ROLES OF INFORMATION SECURITY AWARENESS AND PERCEIVED FAIRNESS IN INFORMATION SECURITY POLICY COMPLIANCE

Burcu Bulgurcu, Management Information Systems
Sauder School of Business, University of British Columbia, CA
burcu.bulgurcu@sauder.ubc.ca

Hasan Cavusoglu, Management Information Systems
Sauder School of Business, University of British Columbia, CA
hasan.cavusoglu@sauder.ubc.ca

Izak Benbasat, Management Information Systems
Sauder School of Business, University of British Columbia, CA izak.benbasat@sauder.ubc.ca

Abstract

Drawing on the Theory of Planned Behavior (TPB), this research investigates two factors that drive an employee to comply with requirements of the information security policy (ISP) of her organization with regards to protecting information and technology resources: an employee's information security awareness (ISA) *and her perceived* fairness of the requirements of the ISP. *Our results, which is based on the PLS analysis of data collected from 464 participants, show that ISA and perceived fairness positively affect attitude, and in turn attitude positively affects intention to comply. ISA also has an indirect impact on attitude since it positively influences perceived fairness. As organizations strive to get their employees to follow their information security rules and regulations, our study sheds light on the role of an employee's ISA and procedural fairness with regards to security rules and regulations in the workplace.*

Keywords: Information Security Management, Information Security Awareness, Information Security Policy, Behavioral Issues of Information Security, Compliance, Theory of Planned Behaviour

1 INTRODUCTION

Information security is one of the top priorities of managers in many organizations (Brancheau, Janz and Wetherbe, 1996; Ransbotham and Mitra, 2008) as risks related to information security may result in consequences ranging from monetary damage to loss of credibility (Cavusoglu, Cavusoglu and Raghunathan, 2004). While technology-based solutions are important to ensure information security (Straub, 1990), they are not sufficient to deal with ever changing security threats (Dhillon and Backhouse, 2001; Siponen, 2005). As insiders pose an increasing challenge to an organization since ignorance, mistakes, and deliberate acts of employees can jeopardize the ultimate goal of establishing information security in the organization (Lee and Lee, 2002; SANS Institute, 2007), the literature recognizes that socio-organizational solutions, along with technology-based ones, can effectively curb the risks born by the insiders.

The extant literature, often based on the general deterrence theory, suggests deterrent and preventive strategies, such as providing disincentives and imposing sanctions, to reduce insiders' misuse and abuse of IS resources (Lee and Lee, 2002; Straub and Nance, 1990; Willison 2006). Unlike studies focusing on the role of negative reinforcement, a few recent studies argue for the role of positive reinforcements, such as rewards for employees' compliance with the security requirements, to deal with the insiders' threat (Boss and Kirsch, 2007; Pahnila, Siponen and Mahmood, 2007).

While existing studies mostly highlight the importance of negative reinforcing factors in shaping employees' attitude toward compliance, we believe that motivational factors regarding the act of compliance are as important as deterrent or preventive factors in effective information security management. Hence, in this study, we focus on two of the motivational factors – *Information Security Awareness* and *Perceived Fairness of the ISP* – and empirically study their impacts on an employee's attitude and in turn her intention to comply with her organization's ISP. Despite the importance of information security awareness, there is a paucity of empirical studies that analyze the impact of information security awareness on information security. Siponen (2000), who conceptually analyzed ISA, suggested methods to enhance awareness based on several theoretical perspectives. A few conceptual studies (Hentea, 2005; Thomson and Solms, 1998) highlighted the importance of ISA education and training. Still, to the best of our knowledge, the direct and indirect roles of information security awareness have not been studied. Furthermore, to the best of our knowledge, the direct and indirect roles of procedural fairness with regards to security rules and regulations have not been studied in the extant literature. The lack procedural fairness in the workplace may result in arousal of employees' negative emotions toward security compliance, which in turn may lead to their intentional abuse of resources or ignorance of security requirements. Hence, we believe that studying procedural fairness in the context of information security may lead to important results. In consequence, we address two specific research questions in this research:

i. What are the direct and indirect roles of an employee's information security awareness in influencing her attitude toward compliance and in turn intention to comply?
ii. What is the role of an employee's perceived fairness of the requirements of the ISP in influencing her attitude toward compliance and in turn intention to comply?

