Impact of Ransomware on the Healthcare Industry with Policy and Education Considerations

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Connie Zhang
Spring 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor
Richard D. Jacques, Department of Engineering and Society

Introduction

The healthcare sector was the most targeted industry by ransomware attacks, resulting in a 71% increase in attacks from September to October of 2020 (The Check Point Blog, 2020). The healthcare industry serves as a backbone to society, ensuring citizens' well-being and safe treatment. An attack on such a critical system would cause not only a financial burden but disrupt the entire functionality of a system. Anything connected through a network would be impacted, such as scheduling systems, surgery equipment, life-saving medical devices, and communication networks, making it impossible for a modern-day hospital or medical center to remain active. In 2021, the average cost of the direct impact from a ransomware attack was $1.85 billion, doubling the figure from the previous year (Beaman et al., 2021). The result of a successful attack could make necessary devices unavailable, leak patient data, and drain resources, causing life-threatening circumstances and need to be addressed. An attack on a hospital system is an attack on key cybersecurity pillars as they prevent the confidentiality of patient data, availability of medical devices and services, and integrity of treatment from doctors.

In this paper, my approach to this issue will draw attention to the disparity of cybersecurity knowledge needed to prevent attacks and emphasize the need for enforcing security policies. I will also examine the reliance and interconnected relationships between patients, doctors, and data passed between medical devices to prove the profound impact an attack could incur. The current standings of security knowledge and implemented policies reveal a need for improvement and education through the partnership of healthcare workers and security professionals. Additionally, it is imperative that the healthcare and security industry understand the impact of such an event and take measures to ensure recovery.

The impact of a ransomware attack will first be examined focusing on the medical devices, patients, doctors, and the overall long-term financial burden it will impose on a modern-day hospital system. Next, current policies will be reviewed to emphasize the importance of having strong guidelines to protect valuable healthcare-related assets in a security sense. Finally, the lack of proper education of healthcare workers in security training has proven to be a leading cause of initial access by attackers, emphasizing the need for new developments in training. Through recognizing these shortcomings and implementing changes, the healthcare industry will become more resilient and prepared to face impending cyber-attacks.

Literature Review

My research will focus on the impact of a ransomware attack on the healthcare industry and highlighting policies and education strategies to mitigate attacks. To understand the scope and context of an attack, it is important to know how a typical ransomware attack is conducted and recognize the severity of an attack on a critical sector such as healthcare. In addition, a review of prior research on similar topics related to the significance of a ransomware attack on a healthcare system and suggested educational practices to improve security awareness will be conducted.

First, it is important to acknowledge what a ransomware attack is and how one occurs. A previous study established ransomware to be "the class of malware that attempts to defraud users by restricting access to the user's computer or data, typically by locking the computer or encrypting data" (Simoiu et al., 2019). Another study groups Ransomware attacks into three common methods: scareware, locker, and crypto (Beaman et al., 2021). Scareware uses interactive interfaces such as pop-up ads and emails to lure an unsuspecting user to gain access, such as through phishing attacks. Locker ransomware works by encrypting files, locking

computer functionality, and blocking access from the user. Finally, and arguably the hardest to recover files though is cryptomalware. Cryptomalware encrypts data mostly using asymmetric encryption, which makes it especially hard for a victim to decrypt without special access to the attacker's key. Ransomware attacks typically begin by finding areas of vulnerabilities within a system where attackers can hold locked files or limit functionality on a system in order to bargain for payment. This particular type of attack is harmful as it leaves many victims without an option but to pay the ransom and hope for their systems to be up and running. My research expands on this type of attack as it focuses on how these methods disrupt everyday functionality from a healthcare perspective and draws attention to what devices and systems are most at risk.

The article "Ransomware: The Virus Attacking the Healthcare Industry" by Slayton, covers the history and basics of ransomware attacks, detailing the most prominent variants such as Crypto-ransomware and Locker- ransomware. Slayton also discusses the current state of ransomware attacks today and how it could impact patients through identity theft and medical risks. Finally, the article specifically highlights the Health Insurance Portability and Accountability Act (HIPAA) and its coverage on ransomware attacks, as well as suggesting adjusting the baseline of federal cybersecurity standards. This article greatly shaped the structure of my argument, as it covers many facets of impact from a healthcare perspective that supports my argument. In addition, it informed me of the current policies in place that combat ransomware attacks as it relates to patient privacy and safety, including technical and non-technical improvements. Although Slayton touches on the need to include proper training, the parameters of this suggestion are not defined (Slayton, 2018). My research will fill this gap and suggest specific educational training methods as well as topics to include updated policies as a remediation strategy.

