2013

Guilt Proneness as a Mechanism Towards Information Security Policy Compliance

Miranda Kajtazi
Linnaeus University, miranda.kajtazi@lnu.se

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

Information Systems: Transforming the Future

24th Australasian Conference on Information Systems, 4-6 December 2013, Melbourne

Proudly sponsored by

ACIS 2013 Principal Sponsor

Guilt Proneness as a Mechanism Towards Information Security Policy Compliance

Miranda Kajtazi
Linnaeus University
Växjö, Sweden
Email: miranda.kajtazi@lnu.se

Hasan Cavusoglu
University of British Columbia
Vancouver, Canada
Email: cavusoglu@sauder.ubc.ca

Abstract

In this paper, we develop a theoretical framework for understanding the role guilt proneness plays in the Information Security Policy (ISP) compliance. We define guilt proneness as an emotional personality trait indicative of a predisposition to experience a negative feeling about ISP violation. We develop a research model based on the theory of planned behaviour, guilt proneness theory and rational choice theory to explain employees' intentions to comply with ISPs by incorporating the guilt proneness as a moderator between benefit of compliance and benefit of violation as perceived by employees and their attitude towards compliance. Identifying the roles of predispositions like guilt proneness in the ISP compliance will have interesting theoretical and practical implications in the area of information security.

Keywords

Benefit of Compliance, Benefit of Violation, Compliance Behaviour, Information Security Policy, Guilt Proneness.

INTRODUCTION

While security technologies have been evolving, information security breaches in organizations still remain to be inevitable (Bulgurcu et al. 2010; Herath and Rao 2009). As a result, the security of information systems in organizations continues to be a most serious issue (Guo et al., 2011). Equipped with strategies ranging from technical solutions focusing on security technologies (Cavusoglu et al. 2004) to socio-organizational solutions focusing on the employees (Bulgurcu et al. 2010; Siponen and Vance 2010), organizations find it difficult to prioritize investments on information security (Cavusoglu et al. 2004; Hsu et al. 2012). Although technological developments have advanced the way organizations secure their information, employees are still the weakest link as they exhibit tendency to violate Information Security Policies (ISPs) (Herath and Rao 2009; Vance and Siponen 2012). In organizations overemphasizing the technical side of information security, while underemphasizing the importance and challenges of the socio-organizational side of information security is still a dilemma.

Traditionally, information security management in organizations seeks to establish control mechanisms often in the form of security technologies to minimize the risks of unauthorized access to information (Layton 2005; D'Arcy et al. 2009). A good information security management is likely achieved if technical controls are supplemented with an effective ISP, emphasizing among other things, confidentiality, integrity and availability of information (Dhillon and Backhouse 2001).

While, in today's interconnected world, investments in security technologies become necessary to tackle sophisticated attacks, they should not be the only focus of the organization. The organization must also specify the roles of employees in ensuring information security and control their behaviours that might potentially jeopardize the security of the organizational informational assets (Bulgurcu et al. 2010, D'Arcy et al. 2009, Herath and Rao 2009; Siponen et al. 2010; and Siponen and Vance 2010). The extant literature suggests that information security can be greatly improved if organizations placed attention on security thinking (Johnson and Goetz 2007; Pahnila et al. 2007). Security thinking stresses a steady progress towards establishing a security culture in the organization, often by providing employee training and education to influence and activate their thinking about information security (Pahnila et al. 2007; Puhakainen and Siponen 2010). Recent literature (Siponen et al. 2010; Vance and Siponen 2012) shows that security thinking is not yet developed enough in organizations, thus explains why employees tend to violate ISPs. Despite the growing research on security

thinking, little work has been done on understanding employees' motivation towards compliance behaviour in detail (Bulgurcu et al. 2010).

