Article Review #2: Psychology and Cybercriminals

Student Name: Jayden Goldsmith

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: November 11th, 2025

Introduction/BLUF

The main purpose of this article was to find a link between the psychological traits of cybercriminals and how companies can use this knowledge to mitigate future attacks. This study goes through multiple big cyberattacks throughout history, examining their effects and providing recommendations to companies on how to prevent future threats and financial losses from occurring.

Relation/Connection to Social Science Principles

The determinism principle of social sciences relates to this by previous events leading up to the attacks made by cyber criminals. Like the motives behind why specific cyberattacks were committed differ from being political or financial reason. It also relates to the empiricism by using the records of attacks and examining each outcome. Relativism also comes to mind on how the advances in technology is the reason why cybercriminals are able to attack in new ways.

Research Question /Hypothesis/ Independent Variable/Dependent Variable

- Research Question: Learning the technical and psychological aspects of cybercrime will help in future frameworks and mitigating risks.
- Hypothesis: Analyzing previous attacks can help create better frameworks.
- Independent Variable: The different types of impact and consequences each major cyberattack had on a company.

- Dependent Variable: It would be the kind of response given by the company as well as how they will strengthen their cyber security in the future.

Types of Research Methods used

The research method used were case studies on some of the most infamous cyber attacks throughout history. The study used qualitative research, going over six major cyber threats examining things like the impact, repercussion, and the motives of the attacker.

Types of Data Analysis Used

The scientists have done three different kinds of data analysis. The first being to make sure the study is appropriate and the collected data is of good quality. Second, the size of the study population. And third, is making sure that there is no bias that could affect this study's results.

Connections to other Course Concepts

This study reinforces the concepts that were taught in class. For example, the type of motive the hacking group "Guardians of Peace" had was political because in Sony's movie "The Interview", it portrayed their country's leader assassinated. Another example of a motive would be the hacking group "DarkSide"'s attack on the Colonial Pipeline, being purely for financial gain. The group demanded cryptocurrency to give back the access they took.

Connections to the Concerns or contributions of Marginalized Groups

I would say that there is no connection to marginalized groups. This would be because that any group regardless of race, gender, or ethnicity could be motivated by some factor to commit a cybercrime.

Overall societal contributions of the study/Conclusion

In conclusion, there is a wide range of different cyberattacks that cybercriminals can use against an organization. Not only this, but new kinds of attacks are evolving especially with the integration of AI. With that, security in organizations must evolve and adapt just as quickly to retaliate against these advances.

Reference

Thuyen, D., Cam Ha, T., & Ngoc Kim, T. (2025). *Exploring the Psychological Profile of Cybercriminals: A Comprehensive Review for Improved Cybercrime Prevention*. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/452/133