Association for Information Systems
AIS Electronic Library (AISeL)

MCIS 2011 Proceedings

Mediterranean Conference on Information Systems (MCIS)

2011

INFORMATION SECURITY POLICY COMPLIANCE: THE ROLE OF FAIRNESS, COMMITMENT, AND COST BELIEFS

Burcu Bulgurcu
University of British Columbia, bulgurcu@bc.edu

Hasan Cavusoglu
University of British Columbia, hasan.cavusoglu@sauder.ubc.ca

Izak Benbasat
University of British Columbia, izak.benbasat@sauder.ubc.ca

INFORMATION SECURITY POLICY COMPLIANCE: THE ROLE OF FAIRNESS, COMMITMENT, AND COST BELIEFS

Bulgurcu, Burcu, Sauder School of Business, University of British Columbia, 2053 Main Mall, Vancouver, British Columbia, Canada V6T 1Z2, burcu.bulgurcu@sauder.ubc.ca

Cavusoglu, Hasan, Sauder School of Business, University of British Columbia, 2053 Main Mall, Vancouver, British Columbia, Canada V6T 1Z2, hasan.cavusoglu@sauder.ubc.ca

Benbasat, Izak, Sauder School of Business, University of British Columbia, 2053 Main Mall, Vancouver, British Columbia, Canada V6T 1Z2, izak.benbasat@sauder.ubc.ca

Abstract

This research aims to extend our knowledge of the factors that drive an employee to comply with requirements of the Information Security Policy (ISP) of her organization in regards to protecting its information and technology resources. In particular, this paper focuses on the organizational costs associated with an employee's ISP compliance and non-compliance. An employee's organization-based cost beliefs—perceived organizational cost of compliance and perceived organizational cost of non-compliance—are posited to affect his attitude towards compliance. Furthermore, we discuss two organizational factors— ISP Fairness and Organizational Commitment— as moderators posited to change the strength of the impact of organization-based beliefs on attitude. Based on the regression analysis of data collected from 460 participants, the results show that organization-based employee beliefs significantly affect attitude, and as predicted, the strength of each belief-attitude relationship is affected by ISP fairness and organizational commitment. We also show that the proposed moderator factors have significant main affects on attitude.

Keywords: information security policy, information security management, compliance, fairness, organizational commitment, cost of compliance, cost of non-compliance

1 INTRODUCTION

As the focus on information security has shifted beyond technology-oriented perspectives, employees' compliance with information security policies (hereafter ISPs) has emerged as a key socio-organizational resource (Boss and Kirsch 2007; Siponen and Willison 2007). In order to ensure information security, organizations create ISPs to provide guidelines as to what employees should do while performing their tasks (Whitman et al. 2001). Most information-security-related risks can be managed if employees comply with the ISP of their organizations. Although creating guidelines and policies is necessary, it is not sufficient to ensure employees' compliance with them. Therefore, understanding what factors motivate employees to comply with their organizations' ISPs is crucial for information security managers to better manage their security efforts. Recently, Pahnila et al. (2007) in a case study and Bulgurcu et al. (2010) in an empirical study investigated the factors affecting employees' compliance with the ISP.

Studies in the security compliance literature often identify incentives, such as rewards (Boss and Kirsch 2007), or disincentives, such as sanctions (Lee and Lee 2002; Lee et al. 2003; Straub and Nance 1990; Willison 2006) as factors which motivate employees' compliance with security rules and regulations. However, the factors considered are often individual-based. That is, those factors describe consequences that affect *the employee* as a result of his compliance or non-compliance with the ISP of his organization. While an employee's beliefs about the consequences that he will personally face if he complies or not were shown to affect the employee's attitude toward compliance (Bulgurcu et al. 2010), to the best of our knowledge, the roles of employee's beliefs about the consequences of the ISP compliance which affect *the organization* have not been studied in the literature. We argue that an employee's actions concerning security may result in consequences not only to the employee but also to her organization. Therefore, one of the major goals of this study is extending our knowledge about the employee's compliance with the ISP by focusing on employee's beliefs about consequences of compliance or non-compliance to the organization. We define an employee's organization-based beliefs as perceived consequences that the organization incurs/gains based on compliance.

