a great deal of effort beyond that normally expected in order to help my organization be successful.	ORCOM1	6.226	0.921	0.849	Herath & Rao (2009), Mowday, Steers, & Porter (1979)
	I really care about the fate of this organization.	ORCOM2	6.575	0.596	0.859	
	For me, this is the best of all possible organizations for which to work.	ORCOM3	5.733	1.174	0.526	
Perceived Benefits of Compliance (PBEN)	My compliance with the general requirements of the ISP would be favorable to me.	PBEN1	5.882	1.055	0.704	Bulgurcu et al. (2010)
	My compliance with the general requirements of the ISP would result in benefits to me.	PBEN2	5.506	1.201	0.906	
	My compliance with the general requirements of the ISP would create advantages for me.	PBEN3	4.996	1.340	0.814	
Perceived Cost of Compliance (PCOMP)	Complying with the general requirements of the ISP is time consuming for me.	PCOMP1	3.955	1.767	0.863	Bulgurcu et al. (2010)
	Complying with the general requirements of the ISP is time burdensome for me.	PCOMP2	3.475	1.733	0.989	
	Complying with the general requirements of the ISP is time costly for me.	PCOMP3	2.919	1.647	0.805	
Perceived Cost of Non-Compliance (PNONC)	My noncompliance with the general requirements of the ISP would be harmful to me.	PNONC1	5.774	1.284	0.791	Bulgurcu et al. (2010)
	My noncompliance with the general requirements of the ISP would impact me negatively.	PNONC1	5.909	1.144	0.851	
	My noncompliance with the general requirements of the ISP would create disadvantages to me.	PNONC3	5.471	1.568	0.757	

Table 1- Constructs, Items, and CFA Standardized Factor Loadings

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 96 unusable surveys, categorized as such because the survey participants did not complete the survey sufficiently. Therefore, the total useful sample was 221.

Analysis and Results

Covariance-based structural equation modeling (SEM) procedures were 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 (Gefen, Straub, & Rigdon, 2011; Heck, 1998). 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 (Byrne, 2001; Gefen et al., 2011). Due to excessive skew associated with latent construct measurement items, all measurement items were log10 transformed to obtain satisfactory skewness coefficients (Kline, 2011). 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, and Podsakoff (2003) per the guidance in Gefen et al. (2011) and 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.

Covariance-based SEM analysis consists of two parts: a CFA stage and the structural model analysis (also known as path analysis) stage (Heck, 1998; Jöreskog & Sörbom, 1989). 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 of measurement items 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 (χ^2/df = 1.418; χ^2 = 170.16; df = 120; CFI = 0.985; SRMR = .046).

Following establishment of the measurement model in the CFA stage, the data were fitted to the a priori research models (see Table 3). Initial model fit was assessed using multiple criteria such as chi-square, degrees of freedom, and normed chi-square (χ2/df) (Heck, 1998; Kline, 2011; Raykov, 2006). To further account for the potential impact of even mild deviations from perfectly normal data distributions on the χ2 calculations, Bollen and Stine (1992) bootstrapping was conducted to calculate model fit p values, which are all above the common 0.05 threshold. However, reliance upon χ2 measurements alone for model fit determination is cautioned and one goodness-of-fit and one badness-of-fit metric was used to further assess overall model fit(Kline, 2011). The comparative fit index (CFI) is the goodness-of-fit metric reported in this paper. The CFI measures model fit relative to a null model and non-centrality index. All reported CFI values are above the

0.90 (Marsh, Hau, & Wen, 2004) or the 0.95 (L. Hu & Bentler, 1999) recommended thresholds. The badness-of-fit metric reported in this paper is the standardized root mean square residual (SRMR), which compares the residuals (unexplained variance) to what would be reasonably expected from a well-fitting model. In our theorized research model, the SRMR is below the common threshold of 0.08 indicating good model fit (L. Hu & Bentler, 1999). Although not the case in our proposed model (which has all satisfactory fit values), it is acceptable that not all fit indexes be simultaneously within the above threshold rules of thumb (Gefen et al., 2011).

