Information Security Policies Compliance: The Role of Organizational Punishment

Research-in-Progress

Mohammad I. Merhi
Department of Computer Information Systems & Quantitative Methods
College of Business Administration
University of Texas Pan American
1201 W. University Drive
Edinburg, TX 78539
Email: mmerhi@utpa.edu

Punit Ahluwalia
Department of Computer Information Systems & Quantitative Methods
College of Business Administration
University of Texas Pan American
1201 W. University Drive
Edinburg, TX 78539
Email: punit@utpa.edu

ABSTRACT

It has been argued that organizational punishment serves as a deterrent to unwanted employee behavior but there is no clear consensus on the influence of punitive actions on employees' behavior to comply with information security policies. This study proposes a model that explains the influence of organizational punishment on employees' cognitive beliefs and their intention to comply with information security policies. We argue that likelihood of punishment impacts employees' cognitive beliefs that in turn affect their information security compliance behavior. This study uses the theory of planned behavior as a support for its propositions and contributes to the body of knowledge in the IS security stream by addressing a significant gap in the current literature. This is a work in progress and we plan to present results of the empirical study at the conference.

Keywords

Information security policies, organizational punishment, security policies compliance, theory of planned behavior.

INTRODUCTION

Information assurance is defined as the "*reliability, accuracy, security and availability of a company's information assets. This will typically define how these assets -data and/or information both within the tangible and the virtual bounds of the organization- should be secured to provide maximum benefit* (pp. 98)" (Ezingeard, McFadzean, and Birchall, 2007). In order to achieve this goal, organizations develop and implement Information Systems Security (ISS) policies. This is because technology alone cannot solve all security issues within an organization. Information Systems (IS) is now used by most businesses in order to increase work process efficiencies and to differentiate themselves from competition. Employees inside the organizations are one of the core assets that use and interact with IS systems. Undesirable actions by employees, intentionally or otherwise, can cause wide ranging problems for the firms. These problems may range from law suits for non protecting private information, revealing proprietary information to competitors etc. Best of technologies may not be able to protect such unwanted behavior by actual users of IS systems. Thus, most organizations now are increasingly aware of the implications of compromising there systems and therefore frame effective ISS policies and communicate these to the employees (Baskerville and Siponen, 2002; Dlamini, Eloff, and Eloff, 2009). However, several studies point out that ISS compliance by employees remains a significant challenge for IS managers (Bulgurcu, Cavusoglu, and Benbasat, 2010; D'Arcy and Hovav, 2009; Stanton, Stam, Mastrangelo, and Jolton, 2005; Straub and Welke, 1998).

Several recent studies show that incidents and violations of ISS continue to increase over the years and world-wide organizations are experiencing a wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches (Ernst and Young, 2011; Ponemon Institute, 2009; PWC, 2012a; Richardson, 2010).These studies also mention that employees' behaviors are the main cause for these violations. We present some examples of these studies as evidence. According to the survey administered by "Info Security Europe" and "Reed Exhibitions," nearly 82 percent of large organizations which participated in their study experienced breaches caused by their employees (PWC, 2012b). Similarly Ponemon Institute (2012) found that 78 percent of the organizations which participated in their study experienced a data breach as a result of negligent or malicious employees or other insiders. Misuse of the Internet, e-mail, and unauthorized

access to others' user accounts (using someone else's ID) were found to be the most common unwanted behavior. D'Arcy et al., (2009) and Dinev and Hu (2007) have examined employees' behaviors towards ISS compliance. Warkentin et al. (2011) indicated that there are still gaps in the literature. Similarly, Hu, Dinev, Hart, and Cooke (2012) argue that despite the contributions of the current behavioral studies on ISS compliance, a clear vision on how to effectively manage the behaviors of the employees in the organizations is missing in the extant literature. We argue that the deterrent effect of punishment, one of the crucial constructs in organizational management and individual behavior literature, on information security compliance has not been thoroughly examined. Few studies that investigated the effects of punishment on employees' ISS compliance behavior generated mixed findings (e.g. Bulgurcu et al., 2010, D'Arcy et al., 2009, Herath and Rao, 2009, Pahnila et al., 2007). We review these studies in the next section.

