Johns Hopkins University

Engineering For Professionals

Cyber Operations, Risk, and Compliance

EN.635.775.8VL.FA20

Healthcare Industry Risk Management Analysis

Submitted by

Arvind Ponnarassery Jayan

(aponnar1)

Johns Hopkins University

Information Security Institute (JHUISI)

Healthcare Industry Risk Management Analysis

Abstract — The Healthcare Industry faces a lot of cyber threats or risks that could lead to the massive damage more than just the breach of privacy or financial loss. This paper attempts to analyze the risk management process, for the healthcare industry, that are in place to protect the sector from cyber-risks.

***Index Terms* — Cyber-risks , risk management, healthcare Industry**

I. INTRODUCTION

The medical field has been increasingly dependent on technology in recent years. Several cybersecurity incidents that have occurred signifies the growing threat faced by the health care industry in general and hospitals in particular. Various attacks have caused the exposure of sensitive patient data and degradation of the level of service that the industry provides. Due to this the healthcare industry is supported by different security standards and regulations. But how effective are these security protocols placed against the cyber risk?

This paper attempts to analyze the major cyber risks faced by the healthcare industries, the security protocols and risk management placed by the industry. Further, there will be an evaluation of the cybersecurity risk management by the healthcare sector.

[9,11]

II. LITERATURE REVIEW

A. Healthcare Industry and Cyber Threats/Risks

Major critical infrastructures including the healthcare industry are highly dependent on digital systems to execute the operations and process essential data. Since many IT systems used by these infrastructures contain large amounts of personally identifiable information and personal health information, it is pertinent that data breaches and security incidents are mitigated or effectively addressed. The major cybersecurity incident is represented by a pie graph provided the U.S. Government Accountability Office (GAO). From the statistics it can be observed that major threats are Email/Phishing (21%) and improper usage (22%).

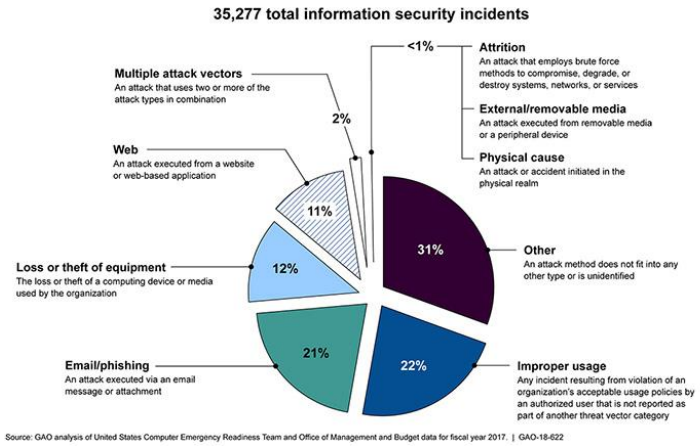

Figure 1: Major Cyber Threats

In the case of the healthcare sector, the industry faces many of the cybersecurity threats present in the pie chart which includes malware that can breach the private data related to the patients as well as the integrity of systems to the distributed denial of service (DDoS) attacks that can adversely affect the patient care. The ramifications of the damages caused by cyber incidents for the healthcare industry are far more than financial and privacy loss. The major cyber-risks, according to the Center for Information Security (CIS), that have caused massive damage to the health industry include:

1. Ransomware
2. Data Breach
3. DDoS Attacks
4. Insider Threat
5. Business Email Compromise and Fraud Scams

It is clear from these statistics provided by the GAO and CIS that almost all critical infrastructure faces a lot of cyber risk and the complications of the risks being exploited especially in the healthcare industry are huge. Juxta positioning the statistics from GAO and the major breaches from CIS the symmetry can be observed.

[9,12]

B. Healthcare Industry and Cyber Risk Management

Risk management is the process of identifying, assessing and controlling all the possible risks related to a particular situation with respect to the environment. In the case of cybersecurity risk management, there should be sufficient view and planning for all events or activities that require the use of any software system. For the healthcare industry due to the several cyber threats and risks it faces, there are several security protocols in place for its protection. The major regulations and compliances that have been established include the US Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA), ISO 27000 Series, with ISO 27799 specifically tailored to healthcare,

GB/T22239-2008, etc. It is understood that there are several risk management in place and that too tailored for healthcare.

