2013

Assessing Self-Justification as an Antecedent of Noncompliance with Information Security Policies

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

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

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

Darek Haftor
Linnaeus University, darek.haftor@lnu.se

Information Systems: Transforming the Future

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

Proudly sponsored by

ACIS 2013 Principal Sponsor

Assessing Self-Justification as an Antecedent of Noncompliance with Information Security Policies

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

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

Izak Benbasat
University of British Columbia
Vancouver, Canada
Email: izak.benbasat@sauder.ubc.ca

Darek Haftor
Linnaeus University
Växjö, Sweden
Email: darek.haftor@lnu.se

Abstract

This paper aims to extend our knowledge about employees' noncompliance with Information Security Policies (ISPs), focusing on employees' self-justification as a result of escalation of commitment that may trigger noncompliance behaviour. Escalation presents a situation when employees must decide whether to persist or withdraw from nonperforming tasks at work. Drawing on self-justification theory and prospect theory, our model presents two escalation factors in explaining employee's willingness to engage in noncompliance behaviour with ISPs: self-justification and risk perceptions. We also propose that perceived benefits of noncompliance and perceived costs of compliance, at the intersection of cognitive and emotional driven acts influence self-justification. The model is tested based on 376 respondents from banking industry. The results show that while self-justification has a significant impact on willingness, risk perceptions do not moderate their relation. We suggest that future research should explore the roles of self-justification in noncompliance to a greater extent.

Keywords

Escalation of commitment behaviour, information security policy, noncompliance behaviour, risk perceptions, self-justification.

INTRODUCTION

While organizations greatly benefit from Information Technologies (ITs) by revolutionizing how they operate, the information security is still a major concern for them (Bulgurcu et al. 2010; Njenga and Brown 2012). As their reliance on IT grows, organizations struggle to determine the right budget for information security to ensure that their informational assets are protected (Cavusoglu et al. 2004). Furthermore, organizations wrestle with finding the right security solutions. They often resort to purely invest in security technologies (Dhillon 2007). The extant research informs us that predominantly investing in security technologies is likely to be suboptimal. Many studies emphasize that addressing socio-organizational issues anchored around the information security related behaviours of employees, who are considered the weakest link in information security (Mitnick and William 2003), has great potential to ensure security by complementing investments in security technologies (Bulgurcu et al. 2010; Dhillon and Backhouse 2001; Vance 2010; and Warkentin et al. 2011).

Developing the best strategy for information security in organizations is a challenging task, considering that the consequences of such strategies have produced disappointing results (Dhillon and Backhouse 2001; Njenga and Brown 2012). While the most attractive information security strategies have become pervasive across organizations, their success in preventing information security breaches has seldom been fruitful (Bulgurcu et al. 2010; McAfee 2009). In this respect, studies have suggested that educating employees in information security

awareness programs can help organizations alleviate challenges associated with information security (Siponen and Vance 2010; and Puhakainen and Siponen 2010). Yet, the 2010/2011 CSI Computer Crime and Security Survey reported the concern that while such programs abound, it is hard to prove that employees obey the security rules and regulations. In fact, it is no surprise to anyone that even employees who are aware of risks associated with information security and their roles to ensure information security, do not necessarily perform information security related responsibilities in their organizations. Why employees do not comply with the ISP of their organizations can be explained by the escalation behaviour, which is known in the context of project management (Keil and Mähring 2004).

Escalation is defined as an irrational act that explains how employees in organizations often get involved in a failing course of action, and reflect the tendency of not knowing whether persistence or withdrawal from that action is the best solution (Staw and Ross 1989). Research has shown that employees often become overly committed to losing courses of action in their everyday practices at work, throwing good efforts after bad (Conlon and Garland 1993; Keil et al. 2000a,b). Employees who engage in such practices are likely to engage in seemingly irrational acts, often intending to find alternative ways to overcome their obstacles (Staw and Ross 1989). It is likely that they have motivations to break the ISP of an organisation as a result of escalation.

Consider the following situation. An employee of an information-intensive organization, such as a bank or a pharmaceutical company is involved in a certain task that needs to be finished on due date. The employee has almost finished that task, but in order to complete it, he/she needs some help from a person that has expertise in that area. He/she knows that his/her organization has an explicit ISP requiring that all information in that specific task, that is confidential, should not be compromised, i.e. communicated or given away to anyone including an expert in the field within or outside the organization. He/she has to make a choice.

