2024

How increased ransomware attacks have impacted hospitals in the United States

Mackenzie Dotson
dotsonmackenzie@gmail.com

HOW INCREASED RANSOMWARE ATTACKS HAVE IMPACTED HOSPITALS IN THE UNITED STATES

ABSTRACT

Introduction: The healthcare industry, particularly hospitals, have fallen prey to the alarming rise of ransomware attacks. In recent years, highly sophisticated cybergroups, armed with substantial funds and advanced technology, have intensified their focus on hospitals. Despite the advice against it, most hospitals have paid the ransom in order to regain access to their electronic systems and patient data, underlining the severity of these attacks.

Purpose of the Study: The purpose of this research was to evaluate the effects of ransomware attacks on hospitals in the US to determine if the patients were at risk due to hackers withholding patient information and causing equipment malfunctions, the associated operational and ransom costs, and the disruption of hospital business operations.

Methodology: This study utilized a literature review complemented by a semi-structured interview with a cybersecurity professor. Three electronic databases, Google Scholar, and other private and government websites were searched for this research, and 32 sources were referenced. Of these, 14 sources were used in the results section.

Results: The research showed that costs such as ransom payments, operations, revenue loss, remediation fees, and legal fines have increased over the last few years. As cybergroups become more sophisticated, the more costly ransomware attacks have become on hospitals in the US. The interconnectedness of hospital electronic systems and technology (i.e., imaging services, ventilators, infusion pumps, etc.) increased patient risk during ransomware attacks. Longer lengths of stay were reported during a ransomware attack. Hospital business operations were shown to be severely disrupted when ransomware attacks occurred. Canceled

appointments/surgeries and ambulance diversions decreased patient volume during the first week of an attack.

Discussion/Conclusion: Ransomware attacks on hospitals in the US significantly impacted costs and business operations. The findings were inconclusive on whether patient risk increased due to ransomware attacks. Some publications showed an increase, while others did not. Further study was needed on all three outcomes due to recent ransomware attacks that have become more frequent and sophisticated.

Keywords: business operation disruptions, cost, hospitals, patient risk, ransomware, United States

INTRODUCTION

The Health Sector Cybersecurity Coordination Center (HC3), as of mid-March 2024, had tracked 730 cyber attacks against the healthcare industry worldwide; 530 attacks were against the US healthcare industry (AHA, 2024). It was estimated that almost half of the cyber attacks against the US were ransomware-related (AHA, 2024). Ransomware has been defined as malware designed to deny access to a user's data until the user pays a ransom to the hacker (HHS, 2021). Hackers have encrypted data with a key, and once an organization has paid the ransom, the decryption key would be sent back; however, sometimes, this was not the case (HHS, 2021). The healthcare industry has become the ideal target for ransomware attacks for these reasons: (1) healthcare is critical for life and death, so most hospitals have paid the ransom; (2) healthcare staff have been busy taking care of patients that they have become susceptible to unknowingly giving access to cybercriminals and (3) the interconnected systems and devices in or used by healthcare have made it easy for threat actors to attack (Neprash et al., 2023).

Hospitals have been behind when it comes to data protection because of the HIPAA penalties. Hospitals may face other collateral damage to their reputation, and cybersecurity was not a high priority for many hospitals (van Boven et al., 2024). Hospitals have been targeted by full-time professional cybergroups that have the technology, funds, and training and have been generally supported by foreign governments (Riggi, 2020). The evolution of cyber attacks, like ransomware, has been financially motivated, but some have been representative of threat-to-life crimes that would endanger public health (Riggi, 2020). Cybercriminals have changed their tactics, which made them more catastrophic and effective; they have pressured victims into paying the ransom, or they would release the data they stole (CISA, 2023).

When a ransomware attack has occured, hospitals have had a few options to regain access to data: 1) attempt to restore data from backups; 2) lose the data; 3) pay the ransom (Singh & Sittig, 2016). The Federal Bureau of Investigation (FBI) has strongly advised against paying the ransom, as it fails to guarantee the return of data and perpetuates the cycle of attacks (FBI, 2016; Ghayoomi et al., 2021). Despite this, one in three healthcare hospitals and organizations, nearly 34%, have chosen to pay the ransom (Duguin, 2023; Weiner, 2021). Many hospitals believed it was a quick solution to retrieve their data, but 80% of small/medium-sized hospitals that paid the ransom did not receive the decryption key; a second ransom was then demanded (Ghayoomi et al., 2021). The increases in ransomware attacks have threatened the healthcare industry, particularly hospitals (Nifakos et al., 2021). The increasing cyber threats to the healthcare industry due to ransomware have consisted of infrastructure attacks, monetary theft, attacks on medical devices, and data loss (Sullivan et al., 2023).