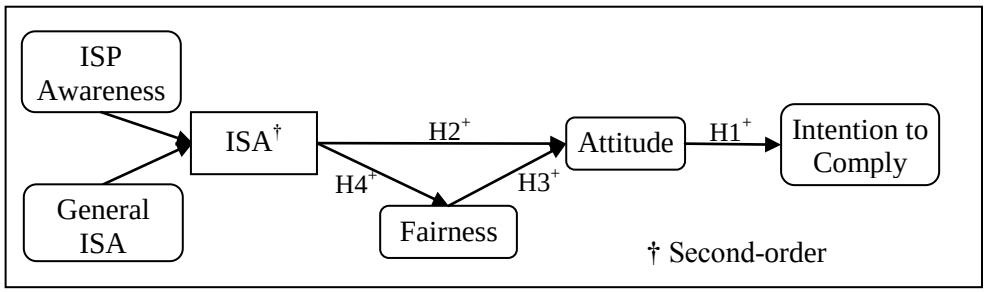

Figure 1. A Proposed Model of the ISP Compliance

Our research framework is based on the Theory of Planned Behavior (TPB) (Fishbein and Ajzen, 1975; Ajzen, 1991). The TPB was developed to explain and predict human behavior and it suggests that intentions to perform a behavior can be predicted with high accuracy from attitudes toward the behavior; and these intentions together with perceptions of behavioral control, account for considerable variance in actual behavior (Ajzen, 1991). Building on the TPB, we expand our understanding of how an employee's attitude toward compliance with the ISP is influenced and formed by her ISA and her perception about the fairness of the requirements dictated by the ISP. With this research model, we also investigate the effect of ISA on an employee's perceived fairness of the ISP.

2.1 Constructs adopted from the Theory of Planned Behaviour

We adopted two important constructs from the TPB, which are attitude toward the behavior and intention to perform the behavior (Fishbein and Ajzen, 1975; Ajzen, 1991). In our context of ISP compliance, we referred these constructs as an employee's attitude toward compliance with the ISP and an employee's intention to comply with the ISP. Attitude toward compliance with the ISP is defined as the degree to which the performance of the compliance behavior is positively valued.

Intention to comply with the ISP is defined as an employee's intention to protect information and technology resources of her organization from potential security breaches (Fishbein and Ajzen, 1975; Ajzen, 1991). In line with the existing literature of the TPB, we posit that an employee's intention to comply with the requirements of her organization's ISP is associated with her attitude toward compliance. Hence, we propose the following:

> Hypothesis 1. *An employee's attitude toward complying with the requirements of the ISP positively affects her intention to comply.*

2.2 Information Security Awareness

Employees' information security awareness is an important part of an effective information security management program (Cavusoglu, Cavusoglu, Son and Benbasat, 2008). In this study, ISA is defined as an employee's general knowledge about information security and his cognizance of the ISP of his organization. *General Information Security Awareness* and *ISP Awareness* are the key dimensions of ISA. *General Information Security Awareness* is defined as an employee's overall knowledge and understanding of potential information-security-related issues and their ramifications, and what needs to be done in order to deal with security-related issues. Beyond general ISA, organizations have specific expectations of their employees that are reflected in the ISP. *ISP Awareness* is defined as an employee's knowledge and understanding of the requirements prescribed in his organization's ISP and the aims of those requirements. This definition is consistent with the view that security awareness is a state in which employees are aware of and are ideally committed to the security objectives of their organizations (Siponen, 2000). ISP awareness can be different from general ISA; for example, one may be generally aware that using passwords is a necessary precaution but may not know that the organization requires that passwords be changed periodically, that they need to be of a certain length and character composition, or that paraphrases should be used for easier recall while ensuring adequate length. Hence, we conceptualize that ISA consists of general ISA, along with ISP awareness.

