Article Review #1: Impact of Cybersecurity and AI's Related Factors on Incident Reporting Suspicious Behaviour and Employees Stress: Moderating Role of Cybersecurity Training

Student Name: Mason Cerezo

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: October 06, 2025

Introduction/BLUF

This article, written by Vimala Venugopal Muthuswamy and Suresh Esakki (2023), examines how cybersecurity and artificial intelligence (AI) related factors influence employees' incident reporting behavior and stress levels. This study highlights how cybersecurity training influences these relationships, providing key insights into how human factors affect cybersecurity effectiveness.

Relation/Connection to Social Science Principles

The study reflects multiple principles of the social sciences, especially behavioral and organizational psychology. It emphasizes how awareness, perception, and stress influence individual decision-making and performance within organizations. This aligns with the principle of empiricism and with determinism, as it identifies factors, such as training and awareness, that shape actions. The research also integrates the principle of social influence by showing how organizational culture affects security behavior.

Research Question /Hypothesis/ Independent Variable/Dependent Variable

- Research Question: How do cybersecurity and AI-related factors affect employees' reporting of suspicious behavior and stress, and how does cybersecurity training moderate this relationship?
- Hypotheses: The study hypothesizes that cybersecurity awareness and AI-related factors influence incident reporting behavior, which correlates with employee stress. Cybersecurity training moderates these relationships.
- Independent Variables (IV): Cybersecurity awareness, perceived AI threat.

- Dependent Variable (DV): Employee stress.
- Mediating Variable: Incident reporting behavior.
- Moderating Variable: Cybersecurity training.

Types of Research Methods used

The researchers employed a quantitative research design using a structured survey questionnaire. Data was collected from employees in organizational settings to evaluate their awareness, perceptions of AI, reporting behaviors, and stress levels. The study utilized a cross-sectional approach to examine relationships among variables.

Types of Data Analysis used

Quantitative statistical analyses were conducted using mediation and moderation testing, possibly through regression or structural equation modeling (SEM). Reliability tests, such as Cronbach's alpha, ensured data consistency, and path analysis tested both direct and indirect effects of variables.

Connections to other Course Concepts

The article connects to course concepts such as human behavior in cybersecurity, insider threat mitigation, and shaping secure practices. It reinforces the idea that cybersecurity is not just technological but social awareness, employee mindset, and workplace culture. The use of AI-related perceptions aligns with discussions on how emerging technologies influence user trust and security compliance.

Connections to the Concerns or contributions of Marginalized Groups

Although the study does not focus directly on marginalized populations, its implications apply to them. Marginalized employees may face unique challenges in reporting suspicious behavior due to organizational hierarchies or fear of retaliation. Additionally, unequal access to cybersecurity training could increase gaps in awareness and stress. Addressing these gaps would promote inclusivity and fairness in cybersecurity culture.

Overall societal contributions of the study/Conclusion

This study improves our understanding of the social aspects of cybersecurity by linking psychological and organizational factors with employee performance. It emphasizes the importance of continuous training, stress management, and inclusive security practices. By integrating AI perceptions and human behavior, it contributes to building safer, more resilient organizations and highlights the need for social science perspectives in cybersecurity research.

Reference

Muthuswamy, V. V., & Esakki, S. (2023). Impact of cybersecurity and AI's related factors on incident reporting suspicious behaviour and employees stress: Moderating role of cybersecurity training. International Journal of Cybercriminology, 17(2), 330–347.

Article Link:

https://www.cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/download/330/99/637