Our study addresses this gap in the literature by seeking to answer the question: ***what is the role of punishment in shaping employees' cognitive beliefs towards ISS policies and their intention to comply with ISS policies?*** We propose that organizational punishment has an effect on employees' cognitive factors which in turn affects employees' ISS compliance behavior. We propose an integrated model that integrates the organizational punishment construct and the theory of planned behavior.

We believe that this research will make significant contributions to the scholarly and practitioner communities namely, IS designers, ISS specialists, and managers intending to enhance ISS compliance in their organizations. By finding out how organizational punishment affect ISS compliance, we have the potential to offer organizations a practical approach for designing best practices at workplaces that motivate employees to comply with ISS. In doing so, we (1) fill a significant gap in the ISS research and practice, specifically by demonstrating how punishment can alter employees' cognitive beliefs and ISS compliance; (2) extend the theory of planned behavior.

The remainder of this paper is organized as follows. The first section provides a theoretical background, followed by the research model and a set of research hypotheses. Then, we discuss the proposed methodology that will be used to empirically test the proposed hypotheses.

THEORETICAL BACKGROUND AND LITERATURE REVIEW

Punishing employees is used in organizations as a deterrent to reduce undesirable behavior such as non-compliance with policies and rules (Ball, Trevino, and Sims, 1994). As a management tool within organizations, punishment is defined as "*the application of a negative consequence to, or the withdrawal of a positive consequence from, an employee*" (Trevino, 1992). When employees' interests and goals are not in harmony with that of organization's (Liang and Xue, 2010), managers need to control employees' behavior to ensure that the policies and rules are applied (Eisenhardt, 1989). It is often argued that likelihood of punishment influence employees' behaviors towards unwanted actions; however, the findings of many studies that examined this issue are mixed. Ball, Trevino, and Sims (1994) noted that research on organizational punishment has often led to contradictory conclusions and uncertain results. Some scholars argue that employees in general tend to repeat actions that do not produce negative outcomes and prefer to avoid those actions that lead to negative actions; thus reducing likelihood of punishment. The rationale behind this argument is that punishment creates an anxiety in minds of employees which forces them to change their behaviors towards organizational policies. Arvey and Ivancevich (1980) state: "*punishment may be a very effective procedure in accomplishing behavior change* (pp. 131)." Johnston (1972) argues that no other procedure "*provides an effect which is as immediate, enduring, or generally effective as that produced by the proper use of punishment procedures* (pp. 1051)." In line with these arguments, researchers examined organizational punishment as an important concept in order to increase employees' work motivation, performance, job satisfaction, attitudes, perceptions, and behaviors (Arvey, Davis, and Nelson, 1984; Podsakoff, Bommer, Podsakoff, and MacKenzie, 2006). Contrary to the foregoing arguments, Sims (1980) mention that "*punitive behavior is not likely to be effective as an overall pattern of managerial behavior for influencing employees* (pp. 136)" because organizational punishment often tends to come after (result) an employee behavior and not before (cause).

According to General Deterrence Theory, when the possibility of punishment is high and the sanction is severe, potential violators will be deterred from committing unauthorized acts, especially when their motives are weak (Blumstein, 1978). In the ISS context, by using the General Deterrence Theory (GDT) (Blumstein, 1978), researchers have shown that punishment can be used as a deterrent to decrease ISS misuse, thereby increasing ISS compliance (D'Arcy, Hovav, and Galletta, 2009; Herath and Rao, 2009a, 2009b; Hoffer and Straub, 1989). Hoffer and Straub (1989) argue that the prospect of punishment will deter employees' abuse of IT systems if they perceive their employers to be serious about computer abuse. Hoffer and Straub (1989) found that deterrent measures, preventive measures, and deterrent severity act as inhibitors to ISS breaches. This study is descriptive in nature and the relationship between "organizational punishment" and "employee behavior towards ISS" was not empirically tested. Hoffer and Straub (1989) found that certain actions such as "establishing data and

system security organization to monitor systems use and make employees know that the systems are in place; communicating clearly that penalty will be imposed on abusers; and communicating to all personnel what the organization consider improper behavior" reduced computer abuse.

