Keith Bartlett
04/02/2025

Article Review #2
Navigating Cybersecurity and AI: Insights into Incident Reporting, Employee Stress, and Training Moderation

https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/330/99

Research Questions and Methods

The study investigates several hypotheses that aim to uncover how incident reporting systems and cybersecurity training influence employee stress levels in organizations. (Venugopal Muthuswamy & Esakki, 2024)

1. Incident reporting mediates the relationship between CIM and ESL.
2. Incident reporting mediates the relationship between PTIA and ESL.
3. Cybersecurity training moderates the relationship between CIM and incident reporting.

The study employs a quantitative method using structured questionnaires distributed among 229 employees across diverse sectors, including fast food, e-commerce, banking, and related industries. Structural equation modeling with partial least squares estimation (SEM-PLS) is utilized for data analysis, ensuring robust statistical insights into complex relationships among variables. (Venugopal Muthuswamy & Esakki, 2024)

Data Collection and Analysis

The data analysis focuses on descriptive statistics for constructs such as CIM, CA, IUA, PTIA, cybersecurity training, incident reporting suspicious behavior, and ESL. Each construct is rated on a scale from 1 to 5, with mean scores reflecting typical responses and standard deviations indicating variability. For example:

- CA achieved the highest mean score (3.66), indicating high self-reported awareness. (Venugopal Muthuswamy & Esakki, 2024)
- IUA had a lower mean score (2.97), suggesting less frequent use or intention to use AI technologies. (Venugopal Muthuswamy & Esakki, 2024)

Measurement model results confirm strong reliability and validity across constructs, with Cronbach's Alpha values exceeding 0.7 for most variables.

Relation to Marginalized Groups

While the study does not explicitly focus on marginalized groups, its findings highlight broader societal concerns that indirectly affect vulnerable populations. For instance, workplace stress

exacerbated by cybersecurity challenges may disproportionately impact employees in lower socioeconomic positions due to limited access to resources or support systems. Additionally, AI-related technostress could deepen inequalities for groups less equipped to adapt to technological changes. (Venugopal Muthuswamy & Esakki, 2024)

Contributions to Society

The study makes significant contributions:

- It underscores the importance of robust incident reporting systems in enhancing organizational security.
- It highlights the role of cybersecurity training in reducing employee stress levels associated with AI adoption and perceived threats.
- It advocates for integrating psychological support with technical measures in cybersecurity management to safeguard employee well-being.
- The findings provide actionable insights for organizations aiming to improve their cybersecurity posture while addressing employee welfare

Applications of Principles

The study applies several principles of social sciences to explore the interplay between cybersecurity practices and employee well-being. It emphasizes empiricism by collecting quantitative data through structured questionnaires and analyzing them using structural equation modeling (SEM-PLS). The research demonstrates objectivity by examining relationships between cybersecurity incident management (CIM), awareness (CA), intention to use AI (IUA), perceived threats in AI (PTIA), and employee stress levels (ESL) without bias. The principle of determinism is evident in the exploration of how cybersecurity training moderates these relationships, suggesting predictable outcomes based on specific interventions. Additionally, the study incorporates skepticism by critically evaluating the limited impact of training on certain dynamics, such as the link between IUA and incident reporting. (Venugopal Muthuswamy & Esakki, 2024)

Relations to Presentations

The presentations highlight human factors as critical to understanding cybersecurity challenges. This concept connects to the article's exploration of employee stress caused by cybersecurity incident management (CIM) and AI adoption. For example, The "Human Factors" module discusses how psychological states influence technology use, which is mirrored in the article’s findings about how perceived AI threats exacerbate workplace stress. The emphasis on usability and adaptability in human systems integration resonates with the article’s recommendation for integrating psychological support into technical cybersecurity measures. The PowerPoint modules also explore various psychological theories, such as cognitive and behavioral theories, to explain cyber behaviors. Cognitive theories explain how employees may rationalize their stress or perceive AI threats based on faulty thinking patterns. Behavioral theories suggest that workplace training can mitigate risky behaviors, aligning with the article’s emphasis on

cybersecurity training as a moderating factor for stress reduction. (Venugopal Muthuswamy & Esakki, 2024)

Conclusion

By investigating how incident reporting mediates relationships among key cybersecurity factors and how training moderates these dynamics, this research advances understanding of employee stress within technologically driven workplaces. Its recommendations for comprehensive approaches integrating psychological and technical strategies contribute to building resilient organizational environments capable of addressing both security threats and workforce health challenges.

Works Cited

Venugopal Muthuswamy, V., & Esakki, S. (2024, June). Impact of Cybersecurity and AI's Related Factors onIncident Reporting Suspicious Behaviour and Employees Stress: Moderating Role of Cybersecurity Training. CyberCrime Journal. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/download/330/99

(Venugopal Muthuswamy & Esakki, 2024)