The Journal of High School Research

Case Studies on the Disproportionate Impact of Cyberattacks in the Healthcare Sector

Aditya Rai*

Submitted: 01 October 2024 **Accepted:** 11 October 2024 **Publication date:** 05 November 2024

ISSN: 3066-2664: **DOI: 10.70671/gad6q058**

Abstract: Healthcare organizations store valuable data on patient's protected health information, such as past, present, or future physical or mental health or condition and provision of health care to patients, financial information such as credit card and bank account information, personal identifying information, such as social security number and date of birth, and proprietary research in medical science, treatment, and technologies. This information is of significant monetary value and can be used by cyber thieves and hackers to blackmail patients, particularly rich and influential ones. Hence, cyberinfrastructure used by health organizations is constantly under attack by cyber thieves and hackers. For example, healthcare organizations were subjected to an average of 1,463 cyberattacks per week globally in 2022.[1] This paper uniquely investigates the outsized impact of cyberattacks on the healthcare sector through numerous case studies by exploring their impact across all healthcare industry segments. These attacks, targeting computer systems or networks, result in significant financial losses and compromise highly sensitive personal information. Within healthcare, they pose a grave threat to patient privacy, enabling unauthorized access to Protected Health Information (PHI) and other confidential data. With the rising frequency of cyberattacks in healthcare, immediate action is urgently needed and is imperative. A comprehensive understanding of the issue and critical evaluation of existing policies are pivotal in formulating effective and equitable strategies for counteraction.

Introduction

The healthcare domain, entrusted with our most sensitive and crucial personal information, finds itself amid an intensifying crisis—the surge in cyber intrusions. In 2022, the global healthcare sector witnessed an alarming average of 1,463 cyber intrusions per week, a staggering 74% increase compared to the prior year, as highlighted by Check Point Research.[1] This surge is not merely a statistical irregularity; it signifies a significant shift in the threat landscape that directly jeopardizes patient care, data security, and the fundamental functioning of healthcare operations. Frequently, cyberattacks occur due to vulnerabilities like easy-to-crack passkeys, insufficient network security, human error, or even physical security lapses. Cybercriminals then capitalize on these weaknesses to infiltrate a network.[2] When the breach is detected, it is often too late to implement preventative measures such as changing passwords or backing up data. The most important questions in addressing this rapid ascent of cybersecurity threat are: What is the current status of cybersecurity in the healthcare sector, and how can we enhance it?

The gravity of this predicament cannot be emphasized enough. Hospitals and healthcare facilities serve as digital repositories, housing a plethora of sensitive data ranging from patient records to cutting-edge medical research. In such an environment, safeguarding against cyber perils is not just a practical necessity but a moral imperative. The healthcare sector confronts unique challenges in cybersecurity owing to the complexities of patient care, the need to access patient data in emergency situations, the diversity of cybersecurity systems, and the ceaseless evolution of cyber threats.

Furthermore, the urgency of this situation is glaringly evident. The third quarter of 2022 witnessed disconcerting statistics—one out of every 42 healthcare organizations fell prey to a ransomware intrusion.[3] These intrusions, often motivated by financial gains, not only compromise critical health data but also inflict substantial financial hardships on affected institutions. This calls for a comprehensive approach that not only responds to present threats but also foresees and readies for the threats of the future.

To dissect and tackle this crucial issue, this paper employs a multi-faceted approach. It presents an in-depth examination of the prevailing cyber threats affecting healthcare organizations today through an in-depth review of the intricacies of four major types of breaches: cloud compromises, ransomware incidents, data breaches, and business email compromises.[4] In addition, this paper also focuses on both high and low-income communities and possible solutions the government can employ to prevent future attacks. By thoroughly analyzing the techniques, repercussions, and preventative measures for each, the aim is to arm healthcare

*Corresponding Author: Aditya Rai. Email: aditya2021rai@gmail.com

Senior High School Student, Ridge High School, Basking Ridge, NJ, 07920

leaders and practitioners with the knowledge and strategies necessary to bolster their defenses.

In the following sections, we explore the specific dynamics of each prevalent cyber threat, providing not only a comprehensive understanding but also actionable insights to fortify the healthcare sector against these escalating risks. Major outcomes of this research are:

- A thorough examination of major breach types and existing government policies, providing valuable insights for healthcare leaders to bolster their defenses. [Sections 3, 4]
- Case study of specific challenges faced by both large-scale and low-income healthcare settings in cybersecurity. [Section 2]
- Potential impact of new strategies, such as AI-driven solutions, digital tool integration, and government-backed initiatives, to fortify resilience against cyber threats in resource-constrained environments. [Section 5]

Typical Targets During Healthcare Cyberattacks

Available data provide insights into evolving cyber incident distribution across healthcare entities, offering a snapshot of the changing threat scenario. Fig. 1 categorizes cyberattack targets into different segments of the healthcare industry from 2021 to the first half of 2022 based on the data presented in Landi.[5]

It is noted from this figure that the specialty clinics witnessed a significant rise in cyberthreats and breaches, increasing from 23% in 2021 to 31% in the first half of 2022, indicating their growing susceptibility to cyberattacks. Hospital Systems remained a consistent target, accounting for 29.6% of reported breaches during the same period, reaffirming their attractiveness to malicious actors. Notably, attacks on physician groups surged from 2% in the first half of 2021 to 12% in the same period of 2022, signifying an expanded threat landscape where even traditionally less targeted entities face elevated risks. Beyond provider entities, this figure also highlights the vulnerability of cyber

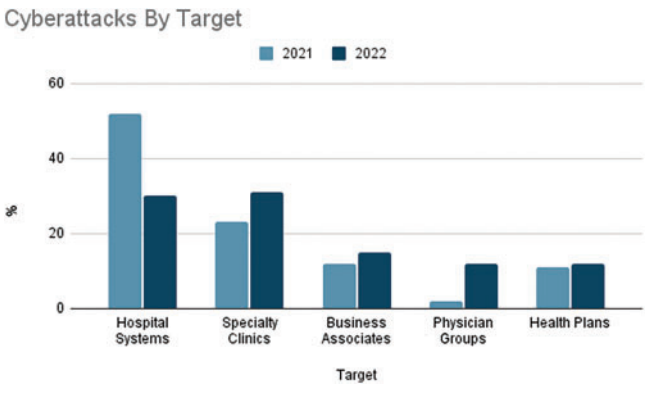

Figure 1. The breakdown of cyberattacks by the target

incidents involving business associates and health plans, constituting 15% and 12% of incidents, respectively. This underscores cyberattackers' broader focus on interconnected components within the healthcare ecosystem.