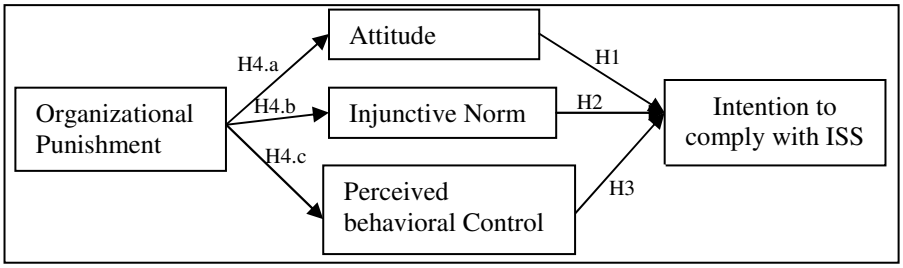
Herath and Rao (2009a, 2009b), D'Arcy et al. (2009), Siponen, Pahnila, and Mahmood (2010) and Vance, Siponen, and Pahnila (2012) examined the direct relationship of likelihood of punishment on ISS compliance. Organizational punishment is measured using two factors: perceived certainty of sanctions which refers to the probability of being punished; and perceived severity which is the degree to punishment. Mixed results were found in these studies but in general, they found that non-adherence to ISS security policies can be deterred by imposing punishment. If the employees perceive the punishment to be severe, and the possibility of getting caught to be high, then the likelihood of their undesired behaviors will reduce.

Using survey data collected from 312 participants from 77 organizations, Herath and Rao (2009a, 2009b) found that the higher the severity of penalty, the lower the ISS compliance intention will be. Results of both these studies contradict the findings of D'Arcy et al. (2009); Siponen and Pahnila (2012); and Siponen et al., (2010) who found the higher the severity of penalty the higher the compliance with ISS policies. This contradiction in the result calls for studies to examine the influence of organizational punishment on ISS policies compliance. Herath and Rao (2009a) argue that the role of the penalties in shaping ISS compliance is unclear and required further research. Venkatesh and Davis (2000) argue that punishment may have an impact on employees' attitudes and beliefs especially injunctive norms because "the important other" is usually a person who has influence and thus he/she would reward or penalize the employee. Yet no research has examined the relationship between punishment and injunctive norm leading to a gap in the literature. For these reasons, in this research we aim to investigate the influence of organizational punishment on employees' cognitive beliefs namely attitude, injunctive norm, and perceived behavioral control which are mediators between punishment and ISS compliance.

RESEARCH MODEL AND HYPOTHESES

Though research on information security policy compliance has expanded in the last decade, gaps in the literature still exist and there is still a room for new studies that help both practitioners and researchers to understand the factors leading to information security compliance (Warkentin et al., 2011). This study aims to contribute to the current literature by examining the effect of organizational punishment on employees' cognitive beliefs. Figure 1 illustrates the proposed model. It asserts that organizational punishment affects intention to information security compliance indirectly through injunctive norm, attitude, and perceived behavioral control. Below is a brief description of the hypotheses.