The noncompliance behaviour in similar situations is fairly typical. Hence, our study aims to extend the knowledge about employees' noncompliance with ISPs by understanding how employees' self-justification of noncompliance behaviour may occur as a result of their escalation of commitment. Such an understanding can be central to extend the literature on information security and to inform organizations how to strategize their information security efforts, in particular, how to encourage employees' compliance with ISPs. The focus is on escalation of commitment in banking and pharmaceutical industries that are known to be more vulnerable to exposing confidential information (Bulgurcu et al. 2010).

The rest of the paper is structured as follows. The next section presents our theoretical framework. We then introduce our research model followed by a number of hypotheses, and a description of data analyses and results. Finally, we present our conclusions, followed by some suggestions for future research.

THEORETICAL FRAMEWORK

While organizations tend to impose rules and regulations for ensuring information security, we argue that the management of information security in organizations has a life of its own. Escalation theories inform us that employees often intend to complete their tasks at any cost (Staw and Ross 1989), therefore engage in escalation behaviour, and in the process of escalation, become noncompliant with ISPs. Salancik (1977) and Staw and Ross (1989) have suggested that employees are likely to engage in escalation, because of six important factors. First is that employees' acts are explicit or unambiguous; second, their behaviour towards an act is irreversible; third, the behaviour involves a high degree of volition; fourth, the act itself is highly important for the individual; fifth, from the start the act is made public, therefore it influences the employee to continue their commitment; sixth, the act has been performed previously and intends to show that employees have the act under control.

In our study, we propose and evaluate a model to understand the effects of self-justification theory and prospect theory on noncompliance behaviour with ISP. We built upon Bulgurcu et al. (2010) and test the cost-benefit factors from the perspective of rational choice theory. Employees' noncompliance behaviour with ISPs is measured as their willingness to engage in noncompliance behaviour (hereafter WENB). We define WENB as an employee's willingness to continue working on his/her tasks even if in the process of completing the task, the employee does not follow the requirements of the ISP, thus becomes noncompliant. In other words, throughout task completion, one is at risk of not completing their task on their own, and when this occurs, one must decide whether or not to continue working on that task by engaging in activities not permitted at work, e.g. asking for the help of an expert to complete the task by revealing some confidential information. WENB suggests that employees are persistent in completing their tasks even if it means that they end up not following the requirements of the ISP. We begin by adopting constructs from escalation theories that serve as predictors in our model, in particular, self-justification theory and prospect theory. We utilize the constructs of self-justification and risk perceptions as important factors that drive employees' WENB.

Escalation of Commitment Theories

Escalation of commitment 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 escalation of commitment behaviour. 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 behaviour as a result of a deliberate decision (Keil et al. 2000b).

Self-justification theory (SJT), suggests that individuals tend to rationalize their previous behaviour by aiming to prove to others that a choice on a failing course of action is the correct decision (Staw 1976). With self-justifying behaviour, individuals also tend to rationalize the consequences of their actions, and that they have committed rationale decision-making (Fox and Staw 1979). In the context of ISP noncompliance, SJT informs us that employees exhibit WENB, because they think the task needs to be completed and not abandoned, otherwise their actions would result in accepting the loss. There are two forms of self-justification that employees use to justify their wrongdoings (Keil et al. 2000b). First, employees committing a *psychological self-justification* do so in order to prove to themselves they are correct in their actions; second, employees committing a *social self-justification* do so in order to prove to others that a possible wrongdoing is rational and that he/she is competent. According to Staw and Ross (1989), the social self-justification observed by (Keil et al. 2000a) is a typical social determinant of maintaining a commitment to a nonperforming task in order not to lose face or credibility with others. This theory is therefore important to the framework, because it facilitates a new understanding of how employees self-justify their noncompliance with an ISP in the face of negative feedback for their tasks at work. The framework focuses on the social self-justification (addressed only as self-justification), because in theory, social self-justification is proved to provide more pressure to employees than psychological self-justification.

