WISP 2012 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-15-2012

Exploring Employees' Escalating Behavior as an Antecedent of Information Security Policy Noncompliance Behaviour

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

Exploring Employees' Escalating Behavior as an Antecedent of Information Security Policy Noncompliance Behaviour

Miranda Kajtazi[1]
Linnaeus University,
Växjö, Sweden

ABSTRACT

Information security trends show that many studies focus on information security in investigating employees' motivated behavior for compliance with information security policies. The literature, however, lacks attention in understanding how escalating behavior may be an antecedent of noncompliance behavior. The objective of this study is to examine the factors that influence employees to violate their organization's information security policy, where violation occurs during the escalation of commitment to a failing course of action.

The proposed model draws on three theories that explain escalation of commitment, namely: prospect theory (PT), approach avoidance theory (AAT) and agency theory (AT). The paper specifies the three theories as complementary to facilitating an understanding of how employees engage in risky decisions to violate information security policy. The paper ends with a discussion of the implications of the proposed model by presenting a unique context for future research in the area of information security.

Keywords: information security, information security policy, escalation of commitment, prospect theory, approach avoidance theory, agency theory.

[1] Corresponding author. miranda.kajtazi@lnu.se

INTRODUCTION

Information security is considered as an inseparable part of information systems, often accompanied with risks that organizations need to handle (Herath and Rao 2009). Today, most organizations' operations depend on information systems requiring the management of risks related to information security (Anderson and Agarwal 2010; Bulgurcu et al. 2010). Preventing failure and managing a healthy status as information processors, organizations need to build secure channels for information sharing (Johnson and Goetz 2007; McAfee 2009). This, however, is not an easy task. Many agencies have recently reported that a dozen high-profile organizations, such as NASA, FBI, Google, have suffered security breaches, with much online personal data compromised, and billions of dollars registered in losses.

Employees in organizations are involved with daily decision-making processes, in which they commonly break organizational rules and regulations to get their tasks completed (Guo et al. 2011; Tyler and Blader 2005). For example, when employees share their personal user name and password with co-workers to complete their tasks, is a violation that is identified to cause damage to organizations assets (Puhakainen and Siponen 2010). It is suggested that such behavior usually happens when employees are unsure whether to persist or withdraw from a failing task is a better decision, a pattern that in theory is understood as escalating behavior (Keil et al. 2000). Escalation is a phenomenon which explains how individuals get involved in a failing course of action, and reflect the tendency of not knowing whether withdrawal or persistence is the best solution (Staw and Ross 1989). A failing course of action refers to any disappointing state of action. For instance, banks must decide how to manage their involvement in nonperforming loans; employees must decide what to do with their tasks they cannot complete, when the deadline is approaching; or when researchers must decide whether to persist or withdraw from disappointing research projects (Staw and Ross 1989). Escalation occurs in various decision contexts, when investments in time, effort, and resources are devoted to a course of action, even if appropriate progress toward the objective of such investments has not been realized (Ross and Staw 1991).

The objective of this study is to examine the factors that influence employees to violate their organizations' information security policy, where violation occurs during the escalation of commitment to a failing course of action. The focus is on escalation of commitment in information – intensive organizations, such as banks or pharmaceuticals that are known to be more vulnerable in protecting their information (Bulgurcu et al. 2010), thus, need contextualized security agendas, personalized for their security needs.

The paper is structured as follows. First, an overview of previous literature in information security is provided as a background. Several motivations for this paper are then listed. Further, the theoretical base of this study is exemplified followed by the introduction of the research model. A number of hypotheses are then presented, which together with the research model, compose a conceptual framework for analysis. Finally, the methodology is shortly introduced and implications are discussed.

LITERATURE REVIEW

Numerous studies (e.g. Bulgurcu et al. 2010; Herath and Rao 2009) have addressed information security problems in organizations, generally focusing on employees' compliance with information security policies by considering the role that information security awareness plays in preventing security problems. Recent investigations suggest that prior research has focused primarily on motivational factors that may trigger employees' compliance with information security policy (Bulgurcu et al. 2010; D'Arcy et al. 2009; Herath and Rao 2009;

Pahnilla et al. 2007). These studies also suggest that the focus on information security has shifted towards investigating the role employees play in securing an information risk-free environment in their organization.