Figure 1: Proposed Model



In literature, many models and theories exist to explain the individuals' behavior. In this study, we draw on and extend the Theory of Planned Behavior, which is a well-established theoretical model for individual behavior. Although predicting individuals' actual behavior is the goal of the theory, measuring the actual behavior has not been an easy task for researchers, especially those behaviors studied in organizational settings (Hu, et al., 2012). IS researchers (Bulgurcu et al., 2010; Gefen, Karahanna, and Straub, 2003; Herath and Rao, 2009a, 2009b; Pavlou and Fygenson, 2006; Siponen and Vance, 2010) have often chosen to investigate intention to behave as the dependent variable instead of the actual behavior because of the strong correlation between intentions and actual behavior (Ajzen, 2005). Similar to these studies and because it is not easy to measure the actual ISS compliance, we use employees' intention to comply with ISS as the main factor. Intention to comply is assumed to capture the motivational factors that influence an employee's behavior.

In the Theory of Planned Behavior framework, three factors are considered to shape the behavior: attitude towards the behavior, subjective norm, and perceived behavioral control (PBC). Attitude refers to a person's judgment as to whether it is good or bad to perform a behavior of interest. Subjective norm (injunctive norm in this study) is the person's perceptions of

whether the behavior is accepted by those people who are important to him or her such as peers, supervisors. Perceived Behavioral Control is the perceived ease or difficulty of performing a behavior and personal sense of having the skills and control over performing it (Taylor and Todd, 1995). Numerous studies from many disciplines have found strong support for Theory of Planned Behavior's propositions (Pavlou and Fygenson, 2006). That is an individual's attitude, subjective norm, and Perceived Behavioral Control significantly impact the individual's behavioral intention. Most recently, Hu et al. (2012) found that positive attitude, injunctive norm, and Perceived Behavioral Control have significant impact on employee intention to comply with ISS policies. Therefore, by adapting the same logic to the context of this study, we postulate that:

H1: *Positive attitude towards ISS will be positively associated with employees' intention to comply with ISS.*
H2: *Injunctive norm will be positively associated with employees' intention with ISS.*
H3: *Perceived behavioral control will be positively associated with employees' intention to comply with ISS.*

To control its employees from committing undesirable behaviors, management in organizations tends to use punishment as a kind of threat. Punishment can take many shapes from verbal warning to terminations or delaying promotions and pay raise. The main purpose of punishment is to stop or decrease the frequency of undesirable employees' behavior or increase employees' compliance with the organization's policies and rules (Ball, et al., 1994). Typically, organizations and employees have different self-interests and distinct goals (Liang, Xue, and Wu, 2012). In order to control this conflict and ensure cooperation, organizations must control their employees' behavior to ensure the teamwork (Eisenhardt, 1989). In organizational settings, various studies have suggested that punishment can successfully control the employees' behavior and increase their performance (Arvey, et al., 1984; O'Reillys and Puffer, 1989; Podsakoff, et al., 2006).

Regulatory focus theory (Higgins, 1997) posits that people are motivated to approach pleasure and avoid pain. Liang et al. (2012) assume that to regulate the employees' behavior, organizations can manipulate the incentives to ensure that pleasure is approached and pain is avoided if their employees comply with the organization policies. Similarly, the deterrence theory suggests that perceived severity of the punishment diminishes the likelihood of committing misbehavior. When employees feel the seriousness and the consequences of the punishment, they will most likely change their attitude toward ISS compliance because the only way to avoid the punishment is the change. Also, punishment gives employees an indication that it is a must to behave in a certain way. This certainly changes the employees' opinion on their supervisors' expectation. They will know that their supervisors are expecting them to behave in the desired behavior. Consequently, we propose:

H4.a: *Organizational punishment will be positively associated with positive attitude towards IS security.*
H4.b: *Organizational punishment will be positively associated with injunctive norms.*
H4.c: *Organizational punishment will be positively associated with perceived behavioral control.*

PROPOSED METHODOLOGY

Research Method and Measures

In order to assess and investigate the proposed model, survey methodology is going to be utilized. The goal is to examine various factors that directly or indirectly affect employees' behavior towards ISS compliance. All the constructs included in the research model tap into experiences or perceptions of working professionals interacting with ISS. Therefore, users of IT systems (employees) who interact with ISS policies are the most appropriate data source for this research. A pilot test of measures will be conducted in order to make sure that the wording of items is clear and the items measure the concept that we intend to study. Administrative staff and faculty at a public university in the Southern part of the United States are going to be the target sample for the pilot study.

