Article Review #2

Cybersecurity Compliance Attitudes & Security Risks: A Social Science Review of Individual Personality Traits

OLD DOMINION UNIVERISTY

CYSE 201S – Cybersecurity & Social Science

November 11, 2025

By: Ethan Spruill

ODU Honor pledge

"I pledge to support the Honor System of Old Dominion University. I will refrain from any form of academic dishonesty or deception, such as cheating or plagiarism. I am aware that as a member of the academic community it is my responsibility to turn in all suspected violations of the Honor Code. I will report to a hearing if summoned."

X 

INTRODUCTION

While traditionally cybersecurity problems are thought to be technical issues or failures, most breaches today happen because of human vulnerabilities. This causes for cybersecurity to not only be an engineering or computer science challenge but also a psychological and behavioral one too generating the term “Psybersecurity”. The article “Perceived Security Risks and Cybersecurity Compliance Attitude: role of Personality Traits and Cybersecurity Behavior” by Ghaleb and Sattarov explores an individual’s personality traits, perceived risk, and cybersecurity behavior to determine how these factors shape their decisions and compliance attitudes within the workplace. This review assesses their research questions, methods, findings, and real-world implications through a social sciences perspective.

REVIEW

This article directly relates to the principles of social science by analyzing human behavior in the context of cybersecurity using the Big Five personality traits. More specifically, the authors of this article evaluate why personality differences influence online safety decisions, showing how cybersecurity failures are linked to psychology and emotional factors rather than a lack of technical skill [1]. Which overall through this article they present how organizations can protect their workers rather than blaming individuals and how policies can be shaped around these human factors rather than assuming everyone behaves identically when confronted with risk.

Research Framework

Before we dive into their findings in this article let us look at the framework, they built centered around the Big Five Personalities. In this study they created 5 main hypotheses: [1]

H1 – *The Big Five personality traits have a significant influence on cybersecurity behavior.*

H2 – *The Big Five personality traits have a significant influence on cybersecurity compliance attitude.*

H3 – *Cybersecurity behavior significantly meditates the relationship between Big Five personality traits and cybersecurity compliance attitude.*

H4 – *Perceived security and privacy risk significantly moderates the relationship of Big Five personality traits and cybersecurity behavior.*

H5 – *Perceived security and privacy risk significantly moderates the relationship of cybersecurity behavior traits and cybersecurity compliance attitude.*

Looking at each of these hypotheses we can see that the main point of this article is to show that personality traits shape cybersecurity compliance attitudes through cybersecurity behavior, and these effects will change based upon the perceived security risk. The independent variables in this article are The Big Five personality traits: agreeableness, conscientiousness, extraversion, neuroticism, openness as well as the perceived security risk. While the dependent variables that they are looking at are cybersecurity compliance attitude and cybersecurity behavior. With all the parameters of this research laid out for us we can now take our deeper look into the methods and analysis conducted in this article.

Research Methodology & Analysis

In their research they used a quantitative research approach examining the impact of Big Five personality traits in a sample size of 259 workers who have been exposed to cybersecurity policies within their work environments [1]. These participants completed empirically validated and commonly applied scales measuring personality traits, security behaviors, compliance attitudes, and perceived risk from prior experiments [1]. All these traits of how they are conducting their experiment are easily described using the tactics we have discussed in our slides. Firstly, they are using archival research by using old psychological scales to conduct surveys on each of their 259 subjects. As mentioned, this data is completely survey-like in nature due to the polling of each subject on a given scale and using this self-reported data for their

research. For analysis of this recorded data, they used Structural Equation Modeling as it has excellent capabilities for dealing with intricate structures, and multiple paths of mediation and moderation [1]. Using this, it very obviously reveals in their study that all five personality traits significantly predict cybersecurity behavior and compliance attitudes, as well as showing that the perceived risk does moderate the strength of this relationship between behavior and compliance. Based on their findings there is almost a 75% relation between all behaviors and compliance in each of the tests ran [1]. Overall, this proves that who people are influences their online behavior, and how much risk they feel changes whether they take cybersecurity seriously.

Making Connections

This article strongly aligns with our course lectures in just about every way possible due to its major focus on Big Five personality traits. The most obvious relationship to our course content is the use of Human Factors, in which this article breaks down how cybersecurity failures stem from personality traits and risk perception, not just poor technical training. This line of thinking falls into another topic we have looked at called Psybersecurity, as the research is based on psychology principles and evaluates how emotions and personality shape security decisions. Beyond this it also touches on the use of Victimization as they are presenting a method of understanding how unsafe behavior affects the outcome of attacks rather than blaming the individuals for their actions. While the article doesn't directly state how it corresponds to marginalized groups it is clear how this study could relate to their demographics. Individuals who have a low digital confidence or exposure, which includes elderly workers, or non-technical backgrounds are more vulnerable to cyber threats and are more likely to be blamed for their mistakes assuming that it is their inept technical abilities rather than focusing on the unsafe behavior they may have presented due to their lack of comfort. This article argues instead for a

supportive and psychologically aware system rather than punishment or judgement-based options regarding someone's abilities or mistakes.

CONCLUSION

Overall, this article shows that technical defenses are not enough to combat against cyber criminals if human behavior continues to be disregarded. By showing that the Big Five personality traits and the behavior of workers under a given perceived risk work together to shape their compliance, this research highlights the importance of a more personalized online education, and policy designs that acknowledge psychological diversity rather than assuming that everyone fits the same behavioral mold. By using victimization tactics rather than treating individuals who lean into unsafe habits as the problem, this study contributes towards the progress of a more inclusive and safer environment within the workplace.

REFERENCES

[1] *Ghaleb, M. M. S., & Sattarov, T. F. (2025). Perceived security risks and cybersecurity compliance attitude: Role of personality traits and cybersecurity behavior. Cybercrime Journal, Advance online publication.* *https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/438/124*