Different approaches on information security have addressed security topics for sustaining employees' compliance with information security policy, mainly tackled in terms of socio-organizational or socio-technical perspective (Warkentin and Willison 2009). Organizations' role in information security is considered socio-organizational when the social perspective is inclusively represented in managing situations (Dhillon and Backhouse 2001), while organizations' role in information security is considered socio-technical when a technical system and a social system are considered equally important (Iivari and Hirschheim 1996).

Those that analysed trends in information security have argued that information security research showed dominance of the technical-oriented perspective for maintaining good management practices (Dhillon and Backhouse 2001). Recently, such a view has been supported by studies that have largely focused on the socio-organizational perspective (Bulgurcu et al. 2010; Vance and Siponen 2012). The critique of technical-oriented approaches laid the foundation for a socio-organizational perspective in dealing with information security issues. The non-technical issues became as important as technical issues in safeguarding organization's sensitive information (Dhillon and Backhouse 2001). Research in this direction has received significant attention in the literature. Table 1 categorizes these two perspectives and presents a number of studies related to them.

Table 1. Socio-organizational and socio-technical studies in information security.

Perspective	Concerns in Information Security	Example Studies
Socio-	Information Security Risk Management	(Cavusoglu et al. 2004; Fenz et al. 2011; Straub and Welke 1998).
	Employees behavioral aspects related to Information Security -compliance with	(Anderson and Agarwal 2010; Bulgurcu et al. 2010; Herath and

Organizational	security policies	Rao 2009).
	Information Security Awareness – education for compliance with security policies	(Puhakainen and Siponen 2010; Vance and Siponen 2012).
Socio-Technical	Security Measures	(D'Arcy et al 2009; Hagen et al. 2008).
	Security Awareness Compliance for Digital Protection	(Kruger et al. 2010; Wolf et al. 2011).

A recurrent theme with both perspectives is that the extensive use of modern information practices made organizations more vulnerable in being unwillingly exposed within a global cloud of information (McAfee 2009). From sending emails to sharing digital notes, organizations frequently suffer from violation of their information (Johnston and Warkentin 2010). A recent example is the leaking of more than 250,000 diplomatic cables via Wikileaks, considered one of the worst security breaches ever accomplished.

MOTIVATION

There are several motivations for this study. First, the security of information systems in organizations continues to be one of the most serious issues (Guo et al. 2011; Hagen et al. 2008). Information security plays a crucial role for organization's image, which can be enhanced by including a security-aware culture (Bulgurcu et al. 2010), general security climate (Herath and Rao 2009), neutralization of employees' behavior towards information systems security policy violations (Vance and Siponen 2012), and enforcements of security policies in organizations (D'Arcy et al. 2009). Relatively few such studies are focused on the socio-organizational aspects of ensuring security risk-free environment in organizations (Bulgurcu et al 2010; Hagen et al. 2008; McAfee 2009; among others). This study intends to contribute to the socio-organizational perspective. To increase the generalizability of prior studies and the existing knowledge, we suggest that an examination of employees' noncompliance behavior as a result of their escalating behavior in a task-related context in organizations is necessary.

Second, although employees' information security policy compliance behavior has been investigated from an array of studies (e.g. Herath and Rao 2009), our focus is on escalating behavior as an antecedent of noncompliance, occurring in settings where employees may engage in risky decision-making processes, such as in their assigned tasks. Our study intends to emphasize that escalation of commitment, considered as a relatively frequent problem in organizations (Keil et al. 2000; Park et al. 2012) is a new phenomenon that may change the way we understand noncompliance behavior with information security policies.

Third, despite the growing research on compliance behavior with information security policies, studies suggest that information security is still in the process of forming a tradition where specific research foci are well-established and sufficiently investigated (Vance and Siponen 2012). Thus, little work has been done on understanding employees' compliance behavior in detail, both in terms of utilized theoretical lenses and empirical research. We believe that the approach we propose here is unique to understand how the factors that trigger escalating behavior can be considered as antecedents of noncompliance behavior. Theorizing that escalating behavior influences noncompliance, could possibly help us better understand why noncompliance with information security policies has become a frequent behavior.

