Escalation of commitment as an antecedent to noncompliance with information security policy

Miranda Kajtazi
Department of Informatics, Lund Universitet Ekonomihogskolan, Lund, Sweden and Department of Informatics, Orebro Universitet Handelshogskolan, Orebro, Sweden

Hasan Cavusoglu and Izak Benbasat
University of British Columbia Sauder School of Business, Vancouver, British Columbia, Canada, and

Darek Haftor
Uppsala Universitet Foretagsekonomiska Institutionen, Uppsala, Sweden

Received 8 September 2017
Revised 5 February 2018
Accepted 7 February 2018

Abstract

Purpose – This study aims to identify antecedents to noncompliance behavior influenced by decision contexts where investments in time, effort and resources are devoted to a task – referred to as a task unlikely to be completed without violating the organization's information security policy (ISP).

Design/methodology/approach – An empirical test of the suggested relationships in the proposed model was conducted through a field study using the survey method for data collection. Pre-tests, pre-study, main study and a follow-up study compose the frame of our methodology where more than 500 respondents are involved across different organizations.

Findings – The results confirm that the antecedents that explain the escalation of commitment behavior in terms of the effect of lost assets, such as time, effort and other resources, give us a new lens to understand noncompliance behavior; employees seem to escalate their commitments to the completion of their tasks at the expense of becoming noncompliant with ISP.

Research limitations/implications – One of the key areas that requires further attention from this study is to better understand the role of risk perceptions on employee behavior when dealing with value conflicts. Depending on how risk-averse or risk seeking an employee is, the model showed no significant support in either case to influence their noncompliance behavior. The authors therefore argue that employees' noncompliance may be influenced by more powerful beliefs, such as self-justification and sunk costs.

Practical implications – The results show that when employees are caught in tasks undergoing difficulties, they are more likely to increase noncompliance behavior. By understanding better how project obstacles result in such tasks, security managers can define new mechanisms to counter employees' shift from compliance to noncompliance.

Social implications – Apart from encouraging compliance with enforcement mechanisms (using direct behavioral controls like sanctions or rewards), indirect behavior controls may also encourage compliance. The authors suggest that the ISPs should state that the organization would take positive actions toward task completion and help their employees to resolve their problems quickly.

Originality/value – This study is the first to tackle escalation of commitment theories and use antecedents that explain the effect of lost assets, such as time, effort and other resources can also explain noncompliance with ISP in terms of the value conflicts, where employees would often choose to forego compliance at the expense of finishing their tasks.

Keywords Prospect theory, Information security policy, Approach avoidance theory, Employee's noncompliance behaviour, Escalation of commitment behaviour, Self-justification theory

Paper type Research paper

Information & Computer Security
Vol. 26 No. 2, 2018
pp. 171-193
© Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-09-2017-0066

1. Introduction

Today, securing organization's information is at the top of the executive agenda of many organizations. Despite growing emphasis on information security strategies, information security breaches in organizations continue to occur (Bulgurcu *et al.*, 2010; Dhillon and Backhouse, 2001; Herath and Rao, 2009a; Teh *et al.*, 2015). Organizations find it difficult to prioritize investments in information security (Hsu *et al.*, 2012) as there are many security solutions ranging from technological (Cavusoglu *et al.*, 2004) to socio-organizational approaches (Siponen and Vance, 2010). While technological developments have revolutionized the way organizations secure their information, employees' tendency to violate their organizations' information security policies (ISPs) remains problematic (Herath and Rao, 2009b; Teh *et al.*, 2015; Vance and Siponen, 2012).

This research aims at identifying antecedents to noncompliance influenced by decision contexts where investments in time, effort and resources are devoted to a task that experiences difficulties, thus may end up in a failing course of action (Staw, 1976; Staw and Ross, 1989). In such contexts, employees facing an obstacle have to do a trade-off between failure to accomplish the task and overcoming the obstacle with an ISP violation. This particular trade-off situation explains the phenomenon of value conflicts in its core, when frequently, information security values and work values present a conflictual situation (Hedström *et al.*, 2011; Karlsson *et al.*, 2017), thus leading employees to trade-off between the two, often choosing to have the work done over security (Kolkowska and De Decker, 2012).

When confronted with such situations, one of the most challenging decisions that an employee has to make is whether to abandon a task that is difficult to complete without violating the ISP or persist on it. As clearly identified in the extant literature, the normative beliefs regarding the ISP noncompliance can help prevent such policy violations (Bulgurcu *et al.*, 2010; Herath and Rao, 2009b). Yet, the literature is silent about the impact of self-justification, completion effect and sunk costs on employees' willingness to engage in noncompliance behavior. Therefore, it is not clear if these factors promoting noncompliance overwrite the employees' risk perceptions that would otherwise prevent noncompliance with ISP. This study does not only expand our theoretical understanding of noncompliance but also provides practical guidance to help organizations strategically tackle employees' noncompliance with ISPs. We focus on noncompliance in banking, pharmaceutical and IT – industries that are known to be more vulnerable to the exposure of confidential information (Bulgurcu *et al.*, 2010) and that consider information security practices as essential for their business.

The rest of the paper is organized as follows. Section 2 presents prior literature on information security and highlights the gap that this study fills in. Section 3 reviews the theories that explain escalation of commitment, introduces our research model and outlines our hypotheses. Section 4 provides a description of data analysis and results. The paper concludes with the theoretical and practical implications of our study and suggestions for future research.

2. Prior literature on information security

Prior research on information security has clearly indicated that to improve information security, organizations must establish security control mechanisms, one of which is the human factor (Cavusoglu *et al.*, 2015; Ifinedo, 2014; Willison and Warkentin, 2013).

Studies that directly or indirectly tackle the human factor in relation to ISPs can be classified into two groups. Studies in the first group focus on motivational factors of employees to comply with their organizations' ISPs and identify antecedents to both compliance and noncompliance behavior (Herath and Rao, 2009a, 2009b; Hu *et al.*, 2011;

Ifinedo, 2014; Johnston and Warkentin, 2010). Studies in the second group focus on how to design effective ISPs (Baskerville and Dhillon, 2008; Thomas and Dhillon, 2011).

The first stream of research is based on the premise that employees are often the weakest link in information security and therefore a major hurdle in achieving an organization's information security (Bulgurcu *et al.*, 2010; Ifinedo, 2014; Siponen *et al.*, 2009). It shows that factors such as rewards and sanctions provide external motivation for compliance, although employees' internal motivation is the major influence on noncompliance (Tyler and Blader, 2005). For instance, Ifinedo (2014) shows that social bond improves ISP compliance. Furthermore, it shows that employees frequently engage in noncompliance behavior because organizations lack effective security awareness programs or because ISPs are not enforced by the organization (Herath and Rao, 2009b; Bulgurcu *et al.*, 2010; Puhakainen and Siponen, 2010; Siponen and Vance, 2010).

The second group of studies focuses explicitly on the design and implementation of ISPs in organizations. Studies by Baskerville and Dhillon (2008) and Thomas and Dhillon (2011) suggest that organizations lack the competency to design functional and effective ISPs that conform to their strategic and business goals, because the design of custom-fit and flexible security solutions is not yet a reality in the organization.

Our study aligns with the first research stream, which explores compliance and noncompliance behavior in the context of rational choice (Bulgurcu *et al.*, 2010), deterrence (D'Arcy *et al.*, 2008) or fear appeals (Johnston and Warkentin, 2010). We aim to show that factors leading to escalation, which is considered a relatively frequent problem in organizations (Park *et al.*, 2012), can also explain noncompliance with the ISP.