Types of Cyberattacks

Data breaches

Data breaches follow a systemic trajectory, as outlined in Fig. 2, encompassing three crucial phases: research, attack, and exfiltration. In each phase, hackers capitalize on the weak points of an organization's systems and network, with the end goal of compromising sensitive data.

The initial phase, research, necessitates the perpetrator to carry out meticulous investigations to uncover potential vulnerabilities of a healthcare system that can later be exploited. This investigative work extends to employees, systems, and the network infrastructure. Oftentimes, hackers even go so far as to delve into employees' online profiles to gather insights into the target's technological ecosystem. The research phase requires a substantial investment of time and energy, forming the cornerstone for the subsequent phases of the breach.

Following the research phase, the perpetrator advances to the attack phase, a pivotal juncture characterized by two distinct strategies: network-based attacks and social attacks. In network-based attacks, vulnerabilities within the target's infrastructure are exploited to initiate the breach. This could encompass techniques like SQL injection, session hijacking, and capitalizing on various system vulnerabilities to gain unauthorized access. Conversely, social attacks hinge on manipulation and deception. The assailant crafts persuasive emails tailored to specific employees, often embedding malevolent attachments designed to trigger upon download. These emails aim to deceive recipients into disclosing sensitive information or unwittingly unleashing malware.

Upon infiltrating the network, the perpetrator proceeds to the exfiltration phase. Here, the focus shifts to siphoning valuable data from the compromised organization. This filched information serves diverse objectives, including potential blackmail, cyber propaganda, or even acting as a launchpad for more potent attacks on the organization's infrastructure. The stolen data has the potential to unveil confidential insights into the organization's operations, employees, and clientele, providing the hackers with a potent instrument for further malevolent activities.[6]

Ransomware

The process of a ransomware attack occurs in three key stages, pivotal for cybercriminals aiming to compromise an organization's systems and extract a ransom. While these stages, as illustrated in Fig. 3, are common to all ransomware types, variations exist in execution and techniques employed by attackers.

The first step of an attack is infection. Ransomware, like other malicious software, infiltrates an organization's infrastructure through various means. However, cybercriminals

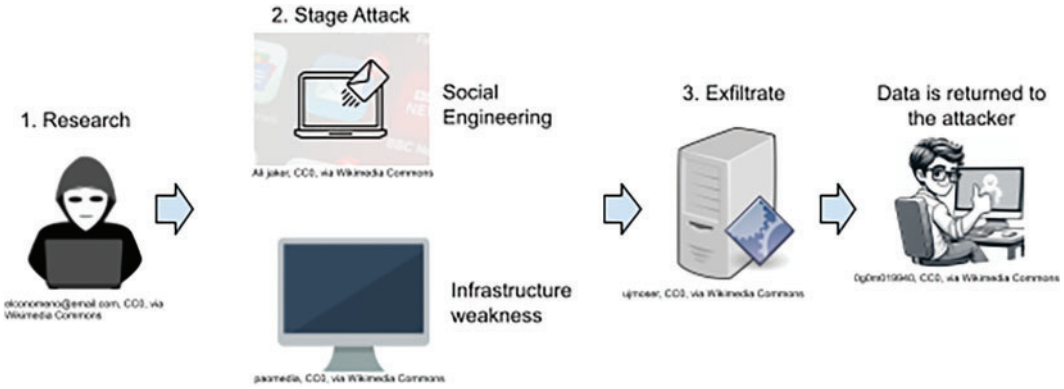

Figure 2. The flow of events of a data breach

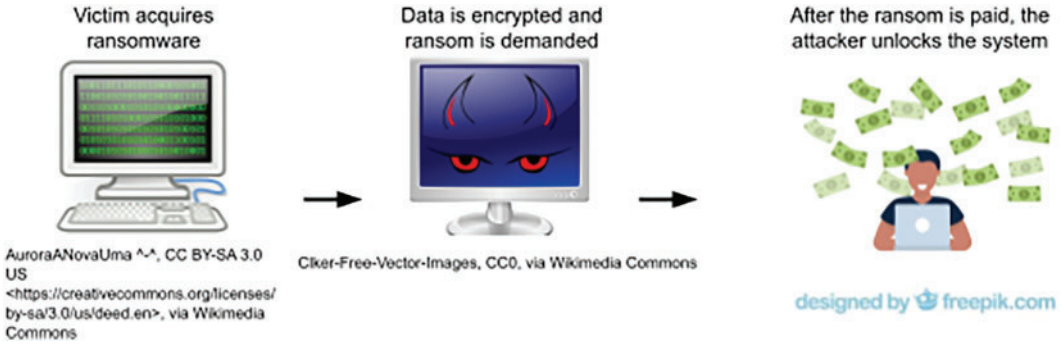

Figure 3. The flow of events of a ransomware attack

tend to lean toward specific infection methods. Among these is the utilization of phishing emails. Crafted with deception, these emails often contain links to websites hosting concealed downloads or attachments with embedded downloader functions. If recipients fall victim to these tactics, the ransomware discreetly downloads and gets activated in their system.

Another avenue exploited by ransomware attackers involves exploiting services like the Remote Desktop Protocol (RDP). Armed with acquired or guessed login credentials, attackers authenticate themselves to access a machine within the targeted network remotely. This foothold enables them to implant and execute the ransomware directly on the compromised system. Some ransomware campaigns even opt for direct system infiltration, mirroring the strategy employed by the WannaCry attack that exploited the EternalBlue vulnerability in Microsoft Windows.[7] Most ransomware strains employ multiple infection pathways, showcasing the flexibility of attackers.

Next is data encryption. Once inside the target system, ransomware initiates the process of encrypting valuable data. Leveraging encryption functionalities inherent in operating systems, this phase involves identifying files, encrypting them with an encryption key controlled by the attacker, and substituting the original files with encrypted versions. To maintain system stability, ransomware variants often exercise caution when selecting files for encryption. Some versions also take additional steps to impede recovery efforts, such as removing backup copies and shadow files that could aid in data restoration.