Accordingly, the objective of this paper is to develop a model that examines *guilt proneness* as a factor that may circumvent employees' motivation towards ISP violation. Guilt proneness is defined as an emotional personality trait indicative of a predisposition to experience negative feeling about personal wrongdoings, even when they are private (Cohen et al. 2012a). Since recent literature in psychology reported that individuals with high guilt proneness make fewer unethical business decisions, commit fewer delinquent behaviours, and engage in fewer transgressions (Cohen et al. 2012b), we postulate that guilt proneness plays a role in shaping employees' attitude towards ISP compliance and their intentions to comply with ISP. Our focus is on employees that work in information-intensive organizations as they frequently face with decisional dilemma regarding information security (Bulgurcu et al. 2010).

Consider the following situation. An employee of a large software development company is involved in implementing a software solution for a pharmaceutical company. Before the implementation, the employee is called to an important meeting, where the management informs him/her that this project will not be implemented at the pharmaceutical company. The situation is very serious, as the company has had little return on investments in the recent years, and is even contemplating going bankrupt. Having access to such sensitive information, the employee has a dilemma. Will he/she secretly alert his/her colleague about the failing project at a competitor software development company just to gain personal advantage? Or will guilt proneness play a major role in inhibiting such an information breach?

We intend to analyze such situations in which employees have to make an information security related decision whether to violate the ISP or not, by investigating the role that guilt proneness may play in circumventing information security violations similar to the situation presented above.

The rest of our paper is organized as follows. We first present our research motivation. We then introduce our proposed theoretical framework followed by a research model and five propositions, also shortly presenting our intended research methodology. We highlight the importance of the identification of meaningful personality trait like guilt proneness. Finally, we discuss future work in this area.

RESEARCH MOTIVATION

Prior research on ISP compliance can be categorized into two groups of studies. The first category includes studies that focus on motivational factors that can lead employees to comply with the ISP. The emphasis of these studies has been directed towards identifying antecedents of compliance and noncompliance behaviour (e.g. Bulgurcu et al. 2010; Herath and Rao 2009; Johnston and Warkentin 2010; Siponen et al. 2010). Studies of this nature tackle compliance and noncompliance by focusing on behavioural aspects of information security and emphasize practices such as information security risk management or information security awareness and training programs.

The second category includes studies that focus on ISP design as they implicitly argue that perhaps the ISPs themselves are inadequate and hence employees tend to circumvent them intentionally or unintentionally (Thomas and Dhillon 2011, Dhillon and Baskerville 2008). These studies view ISPs as a design problem. While the existing studies are adequate and fill important gaps in the literature, more research on information security as a field is still needed to unveil the complex socio-organizational dynamics associated with the information security. In particular, understanding employees' compliance and noncompliance behaviour through empirical research based on different theoretical lenses would advance our current knowledge in the field (Vance and Siponen 2012).

A recurrent theme in existing studies is that while information security research intends to ensure information security in organizations, from a behavioural-oriented approach or a design-oriented approach, these studies are not yet sufficient to understand why employees are cognitively and motivationally driven to choose noncompliance over compliance with ISPs.

Consequently, improving security management in organizations is viewed as one of the major determinants of organizational success, however, current improvements have yet to produce effective results (Siponen et al. 2010), which would eventually lead to a security risk-free environment in organizations (Guo et al. 2011). As a result, the need to re-design current information security strategies has been claimed (Dhillon and Backhouse 2001, Siponen et al. 2010). The latter can perhaps be facilitated by a more careful planning of information security in organizations in terms of focusing on psychological traits of employees, such as guilt proneness this study intends to investigate. Our aim is to suggest that organizations should focus on guilt proneness as an emotional personality trait that can help to identify employees who have more or less dispositions to engage in noncompliance behaviour. Thus, examining guilt proneness as a factor to determine compliance, can potentially

guide organizations to improve the effectiveness of designing a context-specific security strategy for their organizations.

THEORETICAL FRAMEWORK

Our theoretical base to examine employees' compliance behaviour with ISPs draws upon the Theory of Planned Behaviour (TPB), Guilt Proneness Theory (GPT) and Rational Choice Theory (RCT).