This study is important for at least two reasons. First, although employees' ISP compliance has been investigated in an array of studies (Johnson and Goetz, 2007; Pahnila *et al.*, 2007; D'Arcy *et al.*, 2008; Herath and Rao, 2009b; Bulgurcu *et al.*, 2010; Vance and Siponen, 2012; Karlsson *et al.*, 2017), the novelty of our study is that it investigates factors rooted in theories that explain escalation of commitment behavior (ECB), which we inherit as antecedents to noncompliance behavior. Second, while these theories have been discussed in the context of information security in a few studies (Bulgurcu *et al.*, 2010; Chen *et al.*, 2011; D'Arcy *et al.*, 2008; Holmqvist and Pessi, 2006; Straub and Welke, 1998), these theories have not been used in the context of ISP compliance.

3. Theoretical framework

In this study, we consider that four theories can bring new insights into our understanding of noncompliance behavior: self-justification theory, prospect theory, approach avoidance theory and rational-choice theory.

(1) *Self-justification theory (SJT)* suggests that individuals tend to rationalize their behavior by attempting to convince others that their persistence in a failing course of action is the correct decision (Staw, 1976). It argues that individuals escalate their commitment to a failing course of action to self-justify their prior decisions resulting in a fully failed action. In the context of ISP noncompliance, SJT suggests that employees exhibit willingness to engage in noncompliance behavior (WENB) because abandoning the task would have negative consequences.

(2) *Approach avoidance theory (AAT)* posits that ECB results when driving forces that encourage persistence outweigh restraining forces that encourage abandonment. It also suggests that the cost of persistence is often counter-balanced by the driving forces of goal attainment, the cost of withdrawal and the proximity to the goal (Keil *et al.*, 2000). AAT proposes the completion effect: a type of motivation for an

individual to achieve a goal, especially as the individual gets closer to that goal. In the context of noncompliance behavior, the construct of completion effect suggests that when tasks are near completion, an employee's WENB increases.

(3) *Prospect theory (PT)* explains that an individual's intention to be locked in escalation of commitment depends on the effect of sunk cost and their risk perceptions. PT suggests that individuals who have not experienced an earlier loss are more likely to engage in risk seeking, therefore ECB (Park *et al.*, 2012). In terms of noncompliance with ISPs, employees exhibit WENB when they realize that they have already invested substantially in a task.

We propose an integrative model based on the above three ECTs. We also use the rational choice theory, in line with Bulgurcu *et al.* (2010), to complement the examination and explanation of this complex phenomenon of employees' noncompliance with ISP.

(1) *Rational choice theory (RCT)* underlines the cost and benefit trade-offs that the individual considers before deciding among alternatives. Rational decision-making is usually considered a deliberate calculative process and that process is often shaped by rewards or punishments that one encounters (Bulgurcu *et al.*, 2010; D'Arcy *et al.*, 2008; Herath and Rao, 2009b). Therefore, factors rooted in the RCT should explain the notion of self-justification. Consistent with Bulgurcu *et al.* (2010), from RCT perspective, we posit that an employee self-justifies her noncompliance decision based on balancing the costs and benefits that would be incurred as a result of her choices.

3.1 Research model and hypotheses

The central element of our research model (Figure 1) is the WENB. Our model posits that WENB is influenced by three constructs: self-justification, sunk cost and risk perception. Theoretically, we rationalize that self-justification is influenced by the consequences of costs and benefits, whereas sunk cost is influenced by the completion effect.

Prospect theory suggests that risk perception helps to understand employees' assessments of the risks inherent in a situation (Smith and Keil, 2003). It also suggests that employees will become risk-seekers when they believe investment in a failing venture holds

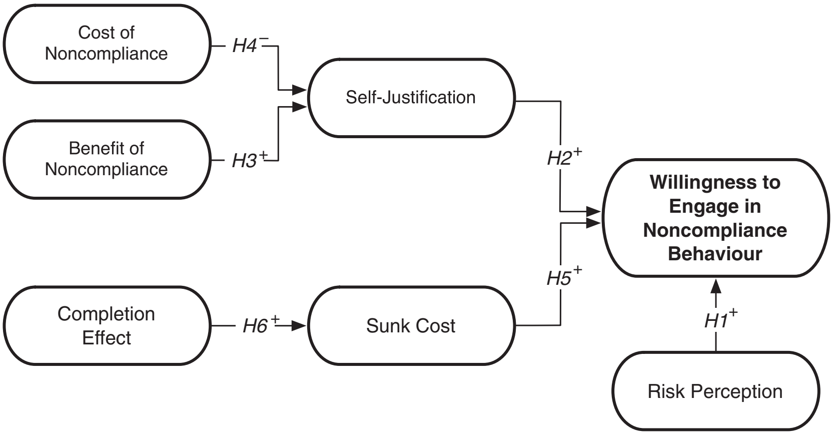


Figure 1.
A model of the antecedents to explain WENB

the promise of making the venture successful (Smith and Keil, 2003). In the compliance context, if an employee assesses that the obstacle possesses a risk to the completion of the task, he becomes more of a risk-seeker and engages in noncompliance with ISP to secure the completion of the task. Given that, risk perception is likely to affect employees' WENB.

H1. Risk perception positively influences the WENB with ISP.

When an employee uses self-justification to rationalize a previous judgement that led to the obstacle that prevents him from completing a task, he will try to convince others that his choice to engage in noncompliance with the ISP is the correct decision. Therefore, we propose:

H2. Self-justification positively influences the WENB with ISP.

In our context, we argue that the determinants of self-justification for noncompliance behavior are cost of noncompliance and benefit of noncompliance (Bulgurcu *et al.*, 2010). We define cost of noncompliance as the overall negative outcomes of not complying with ISP. Such costs are incurred when employees' inability to complete the task on their own results in their sharing protected information with others and would also include punishment, which might be exercised by the organization. Increasing employees' awareness of committing a positive behavior may reduce the frequency of negative behavior (D'Arcy *et al.*, 2008). Incurred costs as a result of a wrongdoing may prevent a future irrational behavior. While incurred costs have shown to positively affect ISP compliance, critics argue that enforcement using such mechanisms may not always affect individual's compliance with ISP, in particular when employees believe that they can get away with a wrongdoing (Pahnila *et al.*, 2007).

The other aspect of self-justification is benefits that will be obtained when the task is accomplished. We define benefit of noncompliance as the overall positive outcomes of not complying with the ISP. The direct positive consequence of noncompliance is the benefits, which accrue from the completion of the task despite the violation of ISP. We believe it is more likely that an employee will justify a wrongdoing for personal benefit than adhere to the ISP for the benefit of the organization. Therefore, we propose:

H3. Cost of noncompliance negatively influences self-justification for noncompliance behavior with ISP.

H4. Benefit of noncompliance positively influences self-justification for noncompliance behavior with ISP.

Prospect theory posits that an individual's risk-taking tendencies are influenced by the uncertainties involved in the decision (Bulgurcu *et al.*, 2010). Obstacles during the progress of a task would necessitate a decision to persist in or abandon the task. The perception that there is too much invested in the task to withdraw from it (i.e. sunk cost) leads decision-makers to adopt a negative frame, which typically triggers risk-seeking behavior. Prospect theory also proposes that individuals locked into a failing course of action view themselves to be in the domain of losses. Conlon and Garland (1993) argue that in such situations, individuals become loss averse and prefer allocating additional resources, in the hope of turning the situation around rather than accept the loss. In the noncompliance context, we suggest that an employee would rather share classified information with an unauthorized expert rather than withdrawing from the task and admitting the loss. Thus, we propose:

H5. Sunk cost positively influences the WENB with ISP.