Finally, after encrypting data, the attackers proceed to demand a ransom. This phase varies across ransomware strains, but a common tactic involves altering the display background to show a ransom note or placing text files within encrypted directories, each containing the extortion message. Typically, these messages specify a specific amount of cryptocurrency as payment in exchange for the decryption key. Upon payment, cybercriminals provide either the private key linked to the symmetric encryption key or the symmetric encryption key itself. Armed with this critical information, victims can use a decryptor program provided by the attackers to reverse the encryption and regain access to their files.[8]

DDoS

DDoS Steps:

DDoS attacks employ a well-orchestrated two-phase approach, as illustrated in Fig. 4, meticulously designed to maximize impact while sowing chaos and disruption.

The initial stage focuses on building a botnet, a network of compromised devices manipulated by a malicious actor, the bot herder or bot master. This interconnected web of devices is repurposed for executing DDoS attacks and other illicit activities, like phishing, spam propagation, and data theft. Beginning with the identification of vulnerable

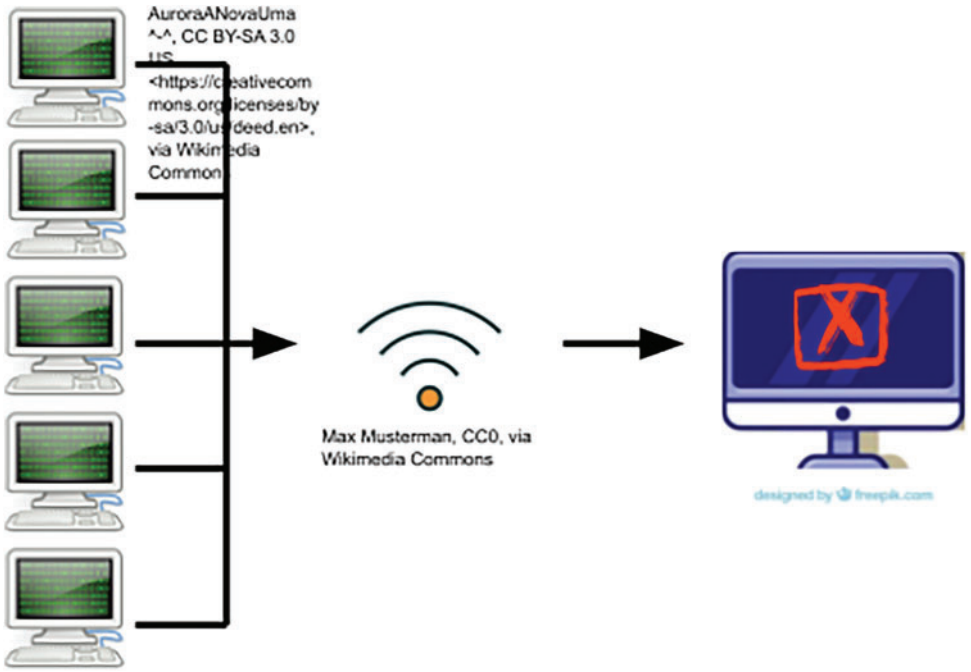

Figure 4. The flow of events of a Distributed Denial of Service (DDoS) attack

devices, those with exploitable weaknesses are targeted to be integrated into the botnet. Malware is introduced to these devices through tactics like phishing emails or leveraging pilfered credentials. Infected devices become active participants in DDoS attacks or are enlisted in propagating malware to expand the botnet. Organizing the compromised devices is meticulously executed by the bot herder. The approach based on traditional centralized control via a host server has become obsolete due to its detectability. A modern approach employs a peer-to-peer model, allowing seamless communication between all botnet devices to enhance the botnet's resilience.

The second phase is about executing the DDoS attack itself, utilizing the assembled botnet to inundate a target server with requests, causing intentional incapacitation. Under the bot herder's directives, compromised devices within the botnet are orchestrated to initiate a synchronized assault on the chosen target. Each device is meticulously programmed to unleash a barrage of requests on the server. This barrage collectively overwhelms the server's resources, saturating its bandwidth and computational power. The outcome is the server's inability to handle legitimate user requests, leading to service disruptions and operational downtime.

Social engineering attacks

Social engineering attacks follow a meticulously orchestrated three-phase sequence, as outlined in Fig. 5, strategically designed to exploit the intricacies of human psychology while exploiting vulnerabilities within security structures.

In the initial stage of reconnaissance, social engineers adeptly gather indispensable intelligence, enabling the careful calibration of their strategic approach. Comprehensive

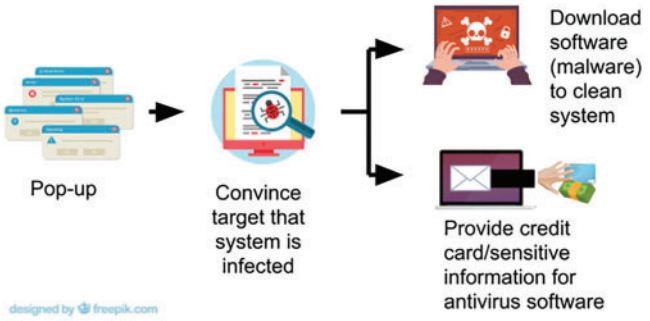

Figure 5. The flow of events of a social engineering attack

insights into target personas pave the way for astute interactions during subsequent stages. Attention is selectively directed towards pertinent information, ensuring that the attack's potency remains unhampered. The pursuit of information encompasses multifaceted avenues: technical sources, encompassing judicious use of online searches, social networks, and websites; physical reconnaissance, encompassing the decoding of employee behavior, office dynamics, third-party affiliations, and access pathways; and discreet scrutiny of discarded materials, often yielding unexpected treasures.

