Article Review 2: "Cyber Victimization in the Healthcare Industry"

Elijah Bernal

Old Dominion University

CYSE-201S: Cybersecurity and the Social Sciences

Professor Yalpi

April 9, 2024

Article Link:

https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1186&context=ijcic

Introduction

In the article “Cyber Victimization in the Healthcare Industry” by Praveen et al. (2024), the authors speak about the problem of cyberattacks in healthcare. Healthcare organizations hold very sensitive customer data, so cyberattacks are a big problem. This specific paper uses two different theories to explain why cyberattacks target these organizations. The two theories are Routine Activity Theory and Cyber-Routine Activity Theory. Routine Activity Theory focuses on how everyday activities or patterns create opportunities for crime. Cyber-routine activity Theory is the same thing but translated to the digital world. This study can be connected to the social sciences because it looks at how human behavior and technology can shape society.

Questions and Hypothesis

The main questions for this study are why healthcare organizations are targeted and what is it that makes them particularly vulnerable. The authors hypothesize that healthcare organizations are particularly vulnerable because they still use outdated systems and hold mass amounts of sensitive customer data. These two things make healthcare organizations a big target for cyberattacks.

Research Methods

For the research methods, the authors likely analyzed case studies of past cyberattacks, specifically on healthcare organizations. They may have even interviewed healthcare

professionals. Asking healthcare professionals who have real-life experience would be very useful for this study. They also most likely used statistical tools so that they could find patterns within the data (ex. frequency of attacks). Using patterns they found within the data can help them pinpoint reasons as to why these healthcare organizations are particularly vulnerable.

Marginalized Groups

Cyberattacks on healthcare organizations are very harmful to marginalized groups. These are people who already have quite limited access to healthcare. When attacks like a data breach or ransomware attack happen, patients could be prevented from getting the care that they desperately need. Medical appointments can be canceled because of data breaches or ransomware attacks. This study emphasizes the need for stronger security measures in the healthcare field so that we can protect these individuals.

Conclusion

Overall, this study sheds light on the massive problem of cyberattacks in healthcare. By using RAT and the Cyber-RAT methods, the authors were able to provide a new way to look at this issue. Their findings could lead to better security measures in healthcare organizations, which will ultimately protect more people and their sensitive data.