How to develop a computerized tool to help managers to design tailored policies?

Elham Rostami

CERIS - Informatics department, Örebro University, Örebro, Sweden
Elham.rostami@oru.se

Abstract

Information security policies (ISPs) as one of the most important controls to reduce security breaches in organizations have received significant attention from researchers. This is due to the fact that information security cannot be accomplished by technical means only and other factors such as human factors are important as well. Researchers admitted that poor security behaviour of employees (e.g. user security errors, carelessness, and negligence) has caused many security threats. Although the need for ISP has been stressed by researchers, they have provided slightly different definitions of this concept. My Focus on my thesis project is on strategic and operational level of ISP (non-technical level). By strategic I mean ISPs that address top managements strategic direction regarding information security and by operational, I mean issue-specific guideline and procedures that should be complied by employees in their daily activities. However, introducing ISP in organizations does not grantee security of information; nor does it necessarily reduce the number of security incidents. This is mostly because employees do not comply with ISPs. This may be because of the fact that ISPs can be cumbersome, incompatible with existing work practices and contradictory. Moreover, reading a big document of the organization ISP may not be interesting or even doable for all employees at different levels since they do not know which part is exactly related to them or the document is complicated for them to read. Considering the problems of ISP document and difficulties that employees have with it, constructing "tailored policies" for different employees by policy makers might be a way forward. By tailored policies we mean instead of providing a monolith ISP document for the organization and expect all employees to read it and find the part that is related to their job, we can construct ISPs that are specific for different employees based on their needs and responsibilities. On the other hand, security policies are not easy to create and the process of designing them is challenging. The process that is conducting manually is even more complex if managers want to repeat it frequently because of the dynamic nature of security policies. The suggestion is developing a computerized tool that can help managers in the process of designing (formulation) tailored ISPs. So, my focus on my thesis is on how we can develop such a tool.