Article Review #1: Routine Activities Theory and Cybercrime Victimization

Joshua Punch

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and Social Sciences

Professor Yalpi

February 23rd, 2026

Introduction

This article review will evaluate research as seen in the International Journal of Cybercriminology. The Journal uses Routine Activities theory to study the ways of cyber crime victimization. It will also investigate how internet usage patterns that are monitored day to day leads to a higher chance of people coming victim to cybercrime. The research will show digital environments in which criminology theory will connect will the relevance of social science.

Relationship to Social Science Principles

This topic will relate to key social science principles. These include both criminology and sociology. Both Marcus Felson and Lawrence Cohen co-created the Routine Activities Theory. This theory says that crime will happen most commonly when the offender of the crime has motivation, and when the victim is suitable with no interference of protection. This theory is used to demonstrate how technology usage and social behavior as well as opportunity structures will create the chance for online victimization to occur. The social science field analyzes human behavior patterns as well as social behavior. It also analyzes risk assessment factors as well has social inequality that is displayed within human society.

Research Question Hypotheses IV and DV

- The main research question asks about the relationship between routine online activities and how often cybercrime victimization is.
- The hypothesis says that individuals who often engage in online activities that are viewed as high risk (such as using public Wi-Fi, viewing unsecured websites, etc.) are often more likely to fall victim to cyber victimization.
- The independent variable is the frequency of risky online activities.

- The dependent variable demonstrates how people will fall victim to cybercrime victimization through multiple fraudulent activities

This study predicts that the more risky online behavior, the more victimization rates would increase.

Research Methods

The researchers (Cohen and Felson) used the quantitative research method. They used surveys to collect data from users of the internet. These participants shared their online habit information while also saying whether they had fallen victim to cybercrimes. This research method helps researchers analyze people's behaviors and determine how likely they would be to become victims.These researchers performed testing to see whether their hypothesis received enough evidence to support the claims they made.

Data and Analysis

Survey data was used a lot by this study. The researchers conducted analysis to determine how the independent variable affected the dependent variable's outcome. The results of this revealed that people who more often engaged in high risk behaviors did fall victim to cyber crime at a greater rate than people who did not.

Connection to PowerPoint Concepts

This article connects strongly to the course concepts, which include things such as opportunity structures, victimization theory, and risk factors. This text supports that social settings together with the negative conduct of humans will lead to more common crime occurrences. The findings of this study relate directly to the powerport presentations that display the patterns of cybercrime methods, and how to prevent these.

Marginalized Groups Challenges and Concerns

This study highlights how groups that are marginalized may face cyber risks at a higher rate. People who don't have much experience with technology, as well as people with a lower socioeconomic access that have a smaller amount of access to education in cybersecurity exist without the protection capacity that qualifies as “capable guardianship.” The existing systems of online security will create an unbalanced amount of protection among these people. The equal distribution of security protection will need to be fixed to successfully lower the victimization rate across all vulnerable communities.

Contributions to Society

The article contributes to society by showing that theory can guide people in prevention strategies. The understanding of how online habits link to victimization provides information for developing cybersecurity programs and policy. This research creates a connection between regular criminology and cyber crime in the modern age.

Conclusion

This study provides knowledge that is essential for how Routine Activities Theory applies to cybercrime victimization. The research in this provides insight on the relationship between risky online behaviors and the chances of becoming a victim, which benefits practical prevention strategies as well as common criminological theory. This also demonstrates fundamental necessities of applying the social science framework to address technological challenges that emerge in unfamiliar contexts.

References:

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608. https://doi.org/10.2307/2094589