Guest 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 November 2017, the 11th event in the series was held in Adelaide, Australia. 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 are mainly focused upon the key issues of awareness and risk, alongside one further paper looking at the impact upon cyber analysts themselves.

Five of the papers explore aspects of user behavior with respect to information security practice (or more particularly, intent). Specifically, Jansen and Van Schaik investigate the role fear plays in ensuring compliance to phishing by using protection motivation theory. The study involved surveying over 1,000 people to understand to what degree fear would play a role in how users respond to phishing attacks. McCormac *et al.* focus upon how understanding the relationship between resilience and work stress impacted information security awareness. Snyman *et al.* present a study exploring how users' information security decisions or practice is impacted by the decisions made by others. Their study introduces the concept of the "lemmings effect" and demonstrates by experimentation that it exists within information security behaviors. Alohali *et al.* present a study exploring the factors that affect the end-user risk-taking behavior, focusing upon a range of factors such as personality, age, education and information technology proficiency to understand which ones may have a statistically strong correlation to risk-making decisions. The survey was completed by over 500 participants, and it was found that personality, in particular conscientiousness, does play a role in a large number of risk-taking decisions. In the fifth paper, Ashenden seeks to explore social acceptability bias in information security research. Using personal construct psychology and repertory grids, the study demonstrated that employees who thought that the organization was driven by the need to protect information also thought that the risks were overstated, and their colleagues were overly cautious.

The remaining two papers focused upon different areas of the human aspects theme: the first on measuring privacy perceptions and the second on gamification of security education. Da Veiga proposes an information privacy culture index framework to measure privacy perceptions across nations. Applied in a South African context, the paper reveals that South Africans have a high expectation of privacy yet feel that organizations are failing to meet both expectations and regulation. The final paper, by Micallef and Arachchilage, seeks to investigate the value gamification can have within security education. This study found that rewards within games do help to motivate users to have a better learning experience; however, social interactions within games

Information & Computer Security
Vol. 26 No. 3, 2018
pp. 262-263

2056-4961
DOI 10.1108/ICS-06-2018-0065

involving other users had an overall negative impact upon the experience. The authors argue that this might be linked to the nature of the topic and a lack of willingness to share security-based information.

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.

Steven Furnell
Center for Security, Communications and Network Research, Plymouth University, Plymouth, UK and Security Research Institute, Edith Cowan University, Western Australia, and
Nathan Clarke
Centre for Security, Communications and Network Research, Plymouth University, Plymouth, UK