New Insights Into Understanding Manager's Intentions to Overlook ISP Violation in Organizations through Escalation of Commitment Factors

M. Kajtazi[1,2], E. Kolkowska[1] and B. Bulgurcu[3]

[1]Örebro University, Örebro, Sweden
[2]Linnaeus University, Växjö, Sweden
[3]Boston College, Boston, Massachusetts
e-mail: {miranda.kajtazi; ella.kolkowska}@oru.se; burcu.bulgurcu@bc.edu

Abstract

This paper addresses managers' intentions to overlook their employees' Information Security Policy (ISP) violation, in circumstances when on-going projects have to be completed and delivered even if ISP violation must take place to do so. The motivation is based on the concern that ISP violation can be influenced by escalation of commitment factors. Escalation is a phenomenon that explains how employees in organizations often get involved in *nonperforming* projects, commonly reflecting the tendency of persistence, when investments of resources have been initiated. We develop a theoretical understanding based on Escalation of Commitment theory that centres on two main factors of noncompliance, namely completion effect and sunk costs. We tested our theoretical concepts in a pilot study, based on qualitative and quantitative data received from 16 respondents from the IT – industry, each representing one respondent from the management level. The results show that while some managers are very strict about not accepting any form of ISP violation in their organization, their beliefs start to change when they realize that such form of violation may occur when their employees are closer to completion of a project. Our in-depth interviews with 3 respondents in the follow-up study, confirm the tension created between compliance with the ISP and the completion of the project. The results indicate that the larger the investments of time, efforts and money in a project, the more the managers consider that violation is acceptable.

Keywords

Escalation of commitment, ISP violation, IT-industry, completion effect, sunk costs.

1. Introduction

For all the benefits of information technology (IT), particularly the revolution in how organizations operate, information security is still a concern for management (Bulgurcu et al., 2010; Vance & Siponen, 2012). As a result, reserving the right budget for information security (IS) is one of the most difficult management tasks (Cavusoglu et al., 2004; Hsu et al., 2012). Organizations find it very challenging to define the value of their IS investments, mainly because an IS investment is expected to return a tangible benefit (Sonnenreich et al., 2006).

Prior research suggests that the focus of IS should be strengthened from the socio-organizational perspective (Boss et al., 2009; Bulgurcu et al., 2010; Dhillon and

Backhouse, 2001; Warkentin et al., 2011; Willison and Warkentin 2013). Highlighting the significance of the insiders is key, as employees are considered the weakest link in IS (Mitnick and William, 2003), since the challenge to keep information safe is not much of a technical challenge, but the challenge is how to make people use the technological services correctly, e.g. the use of passwords in a correct way (Furnell, 2014). Although research in this area has developed extensively (Bulgurcu et al., 2010; D'Arcy et al., 2009; Dhillon and Backhouse, 2001; Herath and Rao, 2009b; Johnston and Warkentin, 2010; Siponen and Vance, 2010), little is understood about business managers' influence on employees' compliance with ISP. Boss at al (2009) argue that business managers are an important part of IS management and play a significant role in affecting the employees' willingness to comply with the existing ISP. Thus it would be problematic if business managers tend to overlook the violation of the ISP.

Drawing on this motivation, the objective of this paper is to explain whether the management level in the organization tends to overlook the ISP violation, especially when they consider that some violation may be positive in certain situations, such as when a project needs to be completed, hence violation is for the benefit of the organization. We utilize the escalation of commitment theory to tackle managers' intention to justify violation with the organization's ISP. We do so by understanding which escalation factors influence managers' intentions to overlook and even accept ISP violation. Escalation of commitment is a phenomenon 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). For instance, employees must decide whether to withdraw or persist continuing on a nonperforming project, in which they should stop their investment of time, efforts and other resources, such as money. Empirically, we do not test if a project is failing or not, but we investigate the impact that escalation of commitment factors of sunk cost and completion effect may have on ISP violation in organizations by understanding managers' intentions to overlook ISP violation and even view it positively.

The rest of the paper is structured as follows. We continue to present our motivation and theoretical background. We then present our methodological approach followed by data analyses and results. Finally, we present the conclusions and some prospects to continue this research in the future.

