Article Review #1: Cyber Victimization in the Healthcare Industry

Jake Modelewski

Old Dominion University

CYSE-201S Cybersecurity and the Social Sciences

February 16, 2025

Article Review #1: Cyber Victimization in the Healthcare Industry

In the cyber world there are thousands of cyber-attacks on institutions daily. The motives vary just as much as the targets. The article in review does a thorough investigation to understand the specific motivations behind cyber-attacks in the healthcare industry while holding strong relevance to material covered in CYSE-201S.

The questions are outlined as such “(1) What are the primary motivations driving Advanced Persistent Threats (APTs) to target the healthcare industry? (2) What are the common characteristics and behaviors of APT groups (whether state-sponsored or cybercriminal) that target healthcare institutions?” (Praveen, Kim, & Choi, 2024).

The researchers followed the Routine Activities Theory (RAT) framework. This framework functions under the belief that “crime will likely occur when three key elements—motivated offenders, suitable targets, and the absence of capable guardians—converge in time and space.” (Praveen, Kim, & Choi, 2024)

The researchers performed archival research for data victimization cases in the healthcare industry during 2018-2023 in several different databases such as Hacksawed, Databreaches.net, CSIDB.org, and the Health Insurance Portability and Accountability Act (HIPAA) Journal. They further categorized each incident in several categories. (See Table 1)

Using a univariate analysis, they were able to break down the percentages of incidents into several categories and subcategories. Conducting a bivariate analysis in attempt to create an association between the motives behind the attacks, whether they are state sponsored, and the method used. The attack seen the most by these institutions were ransomware and phishing. The largest target was high value data, motivated by financial gain and recognition. (See Table 1)

After associating all the relevant points of data, they established two points of the RAT framework. Motivated Offenders: The primary motives were deemed to be financial gain. Financial gain is a common motive for cyber-attacks in the healthcare industry “…as the lucrative nature of healthcare data such as electronic health records (EHRs) and intellectual property provides strong incentives for cybercriminals.” (Praveen, Kim, & Choi, 2024) Suitable Targets: Critical care and patient services were the prime target for cyberattacks. Absence of a Capable Guardian: This is not applicable in this study as the information was not readily available to the researchers.

While marginalized communities were not addressed, there is a connection to be made. Being that electronic health records (EHR) are the primary target from these attacks, this greatly increases the risk of disabled community. Everyone has health records, but a person that more frequently requires treatment will have more data, thus being more susceptible to attacks and more likely to have their records taken. The high velocity of cyber attacks on the healthcare industry indirectly poses a greater risk to the marginalized disabled community.

This study held great relevance towards the material covered in the CYSE-201S. The researchers conducted archival research to amass a large amount data. They used relativism and objectivism to draw connections behind the motivation of a cybercriminal. The contributions of this study could positively

impact the healthcare industry. With how it outlines the percentages, specifications, frequency, target, and motive of the attacks seen in the healthcare industry. The industry can use this develop stronger safeguards and protection policies not only for their data but for their patient’s wellbeing as well.

# 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 & Cybercrime*, 25. https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1186&context=ijcic

Tables

Table 1

|  |  |
| --- | --- |
| Code Type |  |
| Attack Code | N(%) |
| Account Hijacking | 69(6.1) |
| Account Takeover | 45(21.5) |
| Defacement | 6(.5) |
| Distributed Denial of Service | 5(.4) |
| Malware Infection | 55(4.8) |
| Phishing Attack | 211(18.5) |
| Ransomware | 456(40.1) |
| Unidentified | 45(4.0) |
| Vulnerability | 46(4.0) |
| Motive Code |  |
| Financial Gain | 693(60.9) |
| Hacktivism/Ideological Motivations | 8(.7) |
| Research and Intellectual Property/Patient Data Theft | 32(2.8) |
| Unidentified | 405(35.6) |
| State Sponsored? |  |
| No | 89(7.8) |
| Yes | 101(8.9) |
| Unknown | 948(83.3) |
| New\_State |  |
| Russia | 88(7.7) |
| Other | 11(1.0) |
| Unknown | 1,039(91.3) |