Ransomware attacks on the healthcare industry have been not just a nuisance but a significant threat, causing severe operational, financial, and legal consequences (Youmans, 2024). Ransomware has impacted hospitals by delaying treatment, decreased revenues and a 24% increase in mortality rates (Hartman, 2023). Ransomware attacks have caused hospitals to treat fewer patients. During the first week of most ransomware attacks, revenue decreased by around 40%, and patient volume dropped by 20% (Neprash et al., 2023). Since 2016, 539 ransomware attacks on healthcare organizations in the US have affected 52 million patient records and 9,780 facilities (Diaz, 2023). A report from October 2023 showed that ransomware attacks on healthcare, mostly hospitals, have cost the US economy roughly $77.5 billion in downtime (Diaz, 2023).

The purpose of this research was to evaluate the effects of ransomware attacks on hospitals in the US to determine if the patients were at risk due to hackers withholding patient information and causing equipment malfunctions, the associated operational and ransom costs, and the disruption of hospital business operations.

METHODOLOGY

The hypothesis was that increased ransomware attacks on hospitals in the US have caused increased costs (operational and ransom), increased patient risk due to patient information being withheld and equipment shutdowns, and increased disruptions to business operations, resulting in ambulance diversions and the cancellation of appointments and procedures.

The methodology for this qualitative study was a literature review with a semi-structured interview with a cybersecurity professor. The interview was conducted on Microsoft Teams, and only relevant answers were used to support the information found in the literature

review. The interview was recorded and transcribed. The Marshall University Institutional Review Board have approved this study.

Peer-reviewed literature and research articles were located using Marshall University's EBSCOhost, PubMed, and ProQuest research databases. When information could not be located within these three databases, Google Scholar was used. The Google search engine was also utilized to research private and government websites. When conducting the research, keywords included were: 'ransomware' or 'cyberattack' and 'hospitals' and 'cost' or 'ransom' and 'patient risk' or 'mortality' and 'operational disruptions' and 'United States' or 'US'. These keywords were the criteria for inclusion in the study.

The conceptual framework for the research was adapted from the research framework created by Duh (2015)(Figure 1). The framework explained how increased ransomware attacks in hospitals in the US have increased hospital costs due to ransom, legal, remediation, and other costs, the risk to patients due to hackers holding information hostage and equipment malfunctions, and the disruption to business operations.

Using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) method, the search identified 44 relevant citations, and articles were excluded (N=33) if they did not meet inclusion principles. Articles were included (N=14) if they described the impacts of ransomware attacks on hospitals in the US. Articles from other sources (N=21) were also included in this search. These 32 references were subject to full-text review and were included in the data abstraction and analysis. The final number of references was low due to a lack of valid sources discussing patient risk when ransomware attacks occur (PRISMA, n.d.)(Figure 2).

The search was restricted to the English language, and publications from 2015 through 2024 were used. Following the review of relevant abstracts, appropriate articles were used to report information and results. MD completed this literature search. AC validated it, acting as the second reviewer and determining whether the references met the inclusion criteria.

RESULTS

Cost of Ransomware Attacks

Some notable ransomware attacks that have been costly to hospitals and other health organizations have been included. In 2020, the University of Vermont Medical Center experienced a ransomware attack that cost the hospital over $82 million (Chiaradonna et al., 2023). $63 million of the total cost was just from recovery costs; the rest was increased expenses and lost revenue (Chiaradonna et al., 2023). Scripps Health in San Diego, California, experienced a ransomware attack in May 2021 that cost the system $112.7 million in lost revenue and other expenses (Paavola, 2021). In addition to the lost revenue and other expenses, Scripps Health faced multiple lawsuits, which resulted in Scripps paying $3.5 million (McLaughlin, 2023). In October 2022, CommonSpirit Health experienced a ransomware attack that, as of May 2023, had cost the system around $160 million in costs from operational disruptions, remediation fees, legal fees, etc. (Hut, 2023).

As of April 2024, the Change Healthcare ransomware attack in February 2024 has been reported to have had an estimated $870 million impact on UnitedHealth Group (UHG); revenue loss was $280 million, and roughly $595 million in losses were due to clearinghouse restoration costs and medical expenses from suspended care management activities (Hut, 2024). UHG has projected that $1 billion in direct costs would be incurred by the end of the year and revenue loss between $350 million and $450 million (Hut, 2024).

