

This paper makes a significant and timely contribution to the scientific foundations of cybersecurity by advancing a novel, empirically grounded approach to understanding and mitigating one of the most complex and under-addressed threats: malicious insider behaviour. *Inside the Threat Matrix: Using Hybrid Computer Simulations to Educate Adults on Malicious Insider Threat and Technology Misuse* introduces an innovative hybrid computer simulation methodology that fundamentally rethinks the design, evaluation, and scaling of cybersecurity education and training.

At its core, the paper addresses a critical gap in cybersecurity science. While technical controls and awareness-based training dominate current practice, there remains limited scientific understanding of how to educate adults effectively about malicious insider threats, particularly those involving intentional, socially embedded behaviours such as IP theft. This work moves beyond traditional “information-deficit” models by integrating psychological theory, behavioural science, and simulation-based methods into a unified experimental framework.

The primary scientific contribution is the development and validation of a hybrid simulation paradigm that integrates controlled experimental design with immersive, socially realistic environments. Unlike conventional training tools, this approach allows participants to actively engage with or resist insider threat scenarios in a safe yet behaviourally authentic setting. The simulation design, spanning multiple rounds, incorporating organisational structures, and embedding real-world incentives, enables the observation of decision-making processes, ethical reasoning, and behavioural pathways otherwise inaccessible through surveys or static experiments.

Importantly and uniquely, the paper is grounded in Mezirow’s Transformative Learning Theory, demonstrating how “disorienting dilemmas,” critical reflection, and perspective-taking can drive meaningful behavioural change. This integration of adult learning theory into cybersecurity for the first time represents a substantial advancement, offering a principled explanation of why and how training interventions can influence behaviour rather than merely increase awareness. The findings show that participants not only perceived the simulation as highly realistic but also engaged in deep reflection on ethics, insider tactics, and their own potential real-world responses, which is evidence of transformative learning in action.

Methodologically, the paper introduces a new class of experimental tools for cybersecurity research. The hybrid simulation approach enables the study of socio-technical interactions, bridging the long-standing divide between human factors and technical cybersecurity research. It also opens new avenues for studying adversarial behaviour, insider recruitment dynamics, and organisational vulnerabilities in controlled yet ecologically valid settings. This represents a foundational step towards more rigorous, behaviourally informed cybersecurity science.

The broader impact of this work is substantial. By demonstrating that immersive, theory-driven simulations can effectively train individuals to recognise, resist, and reflect on insider threats, the paper offers a scalable pathway for organisations to enhance resilience to high-impact cyber incidents. Moreover, the framework generalises to other domains of technology misuse, including fraud, scams, and online abuse, thereby amplifying its relevance across the cybersecurity landscape.

In sum, this paper exemplifies the interdisciplinary, scientifically rigorous research that the NSA Best Scientific Cybersecurity Paper Competition seeks to recognise. It advances foundational knowledge, introduces a novel methodological paradigm, and delivers actionable insights with clear implications for research and practice.