Article Review #1: Routine Activity Theory Understanding

Student Name: Kaemon Powell

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and Social Sciences

Instructor Name: Professor Yalpi

Date: 2/26/2026

Introduction/BLUF

Cybersecurity victimization is influenced by online factors. Exposure and lack of protection plays a role. The study demonstrates that social science applied to physical crime are relevant highly in explaining digital crime behavior.

Relation/Connection to Social Science Principles

After examining the article, I could see that it clearly reflects the 7 core principles of social science. Empiricism is demonstrated through data collection and statistical analysis of cybercrime patterns around victimization. The authors rely on measurable evidence instead of assumptions. Determinism is evident because the study assumes that cybercrime victimization is encouraged by social and behavioral factors. The article also shows objectivity as the authors use structured surveys and statistical analysis instead of their own personal beliefs. Skepticism is also evident because it tests whether traditional crime theories are still present in digital environments. Parsimony is seen in the use of a theory to explain online criminal behavior. This makes the research easier to understand while still being effective. Ethical neutrality is present because the researchers look at victimization patterns without judging individuals for online behavior that may seem skeptical. Instead, it focuses on understanding the causes. Lastly, Relativism is demonstrated by showing that cybercrime risk can vary and it depends on the social context and user behavior. This means experience with cybersecurity is not the same for everyone. These principles show how the blends of studying social science thinking are meaningful with evidence.

Research Question /Hypothesis/ Independent Variable/Dependent Variable

- Research Question: The main research question asks whether Routine Activities theory might explain why certain individuals are likely to become the victims of cybercrime.
- Hypothesis: in the article, the authors propose that online exposure and weak cyber practices increase the chance of cybercrime victimization
- Independent Variable: The independent variables include online activity levels, and personal cyber habits.
- Dependent Variable: The dependent variable is cyber victimization. This is measured through experiences like hacking, theft, and phishing.

Types of Research Methods used

This article uses quantitative research methods mainly. The researchers collected the data through surveys that participants completed about their personal internet habits and past experiences with cybercrime. This method allows them to collect data from the larger group of people. Survey usage is very common in social science and cybersecurity research as it helps discover patterns and risks.

Types of Data Analysis used

The authors used statistical analysis to see the relationships between online behavior and victimization risk. Techniques like correlation analysis were used to see how certain behaviors are predicted in cybercrime exposure.

Connections to other Course Concepts

This article connects closely to several concepts from our course like the human factors of social engineering and risk exposure. It shows the idea that cybersecurity is not just about the tech aspect, but it is also about the people and how they behave online. The study also supports empiricism because it uses data to understand the threats instead of relying on assumptions.

Connections to the Concerns or contributions of Marginalized Groups

The topic is especially relevant to groups of marginalized types who have limited access to cyber education or protective tools. People from low-income communities or who have low digital literacy can face higher risks of cybercrime victimization.

Overall societal contributions of the study/Conclusion

In conclusion, this study makes an important contribution because it shows cybercrime can be understood better through social science theories and human patterns. It highlights that online routines and security awareness impacts cyber risk. The research helps society because it encourages prevention strategies. Overall, The study improves out understanding of the behavior of humans and everyday internet users

Reference

International Journal of Cybercriminal. Scholarly articles on cybercrime and social science research.

Article Link: https://www.cybercrimejournal.com/