Ashari Key

October 6, 2024

The Review of Analyzing Offender Motivations in the Healthcare Industry

Article Review #1

Introduction

As technology continues to advance in the healthcare industry, the risk of vulnerabilities and cyberattacks also increases. The healthcare sector is vast, encompassing hospitals, health departments, aged care providers, diagnostic service providers, and healthcare practices. The objective of this research is to investigate the motivations behind cyber attackers and identify vulnerabilities within healthcare cybersecurity. The study addresses the following questions: What are the primary motivations driving Advanced Persistent Threats (APTs) to target the healthcare industry? What are the common characteristics and behaviors of APT groups that target healthcare institutions?

Theories

This study utilizes two theories to analyze real-life examples of cyber victimization in high-tech healthcare settings. The Routine Activities Theory (RAT) and the Cyber-Routine Activities Theory (Cyber-RAT) framework are used to identify, analyze, and propose preventive measures against cyberattacks targeting healthcare systems. The Routine Activities Theory (RAT) identifies three key elements that occur simultaneously with a crime: motivated offenders, suitable targets, and the absence of capable guardians. The principles of Routine Activities Theory emphasize situational context. On the other hand, Cyber-Routine Activities Theory (Cyber-RAT) focuses on digital guardianship and online activities that contribute to computer crime victimization.

Data Collection

The type of research method used was open-source data collection. The data was cited from credible sources, including Databreaches.net, CSIDB.org, and the Health Insurance Portability and Accountability Act (HIPAA) Journal. The independent variable in the analysis was to identify the attackers' motives and the techniques used to target healthcare organizations. Among the state-sponsored attacks, Financial Gain was the most common motive (78.2%), though Research and Intellectual Property/Patient Data Theft also had a notable presence (8.9%). Hacktivism or personal motivations, including enjoyment, accounted for only 1% of state-sponsored attacks (Praveen et al., 2024).

Course Studies

The principles of the Routine Activities Theory are related to the social sciences in the contexts of Relativism, Objectivity, and Determinism. The healthcare systems are constantly advancing with technology, which relates to Relativism. Objectivity is essential in the study of the theories when examining topics apropos to open-source data inquiry. Determinism refers to the behavior that is caused, determined, or influenced by preceding events, which correlates with the theories and motives that influence cyber-attacks. This article relates to the concepts used in the CYSE 201S Cybersecurity & Social Science course presentations, such as the Psychological Profile and Cyber Crime Psychology table listed in Module 4. It shows how researchers have categorized cyber offenders by their profiles, including biological factors, external environment, intelligence, personality, motivation, technical abilities, etc. The article also relates to concepts used in Module 2, such as constructing research questions, hypotheses, and variables.

Conclusion

In conclusion, the study contributes to research in understanding the framework of the Routine Activities Theory (RAT) and the Cyber-Routine Activities Theory (Cyber-RAT). The key motives prompting cyber-attacks on the healthcare system were recognized to be financial gain and hacktivism. Though challenging the safety of private records of all citizens and the healthcare operating system, the overall contributions of the studies to society have enlightened the public about the key patterns and trends in cyber threats and attacks. Being educated on the matter has ensured additional prevention methods such as automatic updates for the operating system, strict verification, and Data Loss Prevention (DLP) strategies are active and effective.

Reference

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 & Cybercrime, 7(2). https://doi.org/10.52306/2578-3289.1186