During the pivotal phase of engagement, social engineers forge connections with targets, methodically nurturing rapport to facilitate subsequent infiltration. A spectrum of engagement methods has emerged, some of which operate remotely: phishing tactics, orchestrating an array of emails designed to infiltrate devices or extract credentials; spear phishing, the art of dispatching customized emails to select individuals, often those in privileged positions, for the purpose of compromising systems or harvesting sensitive

access keys; vishing, involving strategic telephone calls, occasionally laced with caller ID manipulation, as a means to skillfully extract confidential insights; SMiShing, exploiting text messages as an avenue for sly manipulation, sometimes shrouded in sender ID subterfuge; and the meticulous craft of impersonation, a finely honed skill involving the creation of compelling pretexts and face-to-face interactions.[9]

Upon the foundation of successful reconnaissance and engagement, the pivotal phase of exploitation ensues. This phase serves as the crucible where well-laid plans come to fruition. Predetermined goals, meticulously delineated before the commencement of engagement, crystallize during this phase. The goals may encompass the discreet extraction of coveted information or skillful navigation to access specific sanctums or systems.[10]

The most common example of exploitation is fake software attacks. Fake software attacks, also known as fake websites, trick victims into thinking they're using trusted software or sites. Victims unknowingly give their login details on these fake sites, which the attacker then exploits on real platforms, like online banking. One example is the tabnabbing attack, where a fake page mimics a popular site's login page. Victims enter their details distractedly, giving the attacker unauthorized access due to the trust placed in such sites.

Attacks against medical equipment

As medical software is put more and more into the light of cybersecurity attacks, researchers are working on new ways to simulate attacks similar to observed cybersecurity attacks. Researchers from the University of Southern Alabama unveiled the susceptibility of a simulated human, iStan, to hacking maneuvers within medical software security, prompting concerns about potential far-reaching consequences. The discovery emphasizes the need to safeguard medical training environments due to the possible long-term impact on medical professionals' ability to analyze critical data accurately.

The researchers meticulously executed the attack on iStan, detailing the stages of their approach. They first scrutinized iStan's documentation, revealing that its platform relied on Adobe Flash Player and Muse software for interaction via TCP (Transmission Control Protocol) and 802.11 (technical standards for LANs) wireless transmissions. The ecosystem involved a Windows or OS X machine, the iStan mannequin, and a properly configured access point.[11]

Moving to the attack itself, the researchers identified known methods to exploit iStan's security weaknesses. These included employing a Denial of Service (DoS) attack using HPING3 (a network tool able to send custom TCP/IP packets) and launching a brute force assault (a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys) on Wi-Fi Protected Setup register PIN numbers through Reaver. After configuring the conditions needed for their attacks, they initiated their maneuvers.

They vigilantly monitored the controlled computer of the medical mannequin during the attacks, capturing the outcomes and planning future digital forensic investigations. The researchers managed to breach two distinct iStan mannequins, highlighting the vulnerability of medical training mannequins.

The gravity of these findings underscores the necessity of fortified medical software security to safeguard against potential breaches with ripple effects impacting medical personnel's abilities to make crucial decisions based on accurate data analysis.

Case Studies

Real-life events are crucial to understanding the vulnerabilities of organizations in the healthcare sector and how they were affected both during an attack and in the aftermath. Although there have been numerous cyber threats and attacks on healthcare facilities during the last two decades, a majority of such events are motivated by financial gains. However, the Boston Children's Hospital attack in 2014 was not financially motivated. Hence, we are analyzing two events in the past decade that present unique aspects of cyber threats on healthcare facilities. By looking at the motives, execution, and implications of both attacks, policymakers can get a better grasp as to how they can enforce better cybersecurity regulations in the healthcare sector.

Boston Children's Hospital Attack

The first of these two attacks is the attack on the Boston Children's Hospital. It was orchestrated by Martin Gottesfeld, an alleged activist hacker and self-claimed human rights activist, and carried out on April 19th, 2014. To date, this attack is one of the largest the healthcare sector has ever seen.

Most cyberattacks seem to be financially motivated. This attack had a different motive, though. Martin Gottesfeld claimed that he was a member of the hacking group known as Anonymous. He, along with the rest of the group, demanded that the hospital change the way they were handling a teen patient, who was already the subject of a custody battle between her parents and the Commonwealth of Massachusetts. Attacks like these are classified as "hacktivism", which is when computers are misused for a socially or politically motivated reason. Oftentimes, like in this example, hacktivists use DDoS attacks to severely slow down an organization's computer network to convey their goals. For these people, inspiring change trumps any actual profit they could make from a possible attack.[12]

After planning the attack for multiple weeks, Gottesfeld used what is known as a distributed denial of service (DDoS) attack to disrupt the hospital's network. The attack flooded 65,000 IP addresses used by Boston Children's Hospital and several other local hospitals with overwhelming volumes of data, obstructing legitimate connectivity on those machines. By flooding the network with an excess of hostile traffic, he essentially shut down not only the Boston Children's Hospital but also other hospitals in the Longwood Medical Area. By targeting a variety of hospitals in the area rather than just one, he was able to amplify the impact of the attack.

The consequences of the DDoS attack on Boston Children's Hospital were multifaceted and significant. First and foremost, the hospital was financially impacted, with response and mitigation actions totaling more than $300,000. Furthermore, the attack interrupted the hospital's fundraising page, resulting in a $300,000 loss in philanthropic donations.[13] This financial stress had a severe impact on the hospital's operating capabilities and the delivery of crucial medical services.

Aside from the financial costs, the attack had a negative impact on patient care and staff operations. For more than two weeks, healthcare providers at Boston Children's Hospital struggled to gain access to internet services required for optimal patient care. The disruption of key services could have jeopardized patient health and well-being during the attack.

Ultimately, the attack underscored the importance of bolstering cybersecurity measures within the healthcare sector. The incident exposed vulnerabilities in critical infrastructure, making it clear that hospitals and medical facilities need to enhance their cyber defenses to safeguard patient data, preserve operational continuity, and protect against future cyber threats.

After the 2013 DDoS attack on Boston Children's Hospital, the institution took decisive steps to prevent future cyber threats and strengthen its cybersecurity infrastructure. Recognizing the urgency of the matter, the hospital invested in upgrading its firewalls, intrusion detection systems, and network monitoring tools to enhance its ability to detect and mitigate potential attacks. Additionally, Boston Children's Hospital established a close working relationship with law enforcement agencies, particularly the Federal Bureau of Investigation (FBI), to facilitate efficient communication and collaboration in the event of any future cyber incidents.

