Computers & Security

Defining organisational information security culture—Perspectives from academia and industry

Botha, Adéle
Council for Scientific and Industrial Research
Pretoria, 0001, South Africa
Email: ABotha@csir.co.za

Abstract

The ideal or strong information security culture can aid in minimising the threat of humans to information protection and thereby aid in reducing data breaches or incidents in organisations. This research sets out to understand how information security culture is defined from an academic and industry perspective using a mixed-method approach. The definition, factors necessary to instil the ideal information security culture and the potential impact of the ideal information security culture were investigated from both perspectives. A survey approach was implemented to obtain the views from industry and 512 respondents from organisations, many of which operate at an international level, participated in the survey. The research presents a description of information security culture, integrating the existing literature and expanding on it with the views of industry, thereby giving clarity to the concept. The ideal information security culture was identified with the top traits relating to aspects such as an aware and knowledgeable workforce implementing conscientious, caring behaviour to comply with policies as guided by management. The factors that could positively influence an information security culture were identified, consolidated and expanded to five external factors and twenty internal factors. Organisations that have a strong information security culture were identified as achieving mutual trust and integrity through the protection of their information. The description of an information security culture can be used as a baseline to define and understand the concept, identify a single, comprehensive set of factors to be implemented, comprehend the traits of such a culture, as well as what an organisation can achieve by having a strong information security culture. The analysis showed that scientific interpretations of the definitions and factors of information security culture are much wider than their understanding of the industry. Both the results from the scoping review of papers and the feedback from the industry experts are synthesised visually to provide an organisational information security culture model (OISCM). The definition, factors, and model that influence the organisational culture of information

security, have prognostic value for industry. For scientists, this is an important topic of research on methods and forms of increasing the level of this knowledge.