Prospect theory (PT), explains that an individual's intention to get locked in escalation behaviour depends on the effect of risk perceptions. PT suggests that individuals who have not come to experience an earlier loss are more likely to engage in risk-seeking behaviour (Park et al. 2012). In terms of noncompliance behaviour with ISPs, employees exhibit WENB, when they realize that they have already invested a large amount of time, effort and resources in trying to complete the task, independent of their breaking of ISP. PT provides a rich framework for understanding the 'cognitive biases' that can be used to understand their influence on employees' decision making, in particular under the conditions of risks (Kahneman and Tversky, 1979). According to PT, employees exhibit two types of risk behaviour: *risk-averse* or *risk-seeking*. Risk-averse behaviour is most commonly found when employees notice a sure loss in their actions; whereas risk-seeking behaviour is most commonly found when employees have not experienced earlier losses, and therefore believe that losses may be avoided.

Research Model and Hypotheses

The central element of our proposed model is WENB. Based on escalation theories, the model in Figure 1 depicts the constructs that we test to understand if noncompliance is a cause of escalation behaviour. The model emphasizes that an employee's WENB will be determined by two escalation constructs, namely: self-justification and risk perceptions. Consistent with escalation theories, we propose that these two escalation constructs largely influence WENB. The model then suggests that self-justification is a mediating construct, which we analyse based on the constructs of perceived benefits of noncompliance and perceived costs of compliance. The model also suggests that risk perceptions moderate the effects of self-justification on WENB. Below, we further describe these constructs individually, supported by theories that have been used to design the model presented in Figure 1.

Drawing on prospect theory, we include risk perceptions as an important construct to explain WENB. Risk is defined as the potential loss or the negative outcome for an individual (Mitchell 1999). In general, risks can be categorized in terms of two scopes: risks that derive from decisions that are naively committed, or risks that derive from decisions that are deliberately committed (Straub and Welke 1998). The former is a type of risk that is not predicted, while the latter suggests that individuals predict an acceptable level of risk to engage in risky behaviour (Dowling and Staelin 1994). Risk perception is defined as a decision maker's assessment of the risk inherent in a situation. In our context, decisions that employees take in noncompliance with ISPs are considered risk-seeking. To explain employees' risk-seeking behaviour in violating the ISP, prospect theory suggests that risk perceptions help to understand employee's assessment of risks in a situation (Smith and Keil 2003).

H1: Risk perceptions moderate the relationship between self-justification and WENB such that the relationship will be weaker when risk perceptions are high.

In line with self-justification theory, the determinants of self-justification construct are perceived benefits of noncompliance and perceived costs of compliance. Consistent with rational choice theory, perceived costs and benefits will inform us how employees act when faced with choices they foresee (Bulgurcu et al. 2010). We define perceived benefits of noncompliance as the overall positive outcome of noncompliance with rules and

regulations of the ISP, such as completing the task at hand is seen more favourable or advantageous to the employee, rather than respecting the ISP that would result in withdrawing from the task. We define perceived costs of compliance as the overall perceived costs for complying with the rules and regulations of the ISP, typically driven by emotions, e.g. costs related to the inability to complete the task, which would make an employee accept the loss and lose the face in front of their organization. These costs and benefits may evidently determine the behaviour employees will exhibit when faced with difficulties during their task completion process. Figure 1 depicts these relationships.

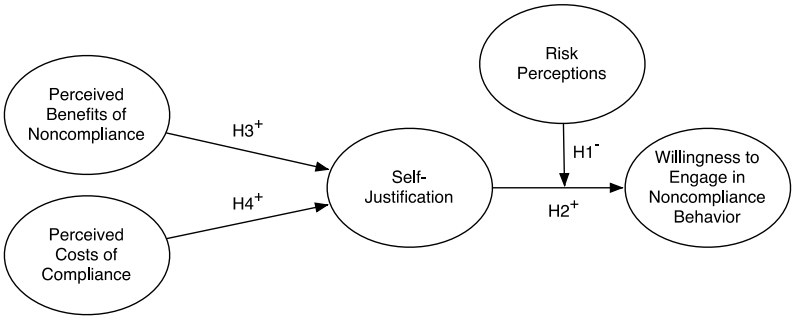

Figure 1: Research Model

According to rational choice theory, individuals act rationally, by considering the various forms of values that emerge from a rational behaviour (Becker 1993; Scott 2000). However, studies have argued that individuals do not always act rationally (Scott 2000). Facing tough choices, individuals tend to find difficulties in decision-making. Making the right decision has been studied for many decades, most notable in terms of understanding how individuals choose among the alternatives as "the optimum" (Simon 1955). A rational choice is usually considered a deliberate calculative strategy and that the individual's calculation for their rational behaviour is often shaped by rewards or punishments that one encounters (Bulgurcu et al. 2010; D'Arcy et al. 2009; Herath and Rao 2009). Earlier, we mentioned that to rationalize their previous behaviour by self-justifying, employees tend to prove to others that their choice to engage in escalation behaviour is the correct decision.

