Editorial: Human aspects of cyber security

Human aspects are now widely recognized as being a key factor in providing a holistic cyber security solution. The nature of what we mean by human aspects can vary quite considerably, from intuitive aspects such as information security awareness and human–computer interaction to the less instinctive yet still important aspects such as the development of technical solutions that remove or reduce the security burden placed upon individuals. What all these areas have in common is the impact they have upon the people involved.

With this in mind, the Human Aspects of Information Security and Assurance symposium series seeks to provide a forum for a community of related researchers working in this area. In July 2022, the 16th event in the series was held in Lesvos, Greece. A total of 25 reviewed papers were presented over three days. From these, seven authors were invited to submit extended versions of their work for publication in this special issue. The resulting papers draw upon a range of areas including cyber security culture, information security management, security fatigue and the issue of privacy from a number of different perspectives.

Privacy is a topic that has seen increased interest from the research community in recent years. Three of the selected papers have focused upon this. Lindqvist and Kävrestad explored the degree to which privacy concerns are impacting citizens' willingness to report crimes. Following widely reported news articles raising the concern, this paper surveys 400 Swedish adults to seek their perspectives. Interestingly, whilst the willingness to share a mobile phone was low, a direct link to privacy was not established. Shanley *et al.* explored another aspect of privacy; that of Australian attitudes towards surveillance and the impact of COVID tracing applications. A survey of over 900 Australian adults showed a relatively high level of trust in government; however, they remain cautious and concerned over data being collected and had a strong desire to maintain control over their personal privacy. The final privacy-related paper by Chhetri and Motti sought to explore the development of privacy controls for Smart Homes. Using a mixed-methods approach, they undertook a series of evaluations for a novel prototype that helped to address the privacy gap.

A further three papers focused upon culture, management and policy-related issues. Da Veiga explores the use of innovation and creativity as enablers to develop information security culture. Through a literature review, the paper identifies a set of elements that help to stimulate creativity and innovation. Rostami *et al.* present a conceptual model for tailoring information security policies with a view to acting as a foundation for developing software to aid the automated development and tailoring of policies for organisations. Bhana and Ophoff further explore the issue of security fatigue of data specialists. Through a semi-structured interview of stakeholders, they reveal several interlinked themes that evidence security fatigue.

The final paper in the selection, from Glas *et al.*, is focused upon security education and awareness – in particular the use of visual programming in cyber range training to improve skill development. Evaluated against a control group, the study found that visual training provided a positive impact on the learning experience.

Information & Computer Security
Vol. 31 No. 3, 2023
pp. 265-266
© Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-07-2023-213

The papers collectively illustrate a range of relevant activities in the domain of human aspects, and it is certain that the breadth of the area as a whole will continue to offer rich opportunities for further research in the years to come.

Nathan Clarke
University of Plymouth, Plymouth, UK, and
Steven Furnell
School of Computer Science, University of Nottingham, Nottingham, UK