The instrument used for this study is based on previously validated measures. Measures for ISS compliance intention are adapted from Vance et al. (2012) and Siponen et al. (2010). The measures tap into employees' intention to comply with ISS policies using five-item Likert scales. Perceived behavioral control scales tap into employees' beliefs in their abilities, resources, and control they have to take an action. Scale for perceived behavioral control are five Likert scale from Anderson and Agarwal (2010); Herath and Rao (2009a); LaRose, Rifon, and Enbody (2008); Workman, Bommer, and Straub (2008).Injunctive norm scales extract the employees' expectations of whether ISS compliance is accepted and encouraged by people who are important to them in the organization. Injunctive norms measures are a five Likert scale adapted from Anderson and Agarwal (2010); Bulgurcu et al., (2010); Herath and Rao, (2009a). Organization punishment scales extract employees' perception of the degree of the punishment and the probability of being punished if they do not follow the rules. Organization punishment measures are five Likert scale adopted from Herath and Rao (2009a); Peace et al. (2003).

Proposed Analysis Methods

The data collected from the survey instrument are subjected to various statistical tests. The first analysis tests the data for outliers and normality. After this, construct validity, convergent validity, and discriminant validity will be checked. Construct validity is the extent to which a set of measured variables represent the theoretical latent construct they are designed to measure (Hair et al., 2010). A construct shows high validity when all items measuring that construct load on one factor. In order to check for construct validity, confirmatory factor analysis (CFA) will be used. Construct validity is conducted by assessing convergent validity and discriminant validity.

Convergent validity shows us that many variables were used to form the construct, while discriminant validity shows us that each construct correlate freely with its items. Convergent validity can be assessed using two measures: composite reliability and Average Variance Extracted (AVE). Composite reliabilities tests ensure that the variables in each construct are internally consistent. They are similar to Cronbach's alphas and thus there values should exceed 0.70 (Hair et al., 2010). The AVE estimates should exceed 0.50 (Hair et al., 2010). Discriminant validity can be assessed by comparing the correlation between pair constructs and the AVE of each construct. According to Anderson and Gerbing (1988), the squared correlation between a pair of latent variables (constructs) should be less than the AVE estimate of each variable. Therefore, each AVE value should be greater than the correlations in its row and column.

In addition to convergent and discriminant validity, the model fit should be checked as well. In model fit, usually researchers look at the chi-square, NFI, CFI, TLI, GFI, AGFI, and RMSEA. The chi-square should not be significant that means the P-value should be greater than 0.05 and its value should be small enough. Also, the other model fits indices such as NFI, CFI, TLI, GFI, and AGFI should be higher than 0.9 in order to get a good model fit. Finally the RMSEA should be less than 0.08. After confirming the validity of the instrument, Structural Equation Modeling (SEM) will be used to assess and investigate the hypothesized causal paths among the constructs by performing a simultaneous test. This helps to determine if the presented conceptual model had provided an acceptable fit to the empirical data gathered or not.

CONCLUSION

This research-in-progress is an effort to identify whether organizational punishment affects ISS compliance through employees' cognitive beliefs (attitude, injunctive norm, and perceived behavioral control). For information security researchers, this study makes an important contribution in conceptualizing and measuring the mediator role of employees' beliefs if exist between punishment and ISS compliance. To our best knowledge, this study for the first time proposes to examine the influence of organizational punishment on employees' beliefs. Literature has always investigated the influence of organizational punishment on employee satisfaction and performance (Williams, 1998). Thus, from the standpoint of information security, this study is a crucial contribution to theory and practice.