Theory of Planned Behaviour (Ajzen 1991) has emerged as one of the most influential conceptual frameworks to study human actions (Ajzen 2002). TPB helps to specify the motivational factors that support employees' compliance behaviour with ISPs (Bulgurcu et al. 2010). According to TPB, human behaviour is viewed as a function of three sets of belief-based perceptions: personal, normative and control (Ajzen 1991). Personal beliefs present an individual's overall evaluation of an intended behaviour, allowing them to conceptualize an attitude toward behaviour. Control beliefs address the perceived ease or difficulty of performing behaviour, understood as perceived behavioural control, thus shares an interchangeable meaning with perceived behavioural control (Fishbein, 2007). Normative beliefs present a type of enforcement, understood as subjective norms. Our study, however, specifically focuses on the personal beliefs, which present an individual's overall evaluation of an intended behaviour, considering that we want to measure the moderating role of guilt proneness on the independent factors of benefits of violation and compliance, for which we believe they may form an overall attitude of an employee. Moreover, we

Drawing on **Guilt Proneness Theory**, we suggest that employees who are high on guilt proneness present an emotional personality trait characterized by a predisposition to experience negative feelings about personal wrongdoings (Cohen et al. 2012a,b). We posit that guilt proneness may be a positive driver of compliance behaviour, as it suggests that individuals feel a sense of responsibility for their actions, in particular related to their engagement in wrongdoings (Schaumberg and Flynn 2012). The most common approach that theorists have taken to understanding guilt proneness as an emotional personality trait has been focused on determining guilt as an important factor for examining, in particular, individual competitive advantage and leadership roles (Cohen et al. 2012a, Covert et al. 2003; Schaumberg and Flynn 2012). Such studies convey a message that individuals, who are predisposed to be higher on guilt proneness, are more loyal to their organizations (Cohen et al. 2011/2012a,b). Observing guilt proneness as an attitude towards ethicality, as perceived by researchers on social psychology (Flynn 2005), may also present an important factor to explain employees' motivation towards compliance behaviour with ISPs in organizations.

Consistent with **Rational Choice Theory** (Simon 1955), we adopt two independent constructs to study compliance behaviour, namely benefit of compliance, and its obverse, the benefit of violation. We predict that these two constructs will inform us how employees act when faced with choices (Bulgurcu et al. 2010). We believe that guilt proneness would allow us to identify the employees who are more inclined to formulate an attitude towards compliance as they trade-off benefit of compliance and benefit of violation. We define *benefit of compliance* as the cognitive-driven perceived benefit for complying with organization's ISP; such benefits are commonly driven by employee's personal gains, advantages and benefits for choosing compliance over violation. Whereas, we define *benefit of violation* as an emotional-driven perceived benefit of violation, thus as a positive choice for violating organization's ISP; such benefits are commonly driven by assigning a negative impact of employee's compliance, thus, compliance is viewed as harmful, burdensome and even costly for the employee. Decision-making under pressure may lead to an irrational behaviour (Tversky and Kahneman 1986), however, the choice between the benefits of violation and benefits of compliance depends on the pay-offs of each derived in a situation.

Building our theoretical framework on the bases of **TPB**, **GPT** and **RCT**, allows us to formulate an integrative approach towards a new understanding of employees' ISP compliance behaviour. A fundamental principle that implicates the relationship between the three theories is based on our aim to understand why some employees are more inclined to sustain compliance with ISPs than others. We also consider that these three theories are complimentary for giving us a new understanding of employees' compliance behaviour with ISPs. As our theoretical framework builds upon prior research, in particular that we utilize the constructs of TPB and RCT similarly to previous studies in the extend literature on information security (e.g. Bulgurcu et al. 2010; Herath and Rao 2009), we characterize an important theoretical redirection. Our study intends to emphasize the important role guilt proneness may play in understanding employees' attitude towards compliance with ISPs and indirectly influencing intentions.