While sunk cost and completion effect may be viewed as similar concepts, they are treated as separate ones. Conlon and Garland (1993) note that ECB, as measured by means of sunk cost, can be influenced by the completion effect, which represents the proximity to the goal. They also posit that individuals are influenced by the benefits they can receive in the future, considering the sunk cost effect for a goal substitution. However, Keil *et al.* (1995) argue that sunk cost may have a more pronounced impact on ECB than the completion effect. Approach avoidance theory also informs us that the motivation to achieve a certain goal increases, as an individual gets closer to completion of their activities (Conlon and Garland, 1993). As the issue of whether sunk cost or completion effect is more powerful has not yet been resolved, studies continue to use both constructs in measuring escalation of commitment (Park *et al.*, 2012). In our study, we also include both constructs, by proposing sunk cost as a mediator of completion effect on WENB. To motivate this relationship, in terms of prospect theory, individuals tend to take more risks on investment decisions when they find themselves in losing situations, in particular when they have the impression that task completion is close (Keil *et al.*, 2000). This condition drives individuals to make new investments, believing that this will turn the situation around (Staw and Ross, 1989). We therefore suggest that the closer an individual gets to completing a task, the more the individual will perceive sunk cost. Thus, we propose:

H6. An employee’s level of completion effect positively influences sunk cost.

The model presented in Figure 1 does not propose direct paths from cost-benefit constructs and the completion effect construct to WENB. However, to test each of our mediation hypotheses, we examine whether the effects of these constructs are partially or fully mediated by the constructs of self-justification and sunk cost.

4. Research methodology

An empirical test of the suggested relationships in the proposed model was conducted through a field study using the survey method for data collection.

We developed a scenario to put survey respondents in a context where during the process of completing their specific tasks, they might become subject to noncompliance behavior with ISPs. While the scenario presented in Scenario in the Appendix is hypothetical, it represents a potential context-specific situation upon which participants were asked to find themselves in.

4.1 Survey development

Our survey was derived from previously used related surveys and was initially tested for content validity, construct validity and reliability; however, it is new and untested before (Gefen *et al.*, 2000; Straub, 1989). The survey underwent a rigorous three-stage development process before it was deemed ready for use in the main data collection.

In the first stage, we developed a draft survey adapted from existing instruments based on a comprehensive literature review, as suggested by Straub (Straub, 1989). This draft survey was then pre-tested by means of open-ended discussions with an assessment by seven experts, including academics in information systems, management and behavioral sciences. Most were specialists in positivist methodology. The experts were contacted largely via e-mail. Discussions with the experts were quite intensive until a level of agreement was reached about the theoretical and practical design of the survey. Based on their suggestions, some revisions were made to the wording of the items and the scenario description to improve clarity.

In the second stage, the first step was a closed card-sorting exercise (Moore and Benbasat, 1991) with five people: two professionals, two students and one professor. The results showed that some of the constructs [adapted from the escalation literature (Keil *et al.*, 2000; Park *et al.*, 2012) and previously tested in information security contexts] were associated with a low percentage of correct sorting. This implied that these constructs were too similar and some should be merged or re-defined. We revised the survey based on these results. In the second step, the revised survey was distributed online to faculty members and graduate students at our institutions, whom had experience in survey research methods. We conducted a pre-test and received 31 responses from faculty members, with some also commenting on the wording and length of the questions. These responses were used for quantitative analysis for initial validity and reliability checks, as well as for qualitative analysis, to improve the appearance of the survey. Cronbach's alpha was used to assess the reliability of our initial measurements and revealed that all items exceeded the threshold of 0.7 for reliability (Gefen *et al.*, 2000).

In the third stage, we continued to perform the exploratory factor analysis by conducting a pilot study at two pharmaceutical companies. We distributed the online survey and 20 per cent (n = 126) of the invitees responded. The validity and reliability of the measurement items were carefully examined based on the 126 responses, with no missing answers. Based on our exploratory factor analysis of the data, some measurement items were further modified: two of five original items in the construct of sunk cost were dropped; and one item in the construct of self-justification was revised because some respondents interpreted the scale as reversed. Then, the results of convergent and discriminant validity indicated that the scenario and the measurement items were suitable and the survey was ready to use for the main data collection. Table AI presents the details.

4.2 Subject pool and main data collection

For the main data collection, the finalized survey was sent to two banks in a European country. One bank had about 60 branches and more than 1,000 employees, while the other bank had about 30 branches and more than 600 employees. From a scientific perspective, we saw these two banks as homogeneous with regard to security practices. Their security departments estimated that all of their employees were capable of responding to the survey. The survey was hosted online at a Web address provided by the home university of a co-author and remained active for approximately a week because of organizational regulations imposed by the banks' headquarters. The invitation to participate in the online survey was e-mailed by the risk management department of the banks to all employees. Participants responded on a voluntary basis and the identity of the participants was kept anonymous.

Among the 1,702 employees in the two banks, approximately 26 per cent (n = 439) responded to the survey, with no missing answers. Table I shows the demographics for our sample. Of all the respondents, 42 per cent were female and 58 per cent were male. Of the total, 80 per cent stated that they have a common understanding of computers and information technology, while 15 per cent stated that they have a very high knowledge of computers and information technology. The remaining 5 per cent showed that they have a basic understanding of computers and information technology. The sample was distributed among the employees' positions as follows: 7 per cent in higher management, 11 per cent in middle management, 6 per cent as project coordinators and the remaining 76 per cent as bank officers.

We also checked for biased responses, such as all questions marked 1 or 7 on the Likert scale, which we did not discover. We also checked for the non-response bias, based on the control variables; no significant differences were found.

Table I.
Sample demographics

Items	Category	Frequency	Ratio (%)
Gender	Female	184	41.91
	Male	255	58.08
Age	Under 20	–	–
	20-29	181	41.23
	30-39	224	51.02
	40-49	31	7.06
	50-59	3	0.6
	60 and above	–	–
Position	Managerial	30	6.83
	Middle management	47	10.7
	Coordinators	30	6.83
	Officers	332	75.62
Knowledge of Computers and IT	Very low	1	0.2
	Familiar	22	5.01
	Common understanding	350	79.72
	Very high	66	15.03

5. Data analysis and results

The measurement model presented in Figure 1 was designed to be reflective with all its constructs. Based on convergent and discriminant validity, the model was tested using structural equation modelling (Straub *et al.*, 2004). Our study used the component-based partial least squares (PLS) approach to evaluate the psychometric properties of the survey by testing the proposed hypotheses (Ringle *et al.*, 2005).

The use of PLS in our study was deemed appropriate for two reasons. First, the PLS technique examines the proposed model and its structural paths by ignoring other covariance that are not explicitly stated in the model (Straub *et al.*, 2004). This method is particularly useful for estimating the proposed relationships in an exploratory fashion and for theory building. Second, PLS is regarded more suitable when the purpose of the structural model is to predict rather than to test well-established theory (Chin, 1998). In our study, adapting three factors from theories that explain ECB to explain noncompliance with the ISP is new; to the best of our knowledge, these theories have not been previously used to predict noncompliance with ISP.

The use of PLS in estimating the proposed model was conducted in two stages: the assessment of the measurement model by conducting reliability and the validity of the findings and the assessment of the structural model.

The validation of the measurement model was achieved by assessing the convergent validity and discriminant validity. To test convergent validity, we first assessed the individual item reliability by examining the loadings of the measurement items on their corresponding construct. All the item loadings should be significant and exceed 0.70 (Chin, 1998). All measurement items were significant at $p < 0.01$ and were kept for further analysis (Scenario in Appendix). We then performed a bootstrap analysis with 1,000 resamples and examined the *t*-values of the item loadings. The *t*-statistics showed significance level of $p < 0.01$ (Table AII). This significance shows strong convergent validity results. We then continued to assess the composite reliability of the constructs (Table AIII). Accordingly, all composite reliabilities were greater than 0.70 and had the recommended peak. The measurement items of all constructs had adequate reliability; thus, all their measures were kept for testing the structural model. Similarly, we also tested the average variance extracted (AVE). The AVE values of all the constructs exceeded the minimum recommended value of 0.50, indicating that the items further satisfied the convergent validity tests. We also calculated the Cronbach's alpha scores. Similar to composite reliability, all Cronbach's alpha scores are recommended to be above the 0.70 score. Our constructs had adequate reliability assessment scores with Cronbach's alpha higher than 0.70.

