Article Review #1: How Compliance Can Help Stop Cyber Crime

Tyler Walker

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Diwakar Yalpi

October 6, 2025

Introduction

In the cyber world, there are a multitude of threats that seek to steal data or damage our infrastructure. From malwares to DDoS attacks, there are many ways for threat actors to infiltrate a computer system. However, one of the most looked over threats to the security of our networks and systems is us, or more specifically, social engineering. Social engineering relies on human error in order to obtain unauthorized access and information. This article from Ghaleb and Pardaev shows how crucial organizational and human factors are in preventing cybercrime. The study looks at how diverse social factors effects people's behavior when it comes to following information security rules. By focusing on these factors, the research gives firms ideas on how to improve their defenses beyond just technology.

Relation to Social Sciences

The article connects cybersecurity to important principles in social science such as organizational behavior and psychology. It demonstrates that compliance with security standards is influenced by culture, trust in management, awareness, and engagement within social systems, rather than just technological factors. By studying how employees respond to leadership, norms, and training, this research shows how social dynamics influence safe or unsafe online behaviors.

Research Question, Hypothesis, Independent Variable, and Dependent Variable

Ghaleb and Pardaev research focuses on organizational and human behavioral factors and aims to determine the extent to which those factors influence compliance behavior, as well as whether employee engagement moderates these relationships and whether trust in top management mediates them. The study provides six hypotheses (H1-H6) to investigate the direct, moderating, and mediating effects of the factors. Organizational culture (H1) and cybersecurity awareness (H2) both have significant positive effects on information security compliance;

employee engagement moderates the relationships between awareness and compliance (H3) and culture and compliance (H4); and trust in top management mediates the effects of both awareness (H5) and culture (H6) on compliance behavior. In this model, the independent variables are organizational culture and cybersecurity awareness, employee engagement serves as the moderating variable, trust in top management acts as the mediating variable, and information security compliance behavior is the dependent variable.

Research Methods

The research used a quantitative survey with 261 employees from several departments, including IT, operations, HR, and QA. It utilized structural equation modeling (SEM) and confirmatory factor analysis (CFA) to evaluate hypotheses and identify relationships.

Data and Analysis

The data was collected using standardized questionnaires that included verified scales. A five-point Likert scale was used to rate the answers. Statistical testing encompassed reliability assessments (Cronbach's Alpha > 0.8), regression analyses, model fit indices (RMSEA, CFI, TLI, SRMR), and mediation/moderation evaluations.

Connections to Course Concepts

This article connects with the course concepts from Modules 3, 4, and 6, which link cybersecurity to social science principles. Module 3 focused on survey research and behavioral analysis, which connects to the study's quantitative design. Module 4 looked at human factors including awareness, trust, and participation, which are fundamental to the concept of the article. Module 6 talked about how psychology plays a role in cybersecurity. It stressed that to be safe, you need to know how people act and how technical systems work.

Connection to Marginalized Groups

While the article didn’t really target marginalized groups, its results are still important. Employees who don't have as much exposure to support from leadership, training, or cultural adjustment may be more likely to break the rules. In many companies, lower-level employees or those who don't work in technology may not have much independence. This shows how a lack of resources or communication channels can make cybercrime more likely to happen.

Conclusion/Contributions to Society

In conclusion, the research done by Ghaleb and Pardaev is a very important contribution to the structure of security within a business. By demonstrating that the efficiency of cybersecurity depends on both human and organizational factors, rather than solely on technology. By creating a model that includes culture, trust in management, awareness, and engagement, it gives useful tips on how to improve compliance and minimize insider threats. The results show that building a culture of trust and understanding helps people stay strong over time. In general, it stresses how important it is to understand social behavior and how important it is to get technology, psychology, and management to work together to make digital spaces safer.

References

Ghaleb, M., & Pardaev, J. (2025). Controlling cyber crime through information security compliance behavior. *International Journal of Cyber Criminology, 19*(1), 1–26. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/437/123