[10,13]

III. RESEARCH METHODOLOGY

A. Research Preparations

For this research, I have analyzed the major cyber risks that the Healthcare industry faces along with the risk management process in place to protect from these threats. After which they are analyzed to see whether they have been effective enough to ensure security.

B. Major Cyber Risks and Controls

Ransomware

What is ransomware?

Ransom malware, or ransomware, is a type of malware that prevents users from accessing their system or personal files and demands a ransom payment in order to regain access. If this occurs in the healthcare industry, it would lead to slowing down or shutting down of the acute process. Ransomware can infect a machine through phishing emails or advertisements that contain malware content.

A recent ransomware event:

A recent event, across the country, many hospitals were attacked through the outdated JBoss server software with ransomware malware. Hollywood Presbyterian Hospital in California, one of the many victims had to pay the ransom to regain access to the locked data due to emergency patient care. The ransomware attacks on the hospitals are generally successful since delaying patient care is dangerous as well as it is likely that hospitals will have sufficient financial funds to pay the ransoms.

Ransomware in healthcare:

The healthcare industry is more reactive regarding ransomware attacks. The ransomware events were in decline by the fall of 2018, but this was not the case for the healthcare industry. By 2019 the cases were doubled, and the ransomware payments have increased by 184 percentage. The increase of ransomware malware in the healthcare industry is due to mainly 2 factors:

1. New variants of ransomware malware being created easily and released.
2. The amount to be paid for the ransom by the hospitals are less than the amount of financial damages that can occur due to the hospital's inactivity or slowness.

The hospitals have to be more proactive. The healthcare industries just being compliant is not enough for these modern threats. The healthcare industry should have a more dynamic and

experienced security team or should partner up with one for threats like ransomware. The healthcare industry should consider taking support from security researchers like NIST, HITRUST, MS-ISAC, etc. The latest update in Federal HIPAA Security Rule requires that ransomware breaches are reported to be reported if there are more than a certain number of cases.

Standard recommendation for ransomware attacks:

The MS-ISAC (Multi-State Information Sharing and Analysis Center) have made several recommendations to mitigate the ransomware attack. The following are major recommendations:

1. It is observed that in the healthcare industry the incident response plan does not account for ransomware malware attacks. Incident plans must be created or updated to include these events.
2. Redundancy of data by creating at least one complete backup of all data.
3. Placing firewalls to implement inbound and outbound packet filtering.
4. Monitoring publicly accessible sites and remote access protocols.
5. Email filtering and sandboxing of downloaded attachments for scanning.

[7,8,9]

Data Breach

What is data breach?

Data breach is a security incident where information is retrieved without permission. Data breaches occur due to various types of events like credential-stealing malware, phishing attacks, an insider who discloses the information, lost devices.

A recent data breach event:

A recent event, where theft of a laptop owned by the transportation vendor of the Health Share of Oregon lead to notifying of 654,000 patients that their patient names, DOB and Medicaid IDs might be compromised. Another event is where a Missouri-based BJC Healthcare began notifying 287,876 patients from 19 of its affiliated hospitals that their data was compromised after a successful phishing attack.

Data breaches in healthcare:

From the statistics provided by Ponemon Institute and Verizon Data Breach Investigations Reports, the major sector that has been experiencing data breaches is the healthcare Industry. This is mainly due to the fact that the healthcare industry deals more with Personal Health Information (PHI) over the Personally Identifiable Information (PII). PHI deals with one's personal health history, including ailments, illnesses, surgeries, etc., can't be changed while PII deals with credit card information or Social Security Numbers that can be changed making PHI more valuable compared to PII.

The Federal HIPAA Security Rule requires health service providers to protect electronic health records (EHR) using proper physical and electronic safeguards to ensure the safety of health

information. HIPAA states that breaches must be reported if there are over 500 records, whether due to a hacking incident, accidental disclosure, lost or stolen devices, or unauthorized internal access.

Standard recommendation to mitigate data breaches:

The major recommendations provided by the CIS include:

1. Encryption of data that is stored or in transit.
2. Proper training of employees while handling sensitive data to prevent human error.

[6,9]

DDoS Attacks

What is DDoS?

A distributed denial-of-service (DDoS) is a malicious attack by flooding the normal internet traffic of a victim server or network in order to overwhelm it and slow down or stop the service.

