Article Review 1

Controlling Cybercrime through Information Security Compliance Behavior

Jaylen Kilby

Cybersecurity and Social Science

Diwakar Yalpi

9/28/2025

Relation to Principles of Social Sciences:

This article relates to the principles of social science in a number of ways. The article can fit mainly in the fields of psychology, sociology and even organizational behavior. The writer believes that humans are the source of why data breaches, phishing emails and even ransomware outbreaks are more common in certain organizations (Ghaleb & Pardaev, 2025). The writer makes it clear that humans are at fault for most things that go wrong within cybersecurity. In relation to organizational behavior, the writer believes that a person's culture has an influence on the behavior of employees towards information security (Ghaleb & Pardaev, 2025). This topic relates to the principles of social science because within the article the writer is trying to get us to understand that cybersecurity is not just a technical issue but it is also a social and behavioral challenge that is mainly affected by humans and their behavior.

Studies Research;

The study's research question was, “How do cybersecurity awareness, organizational culture, and trust in management influence employees' information security compliance behavior contribute to controlling cybercrime within organizations?” (Ghaleb & Pardaev, 2025). There are many hypotheses included in this article. One hypothesis is “Cybersecurity awareness has a significant influence on information security compliance behavior” (Ghaleb & Pardaev, 2025). Like the hypothesis there are also many independent variables but in this case the independent variable would be the employees understanding of certain cyber threats and their understanding of security practices. The dependent variable is the compliance with information security policies.

Research Methods:

This article used a number of research methods. One research method that was used was the quantitative research method (Ghaleb & Pardaev, 2025). The article also used a statistical analysis to gather information and results to test the hypotheses (Ghaleb & Pardaev, 2025).

Data/Analysis:

The data that was collected was numerical data through surveys and various interviews that were conducted with employees within organizations (Ghaleb & Pardaev, 2025). The surveys measured a number of things. Such as, trust in management, cybersecurity awareness, and perceptions of organizational cultures (Ghaleb & Pardaev, 2025). Statistically, researchers of this article used techniques to look at relationships between variables.

PPslides Relation:

In the powerpoint slides there are many ways in which they relate to the article. The powerpoint slides give an insight to certain concepts that are found in this article. Understanding the concepts within the powerpoints make it easier to see and understand them within this article. Especially when it comes to the various principles of social science. The article is almost in sync with some of the powerpoint slides given in the modules.

Relation to challenges, concerns and contributions of marginalized groups:

There is a big relationship that this article has with the challenges and concerns of marginalized groups. One of those challenges that this article focuses on would be the limited cybersecurity awareness. Those groups are more vulnerable due to the lack of access. Also, the article puts an emphasis on trust in management which can be a difficult thing for employees in marginalized groups. Overall, this article covers many concerns that people in marginalized groups face.

Conclusion:

In conclusion, this article contributes to society in a major way. It lists various concerns and gives insights that can help organizations, groups, and people be more aware of how cybercrime affects everybody. It emphasizes the importance of being more aware of cybercrime so that you will be better equipped to be able to prevent cybercrime from happening to you. In addition, the article is promoting an educational viewpoint on the different aspects of trying to control cybersecurity.

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