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 22, Issue 1

www.jissec.org

EDITORIAL

The prevalence of online romance scams is a symptom of wider cyber-security issues and generally comes down to bad decision-making by vulnerable individuals which is exploited by increasingly sophisticated cybercriminals able to give an illusion of credibility in a fast-evolving digital world. Healthy skepticism remains essential to prevent scammers, who succeed because they understand how trust develops and how emotions influence decision-making. Recognizing these psychological dynamics remains one of the most effective defenses against online deception.

Risk disclosures of Fortune 500 companies that have experienced a breach are increasingly considered redundant by both regulators and investors according to Sunita Goel and Nishani Vincent in their paper, "A Multi-Method Exploratory Analysis of Risk Disclosures Following a Security Breach". Instead of meaningful risk assessment, risk disclosures are frequently written in vague, boilerplate language which seeks to insulate companies from legal liability, and their length is no guarantee of their quality. Most worryingly, such disclosures rarely report on past breaches and remedial measures implemented to address vulnerabilities, preferring positive forward-looking statements.

Mohamad Hachem, Adam Lanfranchi, Nathan Clarke and Joakim Kävrestad examine password cracking in their paper, "Optimizing Password Cracking for Digital Investigations". The issue is critical for digital forensics and the analysis of electronic evidence within criminal investigations and incidents and is crucial to modern crime solving. Their paper presents a study investigating password cracking optimization, concentrating on whether password cracking rule-sets can be optimized in order to aid timely cracking and the impact of the NCSC recommendation on using three-word passwords on password cracking. Their findings contribute to both forensic efficiency and cybersecurity awareness, highlighting the dual impact of password policies on security and investigative capabilities.

In their paper "An Organizational Self-Assessment Tool for Digital Security by Design", Steven Furnell, Maria Bada, Michal Kukula and Lucija Šmid look at how Digital Security by Design (DSbD) offers a means to improve IT security by eliminating vulnerabilities using a Self-Assessment Tool. The extent of stakeholder alignment in understanding and supporting security needs is also critical, including compatibility with existing risk assessment frameworks within an organization.

I trust that this first issue of 2026 meets with your approval.

Gurpreet Dhillon, Editor-in-Chief