**Article Review 1**

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

Stephen Price

School of Cybersecurity, Old Dominion University

CYSE201S: Cybersecurity and Social Science

Professor Diwakar Yalpi

September 28, 2025

## Introduction

Cybercrime has become a major concern in our society. The rapid evolution of technology has forced organizations to go beyond technical defenses of different attacks like data breaches, phishing emails, and ransomware attacks to prioritize their focus on the human aspect of cybersecurity. This has made researchers want to examine humans' security compliance behavior and the possible factors that could affect it.

## Research Question and Hypotheses

The main research question in this study is researchers investigating the relationship between the factor's cybersecurity awareness, organizational culture, and trust in management and how does it affect humans' information security compliance behavior. The hypothesis of this study predicts that high levels of cybersecurity awareness can improve information security compliance behavior, The independent variables for this study are cybersecurity awareness, organizational culture, employee engagement, and trust in management. The dependent variable for this study is information security compliance behavior.

## Research Methods

The research method that was used in this study is quantitative to look at the organizational and behavioral factors. This research was done by doing surveys and questionnaires from employees who work in different departments like IT and human resources. This method allowed researchers to examine the relationships between cybersecurity awareness, organizational culture, trust in management, and information security compliance behavior. It also helped researchers test their hypothesis by finding signs of compliance behavior.

## Data and Analysis

This study collects quantitative data through surveys and questionaries that were analyzed using structural equation modeling, tables, and regression analysis. This data is being analyzed to find the relationship between cybersecurity awareness, organizational culture, trust in management, and information security compliance behavior. Researchers can test their hypothesis based on the data collected and the relationships between the independent and dependent variables.

## Social Science Concepts

This article can relate to multiple theories of social science like Neutralization theory, Behavioral, and Psychodynamic theory. Neutralization theory is when people know right from wrong and they rationalize their behavior. Employees could use this theory and the five neuralization techniques denial of responsibility, denial of injury, denial of victim, condemnation of the condemners, and appeal to higher loyalties to justify their behavior. Behavioral theory is where the behavior is shaped by the environment their around or praising behavior either good or bad can make someone do it again. Psychodynamic theory can help examine why employees cannot control cybercrime due to psychological factors.

## Marginalized Groups

Employees that are not experienced or from a different culture or background can have issues complying with information security management. In this study based on the data analysis it suggests creating a supportive work environment can address these challenges and help these employees gain awareness in cybersecurity. This can help promote a positive work environment among the employees and could work together and collaborate more.

## Society Contributions

This study can contribute to society by informing policies on the behavior factors that can cause cybercrime and what can be done to prevent it. This can help prevent organizations from experiencing potential financial loss and reputational damage. It can also raise awareness of not only organizations but in education and training programs as well so it can help enhance the skills and gain knowledge about why information security compliance behavior is important to reduce cybercrime.

## Conclusion

In conclusion, the results of this study can conclude that the risk of cybercrime can be reduced by promoting cybersecurity awareness, promoting trust in management, and encouraging compliance with information security policies. This can help organizations improve their security measures so that they can protect themselves from future cyber threats. Security in an organization is important because it ensures business continuity and responsible employees that follow the standards and guidelines that can help control cybercrime.

**References**

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