Myla Gorges

11/16/2025

CYSE 201S

Professor Diwakar Yalpi

ARTICLE REVIEW #2

Perceived Security Risks and Cybersecurity Compliance Attitude

INTRODUCTION

The article *Perceived Security Risks and Cybersecurity Compliance Attitude: Role of Personality Traits and Cybersecurity Behavior* by Ghaleb and Sattarov (2025) examines how people's personality traits and feelings about online security can influence the way people follow and interact with cybersecurity rules at work. Instead of focusing on technology, the study focuses on human behaviors, which make it very strongly connected to the social sciences principles. The authors talk about how people make cybersecurity decisions based on emotions, how they think about risks, and their personal traits. They use ideas from the Protection Motivation Theory (PMT) and the Theory of Planned Behavior (TPB) to show how people in everyday life process threats and decide whether to follow the security guidelines (Ghaleb & Sattarov, 2025). These theories help explain why the psychological side of cybersecurity is something that the social sciences often focus on.

RESEARCH QUESTIONS AND VARIABLES

The main goal of this study is to understand how the Big Five personality traits agreeableness, conscientiousness, extraversion, neuroticism, and openness really affect employees' cybersecurity behavior and their willingness to follow the security rules. The authors also wanted to see if cybersecurity behavior can act as a mediator between personalities and compliances, and whether a person's perception of risk makes relationships stronger or weaker. In this study, personality traits act as independent variables, cybersecurity behavior is our mediator, the perceived security risks are our moderator and the cybersecurity compliance attitude is the dependent variable (Ghaleb & Sattarov 2025).

RESEARCH METHODS

The authors answer the research questions by using a quantitative method by surveying 259 employees from all different types of organizations departments. The participants had completed these validated scales that were measuring their personality traits, their behavior that incorporated with cybersecurity, their attitudes, and as well as their perceived risks. The authors analyzed the data by using a Structural Equation Modeling (SEM), that allows them to test the direct, indirect and monitoring relationship all at one time. The Confirmatory Factor Analysis (CFA) shows that the following measures used in the study are reliable and valid (Ghaleb & Sattarov, 2025)

DATA AND RESULTS

The result from the study shows that all five personality traits had significant effects on both compliance attitudes as well as cybersecurity behavior. The conscientious individuals were more likely to be more responsible with cybersecurity and agreeable individuals were more likely to be cooperative and likely to follow the rules. The neurotic individuals are the ones who are more sensitive to threats, are more aware and act more cautiously online. The individuals who had the personality trait of openness and extraversion showed they had positive relationships with secure behaviors. Behaviors that are relating to cybersecurity was confirmed as a mediator which means that personality traits tend to influence behavior first which will then shape the compliance attitudes. Assessing security risks has also strengthened these relationships which make personality and behavior a lot more important when individuals feel increasingly threatened.

CONNECTION TO COURSE CONCEPTS

The findings that were found from this study, strongly connect with the concepts that we have learned so far in CYSE 201S. Many of the lectures that we have listened to and learn from have highlighted that the human behavior is one of the biggest challenges when it comes to cybersecurity vulnerabilities which this study talks about. Theories like the PMT and TPB, help explain how people process risks, form intentions, and how they develop attitudes. This article really reinforces the idea that cybersecurity isn't really just about technology its also about being able to understand individuals' motivations and thought processes.

CONCLUSION

Overall, the study makes an important contribution to cybersecurity by showing that its not just a technical issue its also a human one. This article explains how behavior, personality, and perceived risks work together as one to influence whether individuals should follow security rules. It talks about how organizations should create more of personalized cybersecurity training programs that can consider differences with individuals. By highlighting this psychological side of cybersecurity, this study helps explains why people act the way they do when they're online and how all organizations can encourage others to be safer when it comes to digital behavior

REFERENCES

Ghaleb, M. M. S., & Sattarov, A. (2025). *Perceived security risks and cybersecurity compliance attitude: Role of personality traits and cybersecurity behavior.* International Journal of Cyber Criminology, 19(1), 27–53.