In this paper, we focus on the organizational cost aspect of an employee's compliance and non-compliance. Hence, we propose two main constructs for organization-based employee beliefs—perceived organizational cost of compliance and perceived organizational cost of non-compliance—and hypothesize their relationships with the employee's attitude towards compliance. Further, we propose two moderating factors—ISP fairness and organizational commitment—and investigate how they moderate the strength of the impact of an employee's organizational based beliefs on his attitude. We define ISP as a statement of the roles and responsibilities of the employees to safeguard the information and technology resources of their organizations. With this definition of the ISP, our study aims to address two questions:

What is the role of an employee's perceived organizational *cost of compliance* (CC) and cost of *non-compliance* (CNC) in influencing his attitude towards ISP compliance?

What is the role of the *ISP fairness* and an employee's *organizational commitment* in moderating the strength of the impact of his *organization-based beliefs* on his attitude towards compliance?

The paper is organized as follows. Section 2 presents the theoretical foundation of the research, discusses the research models, and develops the hypotheses to be tested. Section 3 summarizes the research method. Section 4 describes the data analysis and presents the results and their implications, and Section 5 presents the conclusion and future research directions.

This work was supported by Social Sciences and Humanities Research Council (SSHRC) and the Institute for Computing, Information and Cognitive Systems (ICICS) at the University of British Columbia.

2 THEORETICAL MODEL AND HYPOTHESIS

2.1 Organization-based Beliefs about the Consequences of Compliance and Non-Compliance

In this study, we focus on understanding of the antecedents of an employee's attitude toward compliance with the ISP. It is important to study an employee's attitude since it is expected to lead his intention to comply and actual compliance behaviour. The extant literature has argued that an employee's attitude towards performing a given behaviour is related to his beliefs about behaviour-related consequences (Fishbein and Ajzen 1975). In this study, we only include organization-based employee beliefs so that behaviour-related consequences are expected to be gained/ incurred by the organization. While we do not ignore the potential role of organizational benefits in affecting an employee's compliance behaviour, for brevity in this paper we focus on the organizational costs associated with an employee's compliance and non-compliance with the ISP.

The ISP stipulates an employee's role and responsibilities in protecting the information and technology resources of his organization, so compliance with the ISP is not a passive event. When an employee performs what is prescribed in the ISP (for example, when he spends half a day to back-up his information resources every other month), he considers the costs associated with compliance, since compliance requires some effort and time. His organization incurs costs as a result of his compliance since it may affect the organization's relationships with its partners, customers or the relationships among colleagues. Further, the employee considers the organizational costs associated with non-compliance (because the organization might be penalized if he does not comply). In keeping with Fishbein and Ajzen (1975), who highlighted the punishment and effort involved in performing the behaviour as behaviour-related consequences, we propose two organization-based employee beliefs: (i) Perceived Organizational Cost of Non-Compliance (CNC), and (ii) Perceived Organizational Cost of Compliance (CC).

We define *Perceived Organizational Cost of Non-Compliance* as the overall expected unfavourable consequences to the organization for the employee's non-compliance. Examples are *organizational sanctions* such as monetary or non-monetary penalties and/or damages, litigation, broken relations with customers and/or partners, loss of reputation and customers. *Perceived Organizational Cost of Compliance* is the overall expected unfavourable consequences to the organization for the employee's compliance. Compliance requires time and effort that could have been directed to other primary and strategic business activities. For example, an employee may perceive that compliance holds his organization back from reaching its primary goals, slows down his organization's service to his customers, partners etc., and hinders overall productivity of the organization. Pahnila et al. (2007) shown that ensuring information security may contradict with meeting the primary or strategic goals of the business.

Based on the Theory of Planned Behaviour (Ajzen 1991), we posit that an employee's organization-based beliefs about the consequences will influence his attitude towards complying with the requirements of the ISP. We define attitude as the degree to which the performance of the compliance behavior is positively valued (Fishbein and Ajzen 1975; Ajzen 1991). Drawing on the expectancy-value theory of attitude (Fishbein and Ajzen 1975), it is possible to determine whether an employee's beliefs will positively or negatively influence his attitude towards compliance. According to the expectancy-value theory, an individual learns to favor behaviours he believes have desirable consequences and not to favor those with undesirable consequences. Consequently, in our context, we argue that, if an employee perceives that his organization derives disadvantage from non-compliance or if he perceives that the organization does not expend much effort for compliance, he forms a favourable attitude toward compliance. In the security context, the more costly it is to perform security requirements in terms of time and effort, the less likely it is for employees to perform those requirements (PWC 2008). Therefore, we propose the following hypotheses for the antecedents of the attitude toward compliance:

Hypothesis 1: An employee's *perceived organizational* ***CNC*** positively affects her attitude toward complying with the requirements of the ISP.