	CR	AVE	MSV	ASV	PBEN	ATT	BINT	ORCOM	PCOMP	PNONC
PBEN	0.852	0.660	0.566	0.233	**0.812**					
ATT	0.947	0.856	0.372	0.215	0.444	**0.925**				
BINT	0.979	0.941	0.569	0.266	0.435	0.603	**0.970**			
ORCOM	0.798	0.578	0.569	0.263	0.452	0.610	0.754	**0.761**		
PCOMP	0.918	0.790	0.035	0.013	-0.095	-0.084	-0.111	-0.186	**0.889**	
PNONC	0.842	0.641	0.566	0.207	0.752	0.367	0.445	0.367	0.006	**0.801**

CR = Composite Reliability
AVE = Average Variance Extracted
MSV = Maximum Shared Squared Variance
ASV = Average Shared Squared Variance
PBEN = Perceived Benefits
ATT = Attitude
BINT = Behavioral Intent
ORCOM = Affective Organizational Commitment
PCOMP = Perceived Cost of Compliance
PNONC = Perceived Cost of Non-Compliance

Table 2- Validity Table with Factor Correlation Matrix

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 – 5c. The results of the structural model evaluation results are shown in Table 3.

SEM Model Fit Results	Proposed Model
$\chi 2$ / df	2.053
$\chi 2$	258.734
df	126
Comparitive Fit Index (CFI)	0.962
Standardized Root Mean Residual (SRMR)	0.069
BINT Squared Multiple Correlation (SMC)	0.62
ATT Squared Multiple Correlation (SMC)	0.414
SEM Structual Path Results	
H1: ATT → BINT	.190**
H2a: PBEN → ATT	.107*
H2b: PCOMP → ATT	NS
H2c: PNONC → ATT	NS
H3: ORCOM → BINT	.705***
H4: ORCOM → ATT	.602***
H5a: ORCOM → PBEN	.874***
H5a: ORCOM → PCOMP	(-0.216)*
H5a: ORCOM → PNONC	.694***

Notes: *p<0.05, **p<0.01, ***p<0.001 BINT: Behavioral Intent, ATT: Attitude, ORCOM: Affective Organizational Commitment, PBEN: Perceived Benefits, PCOMP: Perceived Cost of Compliance, PNONC: Perceived Cost of Non-Compliance, NS: Not Significant
Proposed Model as shown in Figure 1

Table 3 - Structural Model Evaluation Results

As shown in Table 3, model fit criteria for our proposed model is satisfactory with both CFI and SRMR are within the limits discussed above. The results of the path analyses, also shown in Table 3, provide the expected support to H1, that attitude positively influences ISP compliance behavioral intent. The postulated positive impact of affective organizational commitment to both attitude (H4) and behavioral intent (H3) are also supported, affirming related ISP compliance related research utilizing the theory of planned behavior and organizational commitment constructs.

The most interesting findings belong to the hypotheses related to the decomposed rational choice attitudinal components with attitude and affective organizational commitment. The hypothesized relationships between affective organizational commitment and the RCT decomposed antecedents of attitude (H5a – H5c) are all confirmed with significant β coefficients and the predicted directionality. However, the only RCT component that has a confirmed causal relationship with attitude in our study is perceived benefits of compliance with ISP-related behaviors (H2a). In our study, the paths between the perceived cost-related components (compliance and non-compliance) were not significant (representing H2b and H2c).

Discussion, Limitations, Conclusion

This paper provides several theoretical and practical contributions to the study of employee ISP behavioral compliance intent. From a theoretical perspective, it builds upon the few related works in the extent ISP compliance literature by acknowledging the importance of both rational choice theory and affective organizational commitment to impact security behavioral compliance. The amount of variance explained by our model for Attitude and Behavioral Intent by the model in this study is well above the 10% rule of thumb generally accepted in order to claim explanatory power (Guo & Yuan, 2012). The proposed model in this study focused on evaluating the Attitude component of the TPB without addressing the contributions from other core behavioral antecedents (such as subjective norms and perceived behavioral control). Likewise, ISP behavioral compliance studies (Bulgurcu et al., 2010; Herath & Rao, 2009; Zhang, Reithel, & Li, 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. That our proposed model, with its limited theoretical focus, explains such high levels of variance shows that both affective organizational commitment and RCT are important variables to explore in better understanding employee ISP compliance intent.

Focusing on the decomposition of Attitude using the RCT, we see that for our study context, employees valued the perceived benefits of ISP behavioral compliance much more so than for the cost related factors (cost of compliance and non-compliance). From a practical perspective, it can be seen as a positive outcome that employees are focused on the benefits of the ISP. However, that employee responses for cost-related RCT components were not significant potentially represents a weakness in the security training and awareness program in the DoD. Ideally, the DoD, and other organizations in general, would like their employees to understand and appreciate the potential negative impact of not-complying with the ISP (beyond the potential threats of sanctions if caught violating ISP requirements) and use that knowledge to bolster their behavioral compliance intent. Likewise, reducing the perceived cost of complying with the ISP should also bolster compliance

intent, but that result would likely not occur in the sample population of this study without direct action by the DoD to improve ISP communication and comprehension.

