JISSec 6(4) 2010

Journal of Information System Security

www.jissec.org

Editorial

I am pleased to offer Volume 6, Issue 4 of JISSec. This issue contains four rather interesting and eclectic articles, which represent different geographical regions.

The first paper, "Information Security Conscience: a precondition to an Information Security Culture?" is by Kerry-Lynn Thomson of Nelson Mandela Metropolitan University, South Africa. The author argues that one of the major difficulties in implementing good information security practices organizations is the ignorance of different attitudes and behaviors of employees. This results in a lack of alignment of management and employee goals. The author then makes a call for an information security obedient culture, which will enable the flow of knowledge creation within the organization.

The second paper, "Economic Analysis of Digital Rights Management for Software Updates" is by Taeha Kim of Chung-Ang University, South Korea and Alexander Talalayevsky of Consortium for Ocean Leadership, USA. The work presented examines the role of digital rights management in the context of software updates/patches. The authors discuss significant concerns, particularly relating to pricing, piracy and quality. The conclusions of the study suggest that digital rights management decision for updates is an effective strategy where piracy rights are high, quality of pirated software is low and the base product is of a high price. The authors present a threshold level for a sufficient number of updates that will act as an incentive to purchase the software.

The third paper, "Password Collection through Social Engineering: An Analysis of a Simulated Attack" is by Joseph A. Cazier, Christopher M. Botelho and Baylor Health of Appalachian State University, USA. The authors demonstrate the vulnerability of individuals to social engineering attacks. Training does not seem to have a significant impact. Results of a simulation are presented to support the argument. Surprisingly, 73% of the respondents shared their passwords with the researchers. This was in spite of the training that was conferred.

The fourth and the final paper, "Patient Safety and Patient Privacy in Information Security from the patient's view: A Case Study" is by Rose-Mharie Åhlfeldt and Eva Söderström of University of Skövde, Sweden. The authors present a Swedish case study pertaining to patient safety and patient privacy. While patient safety and privacy are both information security concerns, the focus usually seems to be more on safety rather than privacy. The authors make a call for inherent concerns in the management of patient privacy. Particularly in light of sharing of information amongst patients and health care organizations.

All together the four papers present diverse viewpoints on aspects of information security management. An interesting theme that seems to run through all the papers is that in spite of awareness campaigns and training, information security problems and concerns seem to persist. It would perhaps be interesting to analyze why training does not seem to improve levels of information security.

Gurpreet Dhillon
Editor-in-Chief