The study “Measuring the Application of Knowledge Gained from the Gamification of Cybersecurity Training in Healthcare” conducted by DeCarlo, is a quantitative study that focuses on evaluating a gamification style training program that is tailored to security awareness in the healthcare industry. The study acknowledges the shortcomings of human error as a fault to secure measures and proposes different training methods as a response to mitigate them in the future. However, DeCarlo does not mention the specific impacts of an attack or policies that may connect to training content for healthcare professionals. DeCarlo’s research solely focuses on improving security knowledge for employees and evaluates methods in training (DeCarlo, 2020). My research will expand on this article as it will bring this unique training method into context by specifying the content needed to support and mitigate vulnerabilities in healthcare.

Current research lacks an understanding of the magnitude of a ransomware attack on a healthcare system in the short term and long term. Additionally, my research will fill in the gaps by including additional policies and education practices that will further educate those in the healthcare industry on strategies to respond to attacks.

Methodology

My analysis of this topic draws on the Actor Network Theory (ANT), which allows me to understand the dependent relationship between hospitals and their internet -connected devices and resources, as well as how threat actors will take advantage of this relationship in a new light. ANT is a theoretical approach to understanding the complex relationships and shifts between stakeholders in one environment. This approach allows me to dissect a ransomware attack in terms of the threat actors and the effects an attack could incur on the entire healthcare ecosystem, rather than focusing on just one actor. This framework provides a profound viewpoint as I can

recognize changes in the flow of the healthcare system before and after an attack has occurred in human and non-human factors.

A literature review will support my argument to understand the severity of the disruption an attack could incur and support the need for healthcare professionals to receive education on security practices and how to maintain and recover a secure environment. Additionally, healthcare policies will be reviewed to understand the need to include the protection of patient health and privacy data in relation to securing databases properly. These reviews will be integrated with the ANT to demonstrate the trickling impact of an attack toward any actor within the system.

To consider the magnitude of an attack, a literature review based on previous ransomware attacks and simulations specifically in the healthcare industry will be conducted. Additionally, research on current security posture in hospitals and future improvements in terms of security and education policies will be analyzed to support a solution for recovery. The literature reviewed will consist of a majority of secondary sources that cover the previously conducted attacks. It will cover three main facets of impact measured, including: resource damage, privacy leaks of patients and disruption to staff, and overall financial impact. The impact I have defined and am seeking covers all actors involved in a ransomware attack to assess the full range of damage. Gathering this data will allow me to identify key areas to focus on protecting to construct long-term and short-term goals. Another aspect of having a secure network includes educating the people who run it. Further review will include education strategies and the effectiveness of training healthcare professionals. The collection of previous research and examples of ransomware attacks on hospitals will sufficiently convey the impact of these harmful attacks and promote change in order to best prevent them.

Next, a policy review will be conducted to analyze current policies that are in place related to the protection of data and devices in the healthcare sector. Specifically, policies that relate to patient privacy and how to protect their data will be reviewed to explain the need to expand policies to cover digital protection and updated services. The healthcare sector emphasizes the need to ensure patient privacy and safety, making policies that regulate them a necessity. Another aspect that will be examined includes policies related to managing the security of medical networks and devices. Many institutions require and follow baseline procedures for maintaining proper security posture within an organization. Finally, policies on ensuring retention and resiliency will also be covered to assess the need for data backups and incident response. These will be reviewed for their coverage and effectiveness in-relation to protecting the healthcare industry. A culmination of these reviews will support my argument that the healthcare industry serves as a vulnerable industry that needs up-to-date policies to aid their security posture and preparedness.

Analysis

Ransomware attacks have grown more common, especially as the reliance on technology to function has increased in daily life. As hospitals grow to depend on interconnected devices to function, threat actor groups become more likely to see hospitals as a target for successful attacks. Looking at ransomware attacks through an ANT lens emphasizes the constant shifts between actors as the results of action of one actor greatly impacts the others. A ransomware attack on the healthcare sector will cause significant damage to the electronic devices used, patients and medical staff, and create a long-lasting financial burden for medical institutions.