Hypothesis 2: An employee's *perceived organizational* ***CC*** negatively affects his attitude toward complying with the requirements of the ISP.

2.2 The Role of ISP Fairness and Organizational Commitment

ISP Fairness: While the information security literature has mostly highlighted the deterrent effects of sanctions (Lee and Lee 2002; Lee et al. 2003; Straub and Nance 1990), the organizational literature has focused on the role of incentives in encouraging desirable employee conduct (Stajkovic and Luthans 1997). However, an employee's willingness to follow rules may not necessarily be motivated only by sanctions or incentives. Although such strategies provide an external motivation, an employee's intrinsic desires provide an internal motivation for an employee to follow (or not follow) rules and regulations (Tyler and Blader 2005). We expect that internal motivations exist in the context of ISP compliance and propose an employee's perceived ISP fairness as one of the intrinsic motivational factors. *ISP fairness* is defined as an employee's belief in the fairness of the requirements prescribed and dictated by the ISP of her organization. Various studies conducted on justice in the field of organizational science support the view that if an organization fails to provide fair processes, treatment, information, or outcomes, deviant behaviours often increase (Aquino et al. 2006; Bies 1987). For example, employees' perceptions of unfairness of the procedures and treatments were directly linked to aggression and violence (Baron 2004), psychological contract violation (Morrison and Robinson 1997), avoidance and revenge (Aquino et al. 2006), sabotage (Ambrose at al. 2002), and theft (Greenberg 1990; Tomlinson and Greenberg 2005). Besides the widely accepted role of organizational injustice on deviant behaviour, group engagement model (Tyler and Blader 2000) argues that justice is central to how and whether people construct their group-related identities and cooperate within the group. In accordance with the literature on organizational justice and group engagement model, we argue that an employee's perceived ISP fairness would positively affect her attitude toward ISP compliance. Hence,

Hypothesis 3: *ISP Fairness* positively affects an employees' attitude towards ISP compliance.

In accordance with the existing literature of organizational behavior, we further argue that employees are more likely to develop intrinsic motivations towards ISP compliance in the presence of high ISP fairness. We suggest that when the employee does not perceive the organization's ISP requirements to be fair, he would need external motivations to comply with these requirements. However, if he believes in the fairness of the ISP requirements, he will be more likely to believe in the necessity of these requirements to enhance the organization's information security. Accordingly, we argue that *ISP fairness* would influence the effectiveness of organization-based cost beliefs in developing positive attitude towards ISP compliance. In other words, in the absence of ISP fairness, any kind of organizational costs of compliance or non-compliance would play a more important role. Based on these arguments, we hypothesize the following:

Hypothesis 4: *ISP Fairness* moderates the relationship between the *CNC* and *attitude*, such that when *ISP Fairness* is low, higher *CNC* will have a higher positive influence on attitude, but when *it* is high, higher *CNC* will be less influential or have no direct impact on attitude.

Hypothesis 5: *ISP Fairness* moderates the relationship between the *CC* and *attitude*, such that when *ISP Fairness* is low, higher *CC* will have a higher negative influence on attitude, but when *it* is high, higher *CC* will be less influential or have no direct impact on attitude.

Organizational Commitment: According to the social bond theory (Hirschi 1969), which is one of the well-received criminology theories, a person commits a crime when weak or non-existent social bonds give the deviant the freedom to be delinquent. The theory assumes that people's tendency to commit crime can be prevented by establishing strong social bonds. In the criminology literature, various empirical studies have found that social bonds can reduce deviant behaviors (Anderson et al. 1999; Jerkins 1997). In the IS security literature, organizational commitment is also suggested to prevent delinquent behavior (i.e. computer abuse, misuse of resources). Attachment, involvement, and commitment were suggested as organizational factors that would build social bonds (Lee 2002; Lee et al. 2003; Willison 2006). In addition to the crime prevention perspective, organization literature

proposed organizational commitment as an antecedent of employee trust and cooperation. For example, according to the social identity theory (Tajfel 1974), individuals' internalized sense of their membership in a particular group results in individuals' sensing the perspective of fellow group members and trusting and cooperating with them (Haslam et al. 2006). In this study, we define *organizational commitment* as an employee's attachment to his organization (Becker 1960; Meyer and Allen 1997) and propose that organizational commitment would positively affect an employee's attitude towards ISP compliance. Hence,

Hypothesis 6: *Organizational Commitment* positively affects an employee's attitude towards ISP compliance.