The effectiveness of these measures became evident during a subsequent attack in 2021. When faced with the threat, the hospital promptly alerted the FBI, allowing for an immediate and coordinated response. Working together with the FBI and leveraging their upgraded cybersecurity division, Boston Children's Hospital successfully thwarted the attack, preventing any unauthorized access to its computer systems. FBI Director Christopher Wray acknowledged the significance of the collaborative approach, emphasizing the importance of private sector and federal investigator partnerships in combating malicious and state-sponsored cyber threats. The experience of both attacks underscored the importance of continuous improvement, information sharing, and proactive responses in fortifying cybersecurity measures to protect critical infrastructure effectively. Stress tests of cybersecurity infrastructure through simulated real-world attacks may also be effective in evaluating the vulnerability of the infrastructure. A close and coordinated collaboration with law enforcement agencies, such as the FBI, is critical in preventing occurrences of such incidents.[14]

Idaho Falls Community Center

The cyberattack on the Idaho Falls Community Center in May 2023 serves as a poignant case study illustrating the profound impact of such incidents on rural communities, particularly highlighting vulnerabilities within their critical healthcare infrastructure. This attack sheds light on the broader implications for rural areas with limited resources and connectivity.

The attack's immediate consequences reverberated throughout the rural Idaho Falls community, showcasing the vulnerability of healthcare facilities in such areas. The incident struck at the heart of healthcare accessibility, impacting both the 44-bed Mountain View Hospital and the 88-bed Idaho Falls Community Hospital—essential medical institutions for a population of approximately 68,000 residents. The shared campus and mutual ownership structure underscored the interconnectedness of healthcare facilities in a close-knit rural community. However, their shared vulnerabilities became all too apparent as both institutions were forced to divert ambulances and patients to other medical centers, exacerbating travel times, creating significant risks to the lives of patients in critical conditions, and creating an undue burden on neighboring hospitals.[15]

Furthermore, the cyberattack's consequences extended beyond the hospital premises, affecting partnering clinics that catered to the healthcare needs of the community. The closure of local clinics, like Mountain View RediCare, due to network outages induced by the attack disrupted routine patient services, impacting primary care access in the region. This disruption showcased the indispensable role of local clinics in rural areas and emphasized the broader societal implications of cyber incidents in these communities.

However, the hospital's information technology (IT) team quickly identified the attack and took immediate action to limit the impacts and keep all patient information safe and secure. The hospital IT suspected a virus (which is a destructive piece of a computer program) or ransomware as a possible cause of the attack. The incident also laid bare the digital disparity between rural and urban regions. Rural communities often lack the resources and advanced cybersecurity measures that urban counterparts possess, rendering them susceptible to cyber threats. However, despite these challenges, the aftermath of the attack highlighted the resilience and determination of rural communities in overcoming adversity. Swift coordination efforts, despite resource constraints, underscored the community's commitment to mitigating the effects of cyber threats and safeguarding healthcare access.

Besides the two case studies discussed above, there are numerous incidents that show that the threats of cyberattacks exist because of various factors, including a lack of capable leadership, antiquated IT systems, episodes of cybersecurity breaches, electronic medical records hurdles, limited investment in security, and compliance issues. Affected hospitals struggled to secure cybersecurity insurance due to exorbitant coverage costs, signaling financial constraints hindering their fortification against cyber threats. For instance, the 2023 UnitedHealthcare Student Resources

breach exploited MOVEIt software, compromising sensitive patient data across various healthcare organizations. This event underscored the pressing need to fortify third-party software used in the healthcare domain to thwart cyber incursions.[16]

Similarly, the 2022 Methodist Family Health data breach exposed the dangers of unauthorized entry into patient information via compromised email channels. Methodist Family Health responded by fortifying cybersecurity measures, highlighting the necessity of robust email security frameworks in healthcare establishments. Moreover, the 2022 cyberattack on Howard Memorial Hospital revealed potential data theft affecting patients and staff, prompting immediate protective actions and security reinforcements. Additionally, the 2022 Arkansas Department of Human Services breach and the 2021 Mena Regional Health System incident showcased inadvertent exposure of sensitive client and patient information, compelling swift responses and enhanced security scrutiny.

The case studies discussed above collectively spotlight recurring vulnerabilities in healthcare systems' cybersecurity. They underscore the urgent need for comprehensive strategies to fortify cybersecurity protocols, enhance defenses against evolving threats, and mitigate risks associated with cyber assaults on healthcare data and patient privacy.

Evolution of Attacks

To understand how to prevent future cyberattacks in the healthcare industry, we first have to understand why they occur in the first place. By analyzing the flow of data, increasing the prominence of attacks, and the motives behind these attacks, policymakers can adapt and eventually put an end to these brutal attacks.

Motivations behind Cyberattacks

Although cyberattacks are motivated by a number of factors, we are listing the primary factors responsible for motivating cyber criminals in the following.

Sensitivity and Value of Data

The healthcare sector's appeal to cybercriminals is driven by a convergence of factors. Stolen healthcare data commands high value on the dark web, with a simple credit card being as low as $1 but the full credit card information retrieved from medical files being worth as much as $100. Some reports even indicate that stolen health records sell for 10 to 20 times the value of a credit card number.[17]

This allure is amplified by the abundance of sensitive data in medical records, including crucial identifiers like social security numbers and credit card details. This renders medical identity theft significantly more profitable than targeting isolated data fragments. While individual data may yield meager returns, complete medical records command exponentially higher prices.

The healthcare sector's inherent vulnerabilities further enhance its appeal. Breaching healthcare data carries real-world implications, potentially impacting lives beyond financial losses.[18] Moreover, the sector's increased likelihood to meet ransom demands serves as an additional enticement for cybercriminals. Reports indicate that 93% of healthcare entities comply with ransom requests, with 58% of these requests being coupled with threats to leak stolen data, creating an environment conducive to attackers seeking financial gain.[19]

Additionally, the sector's growing reliance on technology to enhance patient care makes it a prime target for cyberattacks. The widespread adoption of electronic health records, wearable devices, and telemedicine technology has greatly improved healthcare delivery. However, this interconnectedness also introduces significant cybersecurity vulnerabilities.