H2: Self-justification positively influences the willingness to engage in noncompliance behaviour with ISP.

In sociology, rational choice is often seen as a choice that takes a path towards rewards rather than punishments (Scott 2000). However, individuals may be inclined to take a path towards punishments or sanctions as they depend on the set of alternatives open to choice, in particular, the relationship that determines the pay-offs, most likely seeking satisfaction or goal attainment (Simon 1955). This occurs, if an individual calculates that such behaviour can indeed lead to better results of their actions, and that sanctions may even be avoided. We propose that benefits of noncompliance and costs of compliance with ISPs are likely to influence employees to self-justify their wrongdoings, to become noncompliant. We also suggest that noncompliance occurs, particularly when employees can deliberately hide information during task completion. Thus, the overall calculations of costs and benefits that determine an employee's course of action are shaped by employee's perception of potential outcomes associated with that course of action, usually by balancing the overall assessment of costs and benefits to determine the best alternative (Bulgurcu et al. 2010). Thus, we propose:

H3: Perceived benefits of noncompliance positively influence self-justification for noncompliance behaviour with ISP.

H4: Perceived costs of compliance positively influence self-justification for noncompliance behaviour with ISP.

The model presented in Figure 1 suggests that the effects of the two escalation constructs (the mediating effect of self-justification and the moderating effect of risk perceptions) on WENB are crucial to explain noncompliance behaviour. While the model does not represent direct paths from cost-benefit constructs to WENB, in order to test each of our mediation hypotheses, we examine whether the effects of each of these constructs are partially or fully mediated by the construct of self-justification.

RESEARCH METHODOLOGY

The empirical investigation relies on hypothetical scenario-based survey approach (D'Arcy et al. 2009; Siponen and Vance 2010; Vance and Siponen 2012). The survey instrument measures were based on theory and on previously utilized survey instruments to study noncompliance behaviour with ISPs (Gefen et al. 2000). Table 3 in Appendix presents the scenario and the measurement items.

The initial developed survey was first tested for content validity, construct validity and reliability (Ringle et al. 2005; Straub et al. 2004). Two rigorous stages were conducted before the survey was ready for the pilot study and the main study. Utilizing the suggestions by revising the survey according to academic and industry experts, which defined the first stage, the study continued with the second stage. Two steps were taken here. The first step was a closed card-sorting exercise (Moore and Benbasat 1991) with 5 participants (2 professionals, 2 students and 1 academic). The results showed that some of the constructs adapted from the escalation literature (which previously have not been tested in information security contexts) more specifically from Keil et al. (2000a,b) and Park et al. (2012) gave a low percentage of correct sorting. This revealed that the participants involved in the exercise had the impression that some of the constructs were too similar. These results indicated that one construct in particular should be merged or re-defined. The defined theoretical construct of Risk Perception (that relates to employees perception of the severity of the risk) was designed to influence WENB in parallel with Risk Propensity (that relates to how employees become inclined to behave in a particular way, depending on their risk-seeking and their risk-averse behaviour).

After the survey instrument was revised again, based on the card-sorting analysis, the survey was fine-tuned once again to facilitate its understanding by a wider audience as suggested by the academics, industry experts and the closed-cart sorting participants. The second step was then initiated. The revised survey was distributed online to faculty members and graduate students at an academic institution. A pre-test was conducted, based on which 31 responses were received, with some also commenting on the wording and length of the questions. These responses were both used for quantitative analysis for initial validity and reliability checks, and qualitative analysis for improving the appearance of the survey.

In the third stage, the exploratory factor analysis was performed, by conducting a pilot study at two pharmaceutical companies. An online survey was distributed to their employees, out of which 20% (n=126) responses of the targeted group were received. Using exploratory factor analysis, the initial research model and some measurement items needed slight modifications. After the pilot study was complete and resulted in a steady model for further tests, the main study was initiated.

