Breaking Down Cyber Victimization in the Healthcare Industry

Adrienne Peji

October 2, 2024

CYSE201S

Old Dominion University

Introduction

The constant growth of technology comes with risks. Even though the healthcare industry is a primary target for cyber offenders, healthcare is lagging considerably behind others when developing cyber defense practices and knowledge. Utilizing the Routine Activities Theory (RAT) and Cyber Routine Activities Theory (C-RAT), Praveen et al. analyzed cyber crime cases in healthcare and identified measures to prevent incidents.

Main Research Questions

This study aimed to "apply the core principles of Routine Activities Theory (RAT) and the Cyber-Routine Activities Theory (C-RAT) framework to identify, analyze, and offer preventive measures against the underlying motives and characteristics of cyberattacks targeting the healthcare sector" (Praveen et al., 2024). These theories also allowed the researchers to integrate the economic, psychological, and sociological factors that help study the offenders and victims. By doing this, they can develop action plans to further the healthcare industry's development in cybersecurity defense.

Methods and Data Analysis

This study collected data by utilizing the Hackmageddon website which serves as a collection of cyber incident data. The data on attacks is sorted by "type, target industry, motivation, and outcome" (Praveen et al., 2024). The researchers gathered cases dealing primarily with victimization cases in healthcare and used other credible sources to make up for missing information. Analysis included entering the sample into Excel and transferring it to a statistical software to identify vulnerable groups, methods of attack, and techniques. They also utilized descriptive statistics and Chi-square tests to determine statistically significant relationships and patterns between variables.

Relation to Class Material

This article reviewed attack types, general vulnerabilities, and utilized the Routine Activities Theory that we recently studied in CYSE201S. While reviewing types of attacks and general vulnerabilities, Praveen et al. established the relationship between attack patterns and their relevance in the healthcare industry. They used the RAT and C-RAT as their theoretical framework for the review and studied it in the context of healthcare. The motivated offenders were identified as those wanting to "exploit information or manipulate device functioning for financial, political, or recognition gains" (Praveen et al., 2024). The healthcare industry is a suitable target because of their digital information combined with inadequate defense measures. Healthcare facilities also lack protection from "capable guardians" such as law enforcement, regulatory bodies, and cybersecurity professionals (Praveen et al., 2024).

Relation to Experiences of Marginalized Groups

Marginalized groups such as those in lower-income areas can face higher risks of cyber victimization in healthcare because healthcare facilities in such areas may lack funding and resources for proper information technology security. These groups may also lack knowledge of such technologies and are unaware of the risks associated with the state of their healthcare facility's information technology security.

Contributions to Society

Through this review, Praveen et al. suggested policy implications that include having comprehensive Policy Frameworks with a clear definition of roles and responsibilities and aligns with established standards such as HIPAA, NIST, and HSCC. This Framework must evolve and adapt with risks. They identified qualities of motivated offenders and suitable targets and emphasized the presence of capable guardians to healthcare industries.

Conclusion

The use of the RAT and C-RAT frameworks helped study the motives underlying cyber incidents within healthcare industries as well as qualities making this industry a target to attackers. Such qualities include the valuation of healthcare data, use of technological medical devices, outdated security methods, and inadequate cybersecurity resources that require an open approach utilizing technology, risk assessment, collaboration, and continued education on the topic.

References

Praveen, Y., Kim, M., & Choi, K.-S. (2024). 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 &amp; Cybercrime*, *7*(2). https://doi.org/10.52306/2578-3289.1186