The results for discriminant validity for our proposed model are presented in Tables AIV and AV. In principle, for discriminant validity, measurement items should be distinct from other constructs, but must load high on their own construct (Chin, 1998), which was the case in our study. Thus, in the second test, the AVE scores for all the constructs, which must be greater than the minimum value of 0.50, indicated that our measurement items satisfied this condition. Discriminant validity is assessed by comparing the square root of AVE for each construct with the other correlation scores in the correlation matrix (Table AIII).

We also performed factor analysis to check whether all the items that loaded highly on their own construct, but not highly on the other constructs (Table AIV). As recommended, the item loadings on their own constructs were higher than 0.7 and were at least 0.1 less on their loadings on other constructs. The results thus satisfied the criteria.

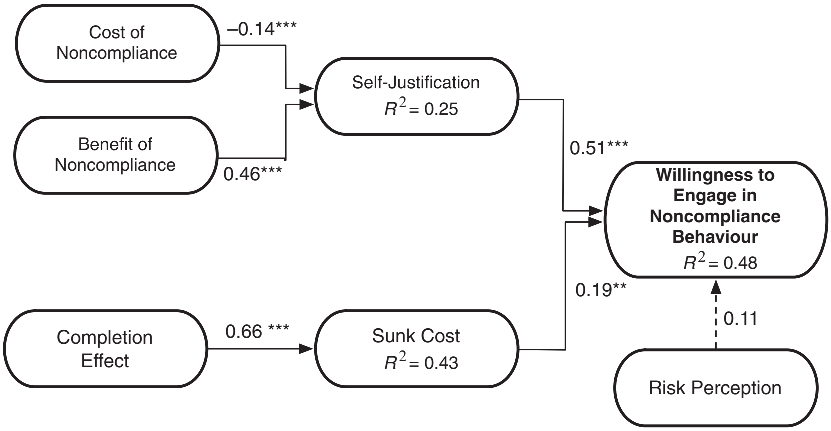
Considering that this study measures the independent and dependent variables in the same survey, there is a potential for common method bias in our results. The variables are one of the main sources of measurement error, in particular when it comes to systematic variance (Podsakoff *et al.*, 2003). We therefore considered the approach suggested by Podsakoff *et al.* (2003), later applied by Liang *et al.* (2007) method to determine whether common method bias was of concern in our study. Our structural model includes a latent method factor, and each indicator is specified for it to be determined by its substantive construct, the method factor and measurement error (Liang *et al.*, 2007). Suggested by Williams *et al.* (2003), as the method factor loadings are insignificant and the indicators' substantive variances are substantially greater than their method variances (Table AV), we concluded that common method bias is not a concern in our study.

5.1 Structural model testing

Having ensured an adequate model, the research hypotheses were tested by the bootstrapping technique in PLS. A bootstrap analysis was performed with 1,000 resamples, with the cases equaling the number of responses on our survey ($n = 439$). The results of the model estimation – including standardized path coefficient, significance of the paths based on a two-tailed *t*-tests and the variance explained (R^2) – are shown in Figure 2.

As we proposed, self-justification ($p < 0.01$) and sunk cost ($p < 0.02$) have significant positive effect on the dependent construct of WENB. The explanatory power of the structural model that we proposed can be evaluated by looking at the variance accounted for the R^2 value. The WENB construct has an R^2 of 0.48, indicating that our model accounts for 48 per cent of variance in the dependent construct. The R^2 values for the mediating constructs are relatively high, with self-justification accounting for an R^2 of 0.25 and sunk cost accounting for an R^2 of 0.43.

All of the hypotheses were supported, except *H1*. As shown in Figure 2, *H2*, *H3*, *H4* and *H6* were all significant at $p < 0.01$. While *H5* was significant at $p < 0.02$. While we also tested for the control variables (e.g. age, gender and position), none of them had a significant influence on WENB, and thus we did not retain them in the analysis presented in this study.



Notes: *p* value < 0.02 **; *p* value < 0.01 ***; - - - - - - not significant

Figure 2.
Structural model testing

Table II.
Mediation analysis based on Baron and Kenny (1986)

	Coefficients	Comments	R^2

Step 1: IV ← Mediator
(CN, BN ← SJ)
(CE ← SC)
	CN = −0.12*** (*t* =3.35)
	BN = 0.46*** (*t* = 4.37)
	CE = 0.65*** (*t* = 8.27)
		The condition holds only when IVs affect the mediator. This is satisfied for all IVs	0.24

Step 2: IV ← DV
(CN, BN, CE ← WENB)
	CN =−0.02 (*t* = 0.78)
	BN = 0.35*** (*t* = 2.73)
	CE = 0.46*** (*t* = 3.21)
		The IVs must influence DV. This condition is satisfied for BN and CE, but not for CN	0.50

Step 3: IV and mediator ← DV
(CN, BN, SJ ← WENB)
(CE, SC ← WENB)
	CN = −0.02 (*t* = 0.87)
	BN = 0.32*** (*t* = 3.14)
	SJ = 0.55*** (*t* = 5.55)
	CE = 0.36 (*t* = 1.67)
	SC = 0.37*** (*t* = 2.10)
		For mediation to occur, there should be no significant relationship controlling for the mediator. This condition is not satisfied for BN, but it is for CE. Thus,
		BN is partially mediated by SJ.
		CE is fully mediated by SC
			0.58

To understand the proposed mediation effects of our structural model, we conducted a mediation test as implied by PLS analysis, in Table II. We followed Baron and Kenny's (1986) widely accepted approach, where the mediation effect should show the strength of the relationship between the predictors, the independent variable (IV) and dependent variable (DV). Three steps were undertaken. We first regressed the mediators on independent variables: self-justification (SJ) on cost of noncompliance (CN) and benefit of noncompliance (BN); sunk cost (SC) on completion effect (CE). Second, we regressed the dependent variable – WENB – on the independent variables of CN, BN and CE. Third, the dependent variable WENB was regressed on the independent variables CN, BN and CE and the mediators SJ and SC.

To establish mediation, first, the independent variables of CN and BN must affect the mediator SJ, while the independent variable of CE must affect the mediator SC, in the first equation. This condition was satisfied for all independent variables. Second, the independent variables of CN, BN and CE must influence the dependent variable WENB in the second equation. CN was not satisfied in this condition, but BN and CE met the criteria. Third, the mediators SJ and SC must affect the dependent variable WENB in the third equation. Both SJ and SC influenced WENB (we did not check for CN, as it did not meet the criteria in the second equation). These conditions all hold in the predicted direction; thus, the effect of the independent variables BN and CE on dependent variable WENB is less in the third equation than in the second. According to Baron and Kenny (1986, p. 1177), "perfect mediation holds if the independent variable has no effect when the mediator is controlled". This was satisfied for SC, which has full mediation on CE, while SJ has partial mediation on BN.

5.2 Follow-up study

A follow-up study was conducted for two reasons. First, while we have anecdotal evidence that the hypothetical scenario represented a commonly observed behavior among employees, we wanted to confirm that. Second, we wanted more feedback – particularly from organizations' security managers – on the scenario's relevance to testing employee noncompliance because of a task that faced an obstacle.

In the follow-up study, participants were first subjected to the same hypothetical scenario presented in the main study (see Scenario in Appendix). Participants were then questioned whether they observed such a scenario as a problem in their organization and whether they would accept noncompliance behavior. They could respond on a Likert scale and openly reflect on the first three questions. The survey then continued with a set of Likert scale questions based on the completion effect construct adapted from Ross and Staw (1991).

