Jacob E. Moore 2/24/26

Article Review #1: Understanding Cybercrime Victimization Through Routine Activity Theory

Relation to Social Science Principles

This article relates strongly to social science principles because it examines human behavior, social environments, and patterns of victimization in online spaces. Social sciences seek to understand how individuals interact with society, and cybercrime is a modern extension of these interactions. The study uses criminological theory to explain how everyday online activities influence exposure to crime, demonstrating how social behavior in digital environments mirrors real-world patterns.

Research Methods

The study uses quantitative research methods, primarily surveys of internet users. Participants reported their online behaviors, security practices, and experiences with cybercrime. This method allows researchers to analyze patterns across a large population and identify statistical relationships between behavior and victimization.

Data and Analysis

Researchers used statistical analysis to determine correlations between risky online activities and cybercrime experiences. Data included frequency of internet use, types of online engagement, and security measures such as antivirus software or password practices. The analysis showed that individuals with higher exposure and lower protection faced greater risk.

Connection to Course Concepts

Concepts from the course PowerPoint presentations, particularly Routine Activity Theory, are central to this article. The theory states that crime occurs when a motivated offender encounters a suitable target in the absence of capable guardianship. In cyberspace, guardianship includes firewalls, strong passwords, and cybersecurity awareness. The article demonstrates how these principles apply directly to modern digital crime.

Marginalized Groups

The study highlights how vulnerable populations may face increased cybercrime risk due to limited digital literacy or access to cybersecurity resources. Older adults, low-income

individuals, and those with less technical knowledge may struggle to implement protective measures, making them attractive targets for scams and fraud.

Conclusion

Overall, the article demonstrates that traditional criminological theories remain relevant in the digital age. Routine Activity Theory effectively explains cybercrime victimization by focusing on behavior, exposure, and protection. The study reinforces the importance of cybersecurity awareness and proactive safeguards to reduce online crime. As society becomes increasingly dependent on digital technologies, understanding these risk factors is essential for protecting individuals and communities.

Reference

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *International Journal of Cybercriminology*. https://www.cybercrimejournal.com