A recent event with DDoS:

In 2014, there was an infringement of a child's right in Boston Children's hospital caused by the doctors after which the group Anonymous conducted a DDoS attack in retribution. The DDoS attack caused a network outage causing a major disturbance for the hospital that required an amount of $300,000 to resolve.

DDoS in healthcare:

The healthcare sector was the second-most attacked industry after the government sector in 2018. It can be observed that the attacks have only been increasing through the years and by 2018, 39% of the healthcare industry was hit daily or weekly.

Standard recommendations to mitigate DDoS:

MS-ISAC provides very specific recommendations for different types of DoS attacks. The general recommendation provided by MS-ISAC includes:

1. Maintaining a healthy relationship with the network providers.
2. Partnering with DDoS mitigation service providers.

[5,9]

Insider Threat

What is Insider Threat?

Insider threat is malicious entities within an organization such as employees, former employees or associates to the business have inside knowledge regarding the vulnerabilities of IT setup or

practices and exploits this to reveal sensitive information. Insider threats include careless employees, inside malicious agents, third parties and disgruntled employees.

A recent insider threat event:

The night security guard of the Texas hospital victimized the organization by downloading malware on several of the workstations that contain patient information and several other setups. He was caught and pleaded guilty to the tampering charges.

Insider threats in healthcare:

It is observed that 46% of the healthcare industry was affected by insider threats and stands on the top to be the most attacked by an insider threat according to the 2019 Verizon Insider Threat Report. Several of the violations are caused by careless employees.

Standard recommendations to mitigate insider threats:

The CIS recommends the following for inside threats as crucial employee training to recognize and report insider threats.

[9]

Business Email Compromise and Fraud Scams

What is business email compromise and fraud scams?

This is the common scam that is conducted where a huge amount of money is asked to be transferred, via emails or compromised accounts, by scammers who imitates as high authority figures in the organization to fraudulent accounts. In the healthcare industry, this can also include money, PII, PHI or goods such as prescription drugs.

A recent fraud scam event:

A local medicinal center, after receiving a call from a pharmacy for prescription drugs over $500,000 worth, got suspicious and reported it. Upon investigation, it was found that the call was made by a scammer and by reporting it the prescription drugs and the money were saved.

Fraud scams in healthcare:

According to the National Health Care Anti-Fraud Association, health care fraud costs the nation about $68 billion annually.

Standard recommendations to mitigate fraud scams:

CIS recommends increasing awareness regarding such scam activities that are going on and train each employee to be vigilant of phone calls and emails.

[4,9]

IV. RESULTS AND DISCUSSIONS

A. Aggregated Information

Ransomware

This is a new and dynamic malware with respect to the healthcare sector and the healthcare industry leans towards being more reactive than proactive. With the help of the research and resourced from HIPAA the following data can be observed:

- 350% increase in ransomware attacks by the third quarter of 2019.
- 91% of ransomware attacks are conducted using phishing emails.
- 75% of the hospitals don't even have an email security solution in place for filtering the attachments, hyperlinks and the content of the email.
- 33% of risk can be reduced just by installing an email filtering tool
- Employee security awareness needs to be better

