

RESEARCH PANEL

INFORMATION SYSTEMS SECURITY STANDARDS: THE SOLUTION OR THE PROBLEM?

Panelists:

Richard Baskerville (Chair), Georgia State University, 35 Broad Street NW, Atlanta, Georgia 30302-4015, USA, baskerville@acm.org

Gurpreet Dhillon, Virginia Commonwealth University, 1015 Floyd Avenue, Richmond, Georgia 23284-4000, USA, gdhillon@vcu.edu

Günther Pernul, LS für Wirtschaftsinformatik I – Informationssysteme, Universität Regensburg, D-93053 Regensburg. guenther.pernul@wiwi.uni-regensburg.de

Filipe de Sá-Soares, University of Minho, Department of Information Systems, Campus de Azurém, 4800-058 Guimarães, Portugal, fss@dsi.uminho.pt

Issues:

Security of information systems is not merely a technical issue, nor merely a systems management issue. It is also entwined in ethics and legal obligations for both commercial and government organizations. Information security managers and designers depend on reliable and consistent guidance for developing, deploying, and managing systems safeguards. They also need such guidance to be explicit in order to provide assurance and evidence that proper and responsible measures are present in the organization's systems. Accordingly, information Systems Security Standards and guidelines have been developed and published to provide both guidance and explicit evidence that information systems professionals are exercising due care in the management, development and deployment of security safeguards for information resources. The most widespread reference is the ISO/IEC 17799 standard, which was developed from the UK standard BS 7799. This UK standard had already become the de facto worldwide reference prior to its adaptation as an ISO standard.

ISO 17799 provides recommendations for security managers and designers that comprise initiating, implementing, and maintaining security safeguards. It standardizes security management practice and its use is intended to provide assurance to customers, shareholders, business partners, and other stakeholders that the organization's information systems are safe and reliable. Its scope is wide-ranging, incorporating guidance for security policies, security infrastructures, asset classification and control, access control, along with personnel, physical, and communications security. It also specifies compliance guidelines.

While ISO 17799 is the most prominent standard, there are other influential standards and guidelines. These include international conventions and myriad national laws defining organizational obligations for personal data security such as the Privacy, Directive 95/46/EC of The European Parliament and of The Council. In addition, legislation and professional guidelines are requiring disclosure, accountability and assurance by organizational management to shareholders and society. Examples include the 1992 Cadbury Code in the U.K and the 2002 Sarbanes-Oxley act in the

U.S. These codes and laws are increasing the pressure to follow generally accepted standards and practices that are detailed in second level frameworks that are more detailed guidelines and defacto standards. An example of such a framework is COBIT, a generally applicable and accepted standard for good information technology security and control practices in organizations.

While such standards provide structure and guidance for specifying security policies, safeguards, and organizational processes, they also add entropy where the fit is poor between organizational needs and the standards. The panellists will discuss the essential features in the security standard landscape, and how these features enable and/or inhibit attainment of organizational goals.

The panel will be organized to inform the audience, but also to promote create critical thinking and participation by those in the audience as well as the panellists.

Presentations:

Richard Baskerville will open the panel with a brief introduction to the role of standards in information systems security. He will outline the basic features of ISO 17799, the Sarbanes-Oxley Act and COBIT, using these three frameworks as a means to highlight the interdependent nature of security standards and guidelines for practice. Richard will briefly highlight the dualism inherent in standards with relation to organizational emergence. In order for organizations to be agile and adaptive, their information systems must be equally adaptive and flexible. A slavish adherence to a narrow interpretation of such general frameworks can impede the ability of organizations to adapt and grow unless carefully managed.

Gurpreet Dhillon will position security standards relative to system development life cycle and comment on the economic efficiency of having such a large number of standards. Besides ISO 17799, Gurpreet will introduce other information systems security related standards – ISO 15408; ISO 13335; ISO 21827, and the NIST 800 series guideline documents. This will form the backdrop for discussing overlaps, conflicts and inconsistencies between different standards. Gurpreet will then briefly comment on the economic inefficiencies of have a large number of standards dealing with the same issue. This will set the context for introducing an integrated due care model for addressing security in organizations.

Günther Pernul will comment on the proliferation of standards, regulations, and legislation related to IT security. There are many organizations and committees involved in building IT security related standards. Besides official standards many defacto standards and proprietary guidelines exist. Additionally, many regulations constantly are under revision and new versions apply. This is also true for the ISO 17799 for which a revision is announced for mid 2005. Although compliance with standards is growing in importance current situation is chaotic and confusing. It is no longer about meeting one compliance obligation, but a complex web of requirements that even grows exponentially as organizations cross international boundaries.

Filipe de Sá-Soares will discuss his analysis of ISO 17799, an international standard for information security management based originally on British Standard BS 7799. He will interpret ISO 17799 according to the Theory of Action and will condense this standard as an espoused theory in the field of information systems security management. Building on this interpretation, Filipe will reflect on the standard's actionability by addressing its stated goals, activities and consequences. He will

briefly relate these three aspects to the theory of information systems security and advance some considerations about ISO 17799 adoption and applicability.

About the Panelists:

Richard L. Baskerville's research and authored works regard security of information systems, methods of information systems design and development, and the interaction of information systems and organizations. He is a Chartered Engineer, holds a B.S. *summa cum laude*, from The University of Maryland, and the M.Sc. and Ph.D. degrees from The London School of Economics, University of London.

Gurpreet Dhillon is an Associate Professor of IS in the School of Business, Virginia Commonwealth University, Richmond, USA. He has M.Sc. and Ph.D. degrees in information systems from the London School of Economics and Political Science, UK. His research interests include management of information security, ethical and legal implications of information systems and aspects of information systems planning and project management.

Günther Pernul has been a full professor at the University of Regensburg, Germany, since 2002. Prior to that he held a similar position with the University of Essen, Germany, and visiting positions with the University of Florida, Gainesville, FL, as well as at the Georgia Institute of Technology, Atlanta, GA. His research interests are web-based information systems, information systems security, advanced applications. Pernul has written or edited 6 books, published in scientific journals and conference proceedings on various information systems topics and has participated in many R&D projects on national and international levels. He also serves on the steering board of the Communications and Multimedia Security conference series and is founding co-editor of the EC-Web (Electronic Commerce and Web Technologies, since 2000) and the TrustBus (Trust, Privacy and Security in Digital Business, since 2002) conference series.

Filipe de Sá-Soares has undertaken research in the area of information systems security and information systems planning. He holds a *Licenciante* in Informatics and Systems Engineering, a M.Sc. in Management of Information Systems and he is currently working on his PhD in information systems security at University of Minho.