This study shows the significant effect affective organizational commitment has on the RCT antecedents of attitudes towards ISP behaviors. In practice, an organization should have a grasp on events that occur that may increase or decrease their employees' affective commitment. For example, in the DoD, organizations that experience extended overseas deployments or high levels of casualties may witness a decline in morale and with it affective commitment. In times such as these, not only is it in the interest of the organization to improve the conditions that lead to the decline in affective commitment, but also focus their efforts to monitor ISP behavioral compliance and take necessary actions to improve compliance. Outside of the DoD, organizations that are downsizing or performing poorly may suffer similar effects and should be aware of the deleterious impact of sinking affective commitment on ISP behavioral compliance.

For the reasons discussed earlier, the focus of this research was limited to affective commitment. Future research should also explore the other two components of organizational commitment – continuance and normative. For example, the organizational commitment literature shows that government employees have higher levels of continuance commitment than other industries (Meyer John & Allen Natalie, 1997; Perry, 1997) for reasons such as job security and strong ethics (Liou, 1995; Perry, 1997). Examining how the ISP behavioral compliance employees of the DoD or other governmental organizations, is affected temporally by uncertain budgets and other events that erode the three manifestations of organizational commitment would may illuminate trends in ISP compliance behavior that can be mitigated in similar future events.

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 to 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, the participants of our study were asked to respond about general information security threats and behaviors. While studying general ISP behaviors can be beneficial to understand underlying behavioral factors across a range of security threats, the results of this study may have been very different if participants were asked to respond about specific threats such as password security, phishing, or physical access control.

Another limitation of this study was that the items used to measure affective organizational commitment were a subset of three questions selected from Mowday et al. (1979)'s organizational commitment questionnaire (OCQ). The OCQ contains 15 questions and has received extensive psychometric evaluation and validation. We chose to use three specific measures from the OCQ to measure affective organizational commitment in this study for two reasons. First, the survey

instrument used in this study contained numerous other measures resulting in an already very long survey. We were concerned about survey mortality, which did occur (see the method section for specifics). Second, the three specific items from the OCQ chosen were also used in Herath and Rao (2009), the only other study in this field that examined the causal effects of affective commitment on ISP behavioral compliance. Future studies exploring the impact of affective organization commitment on ISP compliance should consider using all of the OCQ items or the smaller eight-item affective commitment scale (ACS) offered by Allen and Meyer (1990). Although we used only three items to measure affective commitment, we believe the measures captured the essence of the construct as shown by the satisfactory factor loadings, AVE value, and composite reliability.

In conclusion, organizations, such as the DoD, would be wise to understand the current and changing levels of affective organizational commitment of their employees to gain a clearer understanding of the impact on employee ISP behavioral compliance and the specific perceptive calculus that goes into developing their attitudes towards security behaviors. Additionally, the data in our study indicate that, for the participating employees, the perceived benefit of ISP compliance is the driving rational choice factor in development of security behavior attitudes. The lack of impact on attitude from perceived cost of compliance or non-compliance with the ISP is problematic and may point towards deficiencies in security training and awareness programs.

References

Abrams, R. (2014, August 6, 2014). Target Puts Data Breach Costs at $148 Million, and Forecasts Profit Drop. *The New York Times*.

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes, 50*(2), 179-211.

Ajzen, I. (2001). Nature and operation of attitudes. *Annual review of psychology, 52*(1), 27-58.

Allen, N. J., & Meyer, J. P. (1990). The measurement and antecedents of affective, continuance and normative commitment to the organization. *Journal of occupational psychology, 63*(1), 1-18.

Aurigemma, S. (2013). A Composite Framework for Behavioral Compliance with Information Security Policies. *Journal of Organizational and End User Computing, 25*(3), 20.

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

Bollen, K. A., & Stine, R. A. (1992). Bootstrapping goodness-of-fit measures in structural equation models. *Sociological Methods & Research, 21*(2), 205-229.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS quarterly, 34*(3).

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, 1*(1), 55-86.

Chin, W. W. (1998). Commentary: Issues and opinion on structural equation modeling: JSTOR.

Crossler, R. E., & Bélanger, F. (2014). An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument. *The DATA BASE for Advances in Information Systems*.

Dinev, T., & 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, 8*(7).

Diver, S. (2006). Information Security Policy - A Development Guide for Large and Small Companies (pp. 43): SANS Institute.

Gefen, D., Straub, D. W., & Rigdon, E. E. (2011). An update and extension to SEM guidelines for admnistrative and social science research. *Management Information Systems Quarterly, 35*(2), iii-xiv.

Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. *Information & Management, 49*(6), 320-326.

Heck, R. H. (1998). Factor analysis: Exploratory and confirmatory approaches. *Modern methods for business research*, 177-215.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125.