For the main study, the sampling frame was focused on banking industry. The survey was hosted online via a web address provided by the home university, and remained active for less than a week, due to strict security regulations imposed by the banks headquarters. The distribution of the online survey was sent via an email invitation by the risk management department of the bank. The survey was designed in a way that the identity of the participants was kept anonymous, and all participants responded to the survey on voluntary basis. Among the 1,052 employees, approximately, 35.7% (n=376) responded to the survey. The participants were first asked demographic questions, followed by a scenario and a set of questions. All responses were considered reliable and there were no missing answers.

Of all the respondents, 38% were female and 62% were male. Of those, 81% stated that they have a common understanding of computers and IT, 13% reported that they have a very high knowledge of computers and IT. The sample was evenly distributed among the employees' positions, with 3% in top management, 10% in middle management, 7% were project coordinators, and the rest were bank officers. The distribution of the survey was based on voluntary respondents in order to avoid response bias. The voluntary responses and the variance presented in the control variables suggest that the participants responded randomly and that they present a reliable statistical population to estimate the characteristics for generalizability. Accordingly, the validation of the model went through several phases: it started with the development of the instrument. After an initial validation level was reached, the empirical investigation continued with pre-testing the survey, which led to the pilot study data collection and the main study data collection.

It is, however, important to mention that before data collection, the researcher has established connections with potential organizations that were willing to collaborate. The organizations that agreed to participate in this research have written special nondisclosure agreements. The data collection procedure has guaranteed that the organizations involved in this research process are kept completely confidential, while their employees, who represent the data collection as respondents to the surveys, are completely anonymous.

DATA ANALYSES AND RESULTS

The measurement and the structural model were tested using the component-based partial least squares (PLS) approach to structural equation modelling. The psychometric properties of measurement scales were evaluated and the research hypotheses were tested using the Smart-PLS software package (version 2.0.M3) (Ringle et al. 2005).

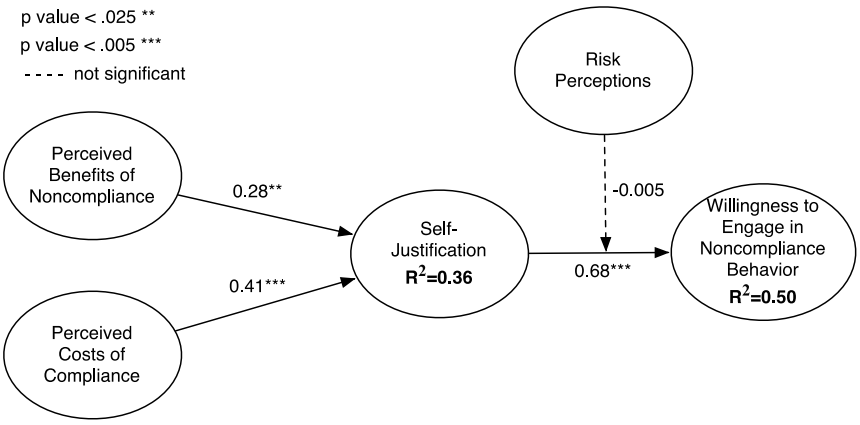

Figure 2: Structural Model Testing

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 et al. 1995). The average variance extracted (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 Appendix 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 0.70, demonstrating that all constructs have adequate reliability assessment scores (Internal Consistency and Scale Reliability) (Gefen et al. 2000). 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. Consequently, we estimated the structural model and tested the research hypotheses using PLS.

The data analysis was conducted by using the bootstrapping technique. The results of the model estimation are presented in Figure 2. The standardized path coefficients, which are based on one-tailed t-tests, show that all of the proposed hypotheses, except H1, are supported at minimum of $p<0.025$. The results show that approximately 50% of the variance is explained for WENB. As predicted, self-justification has a significant positive impact on WENB. However, we did not find significant moderating relationship of risk perceptions between self-justification and WENB. The results also show that both cost-benefit factors have significant impact on self-justification. The appendix presents our validity analysis.

CONCLUSION AND FUTURE RESEARCH

Our study highlights the importance of escalation of commitment in influencing noncompliance behaviour. Three out of four of our proposed hypotheses were supported based on the data collected from 376 respondents who work in banking industry.