The survey was first pre-tested with a 66 per cent (n = 10) response rate out of the targeted group. After revisions, the survey was then distributed to management-level employees in 120 IT companies. Responses from 16 managers (mostly security managers) belonging to 16 different IT companies were obtained (13.3 per cent response rate). Table AVI presents the measurement items and gives details of the survey questions.

According to our data analysis, around 42 per cent of the managers who think they would never accept unauthorized information provision realize that such violation may be out of their control. Manager A who believes that it is likely that such a violation could occur, but would not accept it, states that "depending on the importance of the information given and to whom", he might indulge in this kind of behavior. Manager B thinks that if there is "acceptance from the customer" or the signing of a "non-disclosure agreement with the expert", he might accept such violation. Three other managers, C, D and E, consider that trusting their employees is an important factor in accepting such violation. Manager E feels that employees should let their boss know if such violation is necessary, and in such a case, he could accept the violation. The other two managers believe that a non-disclosure agreement would keep information confidential. Manager F would trust his employee that the violation is in the "employee's best intention", and that the violation would be acceptable, while manager G believes that such "violation would not matter as much" when a non-disclosure agreement is signed. Manager L thinks that an "*ad hoc* approval by higher management can be made possible; however, employees' own decision to talk cannot be acceptable".

The managers, however, were influenced to change their stance on accepting violations of ISP when questions specifying degree of project completion and sunk cost were asked.

If a project is 10 per cent completed, then the majority of managers (75 per cent) would not at all be influenced to accept violation because of the minimal time, effort and money invested. Only 25 per cent would be very little or somewhat influenced by the time spent on the project to accept such violation (18 per cent would be very little influenced while 7 per cent would be moderately influenced).

If a project is 50 per cent completed, then around 68 per cent of managers would not at all be influenced to accept violation because of time, efforts or money expended, the rest, 32 per cent, would be somewhat influenced (25 per cent somewhat influenced while 7 per cent frequently influenced).

If a project is 95 per cent completed, then 62.5 per cent of the managers would not at all be influenced to accept violation. For the rest (37.5 per cent), 12.5 per cent would be very little influenced, 12.5 per cent would be moderately influenced and 12.5 per cent would be very much influenced.

The results show that even if the majority of managers claim that they would never accept unauthorized information provision, some indicated that they would indeed accept it when they understand that many resources had been spent on their project and it was near completion.

6. Discussion

To date, there has been little or no theoretical research demonstrating that employees typically think it is important to complete their work task, even if it requires exposing some confidential information. This trade-off situation (Kolkowska and De Decker, 2012) explains the phenomenon of value conflicts where information security values and work values become conflictual (Hedström *et al.*, 2011; Karlsson *et al.*, 2017). In this study, we demonstrate that noncompliance is not influenced by risk perceptions of employees because they do not consider noncompliance with ISPs as risk, but rather as an impediment to completing their tasks, referring to the trade-off that raises the value conflict.

Second, we identified two important theoretical antecedents to noncompliance behavior: self-justification and sunk cost. These antecedents act as mediators to explain employees' WENB regarding ISPs. In our theoretical model shown in Figure 1, we designed self-justification as a medium that is influenced by a relationship between cost of noncompliance and benefit of noncompliance and we designed sunk cost as a medium that is influenced by completion effect. In our structural model shown in Figure 2, we present the results providing strong empirical support that self-justification is positively influenced by the benefit of noncompliance and negatively influenced by cost of noncompliance; however, the benefits of noncompliance outweigh the costs of noncompliance. Furthermore, our results provide strong empirical support that completion effect influences sunk cost significantly. Therefore, empirical evidence supports our argument that self-justification and sunk cost largely influences WENB.

Third, we have strong empirical support suggesting that self-justification partially mediates WENB, while sunk cost fully mediates WENB. In a study, Bulgurcu *et al.* (2010) showed how the benefit of compliance and cost of noncompliance are influenced by rewards, when employees know that they will be rewarded for their pro-security behavior. While our study uses similar constructs to measure self-justification, we focus on the benefit of noncompliance (in reverse to the benefit of compliance) and the cost of noncompliance to explain noncompliance behavior. We found that the benefits of noncompliance that present cognitive traits outweigh the costs of noncompliance that present emotional traits, and, as a result, self-justification positively influences WENB. We consider this result of great importance. It shows that employees who are in the process of completing their tasks automatically reduce the risks of being caught that would result in some costs by relying on self-justification because incurring future costs may not be a top concern, when they foresee benefits.

Fourth, for the purpose of strengthening our findings, our follow-up study shows that even manager's agendas on showing pro-security behavior can change. When initially most managers claimed it would be unacceptable for an employee to violate their ISP, when the project was positioned as near completion and sunk costs were high, the same managers seemed more prepared to accept ISP violation. When managers were informed that a project was nearly completed, almost half of them were prepared to accept ISP violation because of proximity to the goal and high sunk costs.

6.1 Implications for theory

Theoretically, we explain WENB in terms of two antecedents – self-justification and sunk cost, using their perspectives of both cognitive and emotional traits of employees. Focusing the case on completing a task at hand no matter what the costs, proves to be different from other information security violations in terms of how it facilitates employees in assessing both costs and benefits of their WENB. We find that employees' perceived benefits of noncompliance are the main antecedents to self-justification and provide the necessary stimulation to violate the ISP. However, employees' perceived costs of noncompliance are not as influential. We find sound empirical support that self-justification positively and strongly influences employees' WENB. We also find that self-justification has a partial mediation effect on the benefits of noncompliance.

Our model also shows that sunk cost has full mediation effect on completion effect. Unlike prior theoretical models that tested sunk cost and completion effect as direct influencers on a dependent construct (Park *et al.*, 2012), our theoretical model explains empirically how sunk cost acts as a mediating mechanism for completion effect. In fact, our theoretical model is the first to demonstrate that completion effect has a close interaction with sunk cost in the context of noncompliance behavior. Previous literature suggests that completion effect has a parallel influence on any dependent construct. However, as the effect of completion effect was dramatically decreasing when we tested in parallel with sunk cost, we understood that its effect was dramatically increasing when we tested sunk cost as a mediator; an important realization for future theory building. As completion effect is defined as an increasing motivation to finish a task as the employee gets closer to the goal (Keil, 1995), we found that sunk cost would influence WENB much less if an employee is not close to completion. We believe that this should be an important consideration for future theory building.

Based on previous theoretical and empirical findings that risk perceptions are significant factors in affecting behavior in escalation situations, our theoretical framework proposed that risk perceptions significantly influence WENB. However, our empirical tests proved the contrary. While previous studies found that risk perceptions should influence behavior depending on how risk-averse or risk-seeking an employee is, our model showed no significant support in either case. We therefore argue that employees' noncompliance may be influenced by more powerful beliefs – such as self-justification and sunk cost – that overshadow considerations of risk.

Finally, we believe that our findings also contribute to the threat appraisal process in the protection motivation theory (PMT) (Rogers, 1975, 1983). When explaining individual's protection motivation involving a threat, PMT postulates that the individual develops self-justification for maladaptive behavior by considering intrinsic/extrinsic rewards and assessing the ramifications of maladaptive behavior. Therefore, our characterizations of benefit of noncompliance and cost of noncompliance parallel very well with the PMT. However, sunk cost has been considered in the PMT. Having showed the importance of sunk cost, our findings should be a call for the PMT research to consider the role of sunk cost in the threat appraisal process in PMT.

6.2 Implications for practice

Our theoretical framework and empirical results have important implications for security managers and organizations. Security managers can better understand their employees' WENB by assessing the obstacles that may arise for employees to complete their on-going projects.

