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 21, Issue 3

www.jissec.org

EDITORIAL

It is argued in the editorial essay that Michel Foucault's theories of power are once again gaining currency with the convergence of AI, surveillance and cybersecurity. From the 'panopticon' effect derived from AI-driven cybersecurity, through proactive risk management and the legitimacy of control through the classification of threats, we may find ourselves susceptible to control not only for what we have done, but what we may be predicted to do algorithmically. The shaping of behaviors need not necessarily be coercive where people internalize self-surveillance by conforming to norms. Focault emphasized that power is never absolute; we need not become docile digital slaves – agency may be reclaimed through resistance.

It is the intersection of generative AI and cybersecurity that Adriaan Lombard and Stephen Flowerday, from the USA, explore in their paper 'Exploring the Risks of AI on Human Worth'. Their concern is how to reach an appropriate balance between the advance of AI and cybersecurity risks, such as privacy infringements and psychological manipulation. They correlate Maslow's hierarchy with the Big Five personality traits, providing a nuanced view of how AI influences human self-perception and worth. They look to a future where AI supports human dignity and contributes to a deeper understanding of our shared humanity.

In their paper, 'Not All SMEs Are the Same: Categorizing Security Needs of SMEs', Murray E. Jennex, Jeffry Babb, Amjad Abdullat, Abraham Abby Sen, and Kareem Dana of West Texas A&M University, USA, extend maturity model literature to the SME context, emphasizing the socio-technical interplay of technology adoption and organizational readiness. Their findings emphasize the need to address SME-specific cybersecurity needs – particularly those of 'micro enterprises' that often have budgetary constraints, a lack of cybersecurity expertise in-house, insufficient training, and inadequate security measures, among other challenges.

Alanoud Aljuaid and Xiang Liu consider the vulnerabilities of NLP-based systems to adversarial attacks, evaluate the impact of adversarial attacks on the effectiveness of NLP-based systems, and recommend strategies to fortify NLP-based systems against adversarial attacks in their paper, 'Adversarial Attacks on Natural Language Processing (NLP) Systems: An Emerging Threat in Cybersecurity'. They defend that there are interventional strategies which may be used to reduce the extent and impact of attacks on NLP-based systems.

Join the resistance with this final issue of 2025!

Gurpreet Dhillon, Editor-in-Chief