Article Review: Cybersecurity Studies

Article 1: Impact of cybersecurity and AI related factors on incident reporting suspicious behavior and employees stress: Moderating role of cybersecurity training.

Social Science Principles: The study examines human factors in cybersecurity, focusing on employee behavior, stress levels, and organizational training - key aspects of social psychology and organizational behavior in cybersecurity.

Research Questions/Hypotheses: The study tested 8 hypotheses, primarily examining how incident reporting of suspicious behavior mediates relationships between cybersecurity management, awareness, AI intentions, perceived threats, and employee stress levels. It also explored how cybersecurity training moderates these relationships.

Research Methods: Quantitative approach using structured questionnaires administered to 229 employees across various sectors, including fast food, online retail, and banking.

Data Analysis: Utilized structural equation modeling with partial least squares estimation (SEM-PLS). Descriptive statistics were computed for factors rated on a 1-5 scale, analyzing means and standard deviations for various cybersecurity-related constructs.

Class Concepts: The study relates to organizational cybersecurity practices, human behavior in security contexts, and the intersection of AI with security awareness - all fundamental concepts in cybersecurity social science.

Marginalized Groups: The study doesn’t explicitly address marginalized groups, though it considers diverse sectors and employee roles, potentially capturing varied perspectives across different organizational levels.

Societal Contributions: The research provides insights into how organizations can better manage employee stress related to cybersecurity and AI implementation through effective incident reporting systems and training programs, contributing to improved workplace well-being and security practices.

Article 2: Investigating the intersection of AI and cybercrime: Risks, trends, and countermeasures

Social Science Principles: The study applies criminological theory (Cyber Routine Activities Theory) to understand cybercrime, examining human behavior, social interactions, and the psychological aspects of AI-enabled criminal activities online.

Research Questions: The study was based on three primary questions:

i. How is information involving malicious use of AI distributed and used on both the dark and clear web?
ii. What role does media dissemination play in the spread of AI-facilitated cybercrime?
iii. How can individual cyber hygiene practices be improved to reduce the risks associated with AI-based threats?

Research Methods: The mixed-methods approach combines quantitative data collection from online forums and qualitative semi-structured interviews with six cybersecurity experts between September and December 2023.

Data Analysis: Quantitative analysis of 102 malicious AI prompts across eight online forums in multiple languages. Qualitative analysis used thematic analysis following Naeem et al.'s (2023) process, identifying recurring themes from expert interviews.

Class Concepts: Addresses core cybersecurity concepts including threat actors, attack vectors, and defense mechanisms, specifically in the context of emerging AI technologies.

Marginalized Groups: The study's multi-language analysis suggests consideration of non-English speaking communities and global cybercrime impacts.

Societal Contributions: The research is useful in understanding AI-related cybercrime trends and measures that can be taken to prevent such an occurrence. This helps in policy advisories and cyber hygiene measures. It helps to raise awareness about AI abuse in cybercrimes and provides recommendations on how citizens and corporations can avoid such risks.

References

Muthuswamy V.V. & Essaki S. (2024). Impact of cybersecurity and AI's related factors on incident reporting suspicious behavior and employees stress: Moderating role of cybersecurity training. *International Journal of Cyber Criminology*. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/330/99

Shetty S., Choi K., & Park I. (2024). Investigating the intersection of AI and cybercrime: Risks, trends, and countermeasures. *International Journal of Cyber security, Intelligence & Cybercrime*. https://vc.bridgew.edu/ijcic/vol7/iss2/3