Article Review #2

Chandler A. West

Old Dominion University

CYSE201S

Professor Yalpi

11/7/2025

Cybersecurity Compliance Attitude vs. Big Five Personality Traits

Introduction

The article by Mohanad Ghaleb and Abdisamat Sattarov (2025) looks at how a person's personality and sense of risk affect their behavior and attitude toward cybersecurity rules. They pointed out that most cyberattacks succeed because of human mistakes rather than technical failures. Their study focuses on understanding why some people are more likely to follow security rules than others. They use the "Big Five" personality traits to show how personality connects to user's cybersecurity habits. These traits are agreeableness, conscientiousness, extraversion, neuroticism, and openness. The researchers surveyed employees from different organizations and analyzed the results to find patterns. Overall, the study shows that personality and how people view online risks both play a big role in whether someone follows cybersecurity policies at work or not.

Relation to Social Science Principles

This topic fits strongly with the ideas of the social sciences, especially psychology and sociology. It focuses on human thoughts, feelings, and behaviors rather than just technology. The study explains that cybersecurity problems mostly come from how people think, what they believe, and how they react to rules. The researchers used theories such as the Protection Motivation Theory and the Theory of Planned Behavior, to show that cybersecurity is as much a social issue as it is a technical one. It is important to learn how people handle danger, how much they care about rules, and how they interact within an organization.

Research Question, Hypotheses, and Variables

The main question of the study was: Do personality traits influence people's cybersecurity behavior and their willingness to follow cybersecurity rules, and does the feeling

of security risk change this relationship? The authors believed that certain personality types, like people who are more responsible, would be more likely to follow security rules. They also thought that people's behavior might serve as a bridge between their personality and their attitudes toward compliance. The study tested five hypothesis. Does personality affect cybersecurity behavior, does it affect compliance attitude, does that behavior act as a link between the two, and does security risk strengthen or weaken these relationships. The independent variables were the Big Five personality traits, and the dependent variable was cybersecurity compliance attitude.

Research Methods

This study used a quantitative research method. The authors surveyed 259 employees from different companies. Participants answered questions about their personality traits, cybersecurity habits, and how risky they thought the online world was. The researchers used well-known and tested questionnaires from past studies. After collecting the responses, they used a type of statistical modeling called Structural Equation Modeling, or SEM, to find relationships between the variables. This method helped them see how personality traits, risk perception, and behavior all connect to cybersecurity compliance.

Data and Analysis

The data came from survey answers that measured personality, security behavior, compliance attitude, and risk perception. The researchers checked that the questions were reliable and that the results were consistent. They found that people who were conscientious and agreeable were more likely to show safe cybersecurity behaviors, such as using strong passwords and following company rules. People who were neurotic also tended to be careful online because they feared risks. The analysis showed that behavior was the middle link between personality

and attitude, which means that personality affects behavior, which then affects how someone feels about compliance. It also showed that people who believe online risks are high are more motivated to follow security rules. Overall, their model explained a large portion of why people act securely online.

Class Presentation Relations

The article connects well with what we learned in Module 9 about culture and cybersecurity. Our class discussed how people's values, beliefs, and social norms shape how they act online. The article supports this by showing that personality traits and how people see online risks affect whether they follow cybersecurity rules. This ties into the idea of cybersecurity culture, where attitudes and behaviors come from shared social values, not just technical skills. Both the article and the class materials agree that improving cybersecurity means understanding human behavior and building a culture where everyone wants to keep information safe.

Marginalized Groups

Even though the study did not directly focus on marginalized groups, its findings are useful for understanding how to make cybersecurity training more inclusive. Many organizations use the same training for everyone, but this research suggests that individuals have different personalities and risk perceptions that affect how they learn. For example, people who are anxious about technology or come from communities with less digital access might need more supportive and personalized training. It is important to recognize that people learn about cybersecurity differently. By doing this, it can help companies design programs that include everyone, especially those who might feel left out of traditional training programs.

Contributions to Society

This research contributes to society by showing that cybersecurity is not only about technology, but also about human behavior. Understanding how personality affects security habits can help organizations build stronger security culture. For instance, companies could create awareness programs that fit different personality types, like what we learned from the Big Five traits. Teaching cautious people how to manage their anxiety and helping more relaxed people understand the importance of caution is important. By combining psychology and technology, the study helps businesses and governments build safer environments.

Conclusion

In summary, Ghaleb and Sattarov's study provides a fresh perspective on how personality and perceived risk influence cybersecurity behavior. It connects psychological and social science theories to real-world technology issues, showing that protecting digital information depends on understanding human nature first. The authors demonstrate that when people feel personally responsible and aware of online dangers, they are more likely to follow security rules. Their findings suggest that successful cybersecurity strategies should not only focus on systems and software but also on the people who use them every day.

References

M. Ghaleb, A. Sattarov, Perceived Security Risks and Cybersecurity Compliance Attitude: Role of personality Traits and Cybersecurity Behavior, *International Journal of Cyber Criminology*, Volume 19, Issue 1, January 2025, https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/438/124