Bradford Lee

September 28,2025

**Article Review #1**

**Relation to Social Sciences**

This article directly connects social sciences by analyzing psychological and organizational factors; for example, trust in management, employee engagement, and organizational culture, which influence cybersecurity compliance. Instead of focusing solely on technical defenses, the study employs behavioral science and organizational theory to explain why employees follow or disregard security rules. With a human-centered approach, it reflects the broader social science principle that human behavior, culture, and trust shape security outcomes.

**Research Questions, Hypotheses, Independent and Dependent Variables**

The research questions focus on how organizational culture, cybersecurity awareness, employee engagement, and trust in management affect compliance behavior. Six hypotheses were tested, all supported by results. The independent variable includes organizational culture and cybersecurity awareness, while the dependent variable is information security compliance behavior. Employee engagement serves as a moderator, and trust in management serves as a mediator.

**Research Methods**

The study implemented a quantitative research design using structured questionnaires assigned to 261 employees in production companies. Scales backed by prior research measured organizational culture, cybersecurity awareness, trust, and compliance behavior. Structural Equation Modeling (SEM) was used to test direct, mediating, and moderating effects, with results confirming all 6 hypotheses.

**Data and Analysis**

Data was collected using Likert-scale surveys and was analyzed through Confirmatory Factor Analysis (CFA) and SEM with STATA software. Reliability and validity were confirmed with Cronbach’s Alpha values exceeding 0.80 for most constructs. The model provided a compelling account of the data, showing that organizational and behavioral variables explained by over 50% of the variance in compliance behavior.

**Connection to Course Concepts**

The study aligns with course concepts on the social science side of cybersecurity, particularly theories of organization behavior, trust, and engagement. The Theory of Planned Behavior and Social Exchange Theory were applied to explain how norms, attitudes, and reciprocal trust shape compliance. This reflects class discussions about social and behavioral aspects of security rather than purely technical perspectives.

**Marginalized Groups**

Although the article did not directly study marginalized groups, its findings are relevant to the challenges they face. For example, employees in non-technical roles or those without high levels of digital literacy are often more vulnerable to cyber-attacks. Implementing cybersecurity awareness programs and ensuring a line of trust between those in leadership roles and all staff members can help address inequalities in how security policies impact diverse groups.

**Contributions to Society**

The study contributes to society by highlighting the importance of culture, trust, and awareness in preventing cybercrime. The findings make it clear that organizations thrive when they prioritize support and inclusion where employees feel engaged and valued to achieve effective compliance. By shifting focus from purely technical controls to human behavior, the study builds stronger, more resilient organizations that are able to navigate the complexities of modern cyber risk.

**Conclusion**

Overall, the article demonstrates that cybersecurity is as much a social and behavioral issue as it is a technical one. By confirming the importance of organizational culture, awareness, engagement, and trust, the writers provided a comprehensive framework for understanding compliance behavior. These insights are highly valuable for both researchers and practitioners seeking to strengthen organizational defenses against cybercrime.

**Citation:**

Mohammed, M., Ghaleb, S., & Pardaev, J. (2025). 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://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/437/123