Our results show that when employees are working on tasks undergoing difficulties, they are more likely to increase noncompliance behavior. Previous research in the context of project management provides empirical evidence that managers can encourage employees to report their project progress openly and truthfully. Keil *et al.* (2010) suggest that by maximizing the benefits and minimizing the costs associated with the honest progress reporting for projects that are in danger of failing, employees' tendency to commit failing courses of action can be reduced. With proper assurance mechanisms that make employees comfortable to report the project progress truthfully, employees would be less motivated to engage in ISP noncompliance.

From the organizational design perspective, we believe that by better understanding how project obstacles could result in ISP noncompliance, security managers can redesign their ISP in such a way that it recognizes the fact that obstacles in employees' primary tasks can make the employee who would otherwise be compliant with the ISP noncompliant with the ISP. Therefore, an explicit language and clear guidance in the ISP as to how employees should approach those tasks that are failing and a clear mandate in organizational policies to incorporate security considerations into the performance evaluations of the employees at every task, so that security cannot be ignored when it is most needed.

Our results also indicate that information security professionals should have a better access to project progress-reporting systems. We suggest that if security managers monitor employees' assignment and completion of tasks (e.g. by analyzing weekly status reports), they can identify employees that are likely to experience difficulties in their tasks, and thereby pre-empt noncompliance that might come out with the difficulties.

Another takeaway from this study is that the responsibility of promoting information security should not fall only on the shoulders of security professionals. Business managers should recognize that setting information security quality expectations would make employees less motivated to consider noncompliance with the ISP.

Our results are of practical value for not only security managers but also organizations as a whole. Previous studies found that organizations allocate more than 70 per cent of their security investments to security technologies alone. Echoing the recommendation of D'Arcy *et al.* (2008), we reiterate that organizations should balance such technology investments with investments to the socio-organizational side of information security.

6.3 Limitations

This study is constrained by some limitations. First, while it is reasonable to argue that our results are generalizable to other banks and even pharmaceutical and IT industries, they should be cautiously interpreted, as we did not specifically test the research model more extensively. We consider that extending our study by focusing on organizational and cultural differences is needed to further validate its generalizability. Second, this study was restricted to information-intensive organizations in the pharmaceutical, IT and banking industries, all operating in a European context. While we believe that our results are of significance, particularly in the banking industry, we also believe that analyzing noncompliance in a task-related context should be studied in other industries that would typically have less sophisticated information security practices.

Third, this study is limited to the individual level of analysis, except for some managerial views that are much smaller in number compared to the responses received in the pilot and the main study. Noncompliance tends to be a rather individual type of behavior, but analysis focused on particular groups in an organization can also be beneficial. Organizations would know better where to focus their efforts on information security and could also better identify the constructs that encourage noncompliance behavior within groups.

The fourth limitation of our study relates to our scenario-based design in our main study. As scenarios have recently been strongly recommended for use in noncompliance studies to facilitate the respondent’s understanding of the survey questions (Vance and Siponen, 2012), we used a scenario. Furthermore, we worded constructs to remind respondents of the context. However, some questionnaire items were not stated very specifically. For instance, the construct of completion effect was stated as “task is near completion”. Instead, it could have been stated more specifically as “task is 50 per cent completed” or “task is 95 per cent completed” as we did in our follow-up study. We believe that such specificity can lead to the development of more robust theories for enhancing information security strategies.

Note

1. Our respondents are well-aware of the explicit ISP of their organizations. Each employee undergoes a rigorous awareness program and have frequent updates from their security managers on the ISP of their organization. Insights on this matter have been obtained from face-to-face discussions with the security managers of the organizations involved in this study. Employees that were new and have not yet gone through the awareness programs have not been invited to answer our survey.

References

Baron, R.M. and Kenny, D.A. (1986), “The moderator-mediator variable distinction in social psychological research: conceptual, strategic, and statistical considerations”, *Journal of Personality and Social Psychology*, Vol. 51 No. 6, pp. 1173-1182.

Baskerville, R.L. and Dhillon, G. (2008), “Information systems security strategy: a process view”, in Straub, D.W., Goodman, S. and Baskerville, R.L. (Eds), *Information Security: Policy, Processes and Practices*, M.E. Sharpe, Armonk, NY, Vol. 11, pp. 15-45.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), “Information security policy compliance: an empirical study of rationality-based beliefs and information security awarenss”, *MIS Quarterly*, Vol. 34 No. 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*, Vol. 14, pp. 65-75.

Cavusoglu, H., Cavusoglu, H., Son, J.-Y. and Benbasat, I. (2015), "Institutional pressures in security management: direct and indirect influences on organizational investment in information security control resources", *Information & Management, Elsevier B.V.* Vol. 52 No. 4, pp. 385-400.

Chen, R., Wang, J., Herath, T. and Rao, H.R. (2011), "An investigation of email processing from a risky decision making perspective", *Decision Support Systems, Elsevier B.V.* Vol. 52 No. 1, pp. 73-81.

Chin, W.W. (1998), "Commentary: issues and opinion on structural equation modeling", *MIS Quarterly*, Vol. 19No No. 2, pp. 7-17.

Conlon, D.E. and Garland, H. (1993), "The role of project completion information in resource allocation decisions", *Academy of Management Journal*, Vol. 36 No. 2, pp. 402-413.

D'Arcy, J., Hovav, A. and Galletta, D. (2008), "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach", *Information Systems Research*, Vol. 20 No. 1, pp. 1-20.

Dhillon, G. and Backhouse, J. (2001), "Current directions in IS security research: towards socio-organizational perspectives", *Information Systems Journal*, Vol. 11 No. 2, pp. 127-153.

Gefen, D., Straub, D. and Boudreau, M. (2000), "Structural equation modeling and regression: guidelines for research practice", *Communications of the Association for Information Systems*, Vol. 4, pp. 1-79.

Hedström, K., Kolkowska, E., Karlsson, F. and Allen, J.P. (2011), "Value conflicts for information security management", *Journal of Strategic Information Systems*, Vol. 20 No. 4, pp. 373-384.

Herath, T. and Rao, H.R. (2009a), "Protection motivation and deterrence: a framework for security policy compliance in organisations", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 106-125.

Herath, T. and Rao, H.R. (2009b), "Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness", *Decision Support Systems, Elsevier B.V.* Vol. 47 No. 2, pp. 154-165.

Holmqvist, M. and Pessi, K. (2006), "Agility through scenario development and continuous implementation: a global aftermarket logistics case", *European Journal of Information Systems*, Vol. 15 No. 2, pp. 146-158.

Hsu, C., Lee, J.N. and Straub, D.W. (2012), "Institutional influences on information systems security innovations", *Information Systems Research*, Vol. 23 No. 3-part-2, pp. 918-939.

Hu, Q., Xu, Z., Dinev, T. and Ling, H. (2011), "Does deterrence work in reducing information security policy abuse by employees?", *Communications of the Association for Information Systems*, Vol. 54 No. 6, pp. 54-60.

Ifinedo, P. (2014), "Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition", *Information and Management*, Vol. 51 No. 1, pp. 69-79.

Johnson, E.M. and Goetz, E. (2007), "Embedding information security into the organization", *IEEE Security & Privacy Magazine*, Vol. 5 No. 3, pp. 16-24.

Johnston, A.C. and Warkentin, M. (2010), "Fear appeals and information security behaviors: an empirical study", *MIS Quarterly*, Vol. 34 No. 3, pp. 549-566.

Karlsson, F., Karlsson, M. and Åström, J. (2017), "Measuring employees' compliance – the importance of value pluralism", *Information and Computer Security*, Vol. 25 No. 3, pp. 279-299.

Keil, M. (1995), "Pulling the plug: software project management and the problem of project escalation", *MIS Quarterly*, Vol. 19 No. 4, pp. 421-447.

Keil, M., Mann, J. and Rai, A. (2000), “Why software projects escalate: an empirical analysis and test of four theoretical models”, *MIS Quarterly*, Vol. 24 No. 4, pp. 631-664.