Our study, however, confines the investigation based on TPB by focusing only on the attitude construct. According to Ajzen (2002), however, attitude is the major focus of theory and research that is based on TPB. Furthermore, Ajzen (2002) indicates that an individual's overall attitude toward an object is determined by subjective values of the object's attributes in interaction with the strength of the association. Our study suggests that the employee has different beliefs for compliance with ISPs, but it is assumed that only beliefs that are

readily accessible in their memory influence attitude at any given moment. In information security literature, attitude is found to play a significant role on employees' compliance with ISPs, as reported in studies conducted by Bulgurcu et al. (2010) and Siponen et al. (2010). Loosely defined, attitude presents a summarized evaluation of an employee's understanding in attributed dimensions as good/bad, harmful/beneficial or likable/dislikable, and alike (Ajzen 2002).

Although our study tends to present a theoretical redirection by highlighting the role of guilt proneness as a mechanism to alleviate ISP violation, we acknowledge previous studies in information security that identified important facilitators to enforce employees' compliance with ISPs (D'Arcy et al 2009; Vance, 2011). Sanctions (in particular the perceived severity of sanctions), as deterrence mechanisms, for instance, have been proved to facilitate compliance, when they are enforced in organizations (D'Arcy et al. 2009; Siponen and Vance 2010). Different from such approaches, our approach to explaining compliance with ISPs is to suggest that guilt proneness may be an effective mechanism to circumvent ISP violation. In this area, we believe that guilt proneness may serve as a mechanism to detect employees that are more inclined to sustain compliance with ISPs compared to their colleagues who are more inclined to engage in violating their organization's ISP.

Research Model and Propositions

The integration of the three theories, namely TPB, GPT and RCT is reflected in our proposed model in Figure 1. The central components of the proposed model are the attitude and intentions towards compliance with ISP, while guilt proneness acts as a moderator for the behavioural beliefs and the attitude. With its role in shaping the attitude, guilt proneness indirectly affects employee's intentions to comply with the ISP. Although TPB and RCT have been studied in the security compliance domain, the rationale of the proposed model is to create an integrative model that includes employee's disposition toward feeling guilty when he/she violates the ISP of the organization, along with factors from TPB and RCT, which have been identified in the literature. While the extant research advanced our understanding as to what are the motivational drivers which result in employee's ISP compliance (D'Arcy et al. 2009; Siponen et al. 2010; Siponen and Vance 2010; Straub and Welke 1998), we believe this study intends to bring a different perspective by studying if guilt proneness is an important factor to identify why some employees are more inclined to sustain compliance with their organizations' ISPs, while others are more inclined to violate their organizations' ISPs.

Drawing on TPB, and on the extend literature on information security, we posit that employee's attitude towards compliance with ISP positively influences employee's intentions to comply. We adopted the attitude construct from TPB (Fishbein and Ajzen, 1975; Ajzen, 1991) and in the context of our study, we refer to attitude as an employee's feeling towards compliance with the requirements of the ISP (Bulgurcu et al. 2010). We define attitude as the degree to which the act of the compliance behaviour presents a positive value for the organization. We propose two antecedents of attitude, namely the benefit of compliance and the benefit of violation. We intend to measure the effects of these independent factors moderated by the construct of guilt proneness. Based on previous information security literature that has utilized the construct of attitude and intentions to measure compliance behaviour, we formulate the following proposition.

Proposition 1: *Employee's attitude towards compliance with ISP positively affects intention to comply with the ISP.*

While our theoretical base depends on TPB, we enrich our theory by examining the role that GPT plays, furthermore facilitated by RCT. We propose that the independent constructs of benefit of compliance and its obverse, benefit of violation, derived from RCT can help us determine their effects on employees attitude towards compliance. According to RCT, benefit of compliance and benefit of violation may both present a rational choice with respect to the relations between the pay-offs an employee may receive for choosing one or the other (Simon 1955). In fact, many such decisions are based on the beliefs concerning the likelihood of uncertain events, such as the aftermath of a wrongdoing (Tversky and Kahneman 1986). Consequently, employees' choice between benefit of compliance and benefit of violation depends on employees' calculation of the expected value from such behaviours (Bulgurcu et al. 2010). Such calculations are also presented as odds or subjective probabilities (Tversky and Kahneman 1974). We thus propose the following:

Proposition 2: Benefit of Compliance positively influences employee's attitude towards compliance with ISP.