We explain how ISA directly influences the formation of attitude by adapting Rogers' Model of Five Stages in the Innovation-Decision Process (Rogers, 2003) to information security. Adapting from Rogers (2003), knowledge of the existence of information security threats and safeguards (*awareness-knowledge*) and knowledge about what an employee is expected to do with regards to information security (*how-to-knowledge*) are important in the information security context. The former can be viewed as general information security awareness and the latter can be viewed as specific information security awareness which is ISP awareness. Because knowledge influences persuasion (Rogers, 2003), ISA influences the employee's *attitude* toward compliance in our context. Finally, because the persuasion stage influences decisions (Rogers, 2003), attitude toward compliance influences the decision to comply with the ISP. This approach is consistent with the argument that providing organizational security awareness is the most important factor in persuading employees to change their compliance actions (Siponen, 2000). Hence,

> *Hypothesis 2: An employee's ISA positively affects her attitude toward complying with the requirements of the ISP.*

2.3 Perceived Fairness of the Requirements of the ISP

While the information security literature has mostly highlighted the deterrent effects of sanctions, organization 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 such strategies. Although such strategies provide external motivations, an employee's intrinsic desires provide the internal motivation for an employee to follow (or not follow) rules and regulations (Tyler and Blader, 2005). We expect that similar motivations exist in the context of ISP compliance and propose an employee's *perceived fairness of the*

requirements of the ISP as an intrinsic motivational factor. We define *perceived fairness* as an employee's belief in the procedural justice of the organization's implementation of security rules and regulations prescribed in the ISP. Various studies conducted on justice in the field of organizational science supports the view that if an organization fails to provide fair processes, treatment, information, or outcomes, deviant behavior often increases (Acquino, Tripp and Bies, 2006; Bies, 1987). Any kinds of disincentives were also proved to be ineffective unless the measures are perceived to be legitimate or justified by employees (Baron, 2004). Besides the widely accepted role of organizational injustice on deviant behavior, the group engagement model (Tyler and Blader, 2000) also argues that procedural justice is central to shaping social identities within a group, which in turn positively influence attitudes, values, and cooperative behavior. In accordance with the group engagement model, we argue that the extent to which an employee believes in the procedural fairness of the organization's rules and regulations regarding information security would positively influence her attitude toward ISP compliance. Hence,

> Hypothesis 3: *An employee's perceived fairness of the requirements of the ISP positively affects her attitude.*

Furthermore, we posit that an employee's ISA influences her perceptions about the fairness of the ISP. We argue that an employee's knowledge of the security rules and regulations as well as her understanding of the major goals and objectives behind them would enhance her perceived fairness of these rules and regulations. For example, understanding that requirements of the ISP are developed to improve safety of informational resources of the organization and aim to provide benefits to employees and the organization can be used to rationalize the effort required to comply with requirements of the ISP. Hence, requirements that the ISP prescribes can be perceived to be fair by the employees. One's awareness of information security may be built out of one's direct life experiences, such as having once been harmed by a virus attack or penalized for not adhering to security rules and regulations. Awareness of information security can also be based on information obtained from external sources, such as newspapers, professional journals, and/or organizational policy documents. Fishbein and Ajzen (1975) described forming a belief as linking the object (or behavior) to its attribute; a person links the object to its attribute to the extent that he knows about the object, its attribute and their association. Hence, in the context of information security, we posit that an employee's ISA leads to formation of her belief in the fairness of the requirements of the ISP.

> *Hypothesis 4: An employee's ISA positively affects her perceived fairness of the requirements of the organization's ISP.*

3 RESEARCH METHODOLOGY

We used the survey method to test our model. We developed a questionnaire creating appropriate measurements considering the existing scales in the literature. The reflective measures of attitude and intention to comply were adopted from the TPB (Ajzen, 1991). The measurement items of the other constructs were developed by closely following our definitions of constructs in this study. The initial survey instrument was refined based on card sorting exercises and exploratory data analysis of two small-scale pre-tests. Data were collected by administering the finalized 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. Of all panel members, a total of 928 individuals opted to go on and participate to the survey by agreeing consent agreement. Those panel members then 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 31 were eliminated due to data runs. Hence, sample of 464 usable questionnaires were included in the analysis, giving an effective response rate of 42%. In the final sample of 464, 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.