Keil, M., Truex, D.P., III. and Mixon, R. (1995), “The effects of sunk cost and project completion ation technology project Escala”, *IEEE Transactions on Engineering Management*, Vol. 42 No. 4, available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=482086 (accessed 2 April 2013).

Keil, M., Tan, B.C.Y., Wei, K., Saarinen, T. and Tuunainen, V. (2000), “A cross-cultural study on escalation of commitment behavior in software projects”, *MIS Quarterly*, Vol. 24 No. 2, pp. 299-325.

Keil, M., Tiwana, A., Sainsbury, R. and Sneha, S. (2010), “Toward a theory of whistleblowing intentions: a benefit-to-cost differential perspective”, *Decision Sciences*, Vol. 41 No. 4, pp. 787-812.

Kolkowska, E. and De Decker, B. (2012), “Analyzing value conflicts for a work-friendly ISS policy implementation”, *IFIP Advances in Information and Communication Technology*, Vol. 376, pp. 339-351.

Liang, H., Saraf, N., Hu, Q. and Xue, Y. (2007), “Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management”, *MIS Quarterly & the Society for Information Management*, Vol. 31 No. 1, pp. 59-87.

Moore, G. and Benbasat, I. (1991), “Development of an instrument to measure the perceptions of adopting and information technology innovation”, *Information Systems Research*, Vol. 2 No. 3, pp. 192-222.

Pahnila, S., Siponen, M. and Mahmood, A. (2007), “Employees’ Behavior Towards IS Security Policy Compliance”*, Proceedings of the 40th Hawaii International Conference on Systems Science, Hawaii*, pp. 1-10.

Park, S.C., 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, Nature Publishing Group*, Vol. 21 No. 6, pp. 643-663.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.-Y. and Podsakoff, N.P. (2003), “Common method biases in behavioral research: a critical review of the literature and recommended remedies”, *The Journal of Applied Psychology*, Vol. 88 No. 5, pp. 879-903.

Puhakainen, P. and Siponen, M. (2010), “Improving employees’ compliance through information systems security training: an action research study”, *MIS Quarterly*, Vol. 34 No. 4, pp. 757-778.

Ringle, C. Wende, S. and Will, A. (2005), “SmartPLS”, Hamburg, available at: www.smartpls.de

Rogers, R.W. (1975), “A protection motivation theory of fear appeals and attitude change”, *The Journal of Psychology*, Vol. 91 No. 1, pp. 93-114.

Rogers, R.W. (1983), “Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation”, in Cacioppo, J.T. and Petty, R.E. (Eds), *Social Psychophysiology: A Source Book*, Guilford Press, New York, NY, Vol. 19, pp. 153-176.

Ross, J. and Staw, B. (1991), “Managing escalation processes in organizations”, *Journal of Managerial Issues*, Vol. 3 No. 1, pp. 15-30.

Siponen, M. and Vance, A. (2010), “Neutralization: new insights into the problem of employee information systems security policy violations”, *MIS Quarterly*, Vol. 34 No. 3, pp. 487-502.

Siponen, M., Mahmood, A. and Pahnila, S. (2009), “Are employees putting your company at risk by not following information security policies?”, *Communications of the Association for Information Systems*, Vol. 52 No. 12, pp. 145-147.

Smith, H. and Keil, M. (2003), “The reluctance to report bad news on troubled software projects: a theoretical model”, *Information Systems Journal*, Vol. 13 No. 1, pp. 69-95.

Staw, B. (1976), “Knee-deep in the big muddy: a study of escalating commitment to a chosen course of action”, *Organizational Behavior and Human Decision Processes*, Vol. 16 No. 1, pp. 27-44.

Staw, B.M. and Ross, J. (1989), "Understanding behavior in escalation situations", *Science (New York, NY)*, Vol. 246 No. 4927, pp. 216-220.

Straub, D. (1989), "Validating instruments in MIS research", *MIS Quarterly*, Vol. 13 No. 2, pp. 147-169.

Straub, D.W. and Welke, R.J. (1998), "Coping with systems risk: security planning models for management decision making", *MIS Quarterly, JSTOR*, Vol. 22 No. 4, pp. 441-469.

Straub, D., Boudreau, M. and Gefen, D. (2004), "Validation guidelines for IS positivist research", *Communications of the Association for Information Systems*, Vol. 13, pp. 380-427.

Teh, L.P., Ahmed, P.K. and D'Arcy, J. (2015), "What drives information security policy violations among banking employees? Insights from neutralization and social exchange theory", *Journal of Global Information Management*, Vol. 23 No. 1, pp. 44-64.

Thomas, M. and Dhillon, G. (2011), "Interpreting deep structures of information systems security", *The Computer Journal*, Vol. 55 No. 10, pp. 1148-1156.

Tyler, T. and Blader, S. (2005), "Can businesses effectively regulate employee conduct? The antecedents of rule following in work settings", *Academy of Management Journal*, Vol. 48 No. 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*, Vol. 24 No. 1, pp. 21-41.

Williams, L.J., Edwards, J.R. and Vandenberg, R.J. (2003), "Recent advances in causal modeling methods for organizational and management research", *Journal of Management*, Vol. 29 No. 6, pp. 903-936.

Willison, R. and Warkentin, M. (2013), "Beyond deterrance: an expanded view of employee computer abuse", *MIS Quarterly*, Vol. 37 No. 1, pp. 1-20.

Further reading

Anderson, C.L. and Agarwal, R. (2010), "Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions", *MIS Quarterly*, Vol. 34 No. 3, pp. 613-643. No.

Mehta, N., Mehta, A., Mehta, N. and Mehta, A. (2010), "It takes two to tango: how relational investments improve IT outsourcing partnerships", *Communications of the Association for Information Systems*, Vol. 53 No. 2, pp. 160-164.

Schneier, B. (2012), *Liars and Outliers: Enabling the Trust That Society Needs to Thrive*, John Wiley & Sons, New York, NY.

Appendix

Scenario

Assume that you have been working on a certain project that needs to be finished by a deadline. The deadline is approaching and you almost finished the project except a particular task that you do not know how to accomplish. To complete the project, that particular task has to be completed. You know an expert who can help you complete that task. However, 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[1] stating that no customer information shall be exposed (disclosed, divulged, given away, or given access) to anyone outside the area of responsibility. Think about this situation, and indicate your agreement/disagreement with the following questions.

Constructs	Measurement item	Origin	Mean	STD	Loading
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	New items based on [25,27] and [36]	1.57	1.38	0.72
	I think it is the right choice to continue working on my task, even if I don't follow the information security policy		1.18	0.72	0.89
	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	0.79	0.89
Benefit 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	New items based on [8]	1.19	0.82	0.97
	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		1.16	0.73	0.98
	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		1.16	0.75	0.97
	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		1.15	0.74	0.95
Cost of noncompliance	I will be punished or demoted if I don't comply with the information security policy	Adopted from [8]	6.46	1.21	0.86
	I will receive personal reprimand in oral or written assessment reports if I don't comply with the information security policy		6.57	1.05	0.86
	I will incur monetary or non-monetary penalties if I don't comply with the information security policy		4.56	2.43	0.73

(*continued*)

Table AI. The modelled constructs and their measurement items

Constructs	Measurement item	Origin	Mean	STD	Loading
Sunk cost	It would be regrettable for me to stop working on my task because of the effort I have already spent, even if I have to break the rules of the information security policy	New items based on [25,27] and [36]	1.34	1.07	0.93
	I cannot stop working on my task because of the time I have already spent, even if I have to break the rules of the information security policy		1.34	1.09	0.96
	Overall, it would have been a waste of time and effort if I stopped working on my task, even if I have to break the rules of the information security policy		1.30	1.03	0.86
Completion effect	I believe that I would be successful if I continue working on my task, even if I have to break the rules of the information security policy	New items based on [25,27] and [36]	1.17	0.67	0.97
	I had come too far to stop working on my task, even if I have to break the rules of the information security policy		1.19	0.74	0.95
	I cannot abandon my task because it is near completion, even if I have to break the rules of the information security policy		1.18	0.71	0.96
Risk perception	I believe there are no big risks associated with my breaking of the rules of the information security policy during the task	New items based on [25,27]	1.27	1.03	0.83
	I believe that my breaking of the rules of the information security policy during my task has a low probability of harming my organization		1.28	0.98	0.91
	I believe there are very little risks related to information security in continuing to work on my task		1.58	1.44	0.76
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	New items based on [36]	1.18	0.63	0.96
	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		1.19	0.69	0.96
	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		1.20	0.72	0.95

Table AI.

