Dylan Shaver

Professor Yalpi

CYSE 201S

February 16, 2025

Article Review #1: Cyber Victimization in the Healthcare Industry

BLUF

The healthcare industry is a prime target for cybercriminals due to its valuable data, routine vulnerabilities, and limited cybersecurity resilience. This article uses Cyber-Routine Activities Theory (Cyber-RAT) and a mixed-methods approach to explore how routine behaviors and systemic weaknesses contribute to cyber victimization, particularly among marginalized populations. Grounded in social science principles, the study provides insights into offender motivations, victim impacts, and policy solutions to mitigate risk.

How the Topic Relates to Social Science Principles

Cyber victimization in the healthcare industry reflects several social science perspectives. From criminology, the article explains offender motivation, why attackers target healthcare organizations, often for financial gain or sensitive personal data. Psychology plays a role in understanding the emotional and behavioral impacts on victims, such as fear, stress, and loss of trust. Sociology explores how systemic weaknesses affect vulnerable populations, while economics evaluates the significant costs of breaches to institutions and society. These social sciences together help explain not just the 'how' of cyberattacks, but the 'why' and the human consequences.

Study Research Questions and Hypotheses

The article explores several key research questions:

- Why is the healthcare sector increasingly targeted by cybercriminals?
- What makes healthcare systems so vulnerable to cyberattacks?
- How do routine activities within healthcare environments contribute to cyber victimization?
- How does Cyber-Routine Activities Theory (Cyber-RAT) help explain victimization patterns in this sector?

These questions guide the analysis of how offender opportunities and institutional behavior intersect.

Research Methods Used

The article employs a mixed-methods approach, combining quantitative and qualitative techniques. Descriptive statistics are used to analyze frequencies and patterns of attacks. Comparative analysis examines differences across healthcare organizations, and qualitative interviews with healthcare staff provide insight into human perspectives and risk behaviors.

Types of Data and Analysis

Data sources include:

- Incident data: Registered cybercrimes within healthcare
- Organizational data: Characteristics of targeted health systems
- Survey/interview data: Opinions from healthcare staff
- Offender characteristics: Motivations and behaviors

Analysis methods include:

- Descriptive statistics (attack frequency, type, impact)
- Regression analysis to identify predictive factors
- Pattern recognition tied to routine activities
- Comparative analysis across geographic and organizational settings

Connections to Class Concepts

This article connects to class discussions about Cyber-RAT, routine behavior and vulnerability, and data analysis in cybersecurity. The article also reflects concepts from PowerPoint presentations, including cybersecurity challenges for marginalized groups, and the role of human behavior in digital risk.

Marginalized Groups and Systemic Concerns

The study highlights how cyberattacks on healthcare systems disproportionately affect marginalized groups, especially those with limited digital literacy, access to care, or economic resources. These groups are often less able to respond to identity theft, medical fraud, or breaches of privacy. The article advocates stronger protections and inclusive policies to defend these vulnerable populations.

Overall Contributions to Society

This research offers a clearer understanding of why the healthcare industry is a prime target for cybercrime and what systemic changes are needed. It contributes to cybersecurity policy development, promotes public awareness, and supports interventions aimed at protecting sensitive medical data and improving institutional resilience.

Conclusion

The article effectively blends social science theory with real-world cybersecurity challenges in healthcare. Through research questions, data, and analysis, it shows how attacker motivations, human behavior, and system vulnerabilities interact. The study calls for improved cybersecurity awareness, stronger protection for marginalized populations, and better use of routine activity theory to shape prevention strategies.

Reference

International Journal of Cybersecurity Intelligence & Cybercrime. (2019). *Cyber victimization in the healthcare industry*. Bridgewater State University. https://vc.bridgew.edu/ijcic/vol7/iss2/2/