Korie Cooper

February 22, 2026

Article Review #1: Controlling Cyber Crime through Information Security Compliance Behavior

Introduction

The article "Controlling Cyber Crime through Information Security Compliance Behavior: Role of Cybersecurity Awareness, Organizational Culture and Trust in Management" by Ghaleb and Pardaev (2025) discusses the area of employee compliance behavior and its effect on cybersecurity in organizations. This topic relates to the social sciences because it involves studying the behavior of people, the organization's environment, trust, and social expectations. Many social sciences like criminology and sociology study people in groups and how their behavior is affected by making decisions within those group environments. This study applies those same concepts to cybersecurity to demonstrate that employees make compliant decisions based on the people around them rather than technological barriers.

Research Question, Hypotheses, IV and DV

The primary research question posed in the study is what influences employee information security compliance behavior. The researchers specifically want to know whether employee information security compliance behavior is influenced by factors such as cybersecurity awareness, organizational culture, and trust in management. The variables that the researchers want to study as the independent variables (IVs) are cybersecurity awareness,

organizational culture, and trust in management. The variable that is being assessed as the dependent variable (DV) is employee information security compliance behavior. The researchers' hypotheses suggest that higher levels of employee cybersecurity awareness, positive perceptions of the organizational culture, and higher levels of trust in management will all be associated with increased compliance with security policies. Stated differently, employees who understand cyber risks and who perceive that there is support for them from their organizational leaders will be more likely to comply with the security requirements that have been established.

Research Methods Used

The study employs a quantitative research design. The researchers collect data by administering structured surveys to employees in organizational contexts. Survey methods are popular in social sciences as they allow for the measurement of attitudes and behaviours numerically. The survey method yields numerical measurements for awareness, culture, trust, and compliance behaviour. This approach enables the researcher to test statistical relationships between the independent and dependent variables.

Types of Data and How it was Analyzed

The researcher obtained numerical survey responses. The researcher used statistical models, likely regression or SEM, to test the hypotheses. The models tested the predictiveness of the independent variables for the dependent variable. The models found positive effects of cybersecurity awareness, organizational culture, and trust in management on compliance behavior. Thus, higher levels of each factor increase the likelihood of policy compliance.

Connection with PowerPoint Concepts

There are several concepts from class PowerPoint presentations that relate to this article. Social control theory explains that individuals who are tied to institutions are more likely to adhere to the rules. Similarly, employees who trust management and who are "connected" to the organizational culture will be more likely to adhere to security policies. Concepts of deterrence are relevant as well, as awareness of the potential consequences of behavior will inhibit that behavior. Finally, routine activity theory is also applicable, as the lack of internal controls and a lack of knowledge regarding what threats exist, will create opportunities for cybercrime within an organization.

Marginalized Groups, Contributions, and Challenges

The issue is also relevant to marginalized groups. Minority groups in the workplace may have less trust in management or may feel out of place in the organization's culture. If the cybersecurity training and communication are not inclusive, this could impact compliance. This issue is worth addressing to ensure that all employees are able to participate in the cybersecurity efforts. With inclusive leadership and communications, compliance can be strengthened for all employees regardless of their background

Contributions to Society

This research benefits society by demonstrating that cybersecurity is a social and organisational challenge, not just a technical one. The insights of this research offer concrete training recommendations, leadership insights and recommendations for internal communication for organisations. By focusing on awareness, trust and cultural elements, this research enables

organisations to take a preventative approach to cybercrime, strengthening the security of their digital landscape.

Conclusion

In summary, Ghaleb and Pardaev's study establishes the value of social sciences in cybersecurity governance and demonstrates the importance of awareness, organisational culture, and trust as behaviour predictors. The study has relevant implications for criminology and cybersecurity and reinforces the importance of fostering social ties within organisations as a key cyber risk mitigation strategy to enhance the security of digital environments.

References

Ghaleb, F., & Pardaev, A. (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). https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/437/123