JISSec 4(1) 2008

Journal of Information System Security

www.jissec.org

Special Issue on Social and Ethical Aspects of Secure Computing

Editorial

We are pleased to present the first special issue of Journal of Information System Security. This Special Issue is devoted to the theme of social and ethical aspects of secure computing. In the inaugural issue of JISSec, the editors advanced as their mission to establish a broad appreciation for Information System Security concerns, as a result of acknowledging the wide and eclectic nature of Information System Security. The current issue of JISSec follows that path by fomenting the communication and debate on the social and ethical aspects underlying the maintenance of organizational integrity.

The first paper "Perceptual and Cultural Aspects of Risk Management" is co-authored by Jean-Noël Ezingeard of Kingston University, UK and Corey Hirsch of LeCroy Corporation, USA. In this paper the authors focus the need for a sociological understanding of the information system security risk management process. By grounding their analysis in a case study, the authors are able to show how that process requires attention to aspects that go beyond technological considerations and functionalist practices. The paper suggests a set of formal and informal mechanisms that may be useful to solve some of the challenges that risk management raises in a multi-stakeholder arena, such as the elevation of enterprise risk management practices, the reconciliation of risk perceptions among different organizational actors and the fostering of an aligned approach to risk management that may help an organization to define and migrate toward a robust enterprise risk culture.

The second paper "The Ethics of IT Disaster Recovery Planning: Five Case Studies" is by Nanda Surendra, A. Graham Peace and Daniel Connolly of West Virginia University, USA. This paper constitutes an exploratory study about the relationships between ethical postures and IT disaster recovery planning. The authors argue that virtually no practitioner or academic research has discussed the ethical issues associated with the critical area of disaster recovery. Having found this gap in the literature, the authors concentrated their inquiry on five organizations pertaining to different industry sectors and examined disaster recovery plans and practices through the lens of three major ethical theories currently employed to study how management ought to

behave. After analyzing how a disaster is defined, how business and IT service priorities are determined in a disaster recovery plan and how such a plan is operationalized, the authors concluded that the Stockholder Theory framework dominates the disaster recovery planning process. This paper illustrates how ethical aspects pervade secure computing practices and attempts to begin a discussion of the ethics of disaster recovery planning.

The third paper "Mitigating Consumer Perceptions of Privacy and Security Risks with the Use of Residual RFID Technologies through Governmental Trust" is by Andrew S. Jensen of University of North Caroline at Charlotte, USA, and Joseph A. Cazier and Dinesh S. Dave of Appalachian State University, USA. This paper discusses the perceptions of consumers regarding a technology that raises both security and privacy concerns, namely Residual RFID. Besides the usual constructs related to risk likelihood and risk harm, the authors bring to discussion the novelty construct government trust perceptions. By conducting a survey, the study examines the interplay between consumers' perceptions of trust, privacy risk likelihood and privacy risk harm and their impact on the intention to use RFID technology, taking into consideration the perceived role of government in the regulation of RFID and the protection of consumer privacy. The authors argue that government may play an important role in mitigating the effect of risk perceptions by taking appropriate steps to protect privacy from abuse through Residual RFID tags. Therefore, the study stresses the role of social processes in the adoption and deployment of technology that carries potential security and privacy implications.

We hope you enjoy reading this issue and we invite you to engage in the discussion of the social and ethical aspects of secure computing.

Filipe de Sá-Soares
Special Issue Editor