2. Theoretical Framework

Among the many troubling phenomena that follow organizations, the escalation of commitment tops the list (Sleesman et al., 2012). Even during their phase of peaking with innovation and success, organizations commit costly decision errors, because of the tendency of decision-makers to maintain their commitment to a losing course of action, albeit that negative feedback on that action has occurred (Staw and Ross, 1989). Designing a behavioural model of rational choice, Simon (1955) assumed that employees behave rationally by having a well-organized and stable system of preferences. In fact, the employees are programmed to find rational adjustments that

are good enough for practical circumstances. However, escalation of commitment theory focuses on understanding the commitment of an individual to make risky decisions in a given context, especially when the act is deliberate (Staw and Ross, 1989). Central to it is the understanding of the behaviour of an escalation of commitment. In practice, escalation of commitment is a characteristic of employees who often become committed to a losing course of action, throwing good money or effort after bad (Ross and Staw, 1993; Staw and Ross, 1989), when an employee exhibits high risk-taking behaviour as a result of a deliberate decision (Keil et al., 2000).

Accordingly, this paper presents escalation of commitment as a theoretical framework to account for an understanding of its effects that triggers managers at various organizations to overlook ISP violation, which in return may motivate employees even more to engage with the ISP violation. Such an account can possibly inform the development of future IS strategies to improve the protection of vulnerable information in organizations. Therefore we propose that a detailed understanding of the effects of escalation on managers' intentions to accept their employees' violation of the ISP of their organizations can possibly bring a significant theoretical redirection to increase our understanding of employees' intentions to violate ISPs in the IS domain.

2.1. Two Factors in Action

Completion effect is a type of motivation for an individual to achieve a goal, as the individual gets closer to that goal (Conlon and Garland, 1993). In the context of violation, the completion effect suggests that when projects are near completion, a manager's intention to overlook ISP violation may increase.

The completion effect is a psychological effect suggesting that the desire to achieve the completion of a project can have a significant influence on behaviour (Katz and Kahn, 1966). Similarly, Brockner et al. (1986) stated that an individual's motivation for pursuing a course of action may shift over time due in part to the presumed increased proximity to the goal. Results from a series of experiments appear to provide support for these assertions about the completion effect (Keil et al., 2000; Park et al., 2012).

Despite the fact that the completion effect has served as an important indicator of project management failures, Keil et al. (2000) have indicated that measuring the completion level for a particular action, e.g. the completion effect of a task in a project, may be extremely difficult. In practice this is extremely difficult because employees who depend on due dates for submitting their tasks believe that the closer the due date the closer they are to the completion of the project.

In our theoretical framework, the completion effect plays an important role. It acts as an independent factor to explain noncompliance with an ISP. Theoretically, however, we do not intend to utilize the completion effect for the purpose of measuring the level of project completion. We utilize the completion effect for measuring its

influence on manager's intention to overlook ISP violation. More specifically, the completion effect is intended to explain if ISP violation is seen as a positive behaviour when projects are near completion or vice versa.

Linked to completion effect, we also consider the role of sunk cost effect on manager's intention to overlook ISP violation. Invested resources on a project explain that a manager's intention to get locked into considering that ISP violation may be positive for the project depends on the effect of the sunk costs. This phenomenon is commonly referred to as the sunk cost effect, which relates to at least three types of investments in the project: *time, efforts and money* (Staw and Ross, 1989). To better understand the interaction between completion effect and sunk cost in affecting manager's intentions, Figure 1 gives a visual representation of that interaction.

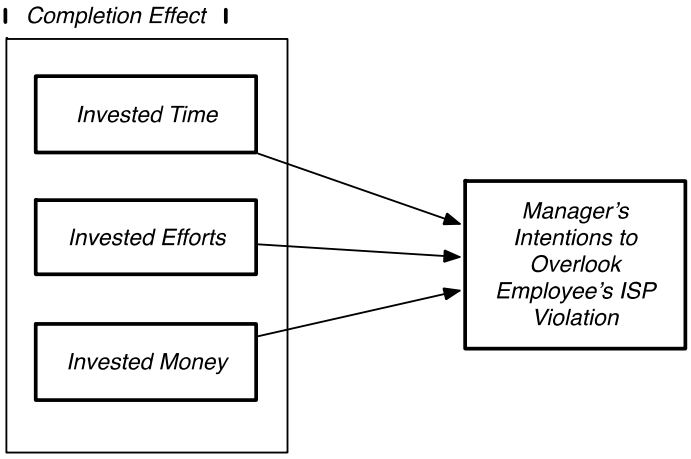

Figure 1: Research model – the escalation of commitment factors of completion effect and sunk cost towards understanding manager's intention to overlook employee's ISP violation

We posit that in terms of overlooking ISP violation, employees would exhibit a willingness to engage in ISP violation when they realize that they have already invested a large amount of time, efforts and money in trying to complete their project. Engaging in such behaviour when the project is nearly completed, allows the managers to believe that some ISP violation may even turn out to be positive for the organization.

