Article Review #1: Review of Controlling Cyber Crime through Information Security Compliance Behavior: Role of Cybersecurity Awareness, Organizational Culture and Trust in Management

Student Name: Mario Martinez

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 10/7/2025

Introduction

The Article *Controlling Cyber Crime through Information Security Compliance Behavior* is a study focusing on the organizational cultural factors that influence adherence to security compliance practices within a company. The study's line of argument is that organizational culture, particularly how (and if) that structure promotes cybersecurity literacy and trust in senior personnel, are the key predictors of employee compliance.

Research Question /Hypothesis/ Independent Variable/Dependent Variable

The article's central research question is: *in what ways does organizational culture affect compliance with information security policies by employees?* The researcher's proposed hypothesis was that factors such as organizational culture and cybersecurity literacy within an organization are the primary drivers of compliance. The DV being measured is the compliance level toward cybersecurity policies and best practices. The IV's being measured are organizational culture's attitude toward cyber literacy and managerial trust.

Research Methods

The researchers distributed questionnaires to company employees, receiving 261 responses that were included in their dataset. The questionnaires were distributed both digitally and physically across multiple departments ranging from IT to Human Resources. Responses were screened to prioritize data from those who interact frequently with digital systems as part of their normal duties.While the collection strategy of distributing questionnaires for empiric results is solid, it seems questionable whether it is wise to screen for only employees who are regularly in contact with digital systems. Often, those who have the least familiarity with systems are much easier targets as they are likely to be ignorant of cybersecurity policies.

Data Analysis

Researchers employed a Structural Equation Modeling (SEM) framework to determine what factors played the greatest role in determining compliance. The SEM framework requires 200 cases at minimum to provide an effective model, so this seems like a legitimate strategy for analysis of their data.

Social Sciences Concept

The article itself is arguably a case study in argument for the principle of Determinism. In asking what cultural factors will result in lower/higher compliance, it's really just seeking to understand what is leading to the specific behavior of complying or not complying with cybersecurity policies and practices. It is seeking to establish a cause and effect chain for the behavioral outcome.

Marginalized Groups

The study has no specific focus on any marginalized group, nor does it make mention of them. However, two groups I could imagine might have an interest would be employees with mental disorders (such as ADHD or Anxiety) and employees with less formal education. In both cases, these employees are likely to have a difficult time integrating with internal organizational culture through the traditional means of networking and attending conferences/seminars. This article could help advocates for those communities make a case for expanding the way 'company culture' is spread through an organization.

Contributions to Society

This article's main contribution is that it could help companies and individuals alike how a corporate culture that places an emphasis on good cybersecurity policy can lead to a more

security-minded workforce. However, a strong secondary contribution is that it points out that a good management/employee relationship built on mutual trust is just as key to encourage that compliance; if you do not trust management, you are unlikely to follow their policy proscriptions.

Conclusion

This study's analysis of the correlation between organizational culture and employee cyber policy compliance is a significant thing to point out, though I think its somewhat questionable if you need a formal study to arrive at such a simple conclusion. That said, I again reiterate that I have some serious concerns about the usefulness of the data collected considering that employees with low interaction with technology were selected out. Just because you are less in contact with technology does not mean you aren't a potential threat vector for a malicious actor, frankly you're probably a softer target. This somewhat diminishes the usefulness of the study in my eyes, even if it does not make it totally useless.

Reference

Ghaleb, M. M. S., & Pardaev, J. (2025, June). Organizational and psychological determinants of employees' information security compliance behavior in production companies. *Cybercrime Journal*. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/437/123