Patient Risks

Ransomware attacks have increased patient risk because hackers have deleted patient information, leading to misdiagnoses and inappropriate treatment (Okafor et al., 2023). Other patient risks due to ransomware attacks have included identity theft and the fraudulent use of private health data (Okafor et al., 2023). The value of patient data, the increased digitization, and the interconnectedness of hospital electronic systems have made hospitals prime targets for ransomware attacks (Okafor et al., 2023).

Threat actors who have caused ransomware attacks have caused electronic system shutdowns and corrupt health data (Siriwardana, 2024). This has caused severe consequences in many hospitals because hospitals have life-supporting systems like ventilators, defibrillators, MRIs, CT scanners, x-rays, dialysis equipment, infusion pumps, and many other types of equipment (Siriwardana, 2024). In a 2022 survey, US healthcare experts stated that 53% of organizations suffered an increase in mortality rates due to ransomware, and 37% reported poor outcomes due to delays in tests and procedures (Petrosyan, 2023a) (Figure 3). In that same survey, 56% of organizations reported longer lengths of stay due to ransomware attacks and a 28% increase in complications from procedures during ransomware attacks (Petrosyan, 2023a).

Operational Disruptions

Unlike other cybersecurity threats, ransomware was designed to interrupt healthcare business operations, which has been why most organizations want to pay the ransom (Neprash et al., 2022). Between 2016 and 2021, out of 374 ransomware attacks studied, 44.4% of attacks caused disruptions in care delivery, and hospitals were most likely to experience operational disruptions (Neprash et al., 2022). Diverted ambulances from emergency rooms, surgeries and appointments canceled, and electronic health records locked out, so staff had to use paper records

instead have been just a few examples of how ransomware has disrupted a hospital's delivery of care (Neprash et al., 2022). There was an estimated 47% increase in patients being diverted or transferred to other facilities in 2022 (Petrosyan, 2023a)(Figure 3).

Ransomware attacks on US healthcare organizations resulted in an average downtime of 18.71 days for 2023, a slight increase from 2022, when the average downtime was 15.71 days (Petrosyan, 2023b)(Figure 4). In a study by Neprash et al., the authors observed a decline in inpatient admissions during the first week of a ransomware attack; urban hospitals fell by 16.9% and 14.7% for rural hospitals (2024). Emergency room visit volumes fell by 19.3% for urban hospitals and 10.0% for rural hospitals (Neprash et al., 2024). According to Neprash et al., three out of four ransomware attacks caused hospital operational disruption (2024). In the study, Neprash et al. noted that operational disruptions like ambulance diversions, appointment/surgery cancellations, and electronic system downtimes were prominent. However, they returned to normal pre-attack levels within a few weeks (2024).

It has not just been the hospitals that have been attacked that have been impacted by ransomware attacks. Research has shown that hospitals near ones that have been attacked experience operation disruptions as well. In May 2021, the University of California San Diego Health Center reported a significant influx of patients, which caused the hospital to bring in backup staff because Scripps Health was experiencing a ransomware attack and was not able to treat patients (McLaughlin, 2023). In a study conducted by Dameff et al., the researchers found an association between targeted hospitals experiencing a ransomware attack and nontargeted hospitals experiencing operational disruptions due to a large influx of patients (2023).

Recent examples of hospital operational disruptions due to ransomware attacks have been included. The ransomware attack on the University of Vermont Medical Center in 2020 caused

the hospital to shut down EHR systems, patient information was inaccessible, scheduling systems were down, appointments and procedures were canceled, COVID-19 tests were not able to be processed, and imaging services were also unavailable (Chiaradonna et al., 2023). The 2022 attack against CommonSpirit Health resulted in canceled surgeries, ambulance diversions, and equipment shutdowns at multiple hospitals in the system (Neprash, 2024). In February 2023, Tallahassee Memorial HealthCare experienced a ransomware attack that caused the system to cancel non-emergency outpatient and surgical procedures, switch to paper documentation, and divert emergency patients to other local hospitals (Blum, 2023). In August 2023, Los Angeles-based Prospect Medical Holdings, which has 11 hospitals in its system, experienced a ransomware attack that required ambulance diversions, canceled select surgeries, made imaging services unavailable, and made a handful of other procedures and therapies unavailable as well (Hut, 2023).

DISCUSSION

The purpose of this research was to evaluate the effects of ransomware attacks on hospitals in the US to determine if the patients were at risk due to hackers withholding patient information and causing equipment malfunctions, the associated operational and ransom costs, and the disruption of hospital business operations. The research evaluated in the study showed, with limited references, that costs and business operation disruptions increased with increased ransomware attacks. Patient risk increased with increased ransomware attacks in some studies but not in others.