Proposition 3: Benefit of Violation negatively influences employee's attitude towards compliance with ISP.

Utilizing the construct of guilt proneness as a moderating mechanism to explain the attitude towards compliance with ISP, we propose that guilt proneness, understood as an individual difference that reflects a predisposition to experience negative feelings for personal wrongdoing (Cohen et al. 2012a; Tangney et al 2007), can act as a moderator between behavioural beliefs and the attitude towards compliance with ISP. We suggest that employees who are high on guilt proneness present an emotional personality trait that would positively influence the impact of the benefit of compliance, while it would negatively influence the impact the benefit of violation. According to

Tangney et al. (2007) guilt proneness is regarded as a negatively valenced self-conscious emotion, which is evoked by self-reflection and self-evaluation. This form of self-evaluation may be explicit or implicit, consciously experienced or transpiring beneath the radar of our awareness (Tangney et al. 2007, p.347). In fact, factors such as guilt provide salient feedback on our social and moral acceptability. Thus we propose:

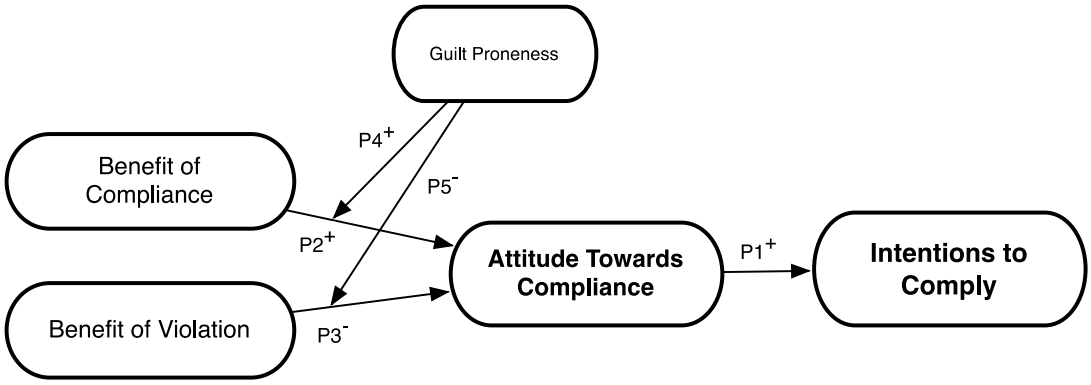

Figure 1: Research Model

Proposition 4: Guilt proneness moderates the relationship between benefit of compliance and attitude towards compliance with ISP, such that the relationship will be positively affected when employees exhibit an increase on guilt proneness.

Proposition 5: Guilt proneness moderates the relationship between benefit of violation and attitude towards compliance with ISP, such that the relationship will be negatively affected when employees exhibit an increase on guilt proneness.

We believe that the model presented in Figure 1 has potentials to further our understanding of the ISP compliance behaviour. Such results could be useful to understand whether guilt proneness facilitates our understanding why some employees are more compliant with ISPs than their colleagues.

Our research methodology will focus on the experimental design approach, by utilizing multiple scenarios. We intend to conduct a pilot study for content validity, construct validity and reliability before the main study. In designing the experiment, control groups will be in focus. We believe that the experimental approach will demonstrate the effect of guilt proneness on intentions to comply, by comparing its effects on the choices employees make to form their attitude. We believe that measuring the emotional trait of guilt proneness using the experimental design approach, will shed light on understanding how employees describe their emotions when feeling bad or good about their choices (violate or comply). Guilt proneness effects will be measured using the scenario-based measures in which employees read about common situations that they are likely to encounter in their jobs, followed by common reactions to those situations. In general, the employees will be asked to imagine themselves in a typical situation that would make them express their level of guiltiness. In doing so, the scenarios will engage them in some exercises, after which we will be asking them to indicate the likelihood that they would react upon the exercises.

