Defining and Developing a Model for an Engaged Information Security Culture

Ashley Bye

Technical Report

RHUL–ISG–2018–1

2 March 2018

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

EXECUTIVE SUMMARY

Effective information security requires more than just implementing technical, physical and procedural controls. The increasing number of security breaches and their broad impact has led to an expanding volume of research into how organisations can implement an information security culture. Legislation such as the European General Data Protection Regulation helps, inter alia, to shape national aspects of this culture. However, it is the reification of often abstract concepts at an organisational level that this research seeks to address. Unlike much of the previous literature, which utilise aspects of organisational theory as a basis for developing a model for information security culture, this report addresses the topic from the perspective of safety culture as articulated by Reason and expanded upon Haddon-Cave QC. By comparing the common requirements of an information security culture and safety critical industries such as aviation and healthcare, it argues that there is sufficient cross-over to make further comparison worthwhile. Using the United Kingdom's Military Aviation Authority's model of an engaged air safety culture as a foundation, a model for an engaged information security culture is developed. The final framework – derived from the learning of various case studies in these safety critical industries and applied to information security objectives – consists of several values and behaviours components (just culture, reporting culture, learning culture, flexible culture and questioning culture) and key underpinning components (leadership commitment, open communication, and effective decision making). Conclusions from the report show that when these components are all implemented, the benefits can include improved risk awareness and reduction, increased organisational and employee knowledge and motivation, reduced litigation attempts, and good reputational value. Whilst the focus of this project and report is primarily concerned with the security benefits from developing an engaged information security culture, it also acknowledges that components of the model can have an indirect positive impact in other business domains. The principles identified in this report could be applied to business environments today, although being based on logic and thought-comparison, further academic scrutiny would enable their refinement and promote further discussion in the context of existing research.