4 DATA ANALYSES AND RESULTS

4.1 Assessment of Measurement Validation

The measurement and the structural models were tested using structural equation modeling. The component-based partial least squares (PLS) approach was used to evaluate the psychometric properties of measurement scales and to test the research hypotheses proposed in this study. The PLS is deemed to be appropriate since it focuses on prediction of data and is better suited for exploratory models and theory development. The Smart-PLS software package (version 2.0.M3) (Ringle, Wende and Will, 2005) was used for the estimations.

The measurement quality of reflective constructs was assessed by examining the convergent validity, individual item reliability, composite reliability, and discriminant validity of the measurement model (Barclay, Higgins and Thompson, 1995). Since the measures of all constructs had adequate reliability and validity assessments, all the measurement items of these constructs were kept for testing the structural model. Subsequently, we estimated the structural model and tested the research hypothesis. Please see Appendix B for the reliability and validity assessments. In addition, Table 2 in Appendix A displays the questionnaire items as well as the descriptive statistics for all the constructs including means and standard deviations, and the level of each item's contribution to the overall factor.

4.2 Structural Model Testing

The measurement of the structural model was estimated by using PLS approach to structural equation modeling. Bootstrapping resampling method was used for the estimation of the structural model. The results of the model estimation including standardized path coefficients, significance of the paths based on one-tailed t-test and the amount of variances explained (R^2) are presented in Figure 2. Based on the significant path coefficients (Figure 2), all hypotheses were supported at minimum of $p<0.001$. Approximately 27% of the variance is explained for attitude and 24% of the variance is explained for the intention to comply.

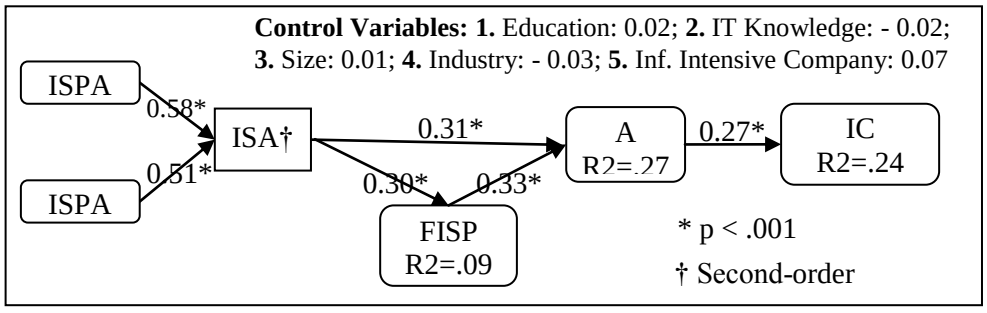

Figure 2. The Results of the Structural Model Testing

5 DISCUSSIONS, IMPLICATIONS, AND FUTURE RESEARCH

5.1 Discussion of the Findings

This study emphasizes the importance of the role of an employee's information security awareness and her perceived fairness of the requirements of the ISP. All the hypotheses were supported based on data collected from 464 employees who had some familiarity with the requirements of the ISP of their organizations.

