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 20, Issue 3

www.jissec.org

EDITORIAL

The Editorial Note highlights the role of AI in empowering employees. By providing access to training, support systems, and AI literacy, human potential can be unlocked as never before, leading to empowerment. The three research papers of this Issue explore diverse preventive measures that reduce the risk of cyber-attacks, namely: phishing avoidance behavior, combating the breaking of key cryptography by increasing powerful quantum computers, and the need to counteract insider threats.

The first paper, entitled 'Media impact on mobile phishing avoidance behavior' is by Xiaoqing Li, from the USA. It investigates the influence of various forms of media on individuals' motivation to prevent mobile phishing attacks. Based on technology threat avoidance theory (TTAT), the study extends a current research model on mobile phishing avoidance by introducing media influence. The research findings indicate the significant role of news media in motivating users to avoid mobile phishing attacks.

In the second paper, 'The Future of Cybersecurity: The Quantum Challenge', the authors, Mário Caldeira and João Sabino, from Portugal, examine the threat of quantum computers for cybersecurity. Cryptography is a key pillar of cybersecurity, which is used to encode and protect data. In this paper, the authors explore how future quantum computers will likely solve extremely challenging computational problems and break public-key cryptography by using brute-force attacks. The paper identifies that in order to protect critical information from more powerful and advanced hacking power enabled by future quantum computers, organizations need to redefine their security procedures and implement new techniques and technologies, such as post-quantum cryptography (PQC) or quantum key distribution (QKD).

The third paper is entitled 'A Synthesis of Research on Insider Threats in Cybersecurity', and is by Daniël Joubert and Jan Eloff, from South Africa. The insider threat problem remains a persistent dilemma. Although it is one of the major cybersecurity threats, it remains one of the lesser researched fields in cybersecurity. Employing a topic modeling approach to identify a series of current insider threat research topics, the authors identify research gaps in relation to current cybersecurity trends, indicating a misalignment between current insider threat research and reality.

I hope that you enjoy reading this last Issue of 2024.

Gurpreet Dhillon, Editor-in-Chief