We also propose organizational commitment as a moderating variable. Similar to the ISP fairness arguments, we argue that employees are more likely to develop intrinsic motivations towards ISP compliance in the presence of high organizational commitment. If the organizational commitment does not exist, the employee would need external motivations to comply with the requirements. Accordingly, we argue that *organizational commitment* would influence the effectiveness of organization-based cost beliefs in developing positive attitude towards ISP compliance. If the employee is not committed to the organization, any kind of organizational costs of compliance or non-compliance would play a more important role. Based on these arguments, we hypothesize the following:

Hypothesis 7: *Organizational Commitment* moderates the relationship between the *CNC* and *attitude*, such that when *it* is low, higher *CNC* will have a higher positive influence on attitude, but when *it* is high, higher *CNC* will be less influential or have no direct impact on attitude.

Hypothesis 8: *Organizational Commitment* moderates the relationship between the *CC* and *attitude*, such that when *it* is low, higher *CC* will have a higher negative influence on attitude, but when *it* is high, higher *CC* will be less influential or have no direct impact on attitude.

3 RESEARCH METHODOLOGY

We used the survey method to test our model. We developed the initial survey instrument by identifying and creating appropriate measurements based on a comprehensive literature review. The initial survey instrument was then refined based on card-sorting exercises and exploratory data analysis from two small-scale pre-tests. Data was collected by administering the final survey instrument online. A professional market research company located in the United States provided a nationwide sample of their panel members. We asked the research company to contact participants who are employed by a diverse set of organizations. Those panel members were first asked questions regarding demographics. Next, they were asked exclusion questions so that the data will not include those who work in organizations without an explicitly written ISP and who are unaware of the requirements of the ISP. Those who met the exclusion criteria were not able to proceed with the survey. Thus, 258 of the participants were screened out from the survey at that point. Of all the remaining 670 responses, 175 were eliminated due to incompleteness, and 35 were eliminated due to data runs. Hence, sample of 460 usable questionnaires were included in the analysis, giving an effective response rate of 42%. 52% of the respondents were female, and 36% were in the 36-45 age range. The average length of computer usage was 17.6 years, and the average usage of the Internet was 12.2 years. Twenty-eight percent of the respondents reported working for information-intensive companies. In terms of the responsibilities of the respondents, as well as the annual sales revenue and size of the companies they were working for, the sample was quite evenly distributed. To test the moderating effects, we divided our sample into three based on different criteria for moderating factors and organization-based beliefs. We represent these three groups as high, medium, low in the following sections. We preferred three categories instead of two to better observe the trend in the data, understand the interactions, and differentiate between low and high groups. We believe that this approach is appropriate, particularly in large data sets. While selecting the division criteria, we aimed to achieve evenly distributed groups, so used standard deviations from the mean as a division criteria. All constructs of this study are represented with seven-scale survey responses. The detailed information about the division criteria and demographics of data can be found in Table 1. To test the

validity and reliability of the constructs we used at least three survey questions for each construct. After ensuring the validity and reliability of the measurement model, we took the average of the measures for each constructs and used them to test our hypotheses.

Constructs	High Group			Medium Group			Low Group		
	Criteria	N	Ave	Criteria	N	Ave	Criteria	N	Ave
CNC	>6	201	6.91	=>5	163	5.58	<5	117	3.24
CC	=>4	120	5.00	=>2	156	2.46	<2	184	1.10
ISP F.	>6	203	6.91	=>5	142	5.82	<5	115	3.58
O. Comm.	=>6	167	6.57	>4	169	5.10	=<4	124	2.96

Table 1: Information about Group Data & Descriptive Statistics

4 DATA ANALYSES AND RESULTS

The measurement model was tested using structural equation modeling. The component-based partial least squares (PLS) approach was used to evaluate the psychometric properties of measurement scales. The Smart-PLS software package (version 2.0.M3) (Ringle et al. 2005) was used for the assessment of measurement validity and reliability. The measurement quality of reflective constructs was assessed by examining the convergent validity, discriminant validity, individual item reliability and composite reliability of the measurement model (Barclay et al. 1995; Chin 1998; Gefen et al. 2000; Gefen and Straub 2005). We concluded that the measures of all constructs had adequate reliability and validity assessments, so all the measurement items of these constructs were kept for testing our hypotheses. Subsequently, for the regression analysis, we took the averages of the measures of each construct. We then used these values to test our hypotheses in the regression analyses.