REFERENCES

1. Ajzen, I. (2005) Attitudes, personality, and behavior: McGraw-Hill International.
2. Anderson, J.C., and Gerbing, D.W. (1988) Structural Modeling in Practice: A Review and Recommended Two-Step Approach, *Psychological Bulletin*, 103, 3, 411-423.
3. Anderson, C. and Agarwal, R. (2010) Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions, *MIS Quarterly*, 34, 3, 613-643.
4. Arvey, R. D., and Ivancevich, J.M. (1980) Punishment in organizations: A review, propositions, and research suggestions, *Academy of Management Review*, 5, 1, 123-132.
5. Arvey, R. D., Davis, G. A., and Nelson, S. M. (1984) Use of discipline in an organization: A field study, *Journal of Applied Psychology*, 69, 3, 448-460.
6. Ball, G.A., Trevino, L.K., and Sims, Jr, H.P. (1994) Just and unjust punishment: Influences on subordinate performance and citizenship, *Academy of Management Journal*, 37, 1, 299-322.
7. Baskerville, R., and Siponen, M. (2002) An information security meta-policy for emergent organizations, *Logistics Information Management*, 15, 5-6, 337-346.
8. Blumstein, A. (1978) Introduction, A. Blumstein, J. Cohen, D. Nagin, Editors, Deterrence and incapacitation: estimating the effects of criminal sanctions on crime rates: National Academy of Sciences, Washington, DC.
9. Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010) Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness, *MIS Quarterly*, 34, 3, 523-548.

10. D'Arcy, J., and Hovav, A. (2009) Does one size fit all? Examining the differential effects of IS security countermeasures, *Journal of business ethics*, 89, 59-71.
11. D'Arcy, J., Hovav, A., and Galletta, D. (2009) User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach, *Information Systems Research*, 20, 1, 79-98.
12. Dinev, T., and Hu, Q. (2007) The centrality of awareness in the formation of user behavioral intention toward protective information technologies, *Journal of the Association for Information Systems*, 8, 7, 386-408.
13. Dlamini, M. T., Eloff, J. H. P., and Eloff, M. M. (2009) Information security: The moving target, *Computers & Security*, 28, 3, 189-198.
14. Eisenhardt, K. M. (1989) Agency theory: An assessment and review, *Academy of Management Review*, 14, 1, 57-74.
15. Ernst and Young, (2011) Into the cloud, out of the fog, available at http://www.ey.com/Publication/vwLUAssets/Into_the_cloud_out_of_the_fog-2011_GISS/$FILE/Into_the_cloud_out_of_the_fog-2011%20GISS.pdf
16. Gefen, D., Karahanna, E., and Straub, D. W. (2003) Trust and TAM in online shopping: An integrated model, *MIS Quarterly*, 27, 1, 51-90.
17. Hair, J. F., Jr., Black, W.C., Babin, B.J. and Anderson, R.E. (2010) Multivariate Data Analysis A Global Perspective (7th ed.), Pearson.
18. Herath, T., and Rao, H. R. (2009a) Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness, *Decision Support Systems*, 47, 2, 154-165.
19. Herath, T., and Rao, H. R. (2009b) Protection motivation and deterrence: a framework for security policy compliance in organizations, *European Journal of Information Systems*, 18, 2, 106-125.
20. Higgins, E. T. (1997) Beyond pleasure and pain, *American psychologist*, 52, 12, 1280-1300.
21. Hoffer, J.A. , and Straub, D. W. (1989) The 9 to 5 underground: are you policing computer crimes? *Sloan Management Review*, 30, 4, 35-43.
22. Hu, Q., Dinev, T., Hart, P., and Cooke, D. (2012) Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture, *Decision Sciences*, 43, 4, 615-659.
23. LaRose, R., Rifon, N. J., and Enbody, R. (2008) Promoting personal responsibility for internet safety, *Communications of the ACM*, 51, 3, 71-76.
24. Liang, H., and Xue, Y. (2010) Understanding security behaviors in personal computer usage: a threat avoidance perspective, *Journal of the Association for Information Systems*, 11, 7, 394-413.
25. Liang, H., Xue, Y., and Wu, L. (2012) Ensuring Employees' IT Compliance: Carrot or Stick? *Information Systems Research*, 1-16.
26. O'Reillys, C. A., and Puffer, S. M. (1989) The impact of rewards and punishments in a social context: A laboratory and field experiment, *Journal of Occupational Psychology*, 62, 1, 41-53.
27. Pahnila, S., Siponen, M., and Mahmood, A. (2007) Employees' behavior towards IS security policy compliance, Paper presented at the System Sciences, 2007, HICSS 2007. *40th Annual Hawaii International Conference on System Sciences*.
28. Pavlou, P. A., and Fygenson, M. (2006) Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior, *MIS Quarterly*, 30, 1, 115-143.
29. Peace, A. G., Galletta, D. F., and Thong, J. Y. (2003) Software piracy in the workplace: A model and empirical test, *Journal of Management Information Systems*, 20, 1, 153-178.
30. Podsakoff, P. M., Bommer, W. H., Podsakoff, N. P., and MacKenzie, S. B. (2006) Relationships between leader reward and punishment behavior and subordinate attitudes, perceptions, and behaviors: A meta-analytic review of existing and new research, *Organizational Behavior and Human Decision Processes*, 99, 2, 113-142.
31. PWC. (2012) Global State of Information Security Survey 2013, Changing the game Retail and Consumer Insights.
32. Richardson, R. (2010) 2010Csi/FbiComputerCrimeandSecuritySurvey, San Francisco: Computer Security Institute.
33. Sims, H. P. (1980) Further thoughts on punishment in organizations, *Academy of Management Review*, 5, 1, 133-138
34. Siponen, M., and Vance, A. (2010) Neutralization: new insights into the problem of employee information systems security policy violations, *MIS Quarterly*, 34, 3, 487-502.

