Article Review #2: Cybercrime and Routine Activity Theory in Online Environments

Name: Chase McKnight

Date: April 16, 2026

BLUF (Bottom Line Up Front)

The article looks at how online behaviors affect the chances of becoming a victim of cybercrime, using Routine Activity Theory. It shows that people who take more risks online are more likely to be targeted, showing the need for cybersecurity awareness and safer habits.

Article Information (APA Citation)

Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *International Journal of Cybercriminology, 10*(1), 1–20.

https://www.cybercrimejournal.com/LeukfeldtYar2016ijcc.pdf

Relation to Social Science Principles

This article ties into key social science ideas. It uses Routine Activity Theory, which says crime happens when a motivated offender, a suitable target, and no protection come together. It also shows how online actions, like revealing personal information, can raise the risk of being a victim. The article connects to rational choice theory too, since offenders weigh their chances and risks. These ideas show that cybercrime is determined by human behavior and social trends, not just random chance.

Research Questions, Hypotheses, IV and DV

The main research question is: *How do everyday online activities affect the chances of becoming a victim of cybercrime?*

The hypothesis is that people who take more risks online are more likely to become victims of cybercrime.

- **Independent Variable (IV):** Types of online activities, such as downloading files, transmitting personal information, or visiting risky websites.
- **Dependent Variable (DV):** Whether someone becomes a victim of cybercrime, like fraud, hacking, or identity theft.

The study shows that taking more risks online leads to a higher chance of becoming a victim.

Research Methods Used

The researchers used surveys to collect data about people's online behaviors and any cybercrime experiences. This quantitative method allowed them to study the results statistically and discover patterns in a large group. It works well because it measures both actions and outcomes with numbers.

Types of Data and Analysis

The study relied on self-reported surveys that asked how often people did certain online activities and if they had been victims of cybercrime. The researchers used statistics, like regression analysis, to see which behaviors raised the risk the most.

Connection to Course Concepts

This article relates to several ideas discussed in class:

- **Cybersecurity risk management:** Shows how behaviors raise vulnerability
- **Threat landscape:** Demonstrates how cyber attackers exploit opportunities
- **Human factor in cybersecurity:** Emphasizes that users are often the weakest link
- **Prevention strategies:** Supports education and awareness as key defenses

These ideas show why it is important to use both technical solutions and human-focused strategies in cybersecurity.

Marginalized Groups: Challenges and Contributions

The article discusses how people with fewer digital skills are more at risk for cybercrime. This group includes older adults, people with lower incomes, and anyone who does not have much access to cybersecurity education.

Problems include:

- Lack of awareness about online threats
- Limited access to secure technology
- Higher susceptibility to scamHowever, the report points out the need for cybersecurity education that includes everyone. This can help protect these groups and make digital safety more equality.

Social Contributions of the Study

This study makes several important contributions to society:

1. It helps explain why cybercrime occurs, enabling better prevention strategies.
2. It stresses the role of user habits, persuading individuals to adopt safer internet behaviors.
3. It supports policymakers and organizations in building targeted cybersecurity education programs.

Overall, this research helps lower the risk of cybercrime and makes the internet safer for more people.

Conclusion

In conclusion, this article shows how Routine Activity Theory can explain cybercrime, proving that what people do online affects their risk of becoming victims. By pointing out the main risk factors and focusing on the human side, the study offers helpful ideas for better cybersecurity. It similarly stresses the need to protect vulnerable groups through education and awareness. The findings add to our understanding and deliver real ways to fight cybercrime.