Dependent on previous theoretical and empirical findings that risk perceptions are significant factors in affecting behaviour in escalation situations, our empirical tests proved the contrary. While risk perceptions should influence behaviour depending on how risk-averse or risk-seeking an employee is, our model showed no significant support in such cases. The results of our study show that the moderating factor of risk perceptions does not have a significant negative impact on WENB. While risk perceptions factor does not affect WENB, we find strong empirical support that self-justification, as an important escalation factor, has significant impact on WENB. We also find strong empirical support that self-justification is driven by perceived benefits of noncompliance and perceived costs of compliance. Our results show that these two constructs play a powerful role on WENB through self-justification.

Our theoretical framework and empirical results have important implications for security managers at organizations. The model can assist security managers to enhance the level of information security compliance in their organization. Employees' noncompliance behaviour is assumed to be a constant and that their organization is always under threat, a concern that has recently received significant attention in the literature. Rather than focusing on such a concern, the security managers can better understand their employees' WENB by assessing the increase of escalation of commitment behaviour on their running projects in their organizations. Examples of measures that could be employed include educational programs that make employees aware of the behavioural pattern with regard to escalation of commitment. We believe that educating the employees about the counter-incentive measures, e.g. tolerance for nonperforming tasks, such that organizations would tolerate nonperforming tasks due to security reasons, may encourage compliance in the future.

Controlling escalation of commitment behaviour is not an easy task. Yet, we suggest that organizations should focus on decreasing escalation of commitment behaviour, which we see as a viable solution to also decreasing noncompliance behaviour. Examining the constructs that influence noncompliance as a result of escalation of commitment behaviour can guide security managers to ensure compliance. For instance, organizations can effectively re-design information security policies for their employees, by carefully focusing on informing the employees that the escalation of commitment is discouraged, whereas, the benefit of reporting project problems is encouraged, as it would allow organizations to find assistance to their employees to overcome their identified problems (without minimal consequences for the employee and managers).

Future theory should clearly define the use of risk perceptions, because employees' behaviour, be that noncompliance behaviour or other, may be influenced by more powerful factors that cause the risks to remain unimportant. Also, it is essential to notice that the strength of our proposed model shows that self-justification has a powerful explanatory force to determine WENB, however, it has partial mediation effect on the perceived benefits of noncompliance and full mediation on the perceived costs of compliance.

Although, we believe that the current model captures a reasonable explanation of noncompliance behaviour as a result of escalation of commitment, an important limitation of our study is that our model does not measure other escalation factors that may shed light on employees' noncompliance behaviour. Our future model will focus on addressing factors such as "completion effect", for which we believe that the closer to completing the task, the higher employees' noncompliance behaviour, and "sunk cost", for which we believe that the more sunk time, efforts or money, the more employees engage in noncompliance behaviour.

This study tests an initial model that explains noncompliance behaviour from the escalation of commitment perspective. We believe that this is the first study that initiated the examination of noncompliance behaviour as a reason of escalation behaviour. We therefore intend to extend our study by using other theoretical constructs at the intersection of cognitive and motivational activities, to better understand why employees make a sudden shift from compliance behaviour to noncompliance behaviour in a task-related context.

REFERENCES

Becker, G. S. 1993. "Nobel Lecture: The Economic Way of Looking at Behaviour", *Journal of Political Economy*, (101:3), pp. 385–409.

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., 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), pp. 65-75.

Conlon, D. E., and Garland, H. 1993. "The Role of Project Completion Information in Resource Allocation Decisions", *Academy of Management Journal*, (36:2), pp. 402–413.

Dhillon, G. 2007. "*Principles of Information Systems Security: text and cases*, NY: John Wiley and Sons.

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

Dowling, G., and Staelin, R. 1994. "A Model of Perceived Risk and Intended Risk- Handling Activity", *Journal of Consumer Research*, (21), pp. 119–134.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach", *Information Systems Research*, (20:1), pp. 79–98.

Fox, F. V., and Staw, B. M. 1979. "The Trapped Administrator: Effects of Job Insecurity and Policy Resistance upon Commitment to a Course of Action", *Administrative Science Quarterly*, (24), pp. 449-471.

Gefen, D., Straub, D., and Boudreau, M. 2000. "Structural Equation Modeling and Regression: Guidelines for Research Practice", *Communications of the Association for Information Systems*, (4), pp. 1-79.