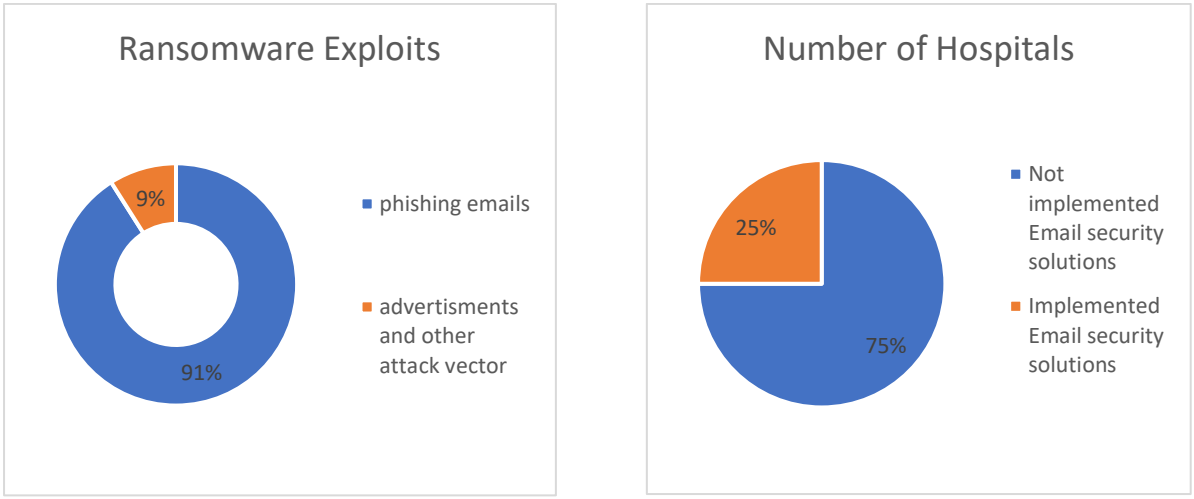

Figure 2: Ransomware attack vectors and hospitals implementing email security solutions

[3]

Data Breaches

Data breaches have become a major cyber threat to healthcare, this risk is handled by HIPAA and appropriate penalties are placed by HIPAA. The statistics of the data breach with the data from HIPAA can be as follows:

- 196% increase from the year 2018
- 59.41% of data breaches are due to IT incidents specifically phishing and spear-phishing attacks.
- Similar to the above case, cyber solutions and employee awareness has to be proper for mitigating most of the data breaches.

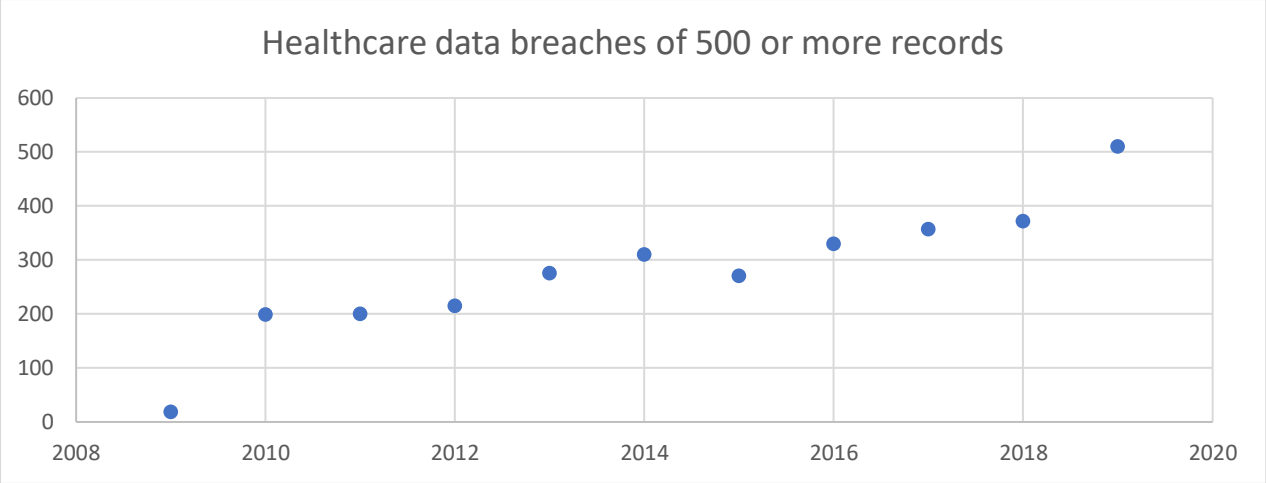

Figure 3: Healthcare data breaches of 500 or more records

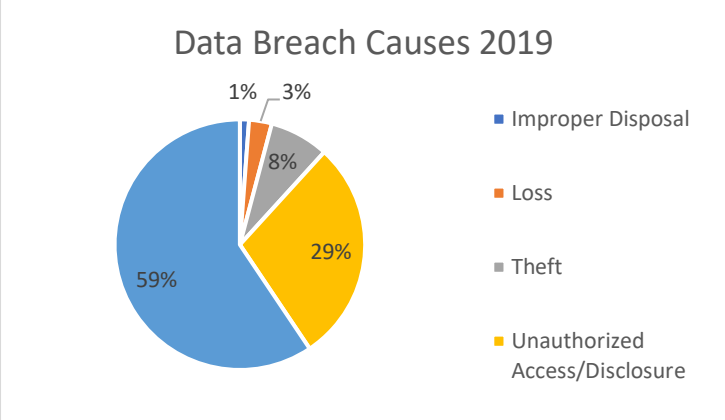

Figure 4: Data Breach Causes 2019

[2]

DDoS

Even DDoS attacks have been increasing by the year. According to the research and resources from HIPAA:

- 129% increase in total DDoS attacks in the second quarter of 2016.
- Healthcare was the second-most attacked industry in 2018.
- 39% of healthcare organizations were hit daily or weekly.