Constructs	Measurement item	*t*-statistics
Self-justification	SJ1← SJ	13.57***
	SJ2 ← SJ	32.39***
	SJ3 ← SJ	24.49***
Benefit of noncompliance	BN1 ← BN	77.84***
	BN2 ← BN	146.80***
	BN3 ← BN	80.33***
	BN4 ← BN	31.73***
Cost of noncompliance	CN1 ← CN	17.07***
	CN2 ← CN	17.69***
	CN3 ← CN	13.12***
Sunk cost	SC1 ← SC	41.40***
	SC2 ← SC	88.28***
	SC3 ← SC	23.54***
Completion effect	CE1 ← CE	69.18***
	CE2 ← CE	28.76***
	CE3 ← CE	75.40***
Risk perception	RP1 ← RP	15.31***
	RP2 ← RP	38.57***
	RP3 ← RP	14.43***
Willingness	WENB1 ← WENB	66.91***
	WENB2 ← WENB	55.71***
	WENB3 ← WENB	36.66***

Table AII. *t*-statistics for convergent validity

	Composite reliability	AVE	A	B	C	D	E	F	G
BN (benefit of noncompliance)	0.98	0.94	*0.97*						
CE (completion effect)	0.97	0.92	0.61	*0.96*					
CN (cost of noncompliance)	0.85	0.66	−0.12	−0.12	*0.81*				
RP (risk perception)	0.88	0.70	0.24	0.28	−0.08	*0.84*			
SJ (self-justification)	0.88	0.71	0.58	0.61	−0.20	0.38	*0.84*		
SC (sunk cost)	0.94	0.84	0.58	0.66	−0.16	0.28	0.55	*0.92*	
WENB (willingness)	0.97	0.91	0.61	0.61	−0.10	0.36	0.67	0.51	*0.96*

Table AIII. Composite reliability, AVE and correlation of the constructs

	A	B	C	D	E	F	G
A. CE1	*0.97*	0.59	0.27	−0.11	0.62	0.59	0.62
A. CE2	*0.95*	0.57	0.26	−0.11	0.60	0.56	0.59
A. CE3	*0.96*	0.59	0.27	0.12	0.68	0.62	0.67
B. BN1	0.59	*0.97*	0.25	−0.12	0.55	0.46	0.58
B. BN2	0.59	*0.98*	0.22	−0.12	0.57	0.46	0.59
B. BN3	0.62	*0.97*	0.24	−0.12	0.58	0.51	0.63
B. BN4	0.54	*0.95*	0.24	−0.10	0.55	0.43	0.55
C. RP11	0.21	0.18	*0.83*	−0.08	0.19	0.28	0.24
C. RP2	0.29	0.26	*0.91*	−0.09	0.27	0.43	0.39
C. RP3	0.17	0.13	*0.76*	0.09	0.16	0.21	0.24
D. CN	−0.08	−0.09	−0.10	*0.86*	−0.11	−0.15	−0.08
D. CN2	−0.12	−0.11	−0.08	*0.86*	0.17	−0.17	−0.10
D. CN3	−0.08	−0.08	−0.02	*0.73*	−0.10	−0.16	−0.05
E. SC1	0.59	0.53	0.22	−0.18	*0.93*	0.54	0.48
E. SC2	0.60	0.53	0.24	−0.16	*0.96*	0.51	0.47
E. SC3	0.63	0.53	0.24	−0.10	*0.86*	0.48	0.45
F. SJ1	0.41	0.31	0.24	−0.16	0.38	*0.72*	0.45
F. SJ2	0.51	0.42	0.39	−0.17	0.47	*0.89*	0.67
F. SJ3	0.62	0.47	0.33	−0.17	0.54	*0.89*	0.54
G. WENB1	0.62	0.60	0.34	−0.11	0.46	0.64	*0.96*
G. WENB2	0.65	0.55	0.37	−0.10	0.48	0.67	*0.96*
G. WENB3	0.60	0.59	0.32	−0.07	0.52	0.60	*0.95*

Table AIV. Factor analysis results/cross loadings

Construct	Indicator	Substantive factor loading (R1)	Squared loadings of substantive factors (R1^2)	Method factor loading (R2)	Squared values of the method factor loadings (R2^2)
Benefit of noncompliance	BN1	0.971*	0.943	−0.184	−0.012
	BN2	0.984*	0.968	−0.181	−0.014
	BN3	0.970*	0.943	1.245	0.095
	BN4	0.956*	0.916	−0.915	−0.069
Completion effect	CE1	0.967*	0.936	−0.393	−0.032
	CE2	0.956*	0.917	−1.05	−0.078
	CE3	0.961*	0.926	1.388	−0.109
Cost of noncompliance	CN	0.898*	0.808	0.513	0.022
	CN2	0.893*	0.797	−0.379	−0.019
	CN3	0.722*	0.486	−0.204	−0.004
Risk perception	RP11	0.860*	0.74	−0.836	−0.039
	RP2	0.871*	0.768	2.143	0.108
	RP3	0.790*	0.628	−2.132	−0.078
Self-justification	SJ1	0.739*	0.553	−3.586	−0.135
	SJ2	0.881*	0.777	0.31	0.022
	SJ3	0.895*	0.804	1.238	0.088
Sunk cost	SC1	0.867*	0.847	−3.81	−0.188
	SC2	0.889*	0.899	−5.203	−0.254
	SC3	0.876*	0.742	−1.454	−0.076
WENB	WENB1	0.961*	0.923	−0.113	−0.008
	WENB2	0.960*	0.922	0.253	0.018
	WENB3	0.947*	0.898	−0.149	−0.009
Average		0.901	0.825	−0.614	−0.035

Note: $p < 0.01$

Table AV. Common method bias analysis

Constructs	Measurement item	Mean	STD
Accepting violation of ISP	How likely is it that an employee of your organization would violate the Information Security Policy, similar to the scenario described above?	2.23	1.42
	How likely is it that you would be OK if an employee of your organization violates the Information Security Policy, similar to the scenario described above?	1.61	0.96
	How likely is it that you would accept an Information Security Policy violation of an employee of your organization, similar to the scenario described above?	1.69	0.94
If a project is 10% completed would you consider the following reasons to accept your employee's violation of the Information Security Policy	Time spent on that project?	1.23	0.43
	Efforts spent on that project?	1.37	0.86
	Money spent on that project?	1.38	0.86
If a project is 50% would you consider the following reasons to accept your employee's violation of the ISP	Time spent on that project?	1.61	0.96
	Efforts spent on that project?	1.76	1.30
	Money spent on that project?	1.76	1.30
If a project is 95% would you consider the following reasons to accept your employee's violation of the ISP	Time spent on that project?	1.92	1.44
	Efforts spent on that project?	2.07	1.75
	Money spent on that project?	2.07	1.75

Table AVI.
Follow-up study survey

Corresponding author
Miranda Kajtazi can be contacted at: miranda.kajtazi@ics.lu.se