**Article Review #1: Title of the Article Review**

Student Name: Bernard Brown-Watkins

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 10/7/2025

**Introduction/BLUF**

Cybersecurity threats continue to grow in frequency, cost, and experience to make human observances with security procedures such as both safe password practices and phishing awareness a key element of administrative and personal security. Personality traits significantly influence how individuals provide security risks, pursue viewpoints toward compliance, and engage in the behaviors of cybersecurity. The main purpose of this article is to investigate how the influence of individual personality traits identifies cybersecurity risks, compliance attitudes, and the behavior of cybersecurity in order to understand both the social and psychological factors of user actions, whether they are secure or insecure.

**Relation/Connection to Social Science Principles**

Focusing on the article, each of the seven social sciences share a connection to the article. For instance, the article relates to the social science of psychology because it explores how mental processes operate the cybersecurity protocols with compliance or noncompliance. This is relevant to the article’s subject matter because it relies on psychological theories like the Big Five Personality Traits, Protection Motivation Theory (PMT), and Theory of Planned Behavior (TPB). Second, the article incorporates principles from the social science of sociology because cybersecurity behavior is not only individual, but formed by social norms, work environment, and peer influence. This is relevant to the article’s subject matter because the social structure within an administration or society either encourages or discourages cybersecurity practices.

Third, the article incorporates principles from the social science of anthropology because it helps explain how both cultural values and traditions form the trust of users in technology, rules, and authority. This is relevant to the article’s subject matter because the awareness of risks and viewpoints towards compliance can change significantly across cultures. Fourth, the article incorporates principles from the social science of political science because it mentions compliance based on rules and authority. This is relevant to the article’s subject matter because decisions can inform public policy on cybersecurity awareness and regulation, such as formulating policies for different personality types. Fifth, the article incorporates principles from the social science of economics through both risk assessment and social economics, such as how observed intensity influences conformity. This is relevant to the article’s subject matter because individuals often weigh the costs and benefits when deciding whether to either follow or evade cybersecurity protocols.

Sixth, the article incorporates principles from the social science of history through both historical breaches and collective memory that influence present awareness. This is relevant to the article’s subject matter because it provides context about the historical trends in both cybersecurity breaches and compliance behaviors, such as the past major data breaches that form current awareness of risk and influence behavior. Finally, the article incorporates principles from the social science of geography because regional and cultural differences can influence behavior and viewpoints as a result of international cybersecurity threats. This is relevant to the article’s subject matter because geographic location affects the exposure to cyber threats, access to cybersecurity resources, and administrative policies.

**Research Question/Hypothesis/Independent Variable/Dependent Variable**

Research Questions:

* How do personality traits influence individuals’ perceived security risks and attitudes toward cybersecurity compliance?
* What is the relationship between perceived security risk, compliance attitude, and actual cybersecurity behavior?
* Do perceived security risk and compliance attitude mediate the relationship between personality traits and cybersecurity behavior?

Hypotheses:

1. The Big Five personality traits have a significant influence on cybersecurity behavior.
2. The Big Five personality traits have a significant influence on cybersecurity compliance attitude.
3. Cybersecurity behavior significantly mediates the relationship between Big Five personality traits and cybersecurity compliance attitude.
4. Perceived security and privacy risk significantly moderates the relationship of Big Five personality traits and cybersecurity behavior.
5. Perceived security and privacy risk significantly moderates the relationship of cybersecurity behavior traits and cybersecurity compliance attitude.

Independent Variable:

* Personality Traits
  + Conscientiousness
  + Openness to Experience
  + Neuroticism
  + Agreeableness
  + Extraversion
* Perceived Security Risks

Dependent Variable:

* Cybersecurity Compliance Attitude
* Cybersecurity Behavior (safe password use, following security policies, phishing avoidance)

**Types of Research Methods Used**

This study utilizes quantitative research methods. This is because it allows for statistical testing of both relationships and theories through numerical data.

Data-Based Survey Collection:

* Personality Traits (Big Five Inventory)
* Perceived Security Risks (items assessing how individuals view cybersecurity threats)
* Compliance Attitude (questions on willingness toward following security rules)
* Cybersecurity Behavior (self-reported likelihood of engaging in secure/insecure actions)

Sample:

* Individuals were likely enlisted from a specific population, such as university students and employees in businesses through convenience or deliberate sampling.

Measurement Scales:

* Responses were collected using rating scales (1 = Strongly Disagree to 5 = Strongly Agree).

Data Analysis:

* The collected data was analyzed using structural equation modeling (SEM) to test the theorized relationships and mediation effects between variables.

**Types of Data Analysis Used**

Descriptive Statistics:

* To summarize and describe the main features of the dataset, including means, standard deviations, and frequency distributions of personality traits, perceived risk, attitudes, and behavior.

Correlation Analysis:

* To examine the relationships between variables as a preceding step before more complex modeling, such as personality traits, perceived risk, compliance attitude, and behavior.

Mediation Analysis:

* Specifically tests whether perceived security risk and compliance attitude mediate the relationship between personality traits and cybersecurity behavior.
* This helps us understand whether the influence of personality traits operates through changes in awareness and attitude.

**Connections to the Concerns or Contributions of Marginalized Groups**

Marginalized groups often face unbalanced access to cybersecurity resources and training due to social and economic factors, educational inequalities, or language barriers. This affects their awareness of security risks and their ability to comply with security policies. Personality expressions and how individuals recognize risk can vary across either cultural or social groups. Marginalized populations might have a unique personality-related response formed by their personal experiences.

They can be more vulnerable to cyber threats and may have less support to recover from these attacks, such as scams targeting low-income users. Decisions from the study can inform customized cybersecurity education and policies that are sensitive to the needs of marginalized groups. However, a resolve to be considered for this issue is that future studies should arrange incorporation of diverse populations to ensure decisions and recommendations are culturally responsive.

**Overall Societal Contributions of the Study/Conclusion**

In conclusion, this article makes a societal contribution by spanning psychology, social science, and cybersecurity. It makes an approach to help us understand how individual differences, such as personality traits, affect their awareness of cybersecurity threats, their viewpoints toward compliance, and their digital behavior. This also highlights the need for more personalized and mentally aware interferences to both improve compliance and reduce the oversight in digital environments.

**Reference**

Provide a citation for the article in your preferred academic style (e.g., APA, MLA).

**Article Link:** [**https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/438/124**](https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/438/124)