4.1 Results, Discussion of Findings, and Implications

Our initial sample size contains 460 cases, with no missing values. The research hypotheses proposed were tested using general linear regression. SPSS (version 13) was used for the estimations. We first proposed our main model with two constructs—CNC and CC—affecting attitude. Then, we proposed three other models with the main effect of each moderating factors—ISP Fairness and Organizational Commitment—as well as their interactions with our main organization-based cost constructs. We applied the following step-by-step procedures in developing each linear regression model: 1) We checked for the assumptions of linear regression and ensured that all assumptions hold for the linear regression. To do so, we conducted diagnostic checks to see whether the linear regression fulfills the assumptions. The diagnostic checks include linearity, no multicollinearity, and influence analysis. 2) We resolved the problems of assumption violations if necessary (i.e. remove the outliers). 3) We ran linear regression for each model using the data set. 4) We analyzed the results and compared them to the results of other models.

Our main model, Model 1, is significant at F (2, 459) = 89.114, SE = .96, p=.000<.05. CNC and CC are both significant at p=.000<0.05 (t_1 = 10.31 and t_2= - 6.17) in predicting employees' attitude towards compliance. This result supports our hypotheses 1 and 2. Moreover, the statistical support for our main model implies that we can add additional predictors to improve the overall model to predict employee's attitude towards ISP compliance.

In model 2, we include the main effect of *ISP Fairness* and its interactions with CNC and CC to our main model. Model 2 is significant at F (5, 459) = 51.875, SE = .91, p=.000<.05. CNC, CC, ISP Fairness, and ISP Fairness-CNC interaction are all significant at p=.000<0.05 (t_1 = 6.96; t_2= - 4.14; t_3= 4.86; t_4= - 5.16) in predicting employees' attitude towards compliance. ISP Fairness-CC interaction is not significant. Hence, hypotheses 3 and 4 are supported. Figure 1 and 2 present the interactions of organization-based employee beliefs—CNC and CC—with ISP Fairness. The main positive effect of ISP Fairness on attitude is also evident in these figures. In Figure 1, it is shown that in the presence of high ISP Fairness, CNC is less influential or has no direct impact. However, when the ISP fairness is low, CNC will have a higher positive impact. We may conclude that ISP fairness and CNC act as

substitutes in affecting the employee's attitude. Even though we observe a similar trend in Figure 2 for CC and ISP fairness interaction, it is not found significant.

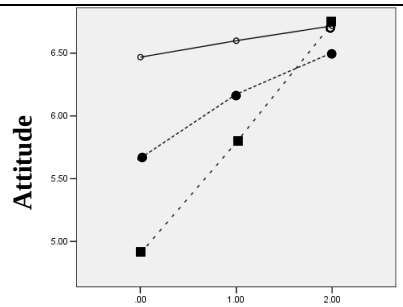

Figure 1: CNC & ISP Fairness Interaction

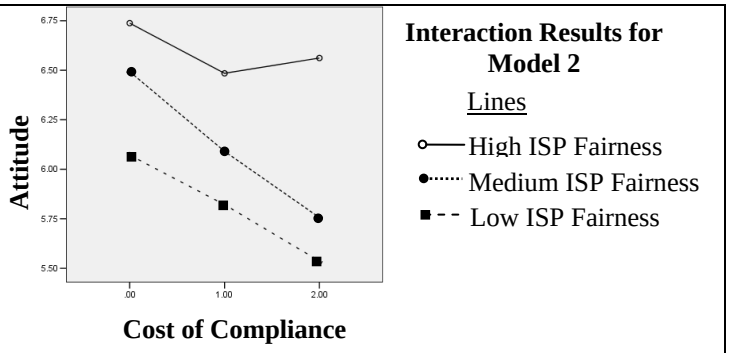

Figure 2: CC & ISP Fairness Interaction

In model 3, we include the main effect of *Organizational Commitment* and its interactions with CNC and CC to our main model. Model 3 is significant at F (5, 459) = 40.619, SE = .95, p=.000<.05. CNC (p=.000), CC (p=.000), Organizational Commitment (p=.005), Organizational Commitment-CNC (p=.026), Organizational Commitment-CC (p=.046) interactions are all significant at $p<0.05$ ($t_1 = 9.33$; $t_2 = -6.34$; $t_3 = 2.82$; $t_4 = -2.24$; $t_5 = 2.00$) in predicting employees' attitude towards compliance. Hence, we support hypotheses 6, 7, and 8. Figure 3 and 4 present the interactions of organization-based employee beliefs—CNC and CC—with organizational commitment. The main positive effect of Organizational Commitment is also evident in these figures. In Figure 3, it is shown that in the presence of high organizational commitment CNC is less influential than in the presence of low commitment. Similarly, In Figure 4, we see that when organizational commitment is high, CC is has a lower negative influence on attitude, whereas, when organizational commitment is low, CC has a higher negative impact on attitude. Hence, the interaction of both terms with commitment is supported. Similar to the conclusion of ISP fairness, it is concluded that organizational commitment and an employee's organizational cost perceptions act as substitutes in affecting the employee's attitude.

