**Article Review 1: Contributing Factors of Healthcare Cyber Victimization**

Evan Jenkins

Old Dominion University

Professor Diwakar Yalpi

10/02/2024

**Contributing Factors of Healthcare Cyber Victimization**

**Background of the Study**

Like many industries, healthcare has seen sweeping changes due to the use of computer technology in modern society. One unfortunate change is that the healthcare sector has become a favored location for cybercriminals to find victims. “Cyberattacks on the U.S. healthcare system represent some of the most significant and consequential threats to the industry” (Praveen et al., 2024, p. 4). The research teams of Yashna Praveen, Dr. Mijin Kim, and Dr. Kyung-Shick Choi aim to apply the Routine Activities Theory to the healthcare industry to understand the phenomena of healthcare cyber victimization better.

**Relevant Social Science Principles**

The subject matter of the article can be related to several principles of social science. First, there is relativism, which is the understanding that separate systems rely on and impact other systems. In this case, changes in technology impacted how the healthcare industry operates, technology has also led to the creation of cybercrimes, and cybercrime is now impacting the healthcare industry, and the needs of the healthcare industry require new laws and technology to address is issues.

 The research team also employed the principle of parsimony, which means to keep explanations simple. For example, the article discussed cyberattacks in easily explained terms such as malware, phishing, or ransomware, but avoided deep dives into the technical aspects of how these attacks work.

 Empiricism is the principle that social scientists need to focus on what is real and not hunches. The research team first observed that the healthcare industry is a common target of cyberattacks. They then collected and analyzed data to reach conclusions based on factual evidence and not guesswork.

**Research Question and Hypothesis**

 The team questions the motives behind cybercriminals targeting healthcare facilities and what factors make the industry such an appealing target. If these factors and understood then they work towards better cybersecurity practices. Ultimately, they hypothesize that applying the Routing Activities Theory to the healthcare system will reveal relevant trends in the victimization of the industry through cybercrimes that can be used to “propose actionable plans to enhance the resilience of the healthcare system against the growing threat of cyberattacks” (Praveen et al., 2024, p. 5).

**Methodology**

 The bulk of the data was pulled from the Hackmageddon database, which catalogs cyberattacks “by type, target industry, motivation, and outcome” (Praveen et al., 2024, p.9). The team used this resource to collect a sample of 1138 unique attacks related to the healthcare industry. Additional data was collected from “Databreaches.net, CSIDB.org, and the Health Insurance Portability and Accountability Act (HIPAA) Journal” to better contextualize the socio-economic and regulatory landscape of the sample cyberattacks (Praveen et al., 2024, p. 10).

 The sample was then broken down into nine categories of the healthcare industry such as Medical technology, pharmacies, care facilities, government agencies, and administrative facilities. This was done to determine which specific parts of the industry were being targeted the most frequently and severely.

**Data Analysis and Findings**

A “coding instrument” was developed to analyze the sample pool by a multitude of factors including attacker motive, attack methodology, whether the attack was state-sponsored or not, and the origin country of the attack (Praveen et al, 2024, p. 10).

Overwhelmingly 76.1% of the attacks targeted hospitals. The second most were pharmacies at 7.5%, and the third most targeted sector was healthcare-related financial and administration operations with 5.0% (Praveen et al, 2024, p. 12-13). All other categories combined accounted for around 11%.

Then in terms of attack type, ransomware accounted for over 40% of attacks, account takeover/hijacking was just under 30%, and phishing attacks were another roughly 20% of data (Praveen et al, 2024, p. 13-14). Of attacks with known motives, 94.5% of the attacks were motivated by financial gain, but around 35% of the attacks had undetermined motives (Praveen et al, 2024, p. 14). It was also difficult to determine with certainty whether most attacks were state-sponsored or not. Of the known state-sponsored attacks, Russia was the biggest country of origin.