As predicted by the TPB, attitude has a significant impact on an employee's intention to comply, explaining 23.8 % of the variance of the construct. Thus, hypotheses 1 is fully supported. Furthermore, as hypothesized we have shown that information security awareness and perceived fairness of the requirements of the ISP have a significant positive impact on an employees' attitude toward ISP compliance, explaining the 26.8% of the variance of the construct. Hence, hypotheses 2 and 3 are fully supported. Consistent with the proposed research model, perceived fairness of the ISP mediates the relationship between ISA and attitude. ISA has a significant positive impact on perceived fairness of the ISP, explaining the 9% of the variance of the construct. Please see Table 1 for t-values. We found no significant impact of control variables—including employee's level of education and technology knowledge, the size and the industry type of the organization in which he worked, and how information-intensive his organization was—on his intention to comply with the ISP.

	t - values	**Supported (one-tail)**	**p-value**
H1	7.65	√	$p < .001$
H2	6.39	√	$p < .001$
H3	6.27	√	$p < .001$
H4	6.06	√	$p < .001$

Table 1. Hypotheses and T-Values

5.2 Theoretical and Practical Contributions and Further Research Directions

Our study makes important contributions to the emerging body of knowledge about the behavioral and organizational issues of information security. We identified the role of ISA on shaping an employee's attitude toward compliance and her perception about the fairness of the requirements of the ISP. Our findings show that ISA not only exerts a direct positive influence on attitude, but also exerts a significant positive influence on an employee's perceived fairness of the ISP, which in turn leads to her positive attitude and intention toward compliance. In particular, our results indicate that an employee's perceived fairness of the ISP as well as her positive attitude toward compliance can be enhanced by her ISA. Thus, ensuring information-security awareness can directly and indirectly alter employees' attitude and in turn their intention to comply with the ISP. As an important practical implication of these results, creating a security-aware culture within the organization will improve information security. Therefore, we suggest that organizations create appropriate training and security awareness programs that ensure employees' information security awareness. Furthermore, we have shown that an employee's perceived fairness of the ISP has a direct impact on her attitude and in turn intention toward compliance. This finding implies that creating a fair environment and ensuring procedural justice in regards to implementing security rules and regulations is the key to effective information security management.

We found that ISA plays a key role in employees' compliance behavior. Accordingly, identifying the factors that lead to information security awareness would be an important contribution to academics, since there is a gap in the literature in this direction, as well as to practitioners, since they can use these factors to formulate their information security awareness programs. Researchers could also investigate the kinds of information security awareness that exist at different levels of the organizational hierarchy since different aspects of awareness may be more effective in altering perception for employees at different levels. These kinds of differences among employees can be used

to tailor the security awareness programs so they meet the varying needs of employees at different levels of the organization. Case studies about ISP compliance that focus on employees from one or a few organizations would also be useful future research since such case studies could provide an opportunity to measure objectively employees' awareness of information security and their actual compliance with the requirements of their organizations' ISP. Lastly, future research could identify other motivational factors and investigate their positive impacts on compliance. Particularly, investigating the antecedents of perceived fairness would be important since we found that fairness significantly influences attitude. This study highlights ISA as an antecedent. While a strong significant relationship between ISA and perceived fairness is found, the variation of perceived fairness explained by ISA is found to be rather small (%9). This implies that other factors leading to employee's perceived fairness explain the variation. Future research should identify those factors.

5.3 Limitations of the Study

One limitation of this study relates to the selection of participants. At the beginning of the survey questionnaire, each respondent was asked whether her organization had established the ISP and whether the respondent was aware of the ISP's requirements, and we excluded from the survey those who work in an organization without a written ISP or who were not aware of the requirements of their organizations' ISPs. The selection of participants who were aware of information security requirements may have created a favorability bias in the responses. However, the investigation of this study would be impracticable with participants who were completely unaware of the requirements of their ISPs.

The perception-based measure for ISA we used and our measuring the compliance intention instead of actual compliance behavior can also be viewed as limitations. Employees' level of awareness on general information security and the requirements of the ISPs can be measured objectively by exhaustive lists of questions, but this approach was not practical for this study because we collected the data from employees who worked in different organizations. Similarly, the actual compliance behavior could be measured by observing the actual compliance-related activities performed by the employees, but this is not practical with such a large and diverse sample. For the sake of the generalizability of our results, we opted out of objective measurements of the ISP and of actual compliance.

