Editorial

Socio-technical issues and challenges in cyber security

It has been widely recognised that the development of information security policies and regulations plays a key role in ensuring an effective information security management in theory. In support of practice, however, there is no real consensus, as there are multiple and competing approaches when assessing the implications of their implementation and the contextual factors. All of this has the potential to influence compliance behaviours and practices and we believe that this highlights a continued need for research into this crucial field.

The discussions presented in this special section all highlight that a socio-technical perspective on cyber-security is necessary to both illuminate the causes and facilitators of compliance to security policies and regulations. This perspective follows in the footstep of the long-standing socio-technical tradition in cyber-security as previously discussed in information security management literature.

This section starts with a presentation of a comparative analysis by Da Veiga *et al.*, between South Africa and the UK on the protection and use of online personal information. The research involved ten insurance organisation websites in each country to evaluate a number of data privacy requirements of the Data Protection Act and Protection of Personal Information Act. The results display a number of deficiencies, in terms of handling and processing of personal information, in both samples. However, the enforcement of regulation combined with achieving a certain maturity level in the implementation process within industry insurance in the UK appears to support more compliant practices. The authors explain that, in the South African context, the organisations within the insurance industry seem to not prioritise data protection and have different approaches to comply with data protection legislation. Therefore, they suggest that their research could potentially inform more effective compliance plans.

In the second paper, Weidman and Grossklags analyse 90 distinct information security policies from universities within the USA to examine the language and construction of these policies. The analysis shows significant disparities, in terms of language and content, between information security policies across organisations. This finding reflects a variety of approaches towards designing security policy and questions the applicability and the relevance in practice of available security standards and frameworks. The exploration of the reading complexity points to issues with clarity and consistency. The research shows that the sampled policies are generally difficult to read, in particular, if the policies are short in length, thereby compromising the accessibility of these policies to wider audience. When it comes to the tone, the analysis finds that policy documents are highly formal in their language structure and to some extent intentionally ambiguous.

Then, in the third paper, Kurowski explores to what extent policy compliance measurements in the current policy compliance research are biased. The author developed a pre-tested scenario-based measurement instrument for policy compliance, referred to as self-reporting policy compliance (SRPC) scale, to assess whether there are any significant differences between SRPC and existing policy compliance scales in the literature. The responses to the online survey, which involved 54 participants, show no significant biases in

This paper forms part of special section "Cyber-Security: Socio-Technical Issues and Challenges", guest edited by Moufida Sadok and Peter Bednar.

Information & Computer Security
Vol. 28 No. 3, 2020
pp. 397-398

2056-4961
DOI 10.1108/ICS-07-2020-148

terms of social desirability and generalised biases in the existing scales for policy compliance. However, the data analysis reveals the existence of a response bias in current scales, that is, they measure both policy compliant and secure behaviour for any reason but a policy. This is outstanding finding questioning the reliability of existing research scales for policy compliance. Kurowski concludes that the generic nature of the items used to measure policy-compliant behaviour is misleading and could consequently create uninformative results. The author argues that SRPC scale captures different compliance statuses and stresses the need for including specific scenario-based behaviours in policy compliance measurements.

Finally, the fourth and concluding paper by Sadok, Alter and Bednar, ties the scope of the key themes together and suggests that work systems theory could be a good starting point to reflect upon how to design and implement effective organisational security policies. This, based on an exploratory research study, involving employees from 39 SMEs, revealed that actual work practices and routines of most employees were either ignored or insufficiently intertwined with security management efforts. Moreover, security processes that are designed outside of the real world organisational context are prone to undermine effective organisational practices and create unintended consequences in the operation of work systems. Consequently, engagement and participation by professionals is needed to promote design of work systems that are not only user-friendly but also genuinely supportive of meaningful use in context.

Together, the four papers in this special section capture collectively the importance that security policies and regulations development is an inherently socio-technical matter, one, which is indivisible and intertwined and that it is neither desirable nor advisable to attempt to separate social and technical strands.

Moufida Sadok
Institute of Criminal Justice Studies, University of Portsmouth, Portsmouth, UK, and
Peter Bednar
University of Portsmouth, Portsmouth, UK