The completion effect and sunk cost factors present two basic arguments why ISP violation as a result of escalation of commitment may take place, often in a large scale. While our intention is not to understand whether a project is actually failing, we consider that understanding the role of such escalation of commitment factors in ISP violation may bring a theoretical redirection in the ISP compliance and noncompliance literature. We continue to highlight the methodological approach and thereafter the results of our pilot study.

3. Methodological Approach

The purpose of this pilot study is to strengthen the view on the problem initially introduced, namely the managers' intentions to overlook their employees' ISP violation as a need to avoid project failure. The empirical investigation was driven by data collected from a mixed approach via an on-line questionnaire that featured a scenario in the beginning. We received qualitative and quantitative feedback from 16 respondents of 16 different organizations, which led us to extend the study with 3 more in depth interviews with the participating managers. The aim of these interviews was to follow-up the results from the questionnaire and to further discuss the problem of managers' intention to overlook employees' violation of ISP. The scenario and the questions for our respondents were based on theory that we effectively used to study how the managers' intentions to overlook ISP violation led us to better understand ISP violation among employees.

As described in Table 1, each participant was subject to the same context-specific scenario. The scenario was intended to inform the respondents that during the process of completion of their employees' specific tasks, their employees might become involved with the ISP violation in that process. The participants were then questioned whether they would find such a scenario to occur in their organization and whether they would accept such behaviour. A set of questions based on the adapted completion effect construct from Keil et al. (2000) and Ross and Staw (1993) were then asked[1]. Two questions were designed to be open-ended, one for the purpose of encouraging the managers to present their own perspectives on the reasons they would find for accepting such a violation of the ISP, the other for the purpose of receiving any other feedback they might have had.

Scenario
Assume that an employee that you supervise in your organization has been working on a certain project which needs to be finished by a deadline. The deadline is approaching and the employee has almost finished the project except a particular task which the employee does not know how to accomplish. In order to complete the project, that particular task has to be completed. The employee knows an expert who can help him/her to 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. Think about this situation, and indicate your agreement/disagreement with the following questions.

Table 1: Pilot Study Scenario

[1] Due to limited space, we only introduce the scenario.

Although the number of respondents is relatively low, we consider that data collected from a qualitative and quantitative perspective with 16 respondents, as well as follow-up in-depth interviews with 3 of the respondents is sufficient to understand and start theorizing whether managers have intentions to overlook ISP violation in specific contexts, such as when projects are near completion. We also consider the number is sufficient to derive such an understanding considering that 16 organizations participated, and that one manager represents one company.

4. Data Analyses and Results

The data collected were analysed in two forms. We first used descriptive statistics for the scale questions, followed by text analyses for the open-ended answers. The analyses present the understanding of the IT industry manager's intentions on overlooking their employee's ISP violation. The total number of respondents to the survey was 16 participants from the management level of 16 IT-companies. Around 50% of these managers believe that it is very likely that ISP violation can be caused as a result of escalation of commitment behaviour, while 31% of the managers strongly believe that such misbehaviour is likely to occur. The remaining 19% of the respondents have vague beliefs that such behaviour occurs. The other half, 50% believe it is unlikely that ISP violation in organizations occurs as a result of escalation of commitment behaviour. Furthermore, 87% believe it is not acceptable if an employee of their organization violates information management rules and regulations of their organization by ISP violation, while 13% believe that this is not a serious issue. Following these responses, the same 87% of managers would never accept such violation, while the same 13% of managers would accept such violation.

Around 42% of these managers who think they would never accept ISP violation, realize that such violation may be out of their control. In this regard, one manager who believes that it is likely that ISP violation occurs, but would not accept violation, states that "*depending on the importance of the information given and to whom, I might be indulged with that kind of behaviour*". Similar to those beliefs, another manager thinks that if there is "*acceptance from the customer*" or by signing a "*non-disclosure agreement with the expert*", he might accept such violation. Three other managers consider that trusting their employees is an important factor to accepting such violation. One manager expects that their employees should let him know if such violation is necessary, therefore he would accept the violation. The other two managers believe that a non-disclosure agreement would keep information confidential. One manager would trust his employee that the violation is in the "*employee's best intention*", and that the violation would be acceptable, while the other believes that such "*violation would not matter as much*", when the non-disclosure agreement is signed. Another manager thinks that an "*ad hoc approval by higher management can be made possible, however employees own decision to talk cannot be acceptable*". Consequently even if the managers state that they would not accept the employees ISP violation, their answers to the open-ended questions indicate that they tend to explain and justify employees ISP violation.

The managers, seem to be influenced to change their beliefs about accepting the violation of their employees when very specific escalation of commitment related questions were asked. They seem to be influenced when their employees' escalation of commitment in terms of their invested time, efforts and money are considered important factors the closer their employee would get to the project completion.

