Article Review 1:

Cyber Victimization in the Healthcare Industry

Tierra Fields

Department of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor. Diwakar Yalpi

Oct. 2nd 2024

Introduction

An insightful analysis of cyber risks faced by healthcare systems is provided by Praveen, Kim, and Choi (2024) in their article Cyber Victimization in the Healthcare Industry: Analyzing Offender Motivations and Target Characteristics through Routine Activities Theory (RAT) and Cyber-Routine Activities Theory (Cyber-RAT). RAT and Cyber-RAT are used by the authors to analyze why healthcare entities are frequently targeted by cybercriminals and how these risks can be mitigated. This article contributes to understanding cybersecurity threats in critical infrastructure sectors by focusing on offender motivations and healthcare vulnerabilities.

Social Sciences Relevance

There is a direct connection between this article and social sciences principles, particularly criminology and cybersecurity. In this study, the Routine Activities Theory (RAT) and its digital counterpart, Cyber-RAT, are applied to examine how certain circumstances and environmental factors contribute to cyber victimization in healthcare. Motivated offenders, suitable targets, and a lack of capable guardianship combine to create opportunities for cybercrime. This study illustrates the intersection of technology, human behavior, and societal impacts.

Research Questions and Hypotheses

The study asks: What motivates offenders to target the healthcare industry, and what vulnerabilities make these entities particularly vulnerable to cyberattacks? Based on the high value of healthcare data and the relatively low levels of digital guardianship, the study hypothesizes that healthcare entities are a prime target for cybercriminals. Cyberattacks on healthcare can lead to severe consequences, such as the compromise of sensitive patient data and disruption of critical medical services. This can

result in financial losses, damage to an organization's reputation, and even risks to patient safety if medical devices or systems are affected.

Research Methods

The research employs a qualitative research methodology, specifically focusing on case studies of healthcare cyberattacks. The case studies will provide insight into the motivations and tactics used by attackers. The research will also identify potential vulnerabilities in healthcare organizations and develop recommendations for mitigating them. By analyzing real-world incidents, the authors identify common factors contributing to successful cyberattacks. The research integrates RAT and Cyber-RAT theory to draw correlations between routine digital behaviors and victimization

Data and Analysis

This article thoroughly documents cyberattack cases reports healthcare breaches, and performs statistical analyses of cyber incidents. It identifies patterns in offender motivations and vulnerabilities in healthcare systems by analyzing these cases through the lens of RAT and Cyber-RAT. The article also discusses several technological advancements, including telemedicine and IoT devices, and explains how they exacerbate these vulnerabilities.

Relation to Course Concepts

The article directly relates to key concepts from the course's PowerPoint presentations, including digital guardianship and cybersecurity frameworks. These concepts are used to explain the importance of protective measures in mitigating cyber threats. The authors propose solutions to enhance healthcare security using specialized frameworks such as the Digital Capable Guardianship Framework and the Policy Framework.

Challenges for Marginalized Groups

Marginalized communities need more support in obtaining reliable healthcare services. Cyberattacks on healthcare systems can have a particularly severe impact on vulnerable populations, including individuals reliant on public health services or lacking access to private care. In areas with limited resources, such as low-income neighborhoods, cyber incidents can result in privacy breaches.

Contributions to Society

This study is a crucial contribution to society, emphasizing the critical and immediate need for enhanced cybersecurity measures in the healthcare industry. By shedding light on the tactics used by cybercriminals to exploit healthcare systems, the report not only provides valuable insights but also presents actionable recommendations to thwart future attacks. The study advocates for the implementation of robust prevention frameworks, aiming to create a more secure healthcare environment that effectively protects patient data and ensures seamless continuity of care.

Conclusion

Praveen, Kim, and Choi(2024) conducted a thorough analysis of cyber victimization in the healthcare industry, utilizing RAT and Cyber-RAT to uncover the motivations and vulnerabilities behind these attacks. Their work serves as a compelling call to action for the healthcare sector, emphasizing the urgent necessity for enhanced digital protection. This highlights the critical importance of implementing improved cybersecurity practices within the industry.

Reference

Bridgew,

vc.bridgew.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&amp=&httpsredir=1&amp=&article=1060&amp=&context=commstud_fac. Accessed 2 Oct. 2024.