Finally, our study deals with the practice of information management in organizations, an area that has not been researched extensively (Dean and Webb 2011). In the last two decades, well-established information management practices, often based on IT, have been recognized as a source of strategic competitive advantage, by guarantying among other things, a secured organization. Information systems researchers have theorized about the role IT plays in the security of information (Puhakainen and Siponen 2010), by providing recommendations and solutions how to develop advanced technologies as best practices for information security. Such analysis have resulted with heavy investments in security technologies, however, few systems have accurately met organizations' expectations (Bulgurcu et al. 2010). The rational for our approach aligns with this argument and we therefore intend to contribute with vigorous research to understand noncompliance behavior in more details. In this regard, we envision the development of personalized information security analytical strategies and technologies for organizations, which may provide a dual outcome. One is that organizations' heavy investments in technologies could be better rationalized, so that the security strategies and technologies meet organizations' expectations. The other is that employees could be more attracted to complying with information security policy of the organization. This, by understanding how noncompliance behavior in their context-specific tasks may generate unwanted risks (e.g. financial losses) in their organizations.

THEORETICAL FOUNDATION

Escalation of commitment has been investigated from an array of studies. Literature in escalation of commitment provides a solid theoretical base for explaining the escalating behavior (Keil et al. 2000; Park et al. 2012; Ross and Staw 1991; Staw 1976; Staw and Ross 1989). Such literature also shows that different theories have been proposed and advanced to explain the phenomenon of escalation. Escalation theories focus on understanding the commitment of an individual to take risky decisions in a given context, especially when the act is deliberate (Staw and Ross 1989). Central to such theories is the understanding of escalating behavior. Employees often become committed to a losing course of action, "throwing good money or effort after bad" (Staw and Ross 1989), when an employee exhibits high risk-taking behavior as a result of a deliberate decision (Keil et al. 2000). This is often found in situations when employees are involved in a failing course of action, thus deliberately commit more resources and efforts to complete the action, rather than destroying their image in the organization. Escalation of commitment theories have been previously utilized to study project failures, such as software projects (Keil et al. 2000; Park et al. 2012), and have also been adapted to better understand contribution behaviors of individuals who invest time and effort to a failing course of action (Staw 1976).

Three theories that explain escalating behavior are critical here to understand employees' non-compliance behavior with information security policy, namely: prospect theory (PT), approach avoidance theory (AAT) and agency theory (AT).

We draw upon PT by looking at how the factor of sunk cost triggers escalation. We draw on AAT in terms of how completion effect triggers escalation and how the cost of withdrawal presents its driving forces encouraging an individual to commit resources to a failing course of action. We finally draw on AT by looking into the factor of information asymmetry as a condition which triggers individual's escalating behavior, since individual's misconduct cannot be verified easily. Two of these theories, namely PT and AT are also utilized here to understand the risk-taking behavior of employees that triggers them to get locked into a failing course of action, which results in escalating behavior. AT suggests that individuals may differ in terms of their risk preferences, while PT clearly distinguishes between risk averse and risk seeking individuals. Whereas, the AAT may help us to show that value-based choices are also influenced by risk in potential outcomes, whether the outcomes reflect gains or losses. A short introduction for each of these theories is given below.

Research Model and Hypotheses

The integration of the three theories is reflected in the model presented in Figure 1. The central component of the proposed model is focused on the noncompliance behavior with information security policy. In order to expand the understanding of noncompliance behavior, we propose a theoretical model that accounts for employee's willingness to engage in activities not permitted at work, which we believe results in noncompliance behavior with information security policies. In order to measure such behavior, the proposed model incorporates four factors (information asymmetry, completion effect, cost of withdrawal, and sunk cost). These four factors are moderated by the risk perception factor, in order to measure employees' level of risk-seeking behavior for their willingness to engage in activities not permitted at work. We consider risk perception as an important moderating factor.

