Analysis of Cyberattacks in US Healthcare: Review of Risks, Vulnerabilities, and Recommendation

Adya Mishra

Independent Researcher
Great Falls, USA
adyamishra29@gmail.com

Abstract
Healthcare is not opposed to the threat of cyberattacks in today's technology-driven world. Institutions and health systems are vulnerable, and the dangers increase daily. Aggressive data breaches, malware, and ransomware can weaken an organization. The healthcare industry worldwide is at critical risk, putting patient information and safety at risk and destabilizing the healthcare sector—cyberattacks in today's technology-driven world. The good news is that healthcare innovation is leaping; the not-so-good news is that technology updates often create more vulnerability for attackers who see health records as valuable. Unfortunately, the healthcare industry remains behind other sectors in preparing for and avoiding attacks.

Keywords: Education, online, technology, health informatics, health communications

I. INTRODUCTION

Cyberattacks, especially malware attacks, increasingly threaten the healthcare industry. Since 2016, healthcare organizations in the United States have become prime targets for these incidents. During a malware attack, hackers can lock users out of their networks, access sensitive information, or demand ransom from the organization. As medical technology improves and the need for access to patient information rises to ensure critical care, these attacks pose serious risks to patient safety and well-being.

In 2020, email accounts were compromised more than once every two days. However, in 2021, network servers emerged as the primary target for breaches, likely because they store large amounts of sensitive patient data.

A. Scope

In 2020, while electronic protected health information (ePHI) remained a common target, many breaches involved lost, stolen, or improperly disposed of paper or film copies of protected health information.

The shift from paper-based to digital health records has significantly amplified the risk of privacy breaches. While privacy concerns existed even in the era of paper records, the digital age has introduced new vulnerabilities that exacerbate these risks

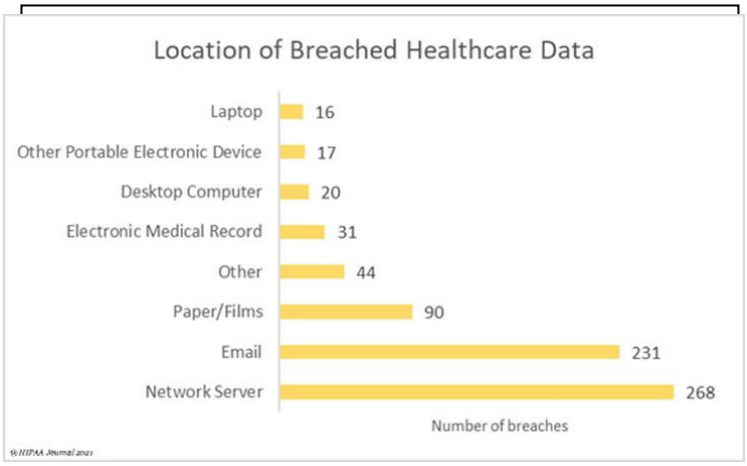

Fig. 1. Healthcare Data Breaches by Location.

B. Vulnerabilities

One of the most critical vulnerabilities in healthcare today is the heightened accessibility of health information. Unlike traditional paper records, which were securely stored in physical locations, digital health records can be accessed remotely. This remote access, combined with the risk of unauthorized entry, significantly broadens the threat landscape for malicious actors.

Consolidating health information into comprehensive digital records has made these data sets more attractive targets for hackers. In the past, patient information was often scattered across various hospitals and departments, which reduced the potential impact of any single breach. However, with electronic health records (EHRs), a single breach can compromise sensitive information and affect many individuals.

The shift to digital health records has also increased the risk of insider threats. While paper records could be physically secured, digital documents can be accessed by a broader range of personnel, including employees with varying authorization levels. Therefore, vigilantly monitoring user access to EHRs is crucial to identify and mitigate these insider threats.

II. CHALLENGES

The complex nature of healthcare organizations provides multiple entry points for cyberattacks. A common vector is email phishing, illustrated in the above diagram. Hackers distribute mass emails containing malicious links or attachments to deceive employees.

