Christopher Rojas
10/1/2025

Article Review #1

"Controlling Cyber Crime through Information Security Compliance Behavior: Role of Cybersecurity Awareness, Organizational Culture and Trustin Management"

- Introduction

The article aims to highlight the psychological effects organizational variables have on cybersecurity compliance and awareness. Using data from a small group of employees (261) "spread across different departments in production companies" (Ghaleb, Pardaev). The purpose of the research was to validate six hypotheses. In effect, workplace variables like culture, leadership trust, employee involvement, awareness, and compliance behavior have a direct correlation on informational security practices.

- Relevance to Social Sciences and PowerPoint presentations

  The article is pertinent to the social sciences in several factors. Most recently in the course when discussing "Applying Psychological Principles of Cyber Offending, Victimization, and Professionals", Behavioral theory suggested that behavior is learned via the environment and social structures. In the case of the research, it was proven that workplace environment (leaders, peers) influenced cybersecurity practices in employees. Highlighting a clear intersection of technology and social science. Determinism can also be seen in the research. The behavior of good cybersecurity practices can be determined by the type of culture or managers a workplace has. It is also important to note that the independent variables of this research are mostly human factors.

- Research Question, Hypotheses, and Variables

Research Question: How does psychological and organizational factors influence employee cybersecurity practice?

Hypotheses:

1. Organizational culture has a direct influence on employee approach to cybersecurity.
2. Leadership trust enhances security practices.
3. Employee involvement predicts security compliance.
4. Awareness of cybersecurity augments information security.
5. Compliance behavior fosters a secure organization.
6. Trust in senior leaders also enhances security practices.

Independent Variables: Organizational culture, trust in management, awareness, employee involvement.

Dependent Variable: Control of cybercrime

- Research Methods

The research uses quantitative research in order to determine how organization and psychological factors correlate to cyber security. Using data from the previously mentioned 261 employees they made tables to reflect numerically the value of culture/trust in the employees.

- Data and Analysis

The data collected was reflected via tables and numerical values. They also reflected the correlation of cybersecurity awareness on compliance behavior via a structural model. The relationships between the IVs and DV previously mentioned show an augmentation of informational security practices.

- Impact on Marginalized Groups

  Although the inclusion of marginalized groups was not stated in this research, it is important to take into consideration how these factors might affect the result. Female employees might not be as trusting of male managers for example, especially if shown unethical behaviors. It is also important to know how to build trust with marginalized individuals in different ways, as traditional methods might not be the most fitting. The need for inclusive organizational culture could lead to the increase of cybersecurity practices.

- Contributions to Society

  A very important contribution to society from this study is the clarification that cybersecurity practice does not rely solely on technical teachings but upon an understanding of the social sciences and its factors. A second important contribution to society could also be the development of a more positive workplace environment, by correlating a benefit for the company (more secure company data) to a benefit for the human side of the employees.

- Conclusion

  By building leadership trust and fostering a positive workplace culture, cybersecurity can thrive as the human factor is very important to motivate individuals to care for informational security practices.

- Article Link

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

- Citation

Sufyan Ghaleb, M. M., & Pardaev, J. (2025). Controlling Cyber Crime through Information Security Compliance Behavior: Role of Cybersecurity Awareness, Organizational Culture and Trustin Management. *International Journal of Cyber Criminology*, *19*(1), 1–26. https://doi.org/10.5281/zenodo.476619101