Guest Editorial Preface

Special Issue on Socio-Technical Perspectives on Information Systems Security

Moufida Sadok, Institute of Criminal Justice Studies, University of Portsmouth, Portsmouth, UK

Research suggests that many of the existing risk analysis models and frameworks in information systems security (ISS) focus on technical modules and pay scant attention to the influence of contextual variables. Human interaction can affect the reliability of the provided solutions, for example security policies can privilege certain groups of stakeholders particularly managers and IT professionals. Exclusive emphasis on a technology-centered view as well as centralized security controls and top-down management may lead to flaws in the design and implementation of security solutions. By failing to appreciate the complex relationships between use, usability and usefulness, imposed security procedures are not only subject to possible misuse but they are likely to create difficulties for work functionality and efficiency. The weakest link is not necessarily in the technical system itself but the difference between the formal model of usage and real usage of system content (data) as such in a human activity system.

There are examples where the workforce finds ways of working around security compliance or bypass security controls in order to do their work effectively. By raising questions about security failures in context would address the relevance of security policies and measures from a stakeholders' perspective. A systemic and value-focused view of security would result in a better understanding of the role and application of security functions in situated practices and promote the attainment of contextually relevant risk analysis. Some researchers suggest that an integrative and multi-layered approach to information security should include human, organizational and technical factors in the design and management of a secure and usable system.

This Special Issue of the International Journal of Systems and Society brings contributions that highlight the potential benefits and effectiveness of adopting a socio-technical perspective on ISS in order to bridge the gap between design and implementation of secure systems.

This issue comprises six papers including an invited paper from Professor Steven Alter and the last word written by Professor Richard Baskerville. Steven Alter is from the University of San Francisco, has a long-standing history of US based research within the Socio-Technical subject area, and is well known for his focus on "work systems". The last word is written by Richard Baskerville, suggests that digital reality has drastically changed "conventional" security models and practices.

In the first paper Hart adopts a socio-technical approach to discuss and to address different perceptions of information security by individual virtual team members. Hart's approach provides the opportunity to conciliate between technical, organisational and human factors for an effective implementation of information security policy. The author suggests a future research agenda in order to gain a better understanding of attitudes and practices in virtual teams and information security practices.

In the second paper AlSabbagh and Kowalski point to issues with current incident response practices and suggest examining these practices through a socio-technical lens. The authors make use of design research framework to develop an artefact that combines technical metrics of security warnings with social security metrics. The implementation of such artefact is expected to effectively support organisations in managing security incidents.

The next paper by Thiem, Kautz, Pittayachawan and Bruno deals directly with a perceived divide between design and use of information security controls. Drawing on social network analysis (SNA) methods, the authors design and implement a cascading information system training/diffusion. Using canonical action research, the authors sought to enhance the information security related interactions between the employees in a large construction organisation in Southeast Asia.

Mühe and Drechsler question the applicability of structured and formalised information security frameworks mainly designed for the use of big companies. The authors point out that an IT risk management framework for SMEs should reflect and be associated to their particular socio-technical context.

The final paper by Serketzis, Katos, Ilioudis, Baltatzis and Pangalos also highlights the lack of contextualisation in most digital forensic frameworks. They argue that there is a dearth of research in this area that focus on contextual factors, which they say have the potential to significantly influence cybercrime investigations. The authors suggest that forensics and incident response represent a socio-technical challenge from an analyst perspective and they propose a framework that supports the investigation process by offering means for informed investigation and mitigation decisions.

This edition concludes with the invited paper and the last word.

In the invited paper Alter argues that work system theory has the potential to provide a background to understanding IS security. Alter discusses six lenses for describing, analysing, and evaluating IS security practices in order to complement data processing systems focused security approaches. The main contribution of the paper is showing that a work system perspective might provide a coherent container for describing, analyzing, and evaluating situations related to IS security and for studying IS.

The *Last Word* written by Baskerville is thought provoking. He says that digital machinery, such as computing and communications devices influence our physical world, leading to a digital reality that overlays physical and social reality. This digital reality is exciting, he says, because it holds wonderful promise for the future world of convenience and access together with the release of human labour from repetitive and programmable tasks. But he reminds us that digital security and digital safety is now security of the first kind. It is growing impossible, he says, for there to be any security or safety, either physical or social in the presence of digital insecurity or digitally unsafe situations. The wonderful promise of the future before us he argues has changed the goal of information security. It is now a much grander challenge than ever before.

Moufida Sadok
Guest Editor
IJSS