Herath, T., and Rao, H. 2009. "Encouraging Information Security Behaviours in Organizations: Role of Penalties, Pressures and Perceived Effectiveness", *Decision Support Systems*, (47), pp. 154-165.

Kahneman, D., and Tversky, A. 1979, "Prospect Theory: An Analysis of Decision Under Risk", *Econometrica: Journal of the Econometric Society*, 47(2), pp. 263–292.

Keil, M., Im, G. P., and Mähring, M. 2007. "Reporting Bad News on Software Projects: the Effects of Culturally Constituted Views of Face-Saving", *Information Systems Journal*, (17), pp. 59-87.

Keil, M., Mann, J., and Rai, A. 2000a. "Why Software Projects Escalation: An empirical analysis and test of four theoretical models", *MIS Quarterly*, (24:4), pp. 631-664.

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

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

Mitnick, K. D., and William, S. L. 2003. "*The Art of Deception: Controlling the Human Element of Security*", NY: John Wiley & Sons.

Mitchell, V. W. 1999. "Consumer Perceived Risk: Conceptualisations and Models", *European Journal of Marketing*, (33), pp. 163-195.

Moore, G. and Benbasat, I. 1991. "Development of an Instrument to Measure the Perceptions of Adopting and Information Technology Innovation", *Information Systems Research* (2:3), pp. 192-222.

Njenga, K., and Brown, I. 2012. "Conceptualising Improvisation in Information Systems Security", *European Journal of Information Systems*, (21), pp. 592-607.

Park, S. C., Keil, M., Kim, J. U., and Bock, G.-W. 2012. "Understanding Over-Bidding Behaviour in C2C Auctions: an Escalation Theory Perspective", *European Journal of Information Systems*, (21), pp. 643-663.

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.

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

Salancik, G. 1977. "Commitment and the Control of Organizational Behaviour and Belief", in B. M. Staw and G. Salancik, eds, "*New Directions in Organizational Behaviour*", Chicago: St. Clair Press, pp. 1-54.

Scott, J. 2000. "Rational choice theory", in G. Browning, A. Halcli and F. Webster, eds, "*Understanding Contemporary Society: Theories of the Present*", Thousands Oaks, CA: Sage Publications.

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

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.

Smith, H., and Keil, M. 2003. "The Reluctance to Report Bad News on Troubled Software Projects: a Theoretical Model", *Information Systems Journal*, (13), pp. 69-95.

Staw, B. 1976. "Knee-deep in the big muddy: A study of escalating commitment to a chosen course of action", *Organizational Behaviour and Human Performance*, (44), pp. 27-44.

Staw, B. M., and Ross, J. 1989. "Understanding Behaviour in Escalation Situations, Science, (246:4927), pp. 216-220.

Straub, D., Boudreau, M., and Gefen, D. 2004. "Validation Guidelines for IS Positivist Research", *Communications of the Association for Information Systems*, (13), pp. 380-427.

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

Vance, A. 2010. "*Why do employees violate IS security policies? Insights from Multiple Theoretical Perspectives*", Doctoral thesis, Oulu University.

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., Johnston, A. C., and Shropshire, J. 2011. "The Influence of the Informal Social Learning Environment on Information Privacy Policy Compliance Efficacy and Intention", *European Journal of Information Systems*, (20), pp. 267–284.

APPENDIX – VALIDITY ANALYSIS

Table 1. Composite Reliability, AVE, and Latent Variable Correlations

	CR	AVE	1	2	3	4	5	6
1. Perceived Benefits of Noncompliance	0.98	0.94	**0.97**					
2. Perceived Costs of Compliance	0.90	0.75	0.48	**0.87**				
3. Risk Perceptions	0.85	0.66	0.26	0.38	**0.81**			
4. Self-Justification	0.89	0.72	0.48	0.55	0.41	**0.85**		
5. WENB	0.96	0.89	0.59	0.64	0.34	0.71	**0.94**	
6. Risk Perceptions * Self Justification	0.97	0.79	0.41	0.59	0.79	0.78	0.58	**0.99**

- **CR** = Composite Reliability; **AVE** = Average Variance Extracted
- Diagonal elements display the square root of AVE for factors measured with reflective items.

