JISSec
Journal of Information Systems Security

The Journal of Information Systems Security is a publication of the Information Institute. The JISSec's 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.

Print ISSN: 1551-0123
Online ISSN: 1551-0808
Volume 19, Issue 2

www.jissec.org

EDITORIAL

This Issue contains an editorial note and three research papers. On the one hand, the editorial note focuses on the importance of information systems security in improving the effectiveness of organizational communication. Developing this theme, the research papers concern diverse examples of the need to strengthen information systems security, ranging from defense against ransomware attacks and insider threats to the need to consider cybersecurity as being much more than just a mere unavoidable infrastructure cost.

The editorial note explains the importance of coordination and the division of labor which define the nature of organizations and by nature are dependent on good communication. In turn, information systems are essential to guarantee the security of both informal and digital communication.

The first paper, entitled 'An Inside View of a Ransomware Attack Response and Recovery', is by Casey Dzimiela and Murray E. Jennex, from the USA. It provides a first-hand account of the response by the state national guard cybersecurity unit to one of the 23 communities that were affected by a ransomware attack in Texas. After a detailed analysis, recommendations are made to help improve cybersecurity awareness and preparedness in SMEs.

In the second paper, 'The next big strategic play: cybersecurity as a competitive advantage', the authors, Tamara Schwartz, Jose Ignacio Parada, Fred Cohn, George Wrenn and Keri E. Pearlson, from the USA, seek to disrupt the paradigm that cybersecurity is a necessary that is delegated to the IT team by exploring how cybersecurity can create a strategic advantage.

The third paper is entitled 'House of Cards: developing KPIs for monitoring cybersecurity awareness (CSA)', and is by Mohammad M. Alshammari and Dionysios S. Demetis, from Saudi Arabia and the UK, respectively. It addresses the need for organizations to contain non-malicious insider threats through the development and monitoring of Cybersecurity Awareness (CSA) programmes through the design of a model to evaluate KPIs. Insider threats continue to pose a significant concern to organizations' cybersecurity defense strategy.

I hope that you find this second Issue of 2023 of interest.

Gurpreet Dhillon, Editor-in-Chief