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal, 6*(1), 1-55.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*. *Decision Sciences, 43*(4), 615-660.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM, 54*(6), 54-60.

Jöreskog, K. G., & Sörbom, D. (1989). *LISREL 7: A guide to the program and applications* (Vol. 2): Spss Chicago.

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: a contextual perspective. *Computers & Security, 24*(3), 246-260.

Kline, R. B. (2011). *Principles and practice of structural equation modeling*: Guilford press.

Liou, K. T. (1995). Professional orientation and organizational commitment among public employees: an empirical study of detention workers. *Journal of public administration research and theory, 5*(2), 231-246.

Marsh, H. W., Hau, K.-T., & 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, 11*(3), 320-341.

Mathieu, J. E., & Zajac, D. M. (1990). A review and meta-analysis of the antecedents, correlates, and consequences of organizational commitment. *Psychological bulletin, 108*(2), 171.

Meyer John, P., & Allen Natalie, J. (1997). Commitment in the Workplace. *Theory, Research and Application, Sage Publications, Inc., London*.

Meyer, J. P., & Allen, N. J. (1984). Testing the" side-bet theory" of organizational commitment: Some methodological considerations. *Journal of applied psychology, 69*(3), 372.

Meyer, J. P., & Allen, N. J. (1991). A three-component conceptualization of organizational commitment. *Human resource management review, 1*(1), 61-89.

Meyer, J. P., Stanley, D. J., Herscovitch, L., & Topolnytsky, L. (2002). Affective, continuance, and normative commitment to the organization: A meta-analysis of antecedents, correlates, and consequences. *Journal of vocational behavior, 61*(1), 20-52.
Mowday, R. T. (1999). Reflections on the study and relevance of organizational commitment. *Human resource management review, 8*(4), 387-401.
Mowday, R. T., Steers, R. M., & Porter, L. W. (1979). The measurement of organizational commitment. *Journal of vocational behavior, 14*(2), 224-247.
Ng, T. W., Feldman, D. C., & Lam, S. S. (2010). Psychological contract breaches, organizational commitment, and innovation-related behaviors: a latent growth modeling approach. *Journal of applied psychology, 95*(4), 744.
O'Driscoll, M. P. (1987). Attitudes to the job and the organisation among new recruits: Influence of perceived job characteristics and organisational structure. *Applied Psychology, 36*(2), 133-145.
Panko, R. (2010). *Corporate Computer and Network Security, 2/e*. Upper Saddle River, NJ: Pearson Prentice Hall.
Perry, J. L. (1997). Antecedents of public service motivation. *Journal of public administration research and theory, 7*(2), 181-197.
Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of applied psychology, 88*(5), 879.
Porter, L. W., Steers, R. M., Mowday, R. T., & Boulian, P. V. (1974). Organizational commitment, job satisfaction, and turnover among psychiatric technicians. *Journal of applied psychology, 59*(5), 603.
Raykov, T., & Marcoulides, G.A. (2006). *A first course in structural equation modeling*: Lawrence Erlbaum.
Riketta, M. (2002). Attitudinal organizational commitment and job performance: a meta-analysis. *Journal of Organizational Behavior, 23*(3), 257-266.
Simon, H. A. (1955). A behavioral model of rational choice. *The quarterly journal of economics, 69*(1), 99-118.
Siponen, M., Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224.
Stanton, J. M., Mastrangelo, P., Stam, K. R., & Jolton, J. (2004). *Behavioral Information Security: Two End User Survey Studies of Motivation and Security Practices.* Paper presented at the 10th Americas Conference on Information Systems, AMCIS 2004, New York, NY, USA, August 6-8, 2004.
Taylor, S., & Todd, P. A. (1995). Understanding information technology usage: A test of competing models. *Information systems research, 6*(2), 144-176.
United States Committee on Commerce Science and Transportation. (2014). A "Kill Chain" Analysis of the 2013 Target Data Breach.
Vance, A., & Siponen, M. T. (2012). IS security policy violations: a rational choice perspective. *Journal of Organizational and End User Computing (JOEUC), 24*(1), 21-41.
Wiener, Y. (1982). Commitment in organizations: A normative view. *Academy of management review, 7*(3), 418-428.
Williams, L. J., & Anderson, S. E. (1991). Job satisfaction and organizational commitment as predictors of organizational citizenship and in-role behaviors. *Journal of management, 17*(3), 601-617.

Willison, R., & Warkentin, M. (2013). BEYOND DETERRENCE: AN EXPANDED VIEW OF EMPLOYEE COMPUTER ABUSE. *MIS Quarterly, 37*(1).

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816.

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security, 17*(4), 330-340.