

Article Review #1: Security Risks & Cybersecurity Compliance: Personality Traits &
Cybersecurity Behavior

Shelton Jones

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity & Social Sciences

Professor Yalpi

February 26, 2026

BLUF:

Cybersecurity compliance is a very important thing to follow; therefore, having certain personality traits from employees in a workplace can influence whether they follow the rules or not. Traits from the Big 5 Model affect attitudes toward security policies in a workplace.

Relation to Social Science Principles:

The article applies psychological and behavioral social science principles to understand human responses to cybersecurity requirements and authority. Instead of focusing on technical solutions, it treats cybersecurity behavior as human behavior that gets influenced by personality, perception, and attitude towards others.

Research Question/Hypothesis/Independent Variable/Dependent Variable:

Research Question: How do security risks & The Big 5 personality traits influence employees' cybersecurity behavior and their attitudes towards compliance with cybersecurity policies?

Hypothesis: The Big 5 personality traits significantly affect cybersecurity behaviors

Independent Variable: The Big Five personality traits (agreeableness, conscientiousness, extraversion, neuroticism, openness).

Dependent Variable: Cybersecurity Compliance Attitude- the employee's attitude to security protocols.

Research Methods Used:

The authors used a quantitative, correlational research approach, which I learned in social science studies is when relationships between variables are tested. Data was collected by standardized survey scales adapted from prior validated research. Big Five personality inventory scales, cybersecurity behavior measures, attitudes toward compliance scales, and risk perception scales were also used. The sample consisted of 259 employees from various organizational settings to capture real-world cybersecurity interactions.

Data Analysis Used:

Structural Equation Modeling (SEM) was used to test the proposed model's direct, indirect, and interactional effects. Confirmatory Factor Analysis (CFA) was also used to ensure measurement scales reliably and validly measure the intended personas. A way of confirming whether the proposed theoretical model fits the observed data, a model fit index was placed within the data research.

Connections to Course Concepts:

Human factors are a connection to the course concepts because the psychological factors from the article exemplify how much they matter as much as technology in understanding compliance attitudes in cybersecurity. The personality theory from the Big 5 model of psychology is applied to explain differences in cybersecurity behavior and attitudes within the article.

Connections to Marginalized Groups:

The article does not specifically have a targeted toward demographic like race, gender, or identities, but there are challenges & concerns. For example, standardized compliance training may not account for cultural, educational, or workplace inequalities that affect how personality traits translate into behavior.

Conclusion & Societal Contributions:

This article shows that human behavior and psychological factors are critical to cybersecurity, being a major societal concern as cyber threats increase. By informing policy and training, organizations can provide insight into personality and perception to develop more effective, evidence-based cybersecurity training, potentially reducing breaches caused by human error and behavior. Holding security awareness programs based on personalities could improve compliance and reduce costly security incidents.

Reference:

<https://cybercrimejournal.com/manuscript/index.php/cybercrimejournal/article/view/438/124>