Mathieu Crosby

3/30/25

Article Review #2: Cyber Victimization in the Healthcare Industry

Introduction

The research study "Cyber Victimization in the Healthcare Sector: Offenders and Cybersecurity Strategies" by Praveen et al. (2024) examines cybersecurity problems of the healthcare sector. The study applies the Routine Activity Theory (RAT) model in studying cyber threats, focusing on Advanced Persistent Threats (APTs). This review examines the article from a social science point of view by evaluating its research questions, methodology, data analysis, and contributions, and in relation to marginalized groups and social implications.

Social Science Principles

The study aligns with several prevailing social science theories. Rational Choice Theory is observed where cybercriminals weigh risks and benefits before targeting healthcare organizations. Structural Functionalism is demonstrated in how compromised security structures in healthcare translate to systemic vulnerabilities that render them an attractive target for cyberattacks. Conflict Theory is also present in the research as it demonstrates power inequalities in which resource-poor healthcare organizations are arrayed against well-resourced cybercriminal networks.

Research Questions and Hypotheses

The study focuses on two research questions: What are the principal motivations of APTs targeting the healthcare sector? What are the common behaviors and characteristics of APT groups attacking healthcare institutions? The assumption is that profit motive and stealing data are principal motivations for cyberattacks, and state-sponsored groups will more frequently target industries of valuable data.

Research Methods

The study adopts a quantitative, secondary data analysis approach by collecting cyberattack events from Hackmageddon, Databreaches.net, and CSIDB.org. The dataset contains 1,138 cases of cyberattacks in the healthcare industry between 2018 and 2023. The study categorizes cyber incidents based on motivation, attack, and organization targeted in order to identify trends and patterns.

Data and Analysis

The study examines different variables with the aim of assessing cyber victimization in health care. The dependent variable is the type of health care organization that has been victimized in cyberattacks. Independent variables include attack motive, which includes financial interest, data theft, and hacktivism, attack method, which includes malware, phishing, and unauthorized access, state sponsorship, and the attacking country. Bivariate analysis in the study is applied to identify relationships between attack motives, targeted organizations, and employed approaches. Key findings indicate that the key motivation is monetary, at 80.1% of attacks, and Russia being the most frequent origin of cyberattacks in the sample. State-sponsored attacks target critical care and high-value data institutions.

Class Concepts and Theoretical Framework

The study relates to several class concepts. Routine Activity Theory (RAT) explains how cyberattacks thrive due to motivated offenders, suitable targets, and a lack of capable guardianship. The study also connects to Cyber Hygiene and Risk Management, highlighting how poor cybersecurity practices leave healthcare organizations vulnerable. Additionally, Data Protection Regulations, such as HIPAA compliance gaps, contribute to security breaches. Lastly, Threat Intelligence and Incident Response are essential for understanding attack patterns and enhancing cybersecurity resilience.

Marginalized Groups and Ethical Considerations

Healthcare cyberattacks disproportionately target marginalized populations. Low-income patients are disproportionately impacted because they have no access to alternative care in the case of breakdowns in medical systems. The disabled and elderly are also disproportionately at risk because they rely on electronic health records and medical devices that are compromised during cyberattacks. Ethically, healthcare cyber victimization is of concern to patient privacy, data use, and access to necessary services. Improving security is crucial to safeguarding vulnerable populations.

Societal Contributions

The study has significant implications for society. It demands stricter cybersecurity in healthcare with an emphasis on policy suggestions. The study findings also assist healthcare organizations in developing stronger defense systems against cyber attacks and ultimately enhancing overall cybersecurity measures.

Conclusion

Praveen et al. (2024) perform a comprehensive analysis of cyber victimization in the healthcare sector and recognize key motivations and attack trends. Routine Activity Theory is appropriately applied and contributes to cybersecurity policy and practice. Greater focus should be given to preventive action in future studies and qualitative experience integration from targeted institutions. Healthcare institutions must develop robust cybersecurity for protection of not only institutional integrity but also vulnerable patient populations.

References

Praveen, et al. (2024). Cyber Victimization in the Healthcare Industry: Analyzing Offenders and Cybersecurity Measures. *International Journal of Cybersecurity Intelligence and Cybercrime*, 7(2), 4-27. Retrieved from https://vc.bridgew.edu/ijcic/