CONCLUSION AND FUTURE RESEARCH

This paper presents a proposed research model, which we intend to test in the future by means of experimental design. Seeking to further our understanding of current approaches in information security, we consider that our study can generate significant contributions both to theory and practice in the area of information security.

Firstly to theory, current information security approaches suggest that compliance and noncompliance behaviour is continuously evolving, yet we cannot design rigid solutions to prevent information insecurity, an area that clearly presents the need for further investigation. Our intention to incorporate guilt proneness theory in studying its effects on compliance behaviour, may thus make an interesting theoretical contribution. We believe that a deep understanding of the effects of guilt proneness on compliance behaviour may change our current perceptions of what frames compliance. Our study has potentials to inform us that guilt proneness, which is understood as an emotional personality trait that accounts for a sense of responsibility towards the organization, can play an important role in theorizing about compliance behaviour. It is suggested that employees who are prone to feeling more guilty than their colleagues, set aside their self-interest for the betterment of the organization (Schaumberg and Flynn 2012). With intentions to find whether high guilt prone employees are similarly affected towards compliance behaviour with ISPs, can account for an important theoretical redirection in the current approaches focused on compliance and noncompliance behaviour with ISPs in organizations.

Secondly, our study may have significant practical implications. We expect that our experimental design approach will generate new findings that will be helpful to security managers for understanding their employees' attitude and intentions towards compliance with the ISP, by the means of diversifying between employees that are more guilt prone than others. Additionally, security managers can take advantage to use guilt proneness as a mechanism for enhancing employees' sense of responsibility towards their organizational rules and regulations.

Our future efforts will focus on expanding the current theoretical base. While our model does not account for actual behaviour towards compliance, we consider that both attitude towards compliance and intention to comply will account for a considerable amount of variance in the actual behaviour (Ajzen 1991). We recognize this as the main limitation of the proposed study. Another limitation relates to the construct of guilt proneness, which is not the only personality trait to enhance employees' sense of responsibility towards their organization. In this regard, we intend to enrich the current moderating role of guilt proneness by including other emotional related personality traits as factors that would control guilt proneness, e.g. organizational commitment and moral commitment. We also foresee other important factors that may significantly influence the intentions to comply, such as job satisfaction and tenure in the organization.

Despite our current limitations, our theoretical analysis presented in this paper can potentially bring a new perspective to information security literature, by providing a deeper understanding of what makes some employees more cognizant as well as motivated to comply with information security policies, compared to others, by highlighting the role of guilt proneness in there.

REFERENCES

Ajzen, I. 1991. "The Theory of Planned Behaviour", *Organizational Behaviour and Human Decision Processes*", (50), pp. 179-211.

Ajzen, I. 2002. "Perceived Behavioural Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behaviour", *Journal of Applied Social Psychology*, (32:4), pp. 665-683.

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), pp. 523-548.

Cavusoglu, H., Mishra, B., and Raghunathan, S. 2004. "A Model for Evaluating IT Security Investments," *Communications of the ACM*, (47:7), pp. 87-92.

Cohen, T. R., Panter, A. T., and Turan, N. 2012a. "Predicting Counterproductive Work Behaviour from Guilt Proneness", *Journal of Business Ethics*, Springer.

Cohen, T. R., Panter, A. T., and Turan, N. 2012b. "Guilt Proneness and Moral Character," *Current Directions in Psychological Science*, (21:5), pp. 355-359.

Cohen, T. R., Wolf, S.T., Panter, A. T., and Insko, Ch. A. 2011. "Introducing the GASP Scale: A New Measure of Guilt and Shame Proneness", *Journal of Personality and Social Psychology*, (100:5), pp. 947-966.

Covert, M. V., Tangney, J. P., Maddux, J. E., and Heleno, N. M. 2003. "Shame-proneness, guilt-proneness and interpersonal problem solving: A social cognitive analysis", *Journal of Social and Clinical Psychology*, (22), pp. 1-12.

D'Arcy, J., Hovav, A., and Galleta, D.F. 2009. "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach," *Information Systems Research*, (20:1), pp. 79-98.

