Cyber Victimization in

The Healthcare Industry

Amari Fisher

CYSE 201S

10/17/24

Introduction

Relation to Social Science Principles

This article relates to the social science principles because it discusses the impact of technology and explicitly malware in the healthcare industry, additionally, it showcases how criminals exploit certain vulnerabilities in healthcare. This study applies two theories, routine activities theory which is “Routine Activities Theory (RAT), introduced by Cohen and Felson in 1979, posits that crime will likely occur when three key elements—motivated offenders, suitable targets, and the absence of capable guardians”(Yashnam P, 2024) and C-Rat which is the same but applicable in the cyber field.

Research Questions and Hypotheses

This study’s primary objective is to determine the motivations of healthcare systems by cyber attackers and the characteristics that these systems have that may make them vulnerable to exploitation. The study believes that the two theories mentioned above contribute to the overall likelihood of an exploit being identified.

Research Methods

This study uses mostly qualitative data, analyzing past case studies and research information from reputable sources and journals, additionally, the article also uses some quantitative data for their tables such as Table 5, which showcases hospital/healthcare vulnerabilities and compares them to the amount of vulnerabilities in other institutions.

Types of Data

Data mainly consists of tables, showcasing how healthcare companies are susceptible to attacks, and of which attacks are primarily used to threaten healthcare companies. The analysis also involves RAT frameworks to help contribute toward identifying patterns and motives of these cybercriminals.

Relation to Powerpoints

This research paper relates to the powerpoints discussing the theories of economy because for these healthcare systems to have these major vulnerabilities, it is likely that the owners of these companies are putting their network security secondary to costs and efficiency.

Relation to challenges concerns of marginalized groups

Since marginalized groups typically rely heavily on these systems, this study shows that this directly affects these groups. These attacks can lead to massive loss of data, and since these attacks target systems used by marginalized groups. They are the ones most at risk due to these attacks, however, these attacks target healthcare in general which also includes all groups not just marginalized groups.

Overall contributions

Overall, this article showcases the need for better security in our healthcare systems to help protect both minorities and the majority. Healthcare providers should look toward implementing the provided protective measures to ensure important data does not fall into the wrong hands.

Conclusion

In conclusion, This research paper accurately shows how vulnerable healthcare systems are to common malware and viruses, through its use of qualitative source, and quantitative tables to help support this claim. Additionally, since these malware primarily target healthcare systems, marginalized groups may be disproportionately affected by these data leaks and attacks which could really only be caused by these healthcare providers choosing to cut costs on security to ensure efficiency or just to not lose any money(theory of economy powerpoint). This research paper also shows that we need to take steps toward better securing our health systems because they are major attraction points of cybercriminals because of that lack in security.

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