A web-based software to assist managers to design tailorable information security policies

Elham Rostami
elham.rostami@oru.se
Center for Empirical Research in Information Systems (CERIS), Örebro University

Information security policies (ISPs) are one of the most important formal controls in organizations (Dhillon, 2017). ISPs explains acceptable and unacceptable behaviour of employees in relation to information assets in a secure manner (Alotaibi et al., 2016). Although organization spend a lot of resources on developing ISPs, we still hear security incidents time to time somewhere in the world because of human errors. It means that employees do not comply with the provided ISPs completely and for this reason they are called the weakest link in the information security chain. In this thesis we tried to change this mindset that security incidents happen because employees are careless, instead we put forward the idea that if managers provide good ISPs then employees might comply with them better, and consequently the security incidents decrease. Different requirements have been mentioned in the literature for having good ISP. One of these requirements is that a good ISP should be tailorable. It means that several ISPs should be provided for different groups of employees in organization based on the employees needs and responsibilities instead of one monolithic ISP for everyone. However, it is not clear how a tailorable ISP should be designed. At the same time, we know developing ISPs manually is a complicated and cumbersome task and there is a need to have a computerized tool to assist managers in designing ISPs (Rostami et al., 2020). Applying a situational method engineering concept and design science process we developed a policy component conceptual model that is a basis for developing computerized tools that support designing tailorable ISPs. Then a web-based software was developed based on the conceptual model. The software was introduced to a group of chief information security managers (CISOs) from public and private agencies in Sweden in a workshop. The main outcome of the workshop was that CISOs liked the idea of tailorable ISPs and emphasized on the need of a computerized tool to design such ISPs. This thesis has several contributions. The developed policy component conceptual model that is considered as a new design theory (Gregor and Jones, 2007) is the theoretical contribution and the web-based software is the artifactual contribution(Ågerfalk and Karlsson, 2020) of this thesis.

References

ÅGERFALK, P. J. & KARLSSON, F. 2020. Artefactual and empirical contributions in information systems research.

ALOTAIBI, M., FURNELL, S. & CLARKE, N. 2016. Information security policies: a review of challenges and influencing factors. *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE.

DHILLON, G. 2017. Information Security - Text & Cases Burlington, USA, Prospect Press.

GREGOR, S. & JONES, D. 2007. The anatomy of a design theory. Association for Information Systems.

ROSTAMI, E., KARLSSON, F. & KOLKOWSKA, E. 2020. The hunt for computerized support in information security policy management: A literature review. *Information & Computer Security*.