

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

Student Name: Dmitriy Yeremin

School of cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 03/10/2026

Introduction/BLUF

This research journal brings attention to corporate shortcomings in relation to cybersecurity. As threat actors have grown more sophisticated in their tactics, so has the defensive side. Yet even with a strong technological front, employees continue to fall victim to phishing attempts and organizations still face damaging cyberattacks. Ghaleb and Pardaev (2025) subscribe to the idea that cybersecurity is not purely a technology problem but a people problem. The authors investigate what drives employee behavior around security and identify four key factors: organizational culture, cybersecurity awareness, employee involvement, and trust in management.

Relation/Connection to Social Science Principles

Empiricism stands out as an early and obvious connection. The authors observed 261 employees across different departments, used well established measurement scales from previous literature, and analyzed the data through STATA. This demonstrates a clear commitment to grounding their findings in observable, measurable evidence. Objectivity is also a principle being exercised throughout the study. The authors acknowledged a bias common in this area of research, noting that prior studies tended to focus on technical or IT dominant roles while employees in non-technical positions, who are equally vulnerable, have been largely underrepresented in empirical models (Ghaleb & Pardaev, 2025).

Research Question/ Hypothesis/ Independent Variable/ Dependent Variable

There are four research questions within this journal. How does organizational culture affect compliance with information security policies? To what degree does cybersecurity

awareness influence compliance behavior? Does employee participation moderate the effects of culture and awareness on behavior? Is trust in top management a mediator of organizational determinants to security compliance?

There are six hypotheses in this journal. H1: Organizational culture has a significant influence on information security compliance behavior. H2: Cybersecurity awareness has a significant influence on information security compliance behavior. H3: Employee engagement significantly moderates the relationship between cybersecurity awareness and information security compliance behavior. H4: Employee engagement significantly moderates the relationship between organizational culture and information security compliance behavior. H5: Trust in upper management significantly mediates the relationship between cybersecurity awareness and information security compliance behavior. H6: Trust in upper management significantly mediates the relationship between organizational culture and information security compliance behavior.

The independent variables are organizational culture and cybersecurity awareness. Dependent variable is informational security compliance behavior. Moderating variable is employee engagement. Mediating variable is trust in top management.

Types of Research Methods Used

The study used a quantitative approach, surveying 261 personnel across a range of departments through physical or digital questionnaires. Participation was drawn from purposive sampling, targeting individuals who regularly interact with digital systems and are exposed to information security measures in their day to day work (Ghaleb & Pardaev, 2025).

Types of Data Analysis Used

All constructs were measured using scales borrowed from previous research to ensure reliability and validity (Ghaleb & Pardaev, 2025). Structural Equation Modeling (SEM) was conducted through STATA software. Confirmatory Factor Analysis (CFA) was performed first to establish convergent and discriminant validity of the measurement model (Ghaleb & Pardaev, 2025).

Connection to other Course Concepts

This journal strongly connects employee behavior and security compliance to organizational culture, arguing that the two are deeply dependent on one another. The attention given to behavioral and social environments reflects clear ties to psychology and sociology, both foundational fields within social science. As the authors put it, employees do not operate in isolation but derive behavioral cues from the broader organizational environment (Ghaleb & Pardaev, 2025). This resonates with a key takeaway from the study. Most established companies have security policies in place, but policy alone does not make security part of the culture. Ghaleb and Pardaev (2025) capture this well by describing what researchers call a security culture, one that moves beyond policy enforcement and embeds security into the organizational identity itself.

Connections to the Concerns or Contributions of Marginalized Groups

This journal did not present any explicit connections to marginalized groups. The study population consisted entirely of employed individuals across departments, and no distinctions based on race, gender, or socioeconomic status were examined.

Overall Societal Contributions of the Study/ Conclusion

The researchers identified a critical gap in how businesses approach security. All six hypotheses were validated by the results, confirming that building a work culture centered on security, establishing trust in leadership, and fostering employee cohesion creates an environment where security awareness can genuinely take hold. This study makes a meaningful contribution by highlighting that protecting organizational information is not just a technical challenge but a human one.

Reference:

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](#)