Disruption of Medical Devices and Services

An estimated 4.5 billion medical devices rely on the Internet, which accounts for $6 billion annually, making the healthcare industry an extremely vulnerable and lucrative market to attack (Ghayoomi et al., 2021). Medical devices are at the center of a functioning modern-day medical center. Medical services have also become increasingly reliant on the internet and network -connected systems. In 2009, The American Recovery and Reinvestment Act, passed by the Obama administration, which included $19.2 billion for the implementation of electronic medical records (also called electronic health records or EHR) to be completed by January 1, 2014 (Miller, 2022). The shift to a fully electronic health recording system increases efficiency in the workplace but introduces a multitude of vulnerabilities from a cybersecurity perspective. Sensitive patient data have now migrated to a space where attackers can penetrate. Following the COVID-19 Pandemic, telehealth services became increasingly popular and available to patients. However, this shift to virtual appointments also introduces circumstances where endpoint devices from employees can be tampered with. Many medical devices rely on the interchange of data to monitor patients, diagnose illnesses, and maintain functionality. If one of these devices was infiltrated, a patient could be mis-diagnosed, or even cause life-saving devices such as implantable cardioverter defibrillators (ICDs), to malfunction. A disruption in the delivery of this sensitive data could impact the entire operation of a hospital system. Threat actors have begun taking advantage of this reliance, seeing it as an opening to create leverage in their transactions. With medical devices compromised, many hospitals are left no choice but to pay ransom in exchange for functionality, shifting the relationships between hospitals, their devices, and attackers.

Safety and Privacy Concerns for Patients and Staff

Hospital staff and patients serve as the main victims of ransomware attacks. Compromised systems can cause major delays and communication issues between doctors, nurses, and patients. Patient care is perhaps the most fatal of impacts from a ransomware attack, with 25% of healthcare providers reporting an increase in the mortality rate (Gliadkovskaya, 2021). Such attacks could cause delayed chemotherapy treatments, ambulances being diverted from affected emergency rooms, and even interruptions in life-saving equipment (Miller, 2022). Perhaps one of the most notable attacks occurred in 2017 known as “WannaCry". This attack spread to five UK hospital emergency departments and 81 National Health System Hospitals, resulting in more than 19,000 appointment cancellations (Riggi, 2022). This level of damage is likely to be unrecoverable in a timely manner for many hospitals, leaving doctors unable to help and patients in untreatable conditions. Doctors also rely on the accuracy and timely delivery of data from medical devices to make life-changing decisions. In April 2020, ransomware attacks caused the first fatal outcome for Teiranni Kidd, who was a victim of the impacts of a ransomware attack at Springhill Hospitals. This hospital suffered an attack causing critical medical equipment that monitored Kidd and her baby to malfunction. Devices that were typically relied on to monitor fetal heartbeat and visual monitoring were down, ultimately causing the death of Kidd’s child (Wenk & Cuoto, 2022). Without being able to assess the validity of these results, doctors are unable to continue with treatment, causing major delays in their schedules and fatal outcomes.

In addition to not being able to access data, another concern is exfiltrated patient data that is posted and sold for profit on the dark web. Threat actors typically turn to this method when hospitals refuse to pay, in an attempt to cause further damage until they receive what they want.

The Leon Medical Center hospital chain faced this issue in January of 2021, as unauthorized criminals accessed personal records that revealed medical record numbers, prescription information, and medical history that were linked to names, addresses, and emails. It was later found that this sensitive data was leaked to 500 patients at the Leon Medical Center (Collier, 2021). The Leon Medical Center is not alone in this leak. Threat actors use this method in an attempt to further their damage and increase their payment. With their data revealed, the possibility of identity theft and false insurance and benefits claims are significantly increased. The use of this tactic violates the integrity and safety of patients and allows unauthorized personnel access and abuse of personal health data.

Financial Burden

From a threat actor's perspective, the financial gain is typically the main motive for conducting an attack. This makes the healthcare industry an especially critical target as it is a necessary part of society, meaning most hospitals would pay a ransom to regain functionality and mitigate disruption. However, paying this ransom is not without a significant financial impact on hospitals. For example, Universal Health Services experienced a ransomware attack in 2020, which cost the chain $67 million after it had to divert ambulance traffic and schedule patient procedures at competing facilities due to the incident (Mensik, 2022). The cyberattack of the Vermont hospital system cost about $54 million, including rebuilding the computer network and lost revenue (Bergal, 2022). Finally, the WannaCry attack racked up a total of $125 million in just 14 days due to a ransomware attack. These are just a few of the hospital systems attacked within the last few years that are experiencing the damaging long-term financial impact of threat actors, in addition to technical and treatment disruptions.

Furthermore, the result of following the attackers' request and paying the ransom was also assessed. Although paying the ransom would seem to yield a positive short -term effect, it was found that it may actually produce more harmful long-term effects toward patients (Ghayoomi et al., 2021). The short-term benefits are also largely dependent on the cooperation with the threat actor groups and if they are willing to decrypt files or if the cycle of this attack repeats itself. In the long term, it is more effective to recover a fully functioning environment with data and equipment backups to return to patient care as the priority. The severity of this type of attack requires a push for a change in policy and education to further improvements in mitigating the likelihood and long -term impact.