If a project is 10% completed, then the majority of managers (75%), would not at all be influenced to accept violation because of time, efforts or money. Few managers, 25%, would be very little or somewhat influenced by the time spent on the project to accept such violation. Out of 25%, 18% indicate they would be very little influenced to accept such violation because of efforts and money spent on the project, while 7% indicate they would be moderately influenced to accept violation.

If a project is 50% completed, then around 68% of managers would not at all be influenced to accept violation because of time, efforts or money. Only 32% of managers indicate that they are somewhat influenced by the time spent on the project to accept such violation. Out of 32%, 25% indicate they would be somewhat influenced by the efforts and money spent on the project to accept such violation, while 7% indicate they would be frequently influenced by the efforts and money spent on the project to accept such violation.

If a project is 95% completed, then more than half of the managers, 62.5%, would not be influenced to accept violation because of the three reasons. 12.5% would be very little influenced to accept violation because of the three reasons. 12.5% would be moderately influenced to accept violation because of time. Approximately, 12.5%, would be very much influenced to accept violation because of time, efforts and money invested.

The results show that even if the majority of managers would never accept ISP violation, their beliefs about refusing to accept such violation seem to change. Their beliefs change when they realize that their employees are closer to completing their projects. In this regard, some managers indicated that they would indeed consider to accept ISP violation, only when they understand that a lot of time, efforts and money have been spent on their project.

Of the 16 managers, 3 managers were interviewed to further discuss if their intentions were to overlook violation when there is a need to complete a project. When asked how often do they face project deadlines that were facing obstacles, one of the three managers responded as "*there are many such projects in our organization, every month we get into difficult situations for the delivery process*", the other said "*just last week, we had a situation when a task in the project was delaying the project delivery, and we wanted to do anything just to complete it and submit the project*", the third displayed a worrisome voice saying that "*these situations happen all the time and the problem is that our employees do not notify me on time about the problems, that is why we need to react fast and make sure we deliver the project, it is the customer who is waiting*".

When the three managers were asked again to discuss in more details whether they would or would not accept their employees violation of the ISP in order to make a successfully delivery of the project, their reactions were different, yet had the same intentions. The first manager discussed how the importance of the ISP in the organization and the rules described in it are often blurred, leaving the manager and the employees believe that violation to complete the project would not be as damaging. The second manager mentioned that despite he would never allow his employees to engage in violation for any reason, if violation would involve some insider with whom the violation is done, he would find this reasonable not to loose a project delivery, which may cost thousands to the organization if delayed. The third manager mentioned that his organization's ISP is so out-dated that any project-related violation would not even be considered as a violation, due to the ISP not covering such forms of violation.

These critical points raised, showed us that these managers were willing to accept and even encourage violation for the sake of a project. As previous literature has not considered these aspects of violation, we think that this is an issue that needs in-depth understanding of the violation of the ISP, which may shed new light on why employees are often noncompliant with the security rules and regulations of their organization.

5. Conclusion and Future Research

For organizations, controlling IS has become a daunting task. Insider attacks, i.e. employees in organizations, and outsider attacks, i.e. hackers, are increasing more than ever, generating far-reaching consequences, most often with millions of online personal data compromised, and billions of dollars registered in losses.

Our theoretical approach tackled a practical organizational problem by intending to understand how managers' intentions to overlook ISP violation among their employees increases, when they consider that enough spent resources of time, efforts and money on a project can be used as an argument to go against the ISP and make sure that they can deliver the project on-time, rather than look like a failure in front of the others in the organization, if the project has to be abandoned due to ISP. The empirical study based on 16 responses from the management level showed that the closer the employees are to completing their projects, the more their managers tend to overlook their ISP violation, if such a wrongdoing would save the project from failing. Time, efforts and money have been seen as three important resources that would identify the resources spent towards the completion of a project. We therefore suggest that organizations should focus on decreasing ISP violation not only by targeting employees at the front desks, but also by carefully targeting managers at any level, who can be considered as the source of allowing ISP violation to increase. While many well-established organizations are very careful about designing security rules and regulations, organizations that tend to overlook security issues, hence do not specify rules in this regard are the most vulnerable. Examining the factors that influence ISP violation as a result of escalation of commitment, such are the completion effect and sunk costs, can guide security managers in ensuring

compliance in the future. For instance, organizations can effectively design new ISPs or re-design their existing ISPs by carefully focusing on informing the employees that the escalation of commitment is discouraged, whereas, the benefit of reporting project problems would allow organizations to find assistance for their employees, reducing the need for ISP violation.

