Controlling Cyber Crime through Information Security Compliance Behavior: Role of Cybersecurity Awareness, Organizational Culture and Trust in Management

Austin Harendt

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Diwakar Yalpi

February 26, 2026

BLUF:

In this article, it is brought to attention that organizations and the employees within it are more likely to follow cyber policies using the correct strategies. As long as the management of these organizations are trustworthy and knowledgeable about these cyber policies, the employees are much more likely to follow through on their end.

Relation/Connection to Social Science Principles:

Relation to the principles of social science, this article would best fit with the idea of empiricism. During the testing of this method of enhancing the follow-through of cyber policies from employees, employers must observe the actions that these employees take in order to understand if the methods that they used have worked. Good trust and spreading the knowledge of the possibilities in the cyber field are the two main strategies that this article is informing the reader about. When employers use these strategies, it helps to enhance the usage of the correct cyber principles.

Another social science principle that fits this article is objectivity. Since it is observed that with the usage of trust and knowledge, then that means it is factual that this enhances proper cyber usage. Objectivity relates to making decisions and conclusions based on factual evidence, rather than assumptions.

Research Question /Hypothesis/ Independent Variable/Dependent Variable:

The research question for this article would be: How does being aware of cybersecurity affect an employee's usage of the correct policies in the workforce?

The hypothesis would be: Better awareness of cybersecurity would enhance the employee's usage of correct protocol.

The independent variable would be: The employees awareness of the cyber policies.

The dependent variable would be: The actions they do that are in regard to their knowledge of the protocols.

Research Methods Used:

This article used quantitative data to gather information. The author gathered their findings from many different organizations and compiled it together to get their data.

Data Analysis Used:

The authors used surveys that were sent out to these organizations that asked if they agreed or disagreed that employee compliance was increased or decreased depending on the employee's knowledge of cybersecurity and the trust between them and their employer.

Connection to Course Concepts:

This article has many connections to what was discussed in CYSE 201S. It shows how in the field of cybersecurity, not everything is strictly technological. The article proves how human interactions and the bonds between people affect how effective cybersecurity practices and protocols are in this workforce.

Concerns of Marginalized Groups:

The only marginalized group that this study would include would be those who do not have as vast of an understanding about cybersecurity as others. The contribution that these people would have made, is that no matter the trust or willingness to follow the correct procedures, they would not be able to since they lack understanding of cybersecurity in its entirety.

Conclusion:

This article shows that cybersecurity relies on human interaction and involvement as much as it does on the technological aspect. It details how society can affect the awareness and usage of cybersecurity through a workforce as long as good understanding and trust between employees and their employers are present. This enhances our understanding of cybersecurity and its social science by how it proves how much human bonds matter and how effective it makes all cyber operations.

Reference:

Ghaleb, M. M. S., & Pardaev, J. (2025). Controlling cyber crime through organizational culture and trust in management. International Journal of Cyber Criminology, 19(1), 1–20. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/437/123