

Mini Track: 'Information Systems Security Management'

Mini Track Chairs:

Mikko Siponen^a

Gurpreet Dhillon^b

^a*Department of Information Processing Sciences, University of Oulu, Finland*

^b*Department of IS, School of Business, Virginia Commonwealth University*

The confluence of information and communication technologies and increased reliance of businesses on such advances has brought a range of information system security issues to the fore. It has indeed become difficult for organizations to protect their information resources with confidence. Perhaps this is the reason why incidents of security breach, computer crime and fraud have increased. The past research and practice has mainly relied on technical means to address the security concerns. Although desirable, an exclusive reliance on technical controls falls short of protecting the information resources. As previous research has suggested there are a range of social, organizational and management issues that need to be considered. The "Information Systems Security Management" minitrack address such IS security issues and present a reference point in providing a direction for addressing IS security issues in organizations.

The minitrack was organized within the track 'Internet and the Digital Economy' for the first time (HICSS-37 in 2004). In all we received 14 papers, which were subjected to a rigorous reviewing. Finally six papers were accepted. Clearly the accepted papers reflect the variety of issues and perspectives in the area of information systems security management. There is no doubt that the paper presentations will result in an interesting discussion.

Jari Råman explores in his paper "Network Effects and Information Security Consequences for Commercial Software" why there are security vulnerabilities in commercial software products. There review of literature takes an information economics perspective and reviews the budget constraints in secure systems development.

Fredrik Björck, in his paper "Institutional Theory: A New Perspective For Research Into IS/IT Security In Organizations", positions institutional theory as a valid mean to study IS security in organizations. In conducting the argument, the author reviews the pros and cons of the applicability of the concept and presents a coherent framework.

Christer Magnusson and Louise Yngström, in their paper "Method for insuring IT risks", present a new approach to risk analysis. Such an approach is based on the insurance principles used in calculating risk to other tangible assets.

Robert Willison in his paper "Understanding The Offender/Environment Dynamic for Computer Crimes: Assessing the Feasibility of Applying Criminological Theory to the IS Security Context", evaluates the dynamic based on criminology literature. Barings Bank as a case in point is used to conduct the analysis.

Fredj Dridi, Björn Muschall and Günther Pernul, in their paper "Administration of an RBAC system" describe the administration of a tool for managing role based access control. The tool is based on the functional specification of the role based access control standard, which is currently being considered for international standardization.

Finally, Raj Sharman and colleagues, in their paper "Functionality Defense by Heterogeneity: A New Paradigm for Securing Systems" present a new paradigm for securing systems. The concept termed as functionality defense by heterogeneity focuses on defense of functionalities rather than systems.