There are several limitations of this study. First, we did not test if a project would actually be in the process of escalation of commitment or not. We only asked our respondents to hypothetically consider that a project would not be delivered if their employees would not violate the ISP. Tests in a real setting where a project may be in the escalation of commitment process can bring very important feedback to better understand if violation may be a result of escalation of commitment. Second, because of the limited number of respondents participating in this pilot study we cannot generalize our results, however findings form this study give us a valuable input to future research aiming to further explore the problem of managers' intention to overlook the ISP violation, especially when they consider that violation would save an on-going project from failing. Third, we consider that this study did not give us a detailed feedback to validate the scenario, which we believe should be tackled deeply in the future. As a result and in reference to this study, we aim to develop our theoretical framework and the survey instrument to be able to empirically test our theoretical assumptions.

6. References

Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A. and Boss, R.W. (2009), "If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security", European Journal of Information Systems, Volume 18, Number 2, 2009, pp151-164.

Brockner, J., Houser, R., Birnbaum, G., Lloyd, K., Deitcher, J., Nathanson, S. and Rubin, J.Z. (1986), "Escalation of Commitment to an Ineffective Course of Action: The Effect of Feedback Having Negative Implications for Self-Identity", Administrative Science Quarterly, Volume 31, Number 1, pp109-126.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information Security Policy Compliance: An Empiricael Study of Rationality-Based Beliefs and Information Security Awareness", MIS Quarterly, Volume 34, Number 3, pp523-548.

Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004), "A Model for Evaluating IT Security Investments", Communications of the ACM, Volume 47, Number 7, pp87-92.

Conlon, D.E. and Garland, H. (1993), "The Role of Project Completion Information in Resource Allocation Decisions", Academy of Management Journal, Volume 36, Number 2, pp402-413.

Dhillon, G. and Backhouse, J. (2001), "Current directions in IS security research: towards socio-organizational perspectives", Information Systems Journal, Volume 11, Number 2, pp127-153.

Eisenhardt, K.M. and Brown, S.L. (1998), "Competing on the Edge: Strategy as Structured Chaos", Long Range Planning, Volume 31, Number 5, pp786-789.

Furnell, S. (2014), "Password Practices on leading websites-revisited", Computer Fraud and Security, Volume 12, Issue 2014, pp5-11.

Hsu, C., Lee, J.N. and Straub, D. W. (2012), "Institutional Influences on Information Systems Security Innovations", Information Systems Research, Volume 23, Number 3, pp918-939.

Katz, D. and Kahn, R.L. (1966), "The Social Psychology of Organizations", New York: John Wiley & Sons.

Keil, M., Mann, J. and Rai, A. (2000), "Why Software Projects Escalate: An Empirical Analysis and Test of Four Theoretical Models", MIS Quarterly, Volume 24, Number 4, pp631-664.

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

Njenga, K. and Brown, I. (2012), "Conceptualising Improvisation in Information Systems Security", European Journal of Information Systems, Volume 21, Number 6, pp592–607.

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, Volume 21, Number 6, pp643-663.

Ross, J. and Staw, B. (1993), "Organizational Escalation and Exit: Lessons from the Shoreham Nuclear Power Plant", Academy of Management Journal, Volume 36, Number 4, pp701-732.

Simon, H.A. (1955), "A Behavioral Model of Rational Choice", The Quarterly Journal of Economics, Volume 69, Number 1, pp99-118.

Sleesman, D.J., Conlon, D.E., Gerry, M. and Miles, J.E. (2012), "Cleaning up the Big Muddy: A Meta-Analytic Review of the Determinants of Escalation of Commitment", Academy of Management Journal, Volume 55, Number 3, pp541-562.

Sonnenreich, W., Albanese, J. and Stout, B. (2006), "Return On Security Investment (ROSI) - A Practical Quantitative Model", Journal of Research and Practice in Information Technology, Volume 38, Number 1, pp55-66.

Staw, B.M. and Ross, J. (1989), "Understanding Behavior in Escalation Situations", Science, Volume 246, Number 4927, pp216-220.

Straub, D.W. and Welke, R.J. (1998), "Coping with systems risk: security planning models for management decision making", MIS Quarterly, Volume 22, Number 4, pp441-469.

Vance, A. and Siponen, M. (2012), "IS Security Policy Violations: A Rational Choice Perspective", Journal of Organizational and End User Computing, Volume 24, Number 1, pp21-41.

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, Volume 20, Number 3, pp267-284.

Willison, R., and Warkentin, M. (2013), "Beyond Deterrence: An Expanded View of Employee Computer Abuse", MIS Quarterly, Volume 37, Number 1, pp1-20.