Policies to Implement Preventative Measures

Ransomware poses a direct threat to patient privacy as it leaks personal health information (PHI). This occurs when threat actors exfiltrate data from their attack and post it to the dark web or other illegal websites to gain attention from the victim. This leak is a direct threat to The Health Insurance Portability and Accountability Act (HIPAA), which protects patient privacy related to the data released to the public. To combat this threat, HIPAA has recently updated security rules that mandate healthcare providers to conduct regular risk assessments to minimize their vulnerabilities as well as protocols in place to detect and prevent malicious software from infecting their computer systems. HIPAA considers four factors to evaluate the magnitude of a breach: the nature and extent of the PHI , including the types of identifiers and the likelihood of re-identification, the unauthorized person who accessed or used the PHI, or to whom the disclosure was made, whether the PHI was actually acquired or viewed, the extent to which the risk to the PHI has been mitigated (Trend Micro, 2016). The policy also

requires healthcare professionals to receive additional training to identify any malicious actions through phishing scams (DeMuro & Norwood, 2021). Following these policies helps ensure and protect the integrity of patients' data and maintain the functionality of critical devices.

Implementing strong policies to mitigate these risks is critical to decreasing the impact of ransomware attacks. The National Institute of Standards and Technology (NIST) provides a secure baseline to functioning technology and the environment that surrounds it. This framework is a set of privacy and cybersecurity policies used to aid critical infrastructure in ensuring a safe and security posture. Although it is not required for healthcare systems to implement this policy, it is highly recommended as a baseline to cover potential threats. NIST categorizes vulnerabilities in three groups: low, moderate, and high as a means to prioritize the areas that need more attention (Tunggal, 2022). Additionally, NIST further organizes security controls into 20 control families to separate duties in monitoring and assessing security features. Examples of implementing these policies include ensuring backups of essential data and contingency planning, requiring proper physical device management, and conducting regular risk assessments. All of these controls serve as a means to check current security standings and to provide guidance on how to improve compliance. From a healthcare perspective, using this set of policies when considering healthcare vulnerabilities is valuable as a reputable source for a baseline. These sets of standards are highly valued in the security industry and should be implemented to protect critical assets and data. Also, because the NIST Framework is so widely used, policies within these standards are often updated to reflect the most pressing issues in the security realm, making it a reputable and up to date source. Following these policies aid in reducing the possible entry points of an attacker, limit damage within a system during an attack, and ensure recoverable circumstances.

Education and Training Needs

Although it may seem that weaknesses in technology lead to threat actors gaining access, many breaches begin through phishing attacks or improper management and use of data, pointing to human factors as a major weakness of the cybersecurity of a hospital system. Therefore, it is imperative that staff receive proper training and education on the updated procedures to respond to and prevent cyber-attacks, creating a "human firewall" (Niki et al., 2022). However, many workers in the healthcare industry are not traditionally trained to respond to cyber-attacks. Including engaging means of training such as gamification or simulations, may aid in the retention of procedures for healthcare professionals. Previous studies have shown that training methods such as gamification improve knowledge and awareness of proper cybersecurity for healthcare professionals at a minimal cost to the organization (DeCarlo, 2020). Such training modules should include data awareness training, phishing simulations, and proper device management when working remotely. Ensuring the proper education of students and staff creates longevity in terms of protecting and securing assets in any industry but is especially important in the medical industry. These training modules should also be updated according to the most recent policies to ensure maximum preparedness for evolving attacks.

Conclusion

A ransomware attack's impact was examined through the potential harm toward the healthcare industry targeting medical devices, staff, and patients, as well as long-term financial and recovery impacts experienced by a hospital system. Furthermore, policies to mediate these attacks and education efforts were suggested in an attempt to reduce the likelihood and disruption from threat actors. Ensuring consistency in security across all facets will contribute to upholding security principles in a healthcare environment. It is important that healthcare and

cybersecurity professionals take these factors into consideration when producing strong security plans for hospitals as they prove to have a very delicate and vulnerable system.

Protecting patients, valuable instruments, and sensitive data require healthcare and security professionals to be aware of vulnerabilities and to have plans to prepare and respond to attacks. A well -defined security posture includes actively following policies, such as having backups and practicing good security like multifactor authentication. Additionally, healthcare organizations should include passive security, which encompasses ensuring proper education and training to prevent attacks with additional and specialized training.

