Article Review #1:

Attitude toward Cybersecurity Compliance and Perceived Security Risks

Michael Everett

October 2, 2025

Overview:

This study by Ghaleb and Sattarov that was published in the International Journal of Cyber Criminology I will be going over in this article review. The authors investigate how people's attitudes toward cybersecurity compliance are influenced by their behavior, perceived security risk, and a person's personality traits. This examines how risk perception and human behavior can shape cybersecurity practices rather than addressing it in a technical matter. This has seemed to have a direct connection to the principles of social sciences.

Hypotheses, Research Question, IVs, and DVs

The research question: How do perceived security risk and the Big Five personality traits affect cybersecurity behavior and compliance attitudes?

Hypotheses:

I have concluded three hypothesis one being The Big Five characteristics have a big impact on cybersecurity behavior. Another being the relationship between compliance attitude and personality is mediated by cybersecurity behavior, and finally the association between compliance attitude and behavior is moderated by perceived security risk. The independent variables are "The Big Five" personality traits which are conscientiousness, extraversion, neuroticism, openness, and agreeableness. The Dependent variables are cybersecurity

compliance attitude and cybersecurity behavior. In all this Cybersecurity behavior acts as a mediator. The moderator can be considered the security risk.

Methods of Research:

The data for this study was collected through surveys using a quantitative research design. Some of the measurement items were big five personality scales, cybersecurity behavior indicators, compliance attitude measures, and perceived risk scales. Hypotheses and model relationships were tested using structural equation modeling.

Information and Evaluation:

The type of data used was cross sectional survey data which is information collected from a single point in time to understand characteristics. Analysis methods include SEM path analysis and CFA.

Results:

There was a strong correlation between cybersecurity behavior and compliance attitudes. Both behavior and compliance were predicted by personality traits, with conscientiousness having the strongest effects. Perceived security risk and compliance attitudes came together well and reduced the impact of traits on behavior.

Relationships to the Course:

In this article and class, the Cognitive Theory was illustrated. To comprehend human behavior and development, this theory focuses on internal mental processes like perception, memory, attention, and thought. It demonstrates how cognitive and affective processes, such as risk perception and personality-based tendencies, impact human behavior.

Effect on Marginalized Communities:

Access to cybersecurity awareness and training is frequently uneven for marginalized groups. To ensure that training is not selective this study makes aware that personality informed approaches could be better for diverse communities. For example, reassurance techniques might work better for people who are more neurotic, but more structured training might be better for people who are less open to things. Reducing this digital divide will increase inclusivity in cybersecurity compliance.

Social Contributions:

By highlighting the human aspect of cybersecurity and going beyond technical fixes, the study benefits society. It provides proof that customized awareness campaigns can be created by utilizing personality traits and perceived risks. Therefore, recommending that companies implement interventions to improve compliance and lower vulnerabilities.

Conclusion

Furthermore, this paper by Ghaleb and Sattarov contributes to how behavior, personality, and risk perception all greatly influence cybersecurity compliance. The study shows that cybersecurity is not just a technical problem, but also highly a social and psychological one. It gives educators, legislators, and organizations useful information by moderating influence of risk perception and the role of behavior.

Reference

Ghaleb, A., & Sattarov, T. (2025). Perceived security risks and cybersecurity compliance attitude. International Journal of Cyber Criminology, 19(1), 43–50. Article Review #1:

Attitude toward Cybersecurity Compliance and Perceived Security Risks

Michael Everett

October 2, 2025

Overview:

This study by Ghaleb and Sattarov that was published in the International Journal of Cyber Criminology I will be going over in this article review. The authors investigate how people's attitudes toward cybersecurity compliance are influenced by their behavior, perceived security risk, and a person’s personality traits. This examines how risk perception and human behavior can shape cybersecurity practices rather than addressing it in a technical matter. This has seemed to have a direct connection to the principles of social sciences.

Hypotheses, Research Question, IVs, and DVs

The research question: How do perceived security risk and the Big Five personality traits affect cybersecurity behavior and compliance attitudes?

Hypotheses:

I have concluded three hypothesis one being The Big Five characteristics have a big impact on cybersecurity behavior. Another being the relationship between compliance attitude and personality is mediated by cybersecurity behavior, and finally the association between compliance attitude and behavior is moderated by perceived security risk. The independent

variables are “The Big Five” personality traits which are conscientiousness, extraversion, neuroticism, openness, and agreeableness. The Dependent variables are cybersecurity compliance attitude and cybersecurity behavior. In all this Cybersecurity behavior acts as a mediator. The moderator can be considered the security risk.

Methods of Research:

The data for this study was collected through surveys using a quantitative research design. Some of the measurement items were big five personality scales, cybersecurity behavior indicators, compliance attitude measures, and perceived risk scales. Hypotheses and model relationships were tested using structural equation modeling.

Information and Evaluation:

The type of data used was cross sectional survey data which is information collected from a single point in time to understand characteristics. Analysis methods include SEM path analysis and CFA.

Results:

There was a strong correlation between cybersecurity behavior and compliance attitudes. Both behavior and compliance were predicted by personality traits, with conscientiousness having the strongest effects. Perceived security risk and compliance attitudes came together well and reduced the impact of traits on behavior.

Relationships to the Course:

In this article and class, the Cognitive Theory was illustrated. To comprehend human behavior and development, this theory focuses on internal mental processes like perception, memory,

attention, and thought. It demonstrates how cognitive and affective processes, such as risk perception and personality-based tendencies, impact human behavior.

Effect on Marginalized Communities:

Access to cybersecurity awareness and training is frequently uneven for marginalized groups. To ensure that training is not selective this study makes aware that personality informed approaches could be better for diverse communities. For example, reassurance techniques might work better for people who are more neurotic, but more structured training might be better for people who are less open to things. Reducing this digital divide will increase inclusivity in cybersecurity compliance.

Social Contributions:

By highlighting the human aspect of cybersecurity and going beyond technical fixes, the study benefits society. It provides proof that customized awareness campaigns can be created by utilizing personality traits and perceived risks. Therefore, recommending that companies implement interventions to improve compliance and lower vulnerabilities.

Conclusion

Furthermore, this paper by Ghaleb and Sattarov contributes to how behavior, personality, and risk perception all greatly influence cybersecurity compliance. The study shows that cybersecurity is not just a technical problem, but also highly a social and psychological one. It gives educators, legislators, and organizations useful information by moderating influence of risk perception and the role of behavior.

Reference

Ghaleb, A., & Sattarov, T. (2025). Perceived security risks and cybersecurity compliance attitude. International Journal of Cyber Criminology, 19(1), 43–50. https://www.cybercrimejournal.com