1. **Initial Access:** A cyberattack typically begins with a hacker gaining initial access to a system. This can occur through various means, with email phishing being a standard method.
2. **Email Phishing and Credential Theft:** Hackers send malicious emails to employees, tricking them into clicking malicious links or downloading attachments. They also steal employee credentials.
3. **Lateral Movement**: Impersonation: Hackers impersonate real users to gain access to employee accounts.
4. **Data Exfiltration:** Hackers with administrative access can locate and steal sensitive data, including protected health information (PHI) and personally identifiable information (PII). They can then exfiltrate this data by transferring it to external servers or encrypting it for ransom.

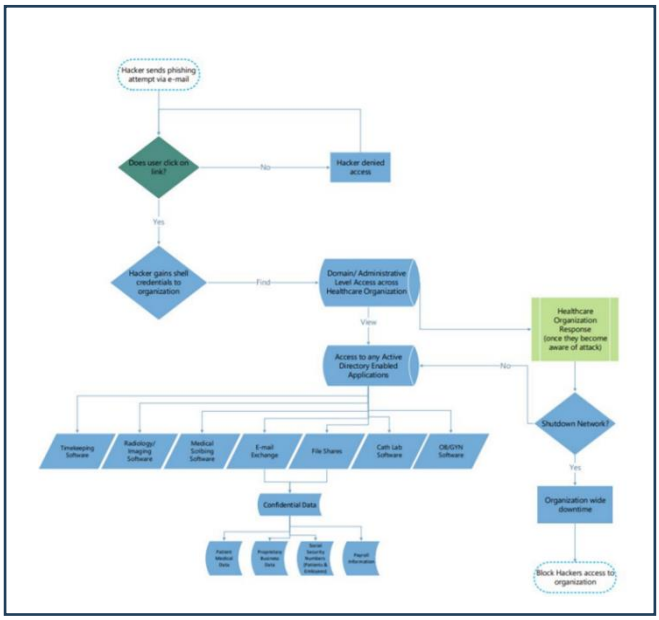

Fig. 2. Flow diagram of email phishing attack steps

A. Potential Impact of a Successful Attack

When a healthcare data breach occurs, sensitive patient information can be compromised, leading to potential identity theft, fraudulent activities, and damage to the healthcare provider's reputation. Critical services like patient care and billing may be disrupted, leading to possible harm to patients and financial losses [1]. Organizations face significant financial burdens from investigating breaches, taking corrective measures, and potential legal repercussions. And most importantly, patient trust in the provider can be eroded, negatively impacting patient satisfaction and loyalty.

B. Recommendations for Risk Mitigation

To reduce the risks of cyberattacks, healthcare organizations should implement the following strategies:

- **Employee Training:** Regularly train employees on cybersecurity best practices, including recognizing and avoiding phishing attacks.
- **Strong Password Policies:** Enforce strict password policies and encourage multi-factor authentication.
- **Network Security:** Implement robust network security measures, such as firewalls, intrusion detection, and intrusion prevention systems.
- **Regular Security Assessments:** Conduct regular security assessments to identify and address vulnerabilities.
- **Incident Response Plan:** Develop and test a comprehensive incident response plan to minimize the impact of cyberattacks.
- **Data Encryption:** Encrypt sensitive data to protect it from unauthorized access.
- **Regular Software Updates:** Keep all software and systems updated with the latest security patches.

C. Regulatory Compliance:

Adhere to HIPAA and other relevant regulations to protect patient data. Healthcare organizations can demonstrate their commitment to responsible data management and patient care by ensuring compliance with these regulations.

D. Continuous Monitoring and Improvement:

Regularly review and update security policies and procedures. Stay informed about emerging threats and vulnerabilities. This ongoing commitment to vigilance and improvement will reassure stakeholders and demonstrate a proactive approach to cybersecurity. By implementing these measures, healthcare organizations can significantly reduce their risk of cyberattacks and protect patient data's confidentiality, integrity, and availability [3].