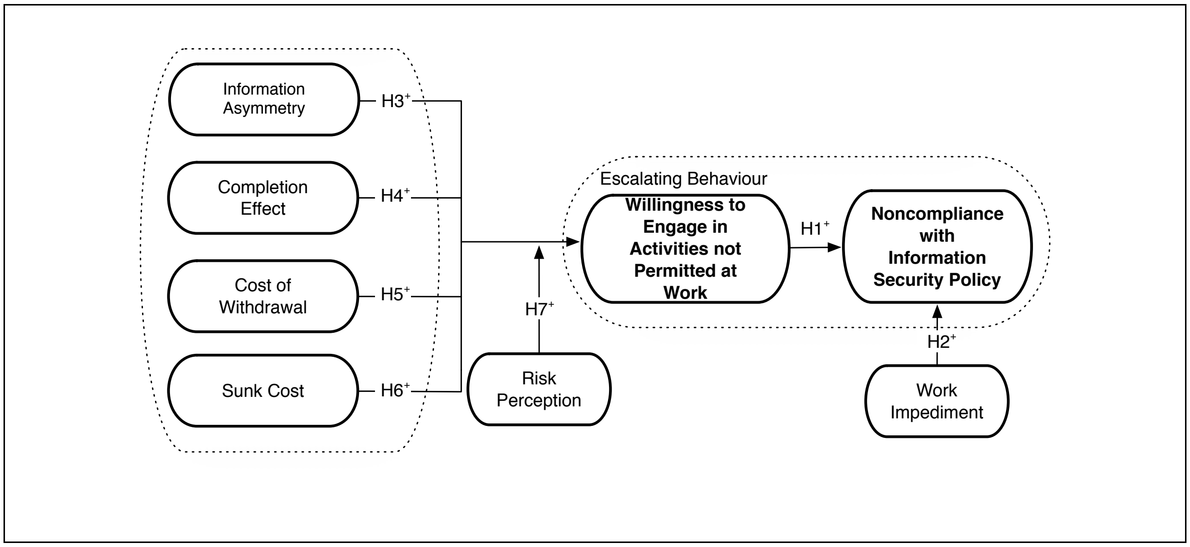

Figure 1. Research Model

According to prospect theory, risk-seeking decision makers are more likely to pay less attention to negative outcomes, therefore become risk-seekers (Keil et al. 2000). We assume that employees who demonstrate risk-seeing behaviors are less likely to comply with information security policies. We develop the following hypothesis in the context of noncompliance with information security policy.

Hypothesis 1*: Employee's willingness to engage in activities not permitted at work positively affects noncompliance behavior with information security policy.*

We postulate that noncompliance behavior is also a result of the work impediment. Work impediment is defined as a detriment to an employee's daily job-related tasks and activities resulting from compliance with the requirements of the information security policy (Bulgurcu et al. 2010). In line with this argument, we also posit that noncompliance behavior with information security policy is also directly related to work impediment, because employees consider such policies as time consuming and at times not of great importance (Vance and Siponen 2012). Thus, we propose:

Hypothesis 2*: Employee's work impediment positively affects noncompliance behavior with information security policy.*

We now continue to explain the rest of the model based on the three escalation theories.

Agency theory. AT suggests that there is an agency relationship as *a contract under which one or more individuals engage another individual (who is the agent) to perform some service on their behalf, which involves delegating some decision making authority to the agent* (Jensen and Meckling 1976). The construct of information asymmetry is central to all principal-agent models. The combination of information asymmetry and the agent's work or risk aversion is what typically allows self-interested behavior to emerge (Keil et al. 2000). AT explains the agency relationship between two individuals, in which one is assumed to have more information than the other. AT is utilized here to understand how information asymmetry is positively related to employees' willingness to engage in activities not permitted at work, when the employee knows they can assure information asymmetry in the process of escalation. This problem arises because the employee's behavior cannot be verified as inappropriate. AT also describes the problem of risk sharing that arises when the principal and agent have different attitudes towards the risk. The problem here is that the principal and the agent may prefer different actions because of the different risk preferences (Keil et al. 2000). Therefore,

Hypothesis 3*: Information Asymmetry is positively associated with an individual's willingness to engage in activities not permitted at work.*

Approach avoidance theory. Under AAT, escalation is theorized as a behavior that results when driving forces that encourage persistence seem to outweigh restraining forces that encourage abandonment. In terms of escalating behavior, AAT suggests that the cost of persistence is often overshadowed by the driving forces of goal attainment, by the cost of withdrawal or the proximity of the goal (Keil et al. 2000). Among other factors, AAT proposes that the completion effect is a type of motivation for an individual to achieve a goal as the individual gets closer to that goal. In the context of noncompliance behavior, the factor of completion effect suggests that when tasks are near completion, employee's willingness to engage in activities not permitted at work increases. Here we propose the following hypothesis:

Hypothesis 4*: Completion Effect is positively associated with an individual's willingness to engage in activities not permitted at work.*