6 APPENDIX A – MEASUREMENT ITEMS

Items	Dimensions/ Questions	Scale	Mean	STD	Loading
IC	**Intention to comply with ISP**				
	IC – Item1	a	6.53	0.92	0.97
	IC – Item2	a	6.57	0.91	0.98
	IC – Item3	a	6.55	0.93	0.98
A	**Attitude**				
	A – Item1	c	6.28	1.13	0.89
	A – Item2	c	6.13	1.28	0.94
	A – Item3	c	6.25	1.27	0.93
	A – Item4	c	6.05	1.40	0.92
GISA	**General Information Security Awareness**				
	BC – Item1	b	6.11	1.06	0.90
	BC – Item2	b	5.74	1.37	0.84
	BC – Item3	b	6.30	0.96	0.85
	BC – Item4	b	5.72	1.23	0.87
ISPA	**ISP Awareness**				
	ISPA – Item1	b	5.89	1.13	0.93
	ISPA – Item2	b	6.00	1.10	0.92
	ISPA – Item3	b	5.44	1.57	0.88
	ISPA – Item4	b	5.72	1.36	0.94
FISP	**Perceived Fairness of the ISP**				
	FISP – Item1	c	5.77	1.49	0.94
	FISP – Item2	c	5.87	1.54	0.94
	FISP – Item3	c	5.75	1.52	0.96
	FISP – Item4	c	5.69	1.56	0.94

Table 2: Measurement Items and Item Loadings

Scale:

a) 1. Strongly Disagree – 7. Strongly Agree**;**
b) 1. Not at all – 7. Very Much**;**
c) 1. Extremely, 2. Quite, 3. Slightly, 4. Neither, 5. Slightly, 6. Quite, 7. Extremely

7 APPENDIX B – VALIDITY ANALYSIS

The AVE values for all reflective constructs were greater than the minimum recommended value of 0.50 (Convergent Validity). The square root of AVE for each construct in the model, as reported in the diagonal of the correlation of constructs matrix is larger than the corresponding off-diagonal correlations of the construct to their latent variables (Discriminant Validity). The composite reliability values for all the constructs in the research model are greater than 0.75 and Cronbach's alpha values are greater than 0.92, demonstrating that all constructs have adequate reliability assessment scores (Internal Consistency and Scale Reliability) (Gefen, Straub, Boudreau, 2000).

	CR	AVE	1	2	3	4	5
1. IC	0.98	0.95	**0.97**				
2. A	0.96	0.85	0.48	**0.92**			
3. GSA	0.92	0.75	0.53	0.37	**0.87**		
4. ISPA	0.95	0.84	0.41	0.38	0.69	**0.92**	
5. FISP	0.97	0.89	0.38	0.42	0.23	0.30	**0.94**

Table 3: Composite Reliability, AVE, and Latent Variable Correlations

- **1. IC** = Intention to Comply; **2. A** = Attitude; **3. GISA** = General Information Awareness; **4. ISPA** = ISP Awareness; **5. FISP** = Fairness of the ISP
- **CR** = Composite Reliability; **AVE** = Average Variance Extracted
- Diagonal elements display the square root of AVE for factors measured with reflective items.

All the measurement items loadings on respective constructs were above recommended minimum value of 0.707, indicating that at least 50 percent of the variance was shared with the construct (Convergent Validity) (Chin, 1998). All the measurement item loadings on the intended constructs were above 0.78, and at least 0.1 less on its loadings on other constructs (Discriminant Validity) (Gefen and Straub, 2005)

	1	2	3	4	5
1. a	**0.97**	0.48	0.52	0.40	0.38
1. b	**0.98**	0.46	0.51	0.40	0.36
1. c	**0.98**	0.47	0.52	0.39	0.36
2. a	0.50	**0.90**	0.39	0.39	0.42
2. b	0.43	**0.93**	0.33	0.35	0.40
2. c	0.42	**0.93**	0.30	0.31	0.36
2. d	0.41	**0.92**	0.32	0.35	0.38
3. a	0.52	0.35	**0.90**	0.60	0.23
3. b	0.34	0.26	**0.84**	0.54	0.14
3. c	0.59	0.38	**0.85**	0.57	0.26
3. d	0.39	0.28	**0.87**	0.66	0.19
4. a	0.42	0.36	0.67	**0.93**	0.26
4. b	0.45	0.36	0.69	**0.92**	0.26
4. c	0.26	0.30	0.55	**0.88**	0.30
4. d	0.36	0.38	0.60	**0.94**	0.29
5. a	0.40	0.42	0.23	0.30	**0.94**
5. b	0.36	0.42	0.21	0.27	**0.94**
5. c	0.32	0.38	0.23	0.28	**0.96**
5. d	0.34	0.37	0.22	0.29	**0.94**