35. Siponen, M., Pahnila, S., and Mahmood, M.A. (2010) Compliance with information security policies: An empirical investigation*, Computer*, 43, 2, 64-71.
36. Stanton, J. M., Stam, K. R., Mastrangelo, P., and Jolton, J. (2005) Analysis of end user security behaviors, *Computers & Security*, 24, 2, 124-133.
37. Straub, D. W., and Welke, R. J. (1998) Coping with systems risk: security planning models for management decision making, *MIS Quarterly*, 22, 4, 441-470.
38. Taylor, S., and Todd, P. A. (1995) Understanding information technology usage: A test of competing models, *Information Systems Research*, 6, 2, 144-176.
39. Trevino, L. K. (1992) The social effects of punishment in organizations: A justice perspective, *Academy of Management Review*, 17, 4, 647-676.
40. Vance, A., Siponen, M., and Pahnila, S. (2012) Motivating IS security compliance: Insights from Habit and Protection Motivation Theory, *Information & Management*, 49, 3-4, 190-198.
41. Venkatesh, V., and Davis, F. D. (2000) A theoretical extension of the technology acceptance model: Four longitudinal field studies, *Management science*, 46, 2, 186-204.
42. Warkentin, M., Carter, L., and McBride, M. E. (2011) Exploring the Role of Individual Employee Characteristics and Personality on Employee Compliance with Cybersecurity Policies, *The 2011 Dewald Roode Workshop on Information Systems Security Research*, IFIP WG8.11/WG11.13. Available online at:http://ifip.byu.edu/2011/Warkentin%20et%20al.%20Employee%20Characteristics.pdf.
43. Williams, S. (1998) A meta-Analysis of the relationship between organizational punishment and employee performance/satisfaction, *Research and Practice in Human Resource Management*, 6, 1, 51-64.
44. Workman, M., Bommer, W. H., and Straub, D. (2008) Security lapses and the omission of information security measures: A threat control model and empirical test, *Computers in Human Behavior*, 24, 6, 2799-2816.