My research is limited by current findings and reports in the healthcare industry in relation to ransomware attacks. Because my research is based on the current standing, future reports may provide a more complete view of ransomware attacks and vulnerabilities in a system. Future work could expand into other common attacks on healthcare, such as phishing, large data breaches, or Distributed Denial of Service attacks. Furthermore, additional research could be conducted to include ransomware in other critical industries such as banking or energy utilities to further expand a knowledge base on secure practices to ensure a holistic functioning society.

References

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges, and future research directions. *Computers & Security*, *111*, 102490. https://doi.org/10.1016/j.cose.2021.102490

Bergal, J. (2022, May 18). *Ransomware Attacks on Hospitals Put Patients at Risk*. https://pew.org/3li9O8z

Collier, K. (2021, February 5). *Hackers post detailed patient medical records from two hospitals to the dark web*. NBC News. https://www.nbcnews.com/tech/security/hackers-post-detailed-patient-medical-records-two-hospitals-dark-web-n1256887

DeCarlo, S. M. (n.d.). *Measuring the Application of Knowledge Gained from the Gamification of Cybersecurity Training in Healthcare—ProQuest*. Retrieved April 2, 2023, from https://www.proquest.com/openview/6e9da5d4461c03a126061dd6a894c547/1?pq-origsite=gscholar&cbl=18750&diss=y

DeMuro, P. R., & Norwood, H. (2021). Ransomware in the Healthcare Industry. *Health Lawyer*, *34*(1). HeinOnline. https://proxy01.its.virginia.edu/login?url=https://search.ebscohost.com/login.aspx?direct=true&site=eds-live&db=edshol&AN=edshol.hein.journals.healaw34.7

Ghayoomi, H., Laskey, K., Miller-Hooks, E., Hooks, C., & Tariverdi, M. (2021). Assessing resilience of hospitals to cyberattack. *DIGITAL HEALTH*, *7*, 20552076211059370. https://doi.org/10.1177/20552076211059366

Gliadkovskaya, A. (2021, September 24). *Ransomware attacks impact patient care, including increased mortality rates, report finds | Fierce Healthcare*. Fierce Healthcare. https://www.fiercehealthcare.com/tech/ransomware-attacks-impact-patient-care-including-increased-mortality-rates-report-finds

Mensik. (2022, September 8). *Healthcare cyberattacks led to worse patient care, increased mortality, study finds*. Healthcare Dive. https://www.healthcaredive.com/news/cyberattacks-hospitals-disrupt-operations-patient-care-Ponemon/631439/

Miller, E. (2022, November 21). *The Growing Threat of Ransomware Attacks on Hospitals*. BitLyft. https://www.bitlyft.com/resources/the-growing-threat-of-ransomware-attacks-on-hospitals

Niki, O., Saira, G., Arvind, S., & Mike, D. (2022). Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that. *DIGITAL HEALTH*, *8*, 20552076221104664. https://doi.org/10.1177/20552076221104665

Riggi, J. (n.d.). *Ransomware Attacks on Hospitals Have Changed | Cybersecurity | Center | AHA*. Retrieved October 25, 2022, from https://www.aha.org/center/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed

Simoiu, C., Gates, C., Bonneau, J., & Goel, S. (n.d.). *"I was told to buy a software or lose my computer. I ignored it": A study of ransomware*.

Slayton, T. B. (2018). Ransomware: The Virus Attacking the Healthcare Industry. *The Journal of Legal Medicine*, *38*(2), 287–311. https://doi.org/10.1080/01947648.2018.1473186

The Check Point Blog. (2020, October 29). *Hospitals Targeted in Rising Wave of Ryuk Ransomware Attacks*. Check Point Software. https://blog.checkpoint.com/2020/10/29/hospitals-targeted-in-rising-wave-of-ryuk-ransomware-attacks/

Trend Micro. (2016, September 7). *Healthcare for Ransom: A Look into the HIPAA Guidelines for Ransomware Incidents - Wiadomości bezpieczeństwa*. https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/healthcare-for-ransom-a-look-into-the-hipaa-guidelines-for-ransomware-incidents

Tunggal, A. (2022, November 24). *What is NIST SP 800-53? Tips for NIST SP 800-53 Compliance | UpGuard*. UpGuard. https://www.upguard.com/blog/nist-sp-800-53

Wenk, L., & Couto, T. (2022). The Rippling Impact of a Ransomware Attack. *Journal of Critical Incidents*, *17*(1), 52–54. Business Source Complete.