JISSec
Journal of Information System Security

Journal of Information System Security is a publication of the Information Institute. The JISSec mission is to significantly expand the domain of information system security research to a wide and eclectic audience of academics, consultants and executives who are involved in the management of security and generally maintaining the integrity of the business operations.

ISSN: 1551-0123
Volume 15, Issue 1

www.jissec.org

EDITORIAL

The three papers of this Issue contribute to the institutional theory of information systems security by examining how information security breaches undermine organizations' reputation and legitimacy. The papers quantify the potential damage from such threats, including the demand for a ransom, and proceed to identify models, forces and activities which can have a positive influence in the prevention of security breaches.

The first paper, entitled "Information Security Risks Propagation and Management in Supply: an Analytical Approach", is by Bin Mai and Jianguo Liu, from the USA. It investigate the impacts and management of information security risks in supply chain management. The authors develop an innovative analytical model of a general multi-tier supply chain with multiple information assets facing multiple information security threats which can guarantee the existence of an optimal strategy of information security investment. The paper indicates the direct and significant impacts of information security threat propagation on information security investment strategy.

In the second paper, "Antecedents of Information Security Activities: Drivers, Enablers, and Constraints", the authors Kevin Gallagher, Xiaoni Zhang, and Vickie Coleman Gallagher, from the USA, examines institutional forces as predictors of higher levels of assimilation of information security-related activities, together with organization-innovation related enablers and constraints. The research found that two of the three institutional forces were significant, as were complexity, compatibility and the control variables, the practical implications being that coercive forces, such as legal and governmental ones, together with parent company requirements, provide the greatest positive influence on instituting these activities.

The third paper is entitled "Ransomware and its Implications: a Report", and is by James Daigle, also from the USA. This paper examines how cyber criminals encrypt data on a computer and demand a ransom for the key to unencrypt the data. The research explores ransomware and its global implications, not only on local and global economies, but also on industrial firms. The paper concludes by proposing what, if anything, can be done to protect against future attacks.

I hope that you enjoy reading this Issue.

Gurpreet Dhillon, Editor-in-Chief