Article Review #1: Perceived Security Risks and Cybersecurity Compliance Attitude: Role of Personality Traits and Cybersecurity Behavior

Albreana Butler

School Of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and Social Sciences

Diwakar Yalpi

02/25/2026

Introduction/BLUF

The article Preceived Security Risks and Cybersecurity Compliance Attitude: Role of Personality Traits and Cybersecurity Behavior describes how personality traits can influence employees' cybersecurity compliance attitudes in a workplace. The author focuses on how individual personalities impact attitudes towards being in compliance with policies such as security and digital safety. The article highlights the human factor in cybersecurity. Understanding personality and perception creates better chances for companies to predict and prevent suspicious behavior.

Relation/Connection to Social Science Principles

This topic relates to the 7 social science principles (Relativism, Objectivity, Parsimony, Empiricism, Skepticism, Ethical Neutrality, and Determinism) because it focuses on human behavior and personality within an organizational perspective. Relativism is shown by understanding that cybersecurity attitudes may differ depending on the personality of the individual and their perception of risks. Objectivity is shown by using surveys and analysis rather than personal opinions. Parismony is demonstrated by examining a limited number of critical variables to explain compliance behavior. Empiricism is presented by conclusions and measurable and observable survey data. Skepticism is reflected by testing hypotheses, determining whether connections between personality and compliance are supported by factual data. Ethical neutrality is introduced by analyzing the participants without labeling them good or bad, but instead analyzing patterns. Finally, determinism is seen from the perspective that personality traits and perceived risk influence cybersecurity behaviors and attitudes.

Research Question/Hypothesis/Independent Variable/Dependent Variable

The main question in this research asks how personality traits and perceived security risks affect cybersecurity compliance attitudes and behavior. The hypotheses explain that some personality traits affect compliance, and higher perceived security risks have a massive influence on compliance attitudes. The independent variables refer to personality traits and perceived security risks. The Dependent variables represent cybersecurity compliance attitude and cybersecurity behavior. The study examines whether changes in personality traits or perceived risks determine differences in cybersecurity compliance.

Types of Research Methods used

This article presents a quantitative study. This consists of survey data collected from participants to measure personality traits, perceived risk, and compliance behavior in an organization. Questionnaires are used to help maintain consistent measurement of variables. The research design examines relationships between variables, and statistical testing is used to evaluate the established hypotheses.

Types of Data Analysis used

Data collected in the study is quantitative data gathered through survey responses. Participants scaled statements related to personality traits, risk perception, and cybersecurity attitudes using structured scales. Researchers analyze data using various techniques, such as correlation and regression analysis, to analyze relationships between variables. These analyses are used to determine if independent variables can predict compliance attitudes and behaviors.

Connections to other Course Concepts

In my opinion, this article resonates to psychological theories discussed in the PowerPoint. Personality theories are directly relevant because the study analyzes how personality traits can impact behavior in cybersecurity. Cognitive theories also apply, since the article explain perceived security risk determines how individuals perceive and interpret threats. Behavioral theories correlate because non-compliant behaviors can become repeated habits over time. Additionally, the article supports the perspective presented in the slides that theories explain and help determine cyber behavior examining relationships in physiological variables.

Connections to the Concerns or Contributions of Marginalized Groups

This topic resonates with marginalized groups because cybersecurity risks can affect individuals with little to no access to resources or training. Marginalized groups often face challenges such as a lack of education or limited support. If personality perceived risk influences behavior, then unequal access to awareness programs could expand security gaps. Understanding these factors can give organizations opportunities to design inclusive training in cybersecurity that fits diverse populations.

Overall societal of the study/Conclusion

Overall, this study contributes to society by highlighting the importance of the human element in cybersecurity. It explains that improving security is not just about expanding technology but also about understanding personality traits and perceived security risks that impact compliance behavior. Using measurable data and psychological theory helps demonstrate how social science principles help explain and predict human behavior in cybersecurity. Organizations can utilize these findings to develop more effective and inclusive training that reduces threats.

Reference

International Journal of Cyber Criminology Vol 19 issue 1, January – June 2025. (n.d.).
https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/download/438/124/878