The shift from paper to digital health records has expanded potential access points for unauthorized parties. This transition has enabled remote access, heightening the risk of undetected data theft. Additionally, electronic records represent a more comprehensive and valuable target for potential attacks.

The healthcare industry has emerged as a major focal point for cyberattacks, resulting in the global theft of millions of medical records. Breaches may occur through hacking, malware, or insider threats, all of which exploit vulnerabilities in staff practices and technology configurations.

The Flow of Money in the Underground Economy

The underground economy operates through a structured hierarchy. At the top are channel administrators, who are responsible for overseeing the market's operations. They maintain a roster of verified participants, enforce client identification policies, and manage automated service bots. Their primary role is to ensure the market's integrity and security.

Buyers and sellers are continually reminded by channel administrators to engage only with verified participants, emphasizing the importance of trust and authenticity within the marketplace.

The predominant activity within this underground economy involves the posting of want and sales advertisements for various illicit digital goods and services. These offerings cater to miscreants who engage in a range of e-criminal activities, including financial fraud, phishing, and spamming.[20]

For instance, a miscreant interested in launching a phishing campaign can enter the market and procure all the necessary tools. This may include targeted email addresses obtained from web crawling or compromised databases, specialized mailers installed on compromised hosts, or web forms susceptible to email injection attacks. They may also acquire compromised machines to host the phishing pages and software promising to bypass spam filters.

Furthermore, the market frequently sees miscreants sharing sensitive information like credit card details and identity data. This information is often posted without explicit labels, assuming that certain fields like names, addresses, and phone

numbers are inherently recognizable. To analyze and measure this data, the approach involves pattern matches for structured data such as credit cards and social security numbers. For free-form data like names, addresses, and usernames/passwords, a combination of random sampling and manual labeling is employed. This allows for a comprehensive understanding of the types and volumes of sensitive data being traded within this underground economy.

What are the US Policies in Place for the Healthcare Sector?

HIPAA

HIPAA, or the Health Insurance Portability and Accountability Act, was put in place with a central mission—to create sturdy confidentiality mechanisms within healthcare establishments and to extend this shield beyond their premises. At its core, HIPAA is about safeguarding the privacy of patients' delicate data, especially their protected health information (PHI).

This extensive legislation casts a broad net in terms of its coverage. It applies comprehensively to all individuals working within healthcare facilities or private offices, including healthcare professionals, students, and non-patient care staff. Furthermore, HIPAA's jurisdiction extends to health plans, billing companies, and electronic medical record companies, recognizing their role in managing PHI.[21]

To guarantee compliance with HIPAA's stringent requirements, healthcare facilities must take comprehensive steps to safeguard both their hardware and software components. This entails securing these elements to prevent unauthorized access to healthcare data and devices, including mechanisms to deter users from making unauthorized changes to passwords at defined intervals. Additionally, performing regular security risk assessments is crucial to pinpoint potential threats such as virus infections and hacking attempts and subsequently crafting protective measures.[22]

HIPAA in ransomware attacks

HIPAA plays a pivotal role in fortifying cybersecurity defenses for healthcare organizations, specifically in countering the persistent menace of ransomware. HIPAA's Security Rule, a central framework, mandates crucial security measures.

Under HIPAA, organizations are obliged to implement an exhaustive security management process that kicks off with a meticulous risk analysis aimed at uncovering vulnerabilities pertaining to electronic protected health information (ePHI). Following this analysis, organizations are directed to put in place security measures to effectively mitigate these identified risks.

Furthermore, the Security Rule puts significant emphasis on the necessity of procedures tailored to confront malicious software, encompassing ransomware. It also highlights the importance of training healthcare personnel to adeptly recognize and promptly report these threats. HIPAA underscores access controls, which serve as a robust deterrent against ransomware infiltrations by strictly regulating access to ePHI.[23]

Significantly, HIPAA's security provisions, while setting minimum standards, encourage organizations to go beyond these requirements, given the ever-evolving cybersecurity landscape.

HIPAA's data backup plan holds immense importance, providing a robust defense against ransomware by facilitating swift data recovery and restoration of normal operations. Contingency planning, as stipulated by HIPAA, covers disaster recovery and emergency operations, ensuring organizations are adequately prepared for a range of crises.

Security incident procedures under HIPAA encompass ransomware responses involving detection, containment, eradication, and recovery strategies. The HIPAA workforce training component equips staff with the knowledge and skills to adeptly respond to emerging threats.

HITECH Act

The HITECH Act, which came into effect on February 18, 2009, brought about significant changes to healthcare cybersecurity and the adoption of Electronic Health Records (EHRs). One of its key provisions was the revision of penalties for violations related to the security and privacy of health information. It introduced four categories of violations, each reflecting increasing levels of culpability and corresponding tiers of penalty amounts. This included a maximum penalty amount of $1.5 million for all violations of an identical provision.[24]

Additionally, the HITECH Act removed previous barriers to penalties, notably by striking the provision that absolved covered entities if they were unaware of a violation. Now, even unintentional violations could be subject to penalties, albeit at the lowest tier, if promptly corrected within a 30-day timeframe.

One of the most notable impacts of the HITECH Act was its role in accelerating the adoption of EHRs. Prior to its introduction, a mere 10% of hospitals had embraced EHRs. However, the Act introduced incentives to motivate healthcare providers to make the transition. This resulted in a substantial increase in EHR adoption rates, with 86% of office-based physicians and 96% of non-federal acute care hospitals having adopted EHRs by 2017.[25]

The HITECH Act comprises four subtitles, each addressing various aspects of health information technology. Subtitle A focuses on promoting health information technology, with Part 1 aiming to improve healthcare quality, safety, and efficiency and Part 2 concentrating on the application and use of health information technology standards and reports. Subtitle B pertains to the testing of health information technology, while Subtitle C delves into grants and loan funding. Subtitle D, the final part, deals extensively with the privacy and security of electronic health information.

In the realm of cybersecurity, the HITECH Act introduced a new era of enforcement. Healthcare entities found themselves subject to financial penalties for non-compliance with EHR requirements, with Medicare-eligible professionals facing reimbursement penalties for non-compliance. The

maximum financial penalty for HIPAA violations was also substantially increased to $1.5 million per violation category per year, and these fines have been adjusted annually to account for inflation.

