Article Review #1: Controlling Cyber Crime through Information Security Compliance Behavior: Role of Cybersecurity Awareness, Organizational Culture and Trustin Management

Pamela davis

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

10/05/25

Introduction / BLUF

The article, *Controlling Cyber Crime through Information Security Compliance Behavior*, addresses the growing importance of human behavior and organizational culture in cybersecurity. With increasing cyber threats like phishing and ransomware, the article emphasizes that technical solutions alone are insufficient—employees' attitudes, awareness, and engagement significantly influence cybersecurity compliance. The bottom line: fostering a security-conscious organizational culture and investing in trust and engagement leads to improved information security behaviors across the workforce.

Relation / Connection to Social Science Principles

The study is deeply rooted in social science principles, particularly behavioral and organizational psychology. It aligns with seven core social science principles: (1) Behavioral influence, as it analyzes how individual actions affect cybersecurity; (2) Social norms, through its focus on organizational culture; (3) Cognitive processes, especially awareness and perception of risk; (4) Group dynamics, seen in the role of departmental cultures and teamwork; (5) Power and authority, reflected in trust in leadership; (6) Socialization and learning, via cybersecurity training programs; and (7) Motivation and incentives, especially how engagement drives

compliance. The article reinforces that effective cybersecurity depends on understanding human behavior in social contexts.

Research Question / Hypothesis / Independent Variable / Dependent Variable

The study is guided by four research questions: (1) How does organizational culture influence employees' compliance with cybersecurity policies? (2) To what extent does cybersecurity awareness affect compliance? (3) Does employee engagement moderate the relationship between culture/awareness and compliance? (4) Does trust in leadership mediate these relationships? The authors propose three main hypotheses: H1 – Organizational culture significantly impacts compliance behavior; H2 – Cybersecurity awareness significantly influences compliance behavior; H3 – Employee engagement moderates the relationship between awareness and compliance. The independent variables are organizational culture and cybersecurity awareness; the dependent variable is information security compliance behavior. Trust in leadership serves as a mediating variable, and employee engagement as a moderating variable.

Types of Research Methods Used

The study employs quantitative research methods, using structured surveys to gather data from employees across various organizations. The survey captures perceptions of organizational culture, awareness levels, trust in leadership, engagement, and self-reported compliance behaviors. The research is grounded in validated theoretical models such as the Theory of Planned Behavior and Protection Motivation Theory.

Types of Data Analysis Used

The authors use statistical modeling and regression analysis to test the hypotheses. Specifically, they apply moderation and mediation analysis to examine how trust and engagement influence the primary relationships between the independent and dependent variables. Interaction effects are also tested to reveal deeper insights into how variables interrelate under different conditions.

Connections to Other Course Concepts

The study strongly connects to course concepts from CYSE 201S, such as the Human Factor in Cybersecurity, Behavioral Compliance Models, and Social Engineering Awareness. It reinforces the idea that policy compliance is not just procedural but psychological. The role of leadership, motivation, and culture echoes themes from modules on organizational behavior and cyber hygiene. Additionally, it challenges the common over-reliance on technology by showing that cultural and behavioral aspects can either strengthen or weaken a cybersecurity framework.

Connections to the Concerns or Contributions of Marginalized Groups

While the article does not directly focus on marginalized groups, its findings have implications for inclusivity. Employees from underrepresented or less empowered groups may experience lower engagement or reduced trust in leadership, potentially impacting their cybersecurity behavior. Future studies should consider how cultural inclusion, leadership representation, and equitable access to training influence compliance, especially among non-technical staff who are often overlooked in cybersecurity strategies.

Overall Societal Contributions of the Study / Conclusion

This study significantly advances our understanding of cybersecurity by framing it as both a technical and social science challenge. It contributes to the broader field by offering an

integrated model that organizations can use to strengthen their information security posture through culture, trust, engagement, and awareness. By highlighting the complex interplay between these factors, it provides a more holistic approach to managing cyber risks in diverse and dynamic work environments. The study's societal value lies in shifting the cybersecurity conversation toward people-centered strategies that are essential in today's digitally driven world.

Reference

Ghaleb, M., & Pardaev, M. (2025). *Controlling Cyber Crime through Information Security Compliance Behavior*. *International Journal of Cyber Criminology*, 19(1), 1–10. https://www.cybercrimejournal.com/Ghaleb2025vol19issue1.pdf