Cost of Ransomware Attacks

In reviewing the impact of cost due to ransomware attacks, research proved that the recent increases in ransomware attacks have increased costs to hospitals targeted. Ransomware

attacks have become more sophisticated, and cybercriminals have started targeting well-resourced hospitals and health systems; the recent attack on Change Healthcare proved this (Neprash, 2024). The 2024 Change Healthcare attack resulted in an estimated $595 million in remediation, operational, legal, and other costs and $280 million in lost revenue (Hut, 2024). The ransomware attack had a roughly $870 million impact on Change Healthcare, and this number was expected to increase by the end of the year.

Cybercriminals involved in recent ransomware attacks have done their research and know how to attack the healthcare systems they did because they know it provides them the most financial gain. According to Chiaradonna et al., hospitals have expected to experience financial losses from a ransomware attack in millions of US dollars; these losses include loss of revenue, ransom payments, business interruptions, and legal fines (2023). The initial ransom, which millions of US dollars have been demanded, has been just the first financial effect most hospitals have faced; extended downtime has caused severe financial losses (Dameff et al., 2023).

Patient Risks

In reviewing the impact ransomware attacks have on patient risk, there was a slight increase in risk to patients. In 2022, 37% of hospitals reported poor outcomes due to delays in procedures and tests from ransomware attacks (Petrosyan, 2023a). There was a 28% increase in complications from procedures. However, hospitals reported a 53% increase in mortality rates, and 56% reported longer length of stays (Petrosyan, 2023a). While this study showed an increase in mortality rates, other sources reported no significant changes in mortality rates.

However, most studies concluded that the increased digitization of documentation and other medical services has caused a greater risk to patients. In multiple attacks, patient information was withheld in order to get the hospital to pay the ransom. This caused hospitals to

switch to paper records, and vital patient information was missing, which led to misdiagnoses and inappropriate treatments and medications given to patients (Okafor et al., 2023).

All studies stated that the interconnectedness of hospital electronic systems resulted in a greater risk to patients. Medical devices and other equipment in hospitals have been connected to the same electronic systems (Chiaradonna et al., 2023). Equipment like imaging technology, ventilators, defibrillators, infusion pumps, and dialysis equipment have been connected to the same systems. When a ransomware attack occurred, all these systems were reported to shut down (Siriwardana, 2024). When all these systems were down, patients were not able to be treated, which increased the risk to patients as they did not receive timely and appropriate care.

Operational Disruptions

A substantial number of publications corroborated that ransomware attacks caused significant business operational disruptions in hospitals in the US. A study conducted by Neprash et al. showed that out of the 374 ransomware attacks between the years 2016 and 2021, 44.4% of attacks caused disruptions in business operations and patient care delivery (2022). Multiple studies showed that patient volume fell during the first week of a ransomware attack. In most cases, ambulance diversions and canceled appointments and procedures resulted in a decreased volume of patients at ransomware-attacked hospitals (Neprash et al., 2024).

Most publications determined that most business operations were disrupted because hospitals had to shut down most, if not all, systems and operations to preserve the unaffected systems and data. The average downtime in hospital systems was 18.71 days in 2023 (Petrosyan, 2023b). Some publications showed that when the targeted hospital was attacked, hospitals in the surrounding area experienced an influx of patients. One hospital had difficulty treating patients due to the influx of patients from the ransomware attack that happened down the road.

Semi-Structured Intevriew

The semi-structured interview with a cybersecurity professor supported some of the review's findings, including the increased costs and disruptions to business operations. The characteristics of how ransomware has been used and who it has affected have evolved over the years. The business model changed in the last five to ten years, and ransomware groups have been going after more prominent companies. This was because ransomware groups would get more money from the larger hospitals because patient data was critical, and the hospitals have paid the ransom. Money has been the driving factor for ransomware attacks. Ransomware groups figured out quickly that the more business operations were disrupted, the more likely the hospital would pay the ransom.

Study Limitations

The quantity of information available about ransomware attacks in the US limited the research. The primary limitation to generalizing those results was that only three databases were used to collect resources; therefore, publication bias could have been introduced. Secondly, the researcher experienced time constraints due to other obligations, which might have limited the time available to explore the research.

Practical Implications

The study's implications show that additional research is needed on how ransomware attacks can cause patient risk. This review showed that ransomware attacks impact hospital costs and cause business operation disruptions. This information can be used to expand on the impacts of ransomware attacks as they continue to evolve and become more sophisticated.

CONCLUSION

Ransomware attacks have significantly impacted costs and disrupted business operations in hospitals in the US. This review's findings proved that patients were at risk, but the amount of risk was inconclusive. Due to the increased sophistication and number of ransomware attacks on hospitals in the US, further study was needed to evaluate patient risk, costs, and business operation disruptions.