[5,9]

Insider Threat

Insider threat is a common malicious event and it mostly conducted for financial gain. According to the research and resources from HIPAA:

- 75% of insider attacks go unnoticed.
- 46% of healthcare organizations are affected by insider threats.
- 39% of healthcare organizations were hit daily or weekly

[1,9]

Business Email Compromise and Fraud Scams

Fraud Scams have been steadily increasing every year. The scam, which has increased 1,300% since 2015. This is similar to the above risks where major cases are due to phishing scams.

Year	2017	2018	2019
Amount recovered through lawsuits ($ in billions)	2.1	2.5	2.6

[9]

B. Conclusions

From the research, we can understand that just being compliant with standards like HIPAA, ISO etc. is not enough since the major types of attacks do not focus on breaking the system or the process but focuses on human error and poor or no placement of any cyber solutions.

- The healthcare industry, a pool of rich financial resource as well as sensitive PII/PHI resources needs to be a more proactive sector rather than being a reactive sector with respect to cybersecurity risks.
- On one hand, the majority of the cyber risk the healthcare organization faces are from IT incidents specifically phishing or spear-phishing emails. These attacks are not mitigated since 75% of the healthcare industry does not have an email filter in place.
- On the other hand, employee awareness needs to be increased so that they will be more vigilant and spot scams, fraudulent emails and insider threats.
- Following HIPAA guidelines and leveraging other cybersecurity resources that focus on these major issues can provide the best case for the healthcare industry to mitigate these cyber risks better in the future.

REFERENCES

[1] (MARCH 22,). *5 Types of Insider Threats in Healthcare – and How to Mitigate Them*. Available: https://www.fairwarning.com/insights/blog/5-types-of-insider-threats-in-healthcare-and-how-to-mitigate-them.

[2] (Feb 13,). *2019 Healthcare Data Breach Report*. Available: https://www.hipaajournal.com/2019-healthcare-data-breach-report/.

[3] (Mar 10,). *Q3, 2019 Saw a 350% Increase in Ransomware Attacks on Healthcare Providers*. Available: https://www.hipaajournal.com/q3-2019-saw-a-350-increase-in-ransomware-attacks-on-healthcare-providers/.

[4] (). *Statistics*. Available: https://www.bcbsm.com/health-care-fraud/fraud-statistics.html.

[5] (August 6,). *Healthcare is in Cybercriminals' Crosshairs*. Available: https://blog.radware.com/security/ddosattacks/2019/08/healthcare-is-in-cybercriminals-crosshairs/.

[6] (July 08,). *UPDATE: The 10 Biggest Healthcare Data Breaches of 2020, So Far*. Available: https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2020-so-far.

[7] (Nov 05,). *Ransomware Resurgence Reveals Gaps in Health IT Security Planning*. Available: https://healthitsecurity.com/news/ransomware-resurgence-shows-gaps-in-health-it-security-planning.

[8] (). *Malware Bytes*
. Available: https://www.malwarebytes.com/.

[9] (). *Cyber Attacks in the Healthcare Sector*. Available: https://www.cisecurity.org/blog/cyber-attacks-in-the-healthcare-sector/.

[10] Amr Jadi, Hussein Zedan and Turki Alghamdi, "Risk management based early warning system for healthcare industry," *2013 International Conference on Computer Medical Applications (ICCMA)*, 2013.

[11] MS, Jalali JP, Kaiser, "Cybersecurity in Hospitals: A Systematic, Organizational Perspective
," *(J Med Internet Res 2018;20(5):e10059)*, Available: https://www.jmir.org/2018/5/e10059. DOI: 10.2196/10059.

[12] (). *Cybersecurity Challenges Facing the Nation – High Risk Issue*. Available: https://www.gao.gov/key_issues/ensuring_security_federal_information_systems/issue_summary.

[13] J. Kaberuka and C. Johnson, "Adapting STPA-sec for socio-technical cyber security challenges in emerging nations: A case study in risk management for rwandan health care,"

in *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 2020, . DOI: 10.1109/CyberSecurity49315.2020.9138863.