AAT also suggests that the cost of withdrawal affects the value-based choices of individuals influenced by risk increasing in potential outcomes of gains or losses. Research suggests that individuals tend to minimize losses, by being entrapped in the action, in order for them to feel they are gaining rather than loosing in that action (Rubin and Brockner 1975). We assume here that in the context on information security, the cost of withdrawal plays an important role for understanding employees' persistence in an action, which we suspect may lead them to noncompliance behavior. The following hypothesis is thus proposed:

Hypothesis 5*: Cost of Withdrawal is positively associated with an individual's willingness to engage in activities not permitted at work.*

Prospect theory. PT explains that an individual's intention to perform an escalating behavior depends on the effect of sunk cost and their risk perceptions. PT suggests that to perform an escalating behavior individuals who have not come to experience an earlier loss are more likely to engage in risk-seeking behavior (Park et al. 2012). This phenomenon is understood as sunk cost, which relates to at least three types of investments: time, effort and money (Staw and Ross 1989). In terms of noncompliance behavior with information security policies, we posit that employees will exhibit a willingness to engage in activities not permitted at work when they realize that they have already invested a large amount of time and effort in completing a task, although they may break the information security policy of the organization. We then propose:

Hypothesis 6*: Sunk Cost is positively associated with an individual's willingness to engage in activities not permitted at work.*

The moderating role of risk perception. Risk has two scopes: risky decisions are unknowingly committed or risky decisions are deliberately committed (Straub and Welke 1998). Risk perception is a decision maker's assessment of the risk inherent in a situation. This suggests that risk perception allows employees to understand that a decision may result in risks. In our context, decisions that employees take against information security are considered risk-seeking. We consider the latter to be a deliberate violation of organization's information security policy.

In order to explain employees' risk-seeking behavior in violating their organization's information security policy, escalation of commitment theory suggests that risk perceptions help to understand employees' assessment of risks inherent in a situation (Ross and Staw 1991; Staw and Ross 1989). Based on an earlier definition of risk, decisions are considered risky if their outcome is uncertain and results in loss (Keil et al. 2000; Straub and Welke 1998). In the model presented in Figure 1, risk perceptions are articulated in terms of a moderating effect, thus we propose:

Hypothesis *7: Risk Perception will moderate the relationship between information asymmetry/cost of withdrawal/completion effect/sunk cost and willingness to engage in activities not permitted at work such that the strength of the relationship will be greater when risk perception is lower.*

The rationale of the approach proposed here is that theorizing about compliance behavior with information security policy on the bases of the three introduced escalating theories has not been investigated as such before.

METHODOLOGY

We base our study on the survey method to test the proposed model. The initial survey is developed by identifying and adapting existing measurements based on a comprehensive literature review. In order to assure validity and reliability of the developed instrument, a pretest based on data collected from 31 responses was conducted. The survey instrument was distributed online to faculty members and graduate students at our institution, some of who had experience in survey research methods. Apart from the survey response, we asked the respondents to provide us with qualitative feedback on the survey.

Based on the feedback we received, we improved the initial proposed items, by enhancing the meaning of each item so that they are clearly distinguished from one another, also by making sure that each construct is measured by multiple items, three and more respectively. We will then continue to test the items based on a pilot study. We expect to collect more than 120 responses in order to ensure higher validity and reliability based on exploratory factor analysis. We will then conduct the final study. The measurement and the structural model will be tested using partial least squares (PLS) approach by performing confirmatory factor analysis.

CONCLUSIONS AND FUTURE RESEARCH

Compliance with information security policies has become central to the success of organizations, an issue that has been partially addressed in the context of noncompliance behavior. This paper presents a conceptual framework for analysis that synthesizes constructs from the escalating theories –agency theory, approach avoidance theory, and prospect theory to address noncompliance behavior with information security policy. The proposed model in this study can be utilized to understand how escalating behavior can be considered an antecedent of noncompliance behavior with information security policies. The proposed model highlights four factors that are regarded central to investigate noncompliance behavior with information security policies, namely information asymmetry, completion effect, cost of withdrawal, and sunk cost.

Escalation behavior may be affected by the task employees' needs to accomplish, which imposes them to diverge towards noncompliance. The escalation behavior is more likely to occur when employees are aware of decisions they take, putting their organization at risk of information insecurity. The four factors reflect the decision-making of employees to actually commit their efforts in taking risky decisions. It is suggested here that employees are more disposed to violate the information security policy when they consider that their escalation behavior does not result in risks to themselves.