Dhillon, G., and Backhouse, J. 2001. "Current directions in IS security research: towards socio-organizational perspectives," *Information Systems Journal*, (11:2), pp. 127-153.

Dhillon, G., and Baskerville, R. L. 2008. "Information Systems Security Strategy: A Process View, in D. W. Straub, S. Goodman and R. L. Baskerville, eds, "*Information Security: policy, processes and practices*", NY: M.E. Sharpe.

Flynn, F. J. 2005. "Identity Orientations and Forms of Social Exchange in Organizations", *Academy of Management Review* (30:4), pp. 737-750.

Fishbein, M. 2007. "A Reasoned Action Approach: Some Issues, Questions, and Clarifications. In Ajzen, I., Albarracin, D. and Hornik, R., eds., *Prediction and Change of Health Behavior: Applying the Reasoned Action Approach*. pp. 281-296, Lawrence Erlbaum and Associates, Hillsdale.

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

Guo, K. H., Yuan, Y., Archer, N. P., and Connelly, C. E. 2011. "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behaviour Model", *Journal of Management Information Systems*, (28:2), pp. 203–236.

Herath, T., and Rao, H. R. 2009. "Encouraging information security behaviours in organizations: role of penalties, pressures and perceived effectiveness," *Decision Support Systems*," (47:2), pp. 154-165.

Hsu, C., Lee, J-N., and Straub, D. 2012. "Institutional Influences on Information Systems Security Innovations", *Information Systems Research*.

Johnson, E. M., and Goetz, E. 2007. "Embedding Information Security into the Organization", *IEEE Security Privacy Magazine*, (5), pp. 16–24.

Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviours: An Empirical Study", *MIS Quarterly* , (34:3), pp. 549–566.

Layton, T. 2005. "*Information Security Awareness: The Psychology Behind the Technology*", AuthorHouse.

Pahnila S, Siponen M and Mahmood A. 2007. "Employees' behaviour towards IS security policy compliance. *In 40th Hawaii International Conference on System Sciences* (HICSS 07) Hawaii, USA.

Puhakainen, P., and Siponen, M. 2010. "Improving employees' compliance through information systems security training: an action research study", *MIS Quarterly* (34:3), pp. 757–778.

Siponen, M., Pahnila, S., and Mahmood, A. 2010. "Compliance with Information Security Policies: An Empirical Investigation," *Structural Equation Modeling*, (5:2), pp. 5-8.

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights Into the Problem of Employee Information Systems Security Policy Violations", *MIS Quarterly*, (34:3), pp. 487-502.

Straub, D., and Welke, R. 1998. "Coping with systems risk: security planning models for management decision-making", *MIS Quarterly*, (22:4), pp. 441–469.

Schaumberg, R. L., and Flynn, F. J. 2012. "Uneasy Lies the Head That Wears the Crown: The Link Between Guilt Proneness and Leadership", *Journal of Personality and Social Psychology*, (103:2), pp. 327-342.

Simon, H. A. 1955. "A Behavioural Model of Rational Choice", *The Quarterly Journals of Economics*, (69:1), pp. 99-118.

Tangney, J. P., Stuewig, J., and Mashek, D. J. 2007. "Moral Emotions and Moral Behaviour", The Annual Review of Psychology, (58), pp. 345-372.

Thomas, M., and Dhillon, G. 2011. "Interpreting Deep Structures of Information Systems Security", *The Computer Journal*, (55:10), pp. 1148-1156.

Tversky, A., and Kahneman, D. 1974. "Judgment under Uncertainty: Heuristics and Biases", *Science*, (185:4157), pp. 1124-1131.

Tversky, A., and Kahneman, D. 1986. "Rational Choice and the Framing of Decisions", *The Journal of Business*, (59:4/2), pp. S251-S278.

Vance, A., and Siponen, M. 2012. "IS Security Policy Violations: A Rational Choice Perspective," *Journal of Organizational and End User Computing*, (24:1), pp. 21-41.

COPYRIGHT