The data was also analyzed to highlight any statistical relationship between these factors. To facilitate this the nine categories of healthcare we simplified into four categories. The first category, High-Value Data, focused on the technology and research side of the industry. Then there was Critical Care and Patient services, think hospitals or care facilities where patients receive treatment. Third was Government and Regulatory bodies, covering agencies or the admin side of healthcare. The final category was Supply Chain, which consisted of third-party vendors.

The bivariate data analysis highlighted several key relationships. Malicious software, such as ransomware, was strongly tied to attacks on the critical care group. Attacks on the High-Value data took advantage of vulnerabilities. Financial motives were largely tied to each of the four combined groupings. Hacktivist motives, while rare, largely were behind attacks on the Government and Regulatory category (Praveen et al, 2024, p. 14). There was no strong relationship found between state-sponsored attacks and any particular area of the healthcare industry.

**Relation to Course Materials**

 The article can be connected to course material in several ways. First, the article serves as an example of social science in practice, which was the topic of Module 1. Module 1 also introduces various topics covered by social scientists including criminology and sociology, which are both relevant to the article. This module also introduced several common research methods including archival research, which I feel aligns with how the research team used databases to gather information on over one thousand healthcare-related cyberattacks over several years.

Module 2 largely discussed the major principles of social sciences, which were discussed in the context of the article previously. It also introduced the purposes of social research studies, such as empirically understanding social phenomena and recognizing ways to improve society. The research team set out to fulfill both of these purposes. Additionally, the module discussed the terms hypothesis, variables, and research questions.

 The third module of the course expands on how research works in social science when applied to cybersecurity methods. Module 3 also discusses the lack of diversity in the field of cybersecurity and cites the lack of female role models working in the industry as a possible cause. Interestingly, two of the three researchers of the article on cyberattacks in the healthcare industry were women.

**Contributions to Marginalized Groups**

When the healthcare industry is attacked it is those who are most dependent on the care provided that suffer. If services are disrupted by a cyberattack, even temporarily, then it could have grave outcomes for the elderly, disabled, and ill who need treatment to live healthy lives. The financial strain of cyberattacks, such as commonly occurring ransomware, could see doctor’s offices, pharmacies, and care centers being shut down, robbing communities of easy access to treatment. These people already have enough to worry about they don’t need to worry about if a cyberattack is going to impact their health. By understanding the issue of healthcare victimization through cyberattacks, we can more effectively combat the problem, thus reducing the harm to the highlighted marginalized groups.

**Contributions to Greater Society**

Even if it is just for something as simple as a physical, flu shot, or getting a few stitches, practically everyone will need healthcare at some point in their life. This means that practically everyone’s data is part of the system and could be at risk. A cyberattack on the healthcare system is an attack that can impact anyone and everyone.

The study provides a deeper understanding of the issue at hand. It revealed that the healthcare industry is seen as a lucrative target due to the large amount of stored patient data that can be stolen and sold. If a hospital falls victim to a ransomware attack and can’t access its necessary systems, then the hospital is rather forced to accept the cybercriminal’s demand, or lives could be lost. The article found what parts of the industry are most at risk, and why cybercriminals are attacking them, and what type of attacks they are launching.

The research team also found several flaws in the healthcare industry that make it an easy target. They conclude that “…the proliferation of IoT devices, outdated infrastructure, and insufficient resources dedicated to cybersecurity. Addressing these vulnerabilities requires a multifaceted approach that combines technological innovation, comprehensive risk assessments, and a commitment to ongoing education and international collaboration” (Praveen et al, 2024, p. 22).

**Conclusion**

The use of technology in healthcare has made it a target for cybercriminals. The research team applied the principles of social science to study this phenomenon. By analyzing hundreds of individual cyberattacks on the healthcare industry they were able to find several contributing factors showing the motives behind these attacks. Most attacks were launched against hospitals, used ransomware or malware, and were motivated by financial gain. From this, the team proposed several options, such as moving to newer and more secure technology and deploying dedicated cybersecurity teams in the industry, intending to secure the healthcare industry thus protecting marginalized communities and potentially improving society overall.

**Work Cited**

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