New Policy Suggestions

Investment tax credit

The problem with the current system is that many hospitals are being forced to choose between paying their workers and increasing their cybersecurity. Because of the futile nature of the healthcare industry, organizations have to choose their priorities in order to ensure that their patients stay alive.

A viable policy proposal to fix this problem involves the introduction of an Investment Tax Credit (ITC) tailored to incentivize and facilitate cybersecurity enhancements within the healthcare domain. Investment Tax Credits are federal tax incentives that allow individuals or businesses to deduct a certain percentage of investment costs from their taxes.[26]

This ITC initiative would be extended to diverse healthcare entities, including hospitals, clinics, physician practices, and various service providers within the healthcare ecosystem. Entities would be eligible, provided they invest in approved cybersecurity measures. These measures would include, but are not limited to, advanced firewalls, intrusion detection systems, encryption technologies for data protection, and investment in threat intelligence systems.

The ITC program would specify a percentage of eligible cybersecurity investments that can be claimed as a credit. This percentage could be adjusted based on the size and nature of the healthcare entity, ensuring equal distribution of benefits across all participants. To prevent any disproportionate allocation of resources, a cap on the total credit amount may be instituted in the future. This would serve as a safeguard to ensure fairness in resource allocation.

Participating healthcare organizations would be required to submit documentation to validate their actual cybersecurity investments and confirm compliance with the in-place standards. On top of that, regular audits and assessments would need to be conducted in order to verify that the tax credits are being used properly. This system of checks and balances would ensure that the ITC program is carried out efficiently and that the resources given by the government are being used effectively.

The anticipated benefits of a policy like this are manifold. For starters, it would lead to a substantial enhancement of the overall cybersecurity posture of healthcare entities. This would not only protect sensitive patient information but also safeguard critical healthcare infrastructure. Additionally, the ITC program would encourage the adoption of industry best practices, setting a benchmark for cybersecurity standards within the healthcare sector. This, in turn, would foster a culture of proactive risk management.

AI threat detectors

Detecting and thwarting cyberattacks in hospitals through AI stands as a potent solution due to its proactive threat identification, risk mitigation, and reinforcement of cybersecurity measures. AI-powered systems employ machine learning algorithms to scrutinize extensive datasets continuously, recognizing patterns, anomalies, and potential threats in hospital networks. These solutions differentiate between regular network behavior and suspicious activities, like unauthorized access attempts to sensitive patient data, unusual file access, or atypical network traffic. Additionally, AI detectors adapt swiftly, learning from new threats and altering vulnerabilities, enhancing their effectiveness over time.

These AI detectors employ diverse methods like anomaly detection, predictive analytics, and behavioral analysis. Anomaly detection pinpoints irregularities or deviations from established norms, signaling potential threats. Predictive analytics use historical data to forecast potential cyber threats, empowering hospitals to reinforce security proactively. Behavioral analysis evaluates user conduct and network activities, pinpointing deviations that could indicate a security breach.

Moreover, these AI solutions seamlessly integrate with existing security systems, bolstering the hospital's defense mechanisms. They automate threat detection, enabling real-time responses and immediate actions upon detecting suspicious activities. For instance, when identifying a potential threat, AI detectors can automatically isolate affected systems, block malicious IP addresses, or terminate suspicious connections to prevent further intrusion.

However, while AI presents significant advantages in cybersecurity, challenges persist. The effectiveness of AI detectors heavily relies on the quality, quantity, and recency of data for training their models. Hospitals need comprehensive, varied, and updated datasets to train AI models effectively. Additionally, these systems must minimize false positives and negatives to avoid unnecessary alarms or overlook actual risks.

Automated kill-switch for data servers

An automated kill-switch for data servers is a safety feature designed to quickly cut off access to sensitive information if a potential security threat is detected. This system works by constantly monitoring server activity for signs of danger, such as unauthorized access attempts, unusual data transfers, or unexpected commands.

When the system spots something suspicious, it automatically activates the kill-switch, which disconnects the server or restricts access to stop any possible breach. This can prevent hackers from stealing or tampering with important data.

The kill-switch can be easily integrated with existing security systems, allowing for a quick and coordinated response across different parts of the network. For example, it can alert security teams, log the event for further investigation, and safely restart the server when the threat is resolved. However, it's important to set up the system carefully so it doesn't accidentally disrupt normal activities. The key is to fine-tune the system to distinguish between real threats and harmless irregularities, ensuring both security and smooth operation.

Deep Learning for Unexpected Sign-In Detection

Using deep learning to detect unexpected sign-ins adds an extra layer of security by spotting unusual login attempts in real time. Deep learning models are powerful because they learn from large amounts of data and can identify patterns in user behavior, making it easier to notice when something is out of the ordinary.

These models continuously monitor sign-ins by looking at things like login times, locations, devices used, and typical user behavior. For example, if a user who normally logs in from one location suddenly tries to sign in from a different country, the system will flag this as suspicious. It can also detect unusual login attempts during odd hours or in ways that don't match the user's normal habits.

When an unexpected sign-in is detected, the system can take immediate action, like asking the user for extra verification, temporarily locking the account, or alerting the security team. This helps prevent unauthorized access before it becomes a bigger problem.

Conclusion

This paper critically reviews the escalating vulnerability of the healthcare sector to cyber threats, emphasizing the urgency for robust cybersecurity measures. It underscores the pressing need for proactive strategies to safeguard sensitive medical data and fortify hospital networks. The multi-faceted analysis of prevalent cyber threats within healthcare, coupled with the solutions proposed in Section 5, underscores the imperative for hospitals to adopt proper defense mechanisms against evolving cyber risks. As these institutions continue to grapple with the repercussions of cyber incidents and the increasing frequency of attacks, the adoption of advanced technologies such as AI detectors emerges as a pivotal step towards fortifying their security infrastructure and protecting patient information from malicious exploitation. Proactive investment in cutting-edge cybersecurity tools and strategies is the best way to safeguard the integrity of healthcare data and ultimately ensure the delivery of quality patient care while also fortifying the resilience of healthcare systems against this evolving threat.

References

[1] CheckPoint Research. Check point research reports a 38% increase in 2022 Global Cyberattacks—check point blog. Check Point Blog; January 5, 2023. https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/ (accessed October 22, 2024).

