

Article Review #2: Controlling Cyber Crime

Matthew Chestnut

School of Cybersecurity: Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Prof. Yalpi

04/16/2026

Bottom Line Up Front

In the article, “Controlling Cyber Crime through Information Security Compliance Behavior: Role of Cybersecurity Awareness, Organizational Culture and Trust in Management”, M. M. S. Ghaleb argues that cybersecurity is not just a technical issue but it also a social science and organizational issue. The author uses a quantitative survey research method in order to test many different theories about employee behavior.

Relation to Social Sciences

This article has direct correlation to human behavior within organizations by proving that business should not just rely on software or policies to mitigate cybersecurity threats. The main point in this article is the author proving that cybersecurity awareness, organizational culture, and trust in management all affect employee’s behavior in follow the best practices.

Research Question / Hypothesis / Independent Variable / Dependent Variable

Research Question

The article examines how work culture, trust in management and organization culture affect employee’s compliance with cybersecurity best practices. Furthermore, the article examines whether employee engagement strengthens these relationships.

Hypothesis

The author proposes that organizational culture and cybersecurity awareness positively influences information security compliance. They also claim that employee engagement moderates the relationship between awareness and compliance. The study in total indicates that there were six hypotheses that were asked and tested.

Independent and Dependent Variable

The independent variable within the article are organizational culture and cybersecurity awareness, and the dependent variable is information security compliance behavior.

Research Methods Used

The Author uses a quantitative research method where the researchers collected data through many surveys from a huge group of people. They reported that it includes 261 employees across various departments. This method allowed the author to rule out any rarities and gather measurable data.

Conclusion

Overall, this study proves the hypothesis that effect cybersecurity depends on human behavior as much if not more than technological defenses. The findings suggest that a balance between employee awareness and engagement will provide a beneficial control to cybercrime within organizations

References

Ghaleb, M. M. S., & Pardaev, J. (2025). *Controlling cyber crime through information security compliance behavior: Role of cybersecurity awareness, organizational culture and trust in management. International Journal of Cyber Criminology*, 19(1), 1–26.

<https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/437/123>