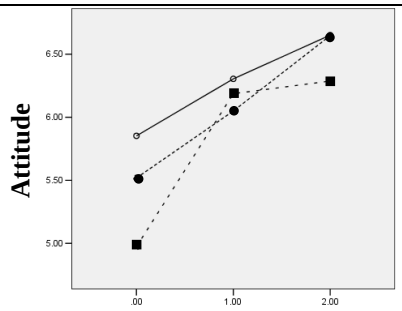

Figure 3: CNC & Org. Comm. Interaction

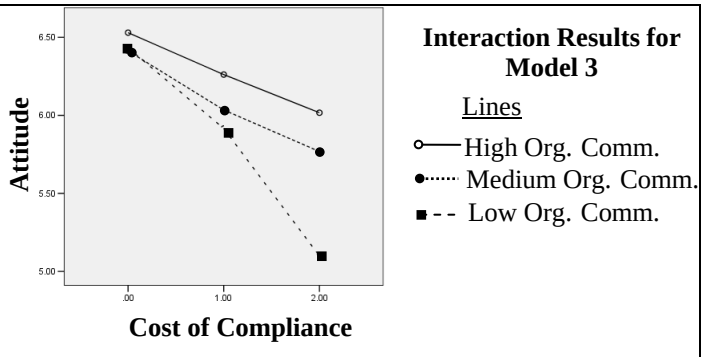

Figure 4: CC & Org Comm. Interaction

The summary of results and the model comparison are presented in Table 2. While all the proposed models were found significant, Model 2 had the highest explanatory power ($R^2 = 0.357$).

		Model 1			Model 2			Model 3		
Variable	***H***	***B***	***SE***	***Sig***	B	***SE***	***Sig***	***B***	***SE***	***Sig***
Intercept		5.82	.10	.00	5.67	.12	.00	5.73	.11	.00
CNC	**H1**	.42	.06	.00	.30	.06	.00	.38	.06	.00
CC	**H2**	-.25	.06	.00	-.17	.06	.00	-.25	.06	.00
ISP Fairness	**H3**				.23	.07	.00			
ISP Fairness X CNC	**H4**				-.20	.07	.00			
ISP Fairness X CC	H5				.04	.07	.34			
Commitment	**H6**							.11	.06	.01
Commitment X CNC	**H7**							-.09	.07	.03
Commitment X CC	**H8**							.08	.07	.05
Adjusted R^2 =		**0.277**			**0.357**			**0.301**		

Table 2: The Summary of Results and Comparison of Models

H: Hypotheses, ***B:*** Standardized Beta Coefficients, ***SE:*** Standard Error of the Estimate, ***Sig:*** Significance

Note: The highlighted hypotheses and the shadowed cells show that these variables are significant ($p<.05$) in their respective models.

5 CONCLUSION AND FUTURE RESEARCH DIRECTIONS

In this paper, we focused on the organizational costs associated with an employee's ISP compliance and non-compliance. We discussed two organizational factors— ISP Fairness and Organizational Commitment— as moderating factors which are posited to change the strength of the impact of organization-based beliefs on attitude. Our results show that organization-based employee beliefs significantly affect attitude, and as predicted, the strength of each belief-attitude relationship is affected by ISP fairness and organizational commitment. As organizations strive to get their employees to follow their information security rules and regulations, our study particularly sheds light on the importance of organization-based cost beliefs and two organizational factors in compliance efforts of organizations.

