Working Title: Employees Escalating Behaviour Towards Security Policy non-Compliance

Miranda Kajtazi
Linnaeus University

This study proposes a conceptual framework based on the escalation of commitment theory with the objective to identify the factors that trigger employees to violate their organisations' security policy, where violation often occurs in the process of escalation of commitment to a failing courses of action. The focus is on escalation of commitment in information – intensive organizations that are known to be more vulnerable in protecting their information. This study aims to address three questions. Does escalation occur in information security policy compliance? What factors seems to promote escalation? And, what factors can break escalation of commitment to information security compliance?

While recent technological developments have revolutionized the way organizations secure their information, employees in organizations still present the weakest link in the defence against information insecurity. Employees in organizations are involved with daily decision-making processes, in which they commonly break organizational rules and regulations to get their tasks completed. It is suggested that such behaviour usually happens when employees are unsure whether to persist or withdraw from a troubled task is a better decision, a pattern that in theory is understood as escalating behaviour. Escalation is a phenomenon which explains how individuals get involved in a failing course of action, and reflect the tendency of not knowing whether withdrawal or persistence is the best solution. Escalation occurs in various decision contexts, when investments in time, effort, and resources are devoted to a course of action, even if appropriate progress toward the objective of such investments has not been realized.

Consider the following situation. An employee of an information-intensive organization, such as a bank or pharmaceutical is involved in a certain task that needs to be finished on due date. The employee has almost finished that task, but in order to complete it, she needs some help from a person that has expertise in that area. She knows that her organization has an explicit security policy requiring that all information in that specific task, that is confidential, should not be compromised, i.e. communicated or given away to someone else within or outside the organization. Several questions arise from this situation. Does she communicate confidential information (via email, phone or face-to-face) to the contacted person to receive help for completing the task on time? Does she give away her password just to get the help for completing the task? Or does she decide to stop working on that task?

The escalation dilemma in this situation is fairly typical. It is assumed here that the employee has already devoted time, effort and resources to complete the task, and has decided to act against the security policy to complete the task, rather than withdraw from it and accept the loss. If an employee performs an action that is prohibited by the security policy, such as revealing confidential information to outsiders or giving away their passwords to their colleagues just to get their help, are some of the most common ways that trigger security policy non-compliance. This is a concern that poses increased unnecessary threats to organizations.

This study proposes a conceptual framework for developing a new understanding of how the escalation of commitment theory presents a unique context for analysing non-compliance behaviour with information security policies.