[2] Coventry L, Branley D. Cybersecurity in healthcare: a narrative review of trends, threats and Ways Forward. *Maturitas*. 2018;113:48–52. doi:10.1016/j.maturitas.2018.04.008. https://www.sciencedirect.com/science/article/abs/pii/S0378512218301658 (accessed October 22, 2024).

[3] CheckPoint Research. *Cyberattacks on the Healthcare Sector—Check Point Software*. Check Point Software Technologies; 2023. https://www.checkpoint.com/cyber-hub/cyber-security/what-is-healthcare-cyber-security/cyberattacks-on-the-healthcare-sector/ (accessed October 22, 2024).

[4] Cyber Attacks: In the Healthcare Sector. CIS Center for Internet Security; July 14, 2021. https://www.cisecurity.org/insights/blog/cyber-attacks-in-the-healthcare-sector (accessed October 22, 2024).

[5] Landi H. *Hackers Shifting Focus to Small Hospitals, Clinics and Tech Companies to Siphon off Patient Data, Report Finds*. Fierce Healthcare; August 24, 2022. https://www.fiercehealthcare.com/health-tech/hackers-shifting-focus-small-hospitals-clinics-and-tech-companies-siphon-patient-data (accessed October 22, 2024).

[6] Data Breach-Definition. Trend Micro; 2023. https://www.trendmicro.com/vinfo/us/security/definition/data-breach (accessed October 22, 2024).

[7] Gantenbein K. *How Does Ransomware Work?|ExtraHop*. ExtraHop. November 13, 2020. https://www.extrahop.com/blog/ransomware-explanation-and-prevention (accessed October 22, 2024).

[8] CheckPoint Research. *Ransomware Attack—What is it and How Does it Work?—Check Point Software*. Check Point Software Technologies; April 9, 2024. https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/ (accessed October 22, 2024).

[9] Salahdine F, Kaabouch N. Social engineering attacks: a survey. *Future Int*. 2019;11(4):89. doi:10.3390/fi11040089.

[10] RangeForce. *Tutorial: The Four Phases of Social Engineering*. RangeForce; October 18, 2023. https://www.rangeforce.com/blog/four-phases-of-social-engineering (accessed October 22, 2024).

[11] Glisson WB, McDonald T, Campbell M, et al. *Compromising a Medical Mannequin*. August 31, 2015. doi:10.48550/arXiv.1509.00065.

[12] Lutkevich B. *What is hacktivism?* TechTarget; May, 2021. https://www.techtarget.com/searchsecurity/definition/hacktivism (accessed October 22, 2024).

[13] Jury Convicts Man Who Hacked Boston Children's Hospital And Wayside Youth & Family Support Network. Department of Justice; August 1, 2018. https://www.justice.gov/usao-ma/pr/jury-convicts-man-who-hacked-boston-childrens-hospital-and-wayside-youth-family-support (accessed October 22, 2024).

[14] Legare R. *Boston Children's Hospital was targeted by Iran-linked hackers, FBI reveals*. CBS News; June 1, 2022. https://www.cbsnews.com/news/childrens-hospital-targeted-by-iran-linked-hackers-fbi-reveals/ (accessed October 22, 2024).

[15] McGee M. *Cyberattack Diverts Patients From Rural Idaho Hospital*. Bank Info Security; May 31, 2023. https://www.bankinfosecurity.com/idaho-attack-a-22201 (accessed October 22, 2024).

[16] Arkansas Rural Hospital Assessment: Final Report. *Arkansas State Legislature*; February 28, 2023. https://www.arkleg.state.ar.us/Home/FTPDocument?path=%2FAssembly%2FMeeting+Attachments%2F000%2F26002%2FHandout+-+Arkansas-Rural-Hospital-Assessment-FINAL.pdf (accessed October 22, 2024).

[17] Wirth A. The economics of cybersecurity. *Biomed Instrum Technol*. 2017;51(s6):52–59. doi:10.2345/0899-8205-51.s6.52.

[18] Marvin M. *Why Is the Healthcare Industry the Most Likely To Pay Cybercriminals for Ransomware Attacks?* portnox; September 19, 2022. https://www.portnox.com/blog/iot-security/healthcare-pay-ransomware-attacks/ (accessed October 22, 2024).

[19] Zero Labs. Measuring your Data's Risk. Rubrik; April 30, 2024. https://www.rubrik.com/content/dam/rubrik/en/resources/report-review/rpt-zero-labs-4.pdf (accessed October 22, 2024).
[20] Franklin J, Perrig A, Paxson V, et al. *An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants*. University of California San Diego; 2007. https://cseweb.ucsd.edu/~savage/papers/CCS07.pdf (accessed October 22, 2024).
[21] Edemekong PF, Annamaraju P, Haydel MJ. *Health Insurance Portability and Accountability Act–StatPearls*. NCBI; February 12, 2024. https://www.ncbi.nlm.nih.gov/books/NBK500019/ (accessed October 22, 2024).
[22] Center for Disease Control and Prevention. *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. CDC; July 10, 2024. https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html (accessed October 22, 2024).
[23] Department of Health and Human Services. *FACT SHEET: Ransomware and HIPAA*. HHS.gov; July 11, 2016. https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf (accessed October 22, 2024).
[24] Department of Health and Human Services. *HITECH Act Enforcement Interim Final Rule*. HHS.gov; June 16, 2017. https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html (accessed October 22, 2024).
[25] Alder S. What is the HITECH Act? 2024 Update. *HIPAA J*. January 11, 2024. https://www.hipaajournal.com/what-is-the-hitech-act/ (accessed October 22, 2024).
[26] Internal Revenue Service. Earned Income Tax Credit (EITC). Internal Revenue Service; May 23, 2024. https://www.irs.gov/credits-deductions/individuals/earned-income-tax-credit-eitc (accessed October 22, 2024).

About the Authors

Mr. Rai is a senior student at Ridge High School, Basking Ridge, NJ. His achievements include a #1 ranking in the High School Congressional Debate in New Jersey and multiple qualifications for the American Invitational Mathematics Examination (AIME). His research interests include public policy, specifically in the fields of public health, cybersecurity, and economics.