As the future directions of this study, the impact of an employee's organization-based *benefit* beliefs on his attitude towards ISP compliance can be investigated and compared to that of the proposed organization-based cost beliefs. Furthermore, the impact of organization-based beliefs can be compared to that of individual-based beliefs. An analysis of individual-based and organization-based beliefs in the presence of moderating factors such as commitment, age, gender etc. can be conducted. Future research can also trace the determinants of an employee's perceptions on ISP fairness, cost of ISP compliance, and cost of ISP non-compliance. This study does explain the determinants of these key constructs. It would be interesting to study the conditions under which employees perceive ISP requirements fair. For example, would employees perceive ISP requirement fair when they believe these requirements are highly costly but necessary and return value (e.g. high cost vs. high distributive justice)? Another important future research direction could be conducting a multilevel study to study how an employee's cost beliefs change depending on other employees' security related actions. For example, if an employee is convinced that her colleagues do not comply with the ISP requirements, she can think that the marginal cost the organization will incur if she personally does not comply will be pretty low, so her compliance intentions can decrease. On the other hand, if she believes to be the only one who will not comply, she can think that the risks of security breaches will only depend on her, and therefore the costs of her non-compliance to the organization will be high.

6 APPENDIX

Constructs, Definitions, Measurement Items, and Scales
Attitude is the degree to which the performance of the compliance behavior is positively valued (Fishbein and Ajzen 1975; Ajzen 1991) ***Measurement Items:*** To me, complying with the requirements of the ISP is _____ unnecessary……necessary unbeneficial……beneficial unimportant……important useless…….....useful ***Scale:*** 1. Extremely, 2. Quite, 3. Slightly, 4. Neither, 5. Slightly, 6. Quite, 7. Extremely
Organizational Cost of Compliance (CC) is the overall expected unfavorable consequences to the organization for the employee's compliance (Bulgurcu et al. 2010). ***Measurement Items:*** Complying with the requirements of the ISP is _____ for my organization. time consuming burdensome costly ***Scale:*** 1 = Not at All — 7 = Very Much
Organizational Cost of Non-Compliance (CNC) is the overall expected unfavorable consequences to the organization for the employee's non-compliance (Bulgurcu et al. 2010). ***Measurement Items:*** My noncompliance with the requirements of the ISP would _____. be harmful to my organization impact my organization negatively create disadvantages for my organization generate losses for my organization ***Scale:*** 1 = Not at All — 7 = Very Much
ISP Fairness is an employee's belief in the fairness of the requirements prescribed and dictated by the ISP of her organization. ***Measurement Items:*** I believe the requirements of the ISP that I am required to comply with are _____. unfair ..... fair unreasonable ..... reasonable unjust ..... just ***Scale:*** 1. Extremely, 2. Quite, 3. Slightly, 4. Neither, 5. Slightly, 6. Quite, 7. Extremely
Organizational Commitment is an employee's attachment to his organization (Becker 1960; Meyer and Allen 1997). ***Measurement Items:*** My organization has a great deal of personal meaning for me. I really feel as if my organization's problems are my own. . I feel emotionally attached to my organization. I feel a strong sense of belonging to my organization. ***Scale:*** 1 = Not at All — 7 = Very Much

Table 3: Constructs, Definitions, Measurement Items, and Measurement Scales

References

Ajzen, I. “The theory of planned behavior,” *Organizational Behavior and Human Decision Processes* (50:2), 1991, pp. 179-211.

Ambrose, M.L., Seabright, M.A., & Schminke, M. "Sabotage in the workplace: The role of organizational injustice," *Organizational Behavior and Human Decision Processes* (89), 2002, pp. 947-965.

Anderson, B.J., Holmes, M.D., & Ostresh, E. “Male and female delinquents' attachments and effects of attachments on severity of self-reported delinquency,” *Criminal Justice and Behavior*, (26:4), 1999, pp.435-452.

Aquino, K., Tripp, T.M., & Bies, R.J. “Getting even or moving on: Power, procedural justice, and types of offense as predictors of revenge, forgiveness, reconciliation, and avoidance in organizations,” *Journal of Applied Psychology* (91), 2006, pp. 653-668.

Barclay, D., Higgins, C., & Thompson, R. “The Partial Least Squares (PLS) Approach to Causal Modeling: Personal Computer Adoption and Use as an Illustration,” *Technology Studies* (2:2), 1995, pp. 285-309.

Baron, R.A. "Workplace aggression and violence," in: *The dark side of organizational behavior*, R.W. Griffin and A. O'Leary-Kelly (eds.), Jossey-Bass, San Francisco, CA, 2004, pp. 23-26.

Becker, H. S. Notes on the concept of commitment. *American Journal of Sociology*, 66, 1960, pp. 40-53.

Bies, R.J. “The predicament of injustice: The management of moral outrage, *Research in Organizational Behavior* (9), 1987, pp. 289-319.

