

**Article Review #1: A analytical review of “Cyber Victimization in the Healthcare
Industry: Analyzing Offender Motivations and Target Characteristics through Routine
Activities Theory (RAT) and Cyber-Routine Activities Theory (Cyber-RAT)”**

Obi Oputa

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Diwakar Yalpi

2/24/26

Introduction

In a 2024 study, authors Yashna Praveen, Mijin Kim, and Kyung-Shick Choi explore the topic of cyber victimization in the healthcare industry. They use theories like the Routine Activities Theory (RAT) and the Cyber-Routine Activities Theory (Cyber-RAT) to explain why this industry is often the focus of cybercriminals. They analyzed 1,138 recorded incidents of healthcare cybercrime from 2018 to 2023 to determine the motivations of the offenders, the attacks, and the targets.

Relation to Social Science Principles/Concepts

When looking at the article's relation to key principles of social sciences, there are four easily identifiable principles that appear throughout the article. The first being **empiricism**, as the study refers to real data regarding cyberattacks as opposed to theoretical concepts. The authors investigate 1,138 healthcare cyberattack incidents and categorize them according to the motivation behind the attack, the method of attack, and the target of the attack. There is also evidence of **determinism**, as the authors suggest that cyber victimization can only occur under the correct circumstances, rather than at random. Using the Routine Activities Theory, the article shows that a motivated offender will attack a healthcare organization if there is an opportunity to steal valuable data and no digital guardianship to help prevent its theft. There are also aspects of **relativism**, as the topic of health care cybersecurity is related to other "systems," such as digital expansion, economic motivation, and state-sponsored political activity. Finally, the findings demonstrate **objectivity**, as they are not based on opinions but rather on theoretical frameworks and documented cyberattack activity.

Research Questions and Variables

Within this article, the authors highlight two key primary research questions in this study. Specifically, the study seeks to address: (1) “What are the primary motivations driving Advanced Persistent Threats (APTs) to target the healthcare industry?” and (2) “What are the common characteristics and behaviors of APT groups (whether state-sponsored or cybercriminal) that target healthcare institutions?” By examining these questions, the authors ultimately seek to gain a better understanding of patterns involving cyber victimization within the healthcare industry and propose possible strategies to help improve security (Praveen et al., 2024, p. 7). While the article does not present a formal hypothesis statement, it implies a theory-driven hypothesis based on Routine Activities Theory (RAT). Originally proposed by Cohen and Felson (1979), RAT states that crime only takes place with the convergence of three elements: a motivated offender, a suitable target, and the lack of protective measures. Cohen and Felson’s original theory is transferred to the cyber domain through Cyber-RAT, where healthcare organizations become suitable targets as motivated offenders meet information-rich institutions lacking proper cybersecurity (Praveen et al., 2024, p. 5).

When looking at the dependent and independent variables in this study, the dependent variable was the type of healthcare organization targeted. This included many different categories, such as hospitals, pharmacies, research institutions, government health agencies, and third-party vendors. The independent variables of this study were designed to capture the characteristics of cyberattacks and offenders and included four measures: attack method (ransomware, phishing, account takeover, account hijacking, malware infection, DDoS, defacement, vulnerability exploitation, or unidentified), attacker motive (financial gain, hacktivism/ideological motivations, research and intellectual property/patient data theft, or

unidentified), state sponsorship (whether the attack was state-sponsored, serving as a proxy for APT involvement), and country of origin (Russia, China, Iran, North Korea, Ukraine, or unknown) (Praveen et al., 2024, p. 8).

Types of Research Methods used

When looking at the type of research method used, the article uses a quantitative research approach through archival research and secondary data analysis. The authors used secondary data from the Hackmageddon database, supplemented by Databreaches.net, CSIDB.org, and the HIPAA Journal, to fill in missing records. A total of 1,138 healthcare-related cyber incidents between 2018 and 2023 were closely examined.

Types of Data Analysis used

The type of data analysis methods used in the study were descriptive statistics to report the frequencies of the types, motives, and target organizations of cyberattacks. Additionally, the researchers also performed Chi-square tests of independence to identify statistically significant associations between categorical variables and utilized Cramer's V to measure the effect size.

Connections to other related Course Concepts

When looking at how this article connects to course concepts covered throughout this course so far. The article uses material covered in module 2; the article uses research questions, hypotheses, and variables, showing how attacker characteristics (IVs) influence which healthcare organization is targeted (DV). Additionally, from Module 5, the article focuses on the individual motives for cyber offending, with motives like financial gain and ideological motivations. This connects directly back to the individual motive framework discussed in module 5.

Connections to the Concerns or contributions of Marginalized Groups

The article authors do not explicitly focus on marginalized groups. However, its findings show important implications for vulnerable populations. The low-income, elderly, and chronically ill patients who rely heavily on consistent healthcare access can suffer the most from the effects of cyberattacks on healthcare facilities and organizations.

Conclusion

In conclusion, authors Praveen, Kim, and Choi make numerous meaningful contributions to both cybersecurity and the social sciences. By adapting RAT and Cyber-RAT to the healthcare industry, this study demonstrates that criminological theories designed to explain physical world crimes can also be applied to complex digital crimes. Such insights provide healthcare organizations and legislators critical information on how and why cyberattacks occur and how they can implement stronger preventive measures to help prevent cybercrime from happening.

References

- Praveen, Y., Kim, M., & Choi, K.-S. (2024a). Cyber victimization in the healthcare industry: Analyzing offender motivations and target characteristics through routine activities theory (RAT) and cyber-routine activities theory (Cyber-RAT). *International Journal of Cybersecurity Intelligence & Cybercrime*, 7(2).
<https://doi.org/10.52306/2578-3289.1186>