For future research, we envision that the proposed model based on these factors can provide empirical evidence in at least two ways. First, analysis can focus on awareness of employees of information security matters by assessing whether motivated behavior can be better specified in affecting compliance behavior, by also investigating risk-taking behavior. Second, measuring how escalating behavior factors affect noncompliance behavior may bring a theoretical redirection. Empirical evidence on escalation can help to clearly distinguish why some factors are significant or insignificant in triggering noncompliance with information security policy, by analyzing the level of risky decisions employees take.

REFERENCES

Anderson, C.L., and Agarwal, R. 2010. "Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions," *MIS Quarterly*, (34:3), pp. 613-643.

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), 87-92.

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.

Dean, D., and Webb, C. 2011. "Recovering from information overload," *McKinsey Quarterly*.

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

Fenz, S., Ekelhart, A., and Neubauer, Th. 2011. "Information security risk management: in which security solutions is it worth investing?," *Communications of the AIS*, (28:1), pp. 329-356.

Guo, K. H., Archer, N.P., and Connelly, C.E. 2011. "Understanding nonmalicious security violations in the workplace: a composite behavior model," *Journal of Management Information Systems*, (28:2), pp. 203-236.

Hagen, J. M., Albrechtsen, E., and Hovden, J. 2008. "Implementation and effectiveness of organizational information security measures," *Information Management & Computer Security*, (16:4), pp. 377-397.

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

Iivari, J., and Hirschheim, R. 1996. "Analyzing information systems development: A comparison and analysis of eight is development approaches," *Information Systems*, (21:7), pp. 551-575.

Jensen, M. C., and Meckling, W. H. 1976. "Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure", *Journal of Financial Economics* (3), pp. 305-360.

Johnson, E. M., and Goetz, E. 2007. "Embedding Information Security into the Organization," *IEEE Security Privacy Magazine*, (5:3), pp. 16-24.

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

Keil, M., Tan, B. C. Y., Wei, K-K., Tuunainen, V., and Wassenaar, A. 2000. "A Cross-Cultural Study on Escalation of Commitment Behavior in Software Projects," *MIS Quarterly*, (24:2), pp. 299-325.

Kruger, H., Drevin, L., and Steyn, T. 2010. "A vocabulary test to assess information security awareness," *Information Management & Computer Security*, (18:5), pp. 316-327.

McAfee, A. 2009. "Enterprise 2.0: New Collaborative Tools for Your Organization's Toughest Challenges," Boston: Harvard Business Press.

Park, S. Ch., Keil, M., Kim, J. U., and Bock, G-W. 2012. "Understanding overbidding behavior in C2C auctions: an escalation theory perspective," *European Journal of Information Systems*, pp. 1 -21.

Puhakainen, P., and Siponen, M. 2010. "Improving employees' compliance through information systems security training: an action research study," *MIS Quarterly*, (34:4), pp. 757-778.

Ross, J., and Staw, B. M. 1991. "Managing escalation processes in organizations," *Journal of Managerial Issues*, (3:1), pp. 15 -30.

Rubin, J., and Brockner, J. 1975. "Factors Affecting Entrapment in Waiting Situations: The Rosencrantz and Guildenstern Effect," *Journal of Personality and Social Psychology*, (31), pp. 1054-1063.

Staw, B. M, 1976. "Knee Deep in the big Muddy: A study of escalating commitment to a chosen course of action," *Journal of Organizational Behavior and Human Performance*, 16, pp. 27-44.

Staw, B. M., and Ross, J. 1989. "Understanding Behavior in Escalation Situations," *The American Association for the Advancement of Science*, (246:4927), pp. 216-220.

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

Tyler, T. R., and Blader, S. L. 2005. "Can Business Effectively Regulate Employee Conduct? The Antecedents of Rule following in Work Settings," *The Academy of Management Journal*, (48:6), pp. 1143 -1158.

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.

Warkentin, M., and Willison, R. 2009. "Behavioral and Policy Issues in Information Systems Security: The Insider Threat," *European Journal of Information Systems*, (18:2), pp.101-105.

Wolf, M., Haworth, D., and Pietron, L. 2011. "Measuring An Information Security Awareness Program," *Review of Business Information Systems*, (15:3), pp. 9-22.