Article Review #2: Controlling Cyber Crime through Information Security Compliance Behavior: Role of Cybersecurity Awareness, Organizational Culture and Trust in Management

Asher L. Embry

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Diwakar Yalpi

November 14, 2025

Introduction

The chosen article for this review is “Controlling Cyber Crime through Information Security Compliance Behavior: Role of Cybersecurity Awareness, Organizational Culture and Trust in Management,” published in the *International Journal of Cyber Criminology*. This article explores the organizational and psychological factors that influence an employee's adherence to information security policies. The study shows that a positive culture, high cybersecurity awareness, and active employee involvement lead to better information security compliance. The critical mediating factor in this is trust in management.

Relation to Social Science Principles

This article is a study of social science, examining the human element of cybersecurity controls and what makes them successful. It directly incorporates social science principles like organizational behavior, psychology, behavior, and trust. At its core, the study analyzes how organizations and their culture influence the actions of their employees, noting that “human actions tend to be the weakest link in cybersecurity frameworks” (Ghaleb & Pardaev, 2025). To achieve this, it investigates the psychology of employees and what makes them more compliant with information security policies. Trust is also a key factor in this model, putting trust in senior managers as the bridge between policy compliance and employees. Without trust in management, why would an employee care to follow proper policies?

Research Questions, Hypothesis, and Variables

The primary focus of this study is determining what organizational and psychological factors significantly affect information security compliance in employees in production companies. Additional research questions ask the following: How does cybersecurity awareness

influences compliance? How does employee participation affect culture and awareness in others? Is trust in management a mediating factor of security compliance.

Based on these research questions, six hypotheses were developed, and all were confirmed by the data. The first being organizational culture has a significant influence on compliance. Second, cybersecurity awareness has a significant influence on compliance. Third, employee engagement moderates the relationship between cybersecurity awareness and information security compliance. Fourth, employee engagement significantly moderates the relationship between organization culture and information security compliance. Fifth, trust in upper management significantly mediates the relationship between cybersecurity awareness and information security compliance. Lastly, trust in upper management significantly mediates the relationship between organizational culture and information security compliance.

The main Independent Variables (IV) were organizational culture, cybersecurity awareness, and employee involvement. The dependent variable was information security compliance behavior. Trust was identified as a mediating variable between the independent and dependent variables.

Research Methods Used

This study used quantitative research. Data was collected from 261 employees across various departments in production companies. The researchers used pre-tested scales from previous research to craft a survey that measured the identified variables. Using a survey allowed researchers to gather a large dataset for statistical analysis.

Data Analysis Used

The researchers used a method called Structural Equation Modeling (SEM) to analyze the data. This method is great at testing complex models based on theory. SEM allowed the researchers to go beyond correlation between variables and test all the hypotheses at once. This confirmed that the independent variables could predict the dependent variables, as well as determined how they related to each other.

Connections to Other Course Concepts

This article directly relates to concepts covered in class. The human factor being the largest one, as it is explicitly researched and probed in this study, emphasizing that employees are part of network defense rather than just a vulnerability. The study also relates to social engineering, reinforcing the importance of cybersecurity awareness being the primary defense against a social engineering attack. It also touches on psychology, showing how trust and policies influence how employees treat information security in their roles. Finally, it connects to policy and governance by showing that policies are ineffective unless they are supported by a strong organizational culture and trust.

Connections to the Concerns or Contributions of Marginalized Groups

This study does not explicitly address concerns or contributions of marginalized groups. It analyzes employees within production companies; demographic data of respondents was not a primary focus within this study. Because of this the study is potentially limited and could be explored more in the future how different demographic information like race, gender, or disability could affect information security compliance in the workplace. Future studies could also be explored if trust in senior management varies across demographic groups.

Overall Societal Contributions of the Study

This study makes a significant societal contribution by providing managers and policymakers with a model backed by hard data on how to improve cybersecurity within an organization. The main contributions include shifting the focus from technology to humans, and actionable data. Organizations need to invest resources into their employees to strengthen their cybersecurity rather than solely relying on technical controls. The creation of actionable data to provide a clear framework for upper leadership that includes a positive culture, cyber awareness, and trust to bolster information security within their organization. This research advances our understanding of cybersecurity being an interdisciplinary field by connecting organization and trust with a positive outcome of security compliance.

References

Ghaleb, M. M., & 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. doi:10.5281/zenodo.476619101 https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/437/123