Article Review #01: Controlling Cyber Crime through Information Security Compliance Behavior: Role of Cybersecurity Awareness, Organizational Culture and Trust in Management

Student Name: Daija Brown
School of Cybersecurity, Old Dominion University
CYSE 201S: Cybersecurity and the Social Sciences
Instructor Name: Diwakar Yalpi
Date: 2/25/2026

Introduction/BLUF

Cybersecurity compliance behaviors can be improved through organizational culture, cybersecurity awareness, employee engagement, and trust in upper management as mediators.

Relation/Connection to Social Science Principles

In the introduction, the authors note there have been studies done on the human side of cybersecurity, but there are persistent gaps. “To begin, though a number of studies have looked at organizational culture and cybersecurity awareness separately, few studies have investigated how these concepts play out in terms of employee engagement and trust in leaders as mediators or moderators (Ugbebor et al., 2024)” (Ghaleb and Paradev, pg 1). This shows skepticism to the data they started with. This is not to say the data isn’t valid, but the authors were seeking a more holistic answer to the human side of cybersecurity for their research. The article also shows objectivity. It does not seek to call out individuals or push a narrative. The sole goal of the research is focused on addressing how employee engagement and trust in leadership impacts the human side of cybersecurity. Empiricism is the foundation the research was built upon. “Overall, this research presents strong empirical evidence that cybersecurity compliance behavior is founded on a mix of organizational structures and behavioral dynamics” (Ghaleb and Pardev, pg 21).

Research Question /Hypothesis/ Independent Variable/Dependent Variable

- **Research Question:** What factors contribute to holistic cybersecurity compliance behaviors?
- **Hypothesis:** This article lists six hypotheses on different factors that may positively impact information security compliance behavior.
    - Organizational culture has a significant influence on information security compliance behavior.

    - The culture around security must come from the top and trickle down to the employees.
- Cybersecurity awareness has a significant influence on information security compliance behavior.
    - Cybersecurity is constantly growing so education is important.
- Employee engagement significantly moderates the relationship of cybersecurity awareness and information security compliance behavior.
    - Security is everyone's responsibility and by engaging in cybersecurity awareness training, the organization can understand what risks are understood.
- Employee engagement significantly moderates the relationship of organizational culture and information security compliance behavior.
    - When employees participate in the culture around security, unnecessary risks are mitigated.
- Trust in upper management significantly mediates the relationship between cybersecurity awareness and information security compliance behavior.
    - Leadership mandates the training, so if there is trust from the employees, the trainings will be taken more seriously.
- Trust in upper management significantly mediates the relationship between organizational culture and information security compliance behavior.
    - When employees see leadership following policies, they are more likely to do so themselves because it shows everyone is accountable.
- **Independent Variable:** Organizational culture, cybersecurity awareness, trust in upper management.

- **Dependent Variable:** Information security compliance behavior.

Types of Research Methods used

The methodology used in this article followed a quantitative approach, with an emphasis on organizational and behavioral factors to determine compliance behaviors. The researchers used a mix of physical and digital surveying to ensure they had a large enough sample size for their research. The sample sized used for this research included data/information from 261 different employees across various departments.

Types of Data Analysis used

The variables or pre-tested scales were tested with Structural Equation Modeling (SEM) to determine if the model was appropriate and to test each hypothesis. "With the use of pre-tested scales from previous literature, constructs like organizational culture, cybersecurity awareness, employee involvement, trust in top management, and compliance behavior were all measured" (Ghaleb and Parev, pg.1). Testing the hypotheses through this modeling process proved organizational culture, cybersecurity awareness, employee engagement, and trust in leadership contributed to an increase of compliance based behavior.

Connections to other Course Concepts

This article explores how human behaviors shape cybersecurity. While technical and logical controls may be in place, human behaviors are a consistent weak link when it comes to cybersecurity and compliance. The researchers also used surveys to conduct a quantitative analysis paired with modeling to ensure an adequate test group was obtained, which proved their six hypotheses. The use of physical and digital surveys helped address the issue of sample sizes not being representative. The psychological aspect behind the human behavior is important to because it dictates potential trends in compliance. From a cognitive behavioral

perspective, human beliefs dictate their behaviors, so if someone doesn't take a risk seriously, they may be more likely to be susceptible to that risk. The research conducted was ethical, which is important because the credibility of the work conducted is important for advancements in cybersecurity such as roadmaps or future research related to the human side of cybersecurity.

Connections to the Concerns or contributions of Marginalized Groups

This study does not specifically call out any marginalized groups, but the research was conducted by people of color, who may be considered marginalized in America. There are concerns regarding the efficacy of "trust in leadership as mediators" if the person in the leadership role is a woman, black, person of color, or any combination of those marginalized groups. Cybersecurity leadership roles have been historically held by white males. This could mean an organization that has a black woman in a leadership role may see issues with compliance behaviors due to the limited representation available.

Overall societal contributions of the study/Conclusion

In conclusion, this study highlights the importance of the psychological aspects behind cybersecurity and compliance. While humans are the consistent weak link, by focusing on the behavioral aspect of cybersecurity, the risks associated with humans can be mitigated. This reduces the risk of cybercrime victimization.

Reference

Ghaleb, Mohanad Mohammed Sufyan, and Jamshid Paradev. “Controlling Cyber Crim through Information Security Compliance Behavior: Role of Cybersecurity Awareness, Organizational Culture and Trust in Management.” *International Journal of Cyber Criminology*, vol. 19, no. 1, 2025, p. 26. *Cybercrime Journal*, https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/437/123.

Article Link:

[https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/437/123]