Table 4: Cross Loadings

References

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

Aquino K., Tripp T.M. and Bies R. J. 2006. '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: 653-668.

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

Baron R.A. 2004. '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, 23-26.

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

Boss S. R. and Kirsch L. J. 2007. 'The Last Line of Defense: Motivating Employees to Follow Corporate Security Guidelines'. *Proceedings of the International Conference on Information Systems*, Montreal, 1-18.

Brancheau J. C., Janz B. D. and Wetherbe J. C. 1996. 'Key issues in information systems management: 1994-95 SIM Delphi results'. *MIS Quarterly*, 20(2): 225-242.

Cavusoglu H., Cavusoglu H. and Raghunathan S. 2004. 'Economics of IT Security Management: Four Improvements to Current Security Practices'. *Communications of the Association for Information Systems*, (14): 65-75.

Cavusoglu H., Cavusoglu H., Son J.-Y. and Benbasat I. 2008. 'Information Security Control Resources in Organizations: A Multidimensional View and Their Key Drivers'. *UBC Working Paper*.

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

Dhillon G. and Backhouse J. 2001. 'Current Directions in Information Security Research: Toward Socio-Organizational Perspectives'. *Information Systems Journal*, 11(2): 127-153.

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

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

Gefen D., Straub D. W. and Boudreau M. C. 2000. 'Structural Equation Modeling And Regression: Guidelines For Research Practice'. *Communications of the AIS*, (4): 1-77.

Hentea M. 2005. 'A Perspective on Achieving Information Security Awareness'. in *The Information Universe: Issues in Informing Science and Information*, E. Cohen (Ed.), Informing Science Institute, (2): 169-178.

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

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

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

Ransbotham S. and Mitra S. 2008. 'Choice and Chance: A Conceptual Model of Paths to Information Security Compromise', *Information Systems Research*, 2008, (http://isr.journal.informs.org/cgi/content/abstract/isre.1080.0174v1).

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

Rogers E.M. 2003 'Diffusion of innovations'. 5th ed. New York: Free Press.

SANS Institute. 2007. 'Understanding the Importance of and Implementing Internal Security Measures'. (https://www2.sans.org/reading_room/whitepapers/policyissues/1901.php); 11/3/ 2007.

Siponen, M. 2000. 'A Conceptual Foundation for Organizational Information Security Awareness'. *Information Management and Computer Security*, 8(1): 31-41.

Siponen, M. (2005) An analysis of the traditional IS security approaches: implications for research and practice, European Journal of Information Systems, 14, 3, 303-315.

Skarlicki D.P. and Folger R. 1997. 'Retaliation in the workplace: The roles of distributive, procedural, and interactional justice'. *Journal of Applied Psychology*, 82: 434- 443.

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

Straub D. W. 1990. 'Effective IS Security: An Empirical Study'. *Information Systems Research*, 1(3): 255-276.

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

Thomson M. E. and Solms R. v. 1998. 'Information security awareness: educating your users effectively'. *Information management & computer security*, 6(4): 167-173.

Tyler T. R. and Blader S. L. 2000. 'The Group Engagement Model: Procedural Justice, Social Identity, And Cooperative Behavior'. *Personality and Social Psychology Review*, 7(4): 349-361.

Tyler T. R. and Blader S. L. 2005. 'Can Businesses Effectively Regulate Employee Conduct? The Antecedents of Rule Following in Work Settings?'. *Academy of Management Journal*, 48(6): 1143-1158.

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