Article Review #2: Role of Cybersecurity Awareness, Organizational Culture and Trust in Management

Niaya Fuller

Old Dominion University

November 16, 2025

For this article written by Sufyan Ghaleb, this relates to Social Science in the fact that it is researching the effects of social behavior on Cybersecurity compliance. It goes to study the "variables like organizational culture, cybersecurity awareness, leadership trust, and employee engagement." (Ghaleb, 2025, Introduction section). His research uses a quantitative style approach to test his hypotheses.

Research Method

The study done by Ghaleb has a few hypotheses that are being tested. These hypotheses are: "In what ways does organizational culture affect compliance with information security policies by employees?", "To what degree does cybersecurity awareness influence compliance behavior?", "Does employee participation moderate culture and awareness effects on behavior?", and "Is trust in top management a mediator of organizational determinants to security compliance?" (Ghaleb, 2025). The independent variable in this study is workplace behavior, specifically organizational

culture, cybersecurity awareness, leadership trust, and employee engagement, with the dependent variable being security compliance behavior.

The research method used is quantitative, being "…numerical data collection and analysis to answer the research question or hypothesis." (Slater, Hasson, 2024). The sample size for this experiment resulted in 261 responses, all comprised of individuals who often use digital systems in the workplace. The individuals were tested using different scales, such as a twenty-four-item scale, a six-item scale, a twelve-item scale, a four-item scale, and a five-item scale developed by Suvaci, Ahamed and Wong, the study of Nurnida, Hwang, and a Likert scale, respectively.

Research Relation

As for the relation to social science, this journal touches on many points that we were taught in the semester. It mentions a behavioral theory (Theory of Planned Behavior), liability with organizational cyber awareness, and building a cybersecurity culture. In order to organize and accurately display the findings of the research, Ghaleb utilized STATA software by using their Structural Equation Modeling (SEM). While not directly mentioning marginalized groups, this study can aid marginalized groups based on the findings of the research conducted.

Conclusion

This study highlights the importance of social behavior in the workplace and how it can directly affect cybersecurity compliance. Having a work culture that is focused on security and based on trust of employers and employees alike can increase compliance and is a crucial step for overall Cybersecurity. The findings can help not only businesses but also marginalized groups that may work in businesses where technology isn't the focus. This can bring awareness

to people and overall may lead to adequate training and possibly a healthier workplace for these groups. This study is a great step towards mitigating Cybersecurity risks, and it can hopefully be one of many papers leading to the change in cyber awareness.

References

Slater, P., & Hasson, F. (2024). Quantitative Research Designs, Hierarchy of Evidence and Validity. *Journal of Psychiatric and Mental Health Nursing*, *32*(3), 656–660. https://doi.org/10.1111/jpm.13135

Ghaleb, M. M. S. (2025). Controlling Cyber Crime through Information Security Compliance Behavior: Role of Cybersecurity Awareness, Organizational Culture and Trust in Management [Review of *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://doi.org/10.5281/zenodo.476619101