Article Review #1: How Cybersecurity Awareness, Organizational Culture, and Trust in Management Influence Information Security Compliance Behavior

Ava McLaughlin

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Diwakar Yalpi

February 26, 2026

Ava McLaughlin

Introduction

This paper is an overview of the article “Controlling Cyber Crime through Information Security Compliance Behavior: Role of Cybersecurity Awareness, Organizational Culture and Trust in Management” by Mohanad Mohammed Sufyan Ghaleb and Jamshid Pardaev. The study explores how cybersecurity awareness, organizational culture, and trust in management influence information security compliance behavior through 261 survey responses from production company employees across different departments. Six hypotheses were developed and all were supported, with the results showing that organizational culture, awareness in cybersecurity, and employee involvement predict information security compliance behavior well (Ghaleb & Pardaev, 2025).

Relation to Social Science Principles

The three most notable Social Science principles related to this article are Empiricism, Determinism, and Objectivity (CYSE201S (Module 2)). Empiricism, the belief that scientific knowledge must be based on physical experiences, is strongest here because data was collected from employees, surveys measured behavior, tests confirmed hypotheses, and specific statistics were used (Ghaleb & Pardaev, 2025). Determinism, the belief that behavior is caused, determined, or influenced by preceding events, is also connected to this article because it demonstrates how information security compliance behavior is influenced by organizational culture, awareness in cybersecurity, and employee involvement. Finally, this article stays objective, which is the belief that scientists should remain value-free in their studies. The researchers test hypotheses and report statistical results rather than assuming and incorporating opinions.

Ava McLaughlin

Research Question, Hypothesis, Independent Variable, and Dependent Variable

The researchers asked four main questions: “In what ways does organizational culture affect compliance with information security policies by employees?” “To what degree does cybersecurity awareness influence compliance behavior?” “Does employee participation moderate culture and awareness effects on behavior?” and “Is trust in top management a mediator of organizational determinants to security compliance?” They also developed six hypotheses: “Organizational culture has a significant influence on information security compliance behavior.” “Cybersecurity awareness has a significant influence on information security compliance behavior.” “Employee engagement significantly moderates the relationship of cybersecurity awareness and information security compliance behavior.” “Employee engagement significantly moderates the relationship of organizational culture and information security compliance behavior.” “Trust in upper management significantly mediates the relationship between cybersecurity awareness and information security compliance behavior.” and “Trust in upper management significantly mediates the relationship between organizational culture and information security compliance behavior.” (Ghaleb & Pardaev, 2025). The main independent variables are organizational culture and cybersecurity awareness. The dependent variable is information security compliance behavior.

Types of Research Methods Used

The study used quantitative research methods. The researchers proposed four research questions, developed six hypotheses, and tested them through data collection. Responses were gathered through structured questionnaires, both physical and digital, which were distributed to production company employees across departments such as operations, IT, human resources, and quality assurance (Ghaleb & Pardaev, 2025). The questionnaires gathered 261 responses.

Ava McLaughlin

Types of Data Analysis Used

First, the researchers performed reliability tests using Cronbach's Alpha and Composite Reliability, and all values were above the minimum acceptable value of 0.70. Next, they tested the validity of the data using Average Variance Extracted (AVE) and values were over 0.5, meaning the results are valid. Then, they tested the model fit using Structural Equation Modeling (SEM), Root Mean Square Error of Approximation (RMSEA), Comparative Fit Index (CFI), Tucker-Lewis Index (TFI), and Standardized Root Mean Square Residual (SRMR), all results indicating that the model structure fits the data well. Next, they found all six hypotheses to be statistically significant using path coefficients, as the values were less than 0.001. The predictability of the independent variables was measured using R-square, and the values show that the model explains about 51-52% of employee security compliance behavior, which is great in social science research (Ghaleb & Pardaev, 2025).

Connections to Other Course Concepts

This article highlights other course concepts such as psychological biases increasing victimization risk and psychological consequences of victimization. Many employees have psychological biases that may prevent them from complying with information security policies, such as optimism bias or hyperbolic discounting (CYSE201S (Module 5)). This article displays how, through strong employee engagement, organizational culture, trust in upper management, and cybersecurity awareness, psychological biases can be deterred and security compliance encouraged (Ghaleb & Pardaev, 2025). Also, cybercrime victims report lower trust, and this article directly links trust in management and coworkers to higher information security compliance.

Ava McLaughlin

Connections to the Concerns or Contributions of Marginalized Groups

This article is connected to the concerns of marginalized groups for several reasons. Low minority participation in cybersecurity careers is linked to factors like discouragement and little high-school preparation (CYSE201S (Module 3)). Marginalized groups may not have access to high-quality cybersecurity education, leading to little cybersecurity awareness and low information security compliance. Also, women often don't enter cybersecurity fields because they feel like they don't have the same opportunities as men or don't have female role models, which can contribute to a lack of trust within cybersecurity work environments (CYSE201S (Module 3)). As the findings of the article display, lower levels of trust are associated with lower information security compliance.

Overall Societal Contributions of the Study

In conclusion, the study uses organizational behavior and trust theory to better understand compliance behavior in production environments (Ghaleb & Pardaev, 2025). It also offers guidance for managers to develop information security policies with culture, awareness, and trust in mind (Ghaleb & Pardaev, 2025). This study incorporates many social science elements, such as empiricism, determinism, objectivity, and victimization to explain why employees struggle with information security compliance. Overall, this study contributes to society by promoting a social science-approach to cybersecurity and encouraging organizations to strengthen both technological defenses and social environments that build responsible cybersecurity behavior.

References

Ghaleb, M. M. 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

Old Dominion University. (n.d.). CYSE201S (Module 2) Principles of Social Sciences and Cybersecurity.

Old Dominion University. (n.d.). CYSE201S (Module 3) Strategies to Study Cybersecurity through an Interdisciplinary Social Sciences Lens.

Old Dominion University. (n.d.). CYSE201S (Module 5) Applying Psychological Principles of Cyber Offending, Victimization, and Professionals.