JISSec 4(3) 2008

Journal of Information System Security

www.jissec.org

Editorial

This issue of the Journal of Information System Security presents three very interesting papers for the reader.

The first paper entitled 'Organizational learning for the incident management process: lessons from high reliability organizations' is written by Gerd Van Den Eede, Willem J. Muhren and Bartel Van de Walle from the Department of Information Systems and Management in Tilburg University. They observe that organizations typically struggle in order to combine effectiveness and efficiency for their individual product and while experimentation and trials are regarded as important tools for organizational learning they do not always achieve the optimum in terms of efficiency. The authors state that certain organizations, commonly referred to as High-Reliability Organizations (HRO's), exist and operate in hazardous environments but manage to structure themselves to be efficient and stay highly reliable. These HRO's involved in high tension industry are deprived of the luxury of the time consuming trial and error methods employed by other organizations and the authors state that it is due to this very fact that is accountable or the HRO's success. The authors investigate through a case study of the IT Incident Management process at a large European financial service provider, how people involved in a process of such a mainstream organization, where reliability is of great concern, can learn from HRO's in order to achieve a greater reliability while working efficiently. The authors state that the characteristics that make an HRO distinct from other organizations, to some extent, are present in the IT Incident Management process. The authors' main conclusion in the paper is that considerable opportunities remain to lift the HRO qualities to a greater level.

The second paper is entitled 'Incident Response Planning Using Collaboration Engineering Process Development and Validation' and is written by Alanah J. Davis, Mehruz Kamal, Terrance V. Schoonover, Leah R. Pietron and Gert-Jan de Vreede from the The Institute for Collaboration Science, the University of Nebraska at Omaha and Josephine Nabukenya from the Institute for Computing and Information Sciences, Radboud University Nijmegen. The authors state that many organizations have plans for incident response

strategies as part of their contingency planning process. They observe the fact that an Incident Response Plan (IRP) is not created by a single individual as it requires the inputs and contributions from a wide range of organizational experts. However, orchestrating the efforts of a group of experts to produce a comprehensive IRP in a short time frame can be extremely challenging. Despite IRP being an essential ingredient in conjuring security planning procedures in organizations, extensive literature reviews have revealed that there are no collaborative processes in place for such a crucial activity. The authors propose a study designed for a facilitated incident response planning process using technology such as group support systems (GSS). The paper concludes that that after three sessions were conducted, an analysis of the sessions revealed that the facilitated IRP design held up strongly in terms of goal attainment and session participant satisfaction. Further research involves devising an all-encompassing integrative general approach that would be applicable to any form of corporate development planning.

The third paper is entitled 'The duality of information security management: fighting against predictable and unpredictable threats' and is written by Paolo Spagnoletti and Andrea Resca from CeRSI - Luiss "Guido Carli" University, Italy. The authors state that Information systems security is a challenging research area in the context of Information Systems. It has strong practical implications for the management of Information Systems and at the same time, it gives very intersting insights into understanding the process of social phenomena when communication and information technologies are deployed in organizations. The current standards and best practices for the design and management of Information Systems Security recommend structured and mechanistic approaches, such as risk analysis methods and techniques, in order to address security issues. However, risk analysis and risk evaluation processes have their limitations and the authors state that when security incident s occur, they emerge in a context, and their rarity and even their uniquity give rise to unpredictable threats. The analysis of these phenomena, which are characterised by breakdowns, surprises and side effects, require a theoretical approach which is able to examine and interpret subjectively the detail of each incident. The authors aim in this paper is to highlight the duality of Information Systems Security, providing an alternative view on the management of those problems, and this is pursued through a formative text that supports bricolage, hacking and improvisation.

Gurpreet Dhillon
Editor-in-Chief