Adrian Valencia

Old Dominion University

CYSE 201S: Article Review #1

October 1, 2025

BLUF

In this article, a study is conducted highlighting the importance of organization and psychological elements that shape employee's information security compliance behavior. It dives into factors consisting of culture, cybersecurity awareness, and other elements that influence employee work ethics. The researchers (Ghaleb and Pardaev) guide the study to show the factors that influence compliance.

Scientific Principles

The study connects to each of the social science principles in different ways. Determinism for example, evidence in the study showed that culture and awareness from influences in the past influence the behavior in cybersecurity. Objectivity can be seen through researchers avoiding bias and opinion and relying more on evidence through things like models and statistics. Additionally, through the gathered explanation of results, parsimony is shown through simplified models, moderators, and methods to make things simpler and less confusing. Through observing the sample employees, evidence is based solely on observations showing the empiricism of the study. Skepticism can easily be noticed from the amount of hypothesis that arise throughout the study from questioning different parts of the research. Ethical neutrality in the study can be the surveys they were asked for without conflicting ethical violations. Lastly, through behavior and the relation between culture, research showed that across companies that behavior is related in many ways.

Research Elements

There were four main questions that were asked throughout the study to inform. The questions were, "In what ways does organizational culture affect compliance with information security polices 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 organization determinants to security compliance?”. These questions are asked to help build the study and the models that put everything into consideration even with the employees at sample. They are asked to help figure out what key factors are going around employees while they are working in the industry.

Furthermore, six hypotheses were formed from the questions. They were used to test participants to see the results of data and come up with conclusions for the questions. Their hypotheses aimed to find out what factors are influencing and how they differentiate from other employees. The independent variable of the study that was changed was the organizational culture and cybersecurity awareness. These helped show the influence of security behavior between the different models. They showed the norms and values in addition to the knowledge of the employees. The dependent variable of the study is the information security compliance behavior with was measuring the employees responding to policies, procedures, and practices.

The research method used in the study was a quantitative survey. The sample consisted of 261 employees that all received the survey. The researchers used structural equation modeling and confirmatory factor analysis to test, mediate, and moderate the employees throughout the research.

Data and Analysis

At the end of conducting research, the researchers confirmed reliability through Cronbach’s measurement system. The results were above 0.80 meaning the results were acceptable and reliable with strong consistency. Additionally, the SEM results for organizational culture and cybersecurity awareness were around 0.520 showing strong relations and compliance.

Relation to Presentations

The PowerPoint presentations relate to the article in many ways. The things discussed in presentations are all part of the research conducted. For example, everything from things like the social science principles to the different research methods and strategies are all used in the study. It gives more insight into things like the CIA triad and how everything can be based on behavior. The study shows the different context and perspectives that imply what was discussed in the presentations of class.

Marginalized Groups

The research shows how similar organizational cultures are between different employees. From things like trust and awareness could be the difference between compliance of employees within an organization. While some factors may affect how one employee sees things, another may see it in a different way. This causes an outlier to take effect in the results to see the mean answer. This shows the importance of communication between a company to its employees with understanding the diverse perceptions of employees.

Contributions to Society

The findings in the study help shape the understanding of behavioral factors through social sciences. It shows the importance of behavior within cybersecurity as two main perspectives of technical and behavioral. It spreads awareness of culture, awareness, and trust within organizations and management that affect compliance.

Conclusion

In conclusion, the article highlights the compliance of employees in cybersecurity through influencing factors. Two major factors being technical and behavioral shape how employees work within the cybersecurity industry.

Reference

Ghaleb, M., & Pardaev, J. (2025). *Controlling Cyber Crime through Information Security Compliance Behavior: Role of Cybersecurity Awareness, Organizational Culture and Trust in Management*, *19*(1), 1–21.

https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/437/123

International Journal of Cyber Criminology. Cyber Crime Journal. (n.d.). https://www.cybercrimejournal.com/