Boss, S. R., & Kirsch, L. J. “The Last Line of Defense: Motivating Employees to Follow Corporate Security Guideliness,” in *International Conference on Information Systems*, Montreal, 2007, pp. 1-18.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. “Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness,” *MIS Quarterly* (34:3), 2010, pp. 523-548.

Chin, W.W. “Issues and Opinion on Structural Equation Modeling,” *MIS Quarterly (*22:1), 1998, pp. vii-xvi.

Fishbein, M., & Ajzen, I. *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research,* MA: Addison-Wesley, 1975.

Gefen, D., & Straub, D. “A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example,” *Communications of the Association for Information Systems* (16), 2005, pp. 91-109.

Gefen, D., Straub, D. W., & Boudreau, M. C. “Structural Equation Modeling And Regression: Guidelines For Research Practice,” *Communications of The AIS* (4), 2000, pp. 1-77.

Greenberg, J. “Employee theft as a reaction to underpayment inequity: The hidden cost of pay cuts”, *Journal of Applied Psychology* (75), 1990, pp. 561-568.

Haslam, S.A. & Reicher, S.“Stressing the group: Social identity and the unfolding dynamics of responses to stress,” *Journal of Applied Psychology* (91), 2006, pp. 1037-1052.

Hirschi, T. *Causes of Delinquency,* Berkeley, CA: University of California Press, 1969.

Jenkins, P.H. “School delinquency and the school social bond,” *Journal of Research in Crime and Delinquency* (34:3), 1997, pp. 337.

Lee, J., & Lee, Y. “A holistic model of computer abuse within organizations,” *Information management & computer security* (10:2/3), 2002, pp. 57-63.

Lee, S. M., Lee, S. G., & Yoo, S. “An integrative model of computer abuse based on social control and general deterrence theories,” *Information & Management* (41:6), 2003, pp. 707-718.

Meyer, J. P., & Allen, N. J. A three-component conceptualization of organizational commitment. *Human Resource Management Review*, (1), 1991,pp. 61-89.

Morrison, E.W., & Robinson, S. L. “When employees feel betrayed: A model of how psychological contract violation develops,” *Academy of Management Review* (22), 1997, pp. 226.

Pahnila, S., Siponen, M., & Mahmood, A. "Employees' Behavior towards IS Security Policy Compliance," in *Proceedings of the 40th Hawaii International Conference on System Sciences*, IEEE, 2007, pp. 156-166.

PricewaterhouseCoopers. "Employee behaviour key to improving information security, new survey finds," June 23, 2008 (http://www.ukmediacentre.pwc.com/Content/Detail.asp?ReleaseID=2672&NewsAreaID=2), 2008.

Ringle, C. M., Wende, S., & Will, A. SmartPLS. (2.0 (beta)). Hamburg, Germany, (http://www.smartpls.de), 2005.

Siponen, M., & Willison, R. "A critical assessment of IS security research between 1990-2004," *Proceedings of the 15th European Conference on Information Systems* (ECIS2007), 2007, pp. 1551-1559.

Stajkovic, A.D., & Luthans, F. "A meta-analysis of the effects of organizational behaviour modification on task performance, 1975-95," *The Academy of Management Journal*, (40: 5), 1997, pp. 1122-1149.

Straub, D. W., & Nance, W. D. "Discovering and disciplining computer abuse in organizations: a field study," *MIS Quarterly* (14:1), 1990, pp. 45-60.

Tajfel, H. "Social identity and intergroup behavior," *Social Science Information*, (13), 1974, pp. 65-93.

Tyler, T.R., & Blader, S.L. "Can Businesses Effectively Regulate Employee Conduct? The Antecedents of Rule Following in Work Settings?," *Academy of Management Journal*, (48), 2005, pp. 1143-1158.

Tomlinson, E.C., & Greenberg, J. "Discouraging Employee Theft by Managing Social Norms and Promoting Organizational Justice," in: *Managing Organizational Deviance*, R.E. Kidwell and C.L. Martin (Ed.), Sage Publications, Thousand Oaks, CA, 2005.

Whitman, M. E., Townsend, A. M., & Aalberts, R. J. "Information systems security and the need for policy," in *Information Security Management - Global Challenges in the Next Millennium*, G. Dhillon, London: Idea Group, 2001, pp. 9-18.

Willison, R. "Understanding the Perpetration of Employee Computer Crime in the Organisational Context," *Information and organization* (16:4), 2006, pp. 304-324.