Table 2. Cross Loadings

	1	2	3	4	5	6
1. a	**0.97**	0.46	0.27	0.45	0.58	0.41
1. b	**0.98**	0.45	0.23	0.47	0.56	0.39
1. c	**0.97**	0.49	0.27	0.51	0.62	0.43
1. d	**0.95**	0.44	0.25	0.42	0.51	0.37
2. a	0.45	**0.95**	0.38	0.54	0.63	0.56
2. b	0.39	**0.69**	0.18	0.24	0.33	0.27
2. c	0.42	**0.93**	0.38	0.56	0.62	0.61
3. a	0.19	0.27	**0.81**	0.28	0.21	0.61
3. b	0.28	0.40	**0.91**	0.45	0.38	0.76
3. c	0.13	0.22	**0.71**	0.18	0.18	0.51
4. a	0.29	0.31	0.27	**0.70**	0.51	0.51
4. b	0.44	0.51	0.36	**0.90**	0.70	0.70
4. c	0.47	0.55	0.40	**0.93**	0.66	0.74
5. a	0.58	0.62	0.33	0.67	**0.94**	0.53
5. b	0.50	0.65	0.36	0.70	**0.95**	0.63
5. c	0.59	0.54	0.28	0.64	**0.94**	0.47
6. a1	0.37	0.48	0.74	0.68	0.45	**0.89**

6. b1	0.35	0.46	0.70	0.66	0.47	**0.82**
6. c1	0.34	0.41	0.66	0.59	0.43	**0.77**
6. a2	0.32	0.50	0.68	0.69	0.46	**0.90**
6. b2	0.35	0.57	0.66	0.76	0.59	**0.90**
6. c2	0.35	0.53	0.72	0.69	0.56	**0.90**
6. a3	0.38	0.55	0.71	0.69	0.49	**0.93**
6. b3	0.42	0.60	0.72	0.72	0.58	**0.96**
6. c3	0.43	0.58	0.75	0.69	0.57	**0.92**

Table 3. Scenario, Constructs, Measurement Items, Mean and Standard Deviation (STD)

Scenario			
Assume that you have been working on a certain project which needs to be finished by a deadline. The deadline is approaching and you almost finished the project except a particular task which you do not know how to accomplish. In order to complete the project, that particular task has to be completed. You know an expert who can help you complete that task. But, some confidential customer information will be exposed to the expert while getting help from him/her. You know that your organization has an explicit information security policy stating that no customer information shall be exposed (disclosed, divulged, given away, or given access) to anyone outside the area of responsibility.			
Constructs	Items	Mean	STD
1.Perceived Benefits of Noncompliance	Completion of the task by getting external help would be favorable to me, even if I have to break the rules of the information security policy.	1.20	**0.77**
	Completion of the task by getting external help would result in benefits to me, even if I have to break the rules of the information security policy.	1.17	0.69
	Completion of the task by getting external help would create advantages for me, even if I have to break the rules of the information security policy.	1.17	0.70
	Completion of the task by getting external help would provide gains to me, even if I have to break the rules of the information security policy.	0.17	0.71
2.Perceived Costs of Compliance	Association with an unsuccessful task would have an adverse effect on my image in the organization.	3.71	2.32
	Association with an unsuccessful task would have an adverse effect on my chance for advancement in the organization.	3.79	2.32
	Association with an unsuccessful task would have an adverse effect on my annual performance evaluation.	4.0	2.33
3.Risk Perceptions	I believe there are no big risks associated with my breaking of the rules of the information security policy during the task.	1.33	1.13
	I believe that my breaking of the rules of the information security policy during my task has a low probability of harming my organization.	1.33	1.06
	I believe there are very little risks related to information security in continuing to work on my task.	1.61	1.46
4.Self-Justification	To stop working in the middle of my task is not the right choice for me, even if I don't follow the information security policy.	1.60	1.42
	I think it is the right choice to continue working on my task, even if I don't follow the information security policy.	1.21	0.75

	I feel that my task should not be stopped once it is initiated, even if I don't follow the information security policy.	1.22	0.75
5. WENB	I keep working on my task by getting help from the expert because it is necessary, even if I don't follow the information security policy.	1.21	0.70
	I keep working on my task by getting help from the expert because it is important, even if I don't follow the information security policy	1.22	0.74
	I keep working on my task by getting help from the expert because it is beneficial, even if I don't follow the information security policy.	1.24	0.82