E. Healthcare Data Breaches by State

Hacking and other IT incidents dominated the healthcare data breach reports in 2020. 429 hacking/IT-related data breaches were reported in 2020, which account for 66.82% of all reported breaches and 91.99% of all breached records. These incidents include exploitation of vulnerabilities and phishing, malware, and ransomware attacks, which have increased considerably in recent months. South Dakota, Vermont, and Wyoming residents survived 2020 without experiencing any healthcare data breaches, but there were breaches reported by entities based in all other states and the District of Columbia. California was the worst-affected state, with 51 breaches, followed by Florida and Texas with 44, New York with 43, and Pennsylvania with 39 [2].

TABLE I. **HEALTHCARE DATA BREACH REPORTS**

State	No. Breaches	State	No. Breaches	State	No. Breaches	State	No. Breaches
California	51	Virginia	18	New Jersey	9	Kansas	3
Florida	44	Indiana	17	South Carolina	9	Nebraska	3
Texas	44	Massachusetts	17	Washington	9	West Virginia	3
New York	43	Maryland	16	Delaware	8	District of Columbia	2
Pennsylvania	39	North Carolina	16	Utah	8	Idaho	2
Ohio	27	Colorado	14	Louisiana	6	Nevada	2
Iowa	26	Missouri	14	Maine	6	Oklahoma	2
Michigan	21	Arizona	12	New Mexico	6	Mississippi	1
Georgia	20	Arkansas	12	Oregon	5	Montana	1
Illinois	20	Kentucky	12	Hawaii	4	New Hampshire	1

Minnesota	20	Wisconsin	12	Alabama	3	North Dakota	1
Connecticut	19	Tennessee	10	Alaska	3	Rhode Island	1

III. CONCLUSION:

Healthcare organizations face significant cybersecurity risks, including ransomware attacks, data breaches, and phishing attacks [4]. To mitigate these risks, it's crucial to prioritize cybersecurity as a fundamental aspect of healthcare operations, and below are the key recommendations to strengthen cybersecurity:

- **Cybersecurity Framework:** Implement a comprehensive framework that includes regular risk assessments, strong access controls, data encryption, incident response plans, and employee training.
- **Network Security:** Utilize firewalls, intrusion detection, and intrusion prevention systems to protect networks.
- **Endpoint Security:** Install and maintain antivirus and anti-malware software, implement strong password policies, and regularly update software.
- **Cloud Security:** Secure cloud configurations and data and monitor cloud activity for suspicious behavior.
- **Third-Party Risk Management:** Assess the security practices of third-party vendors and suppliers.
- **Incident Response Planning:** Develop and test incident response plans to minimize the impact of cyberattacks.
- **Regulatory Compliance:** Adhere to HIPAA and other relevant regulations.
- **Continuous Monitoring and Improvement:** Regularly review and update security policies and procedures and stay informed about emerging threats.

By adopting these suggestions and continued research, healthcare organizations can enormously decrease their risk of cyberattacks and protect sensitive patient information.

REFERENCES

[1] DBranch LE, Eller WS, Bias TK, McCawley MA, Myers DJ, Gerber BJ, Bassler JR. Trends in Malware Attacks against United States Healthcare Organizations, 2016-2017. Global Biosecurity, 2019; 1(1).

[2] Steve Alder. 2020 Healthcare Data Breach Report: 25% Increase in Breaches in 2020. https://www.hipaajournal.com/2020-healthcare-data-breach-report/

[3] Argaw, S.T., Bempong, NE., Eshaya-Chauvin, B. et al. The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review. BMC Med Inform Decis Mak 19, 10 (2019). https://doi.org/10.1186/s12911-018-0724-5

[4] Land, Trudy FACHE. Taking Action Against the Growing Threat of Cyberattacks in Healthcare. Frontiers of Health Services Management 35(1):p 1-2, Fall 2018. | DOI: 10.1097/HAP.0000000000000043