Zombie Health System
(ZHS)

Governance Risk and Compliance Team

Risk Communication Report

Presented by: Berline Beauvais

Cohort: 8/8/2022

Date: 4/30/2023

Table of contents

Executive Summary

Risk management is the process of identifying, assessing and controlling threats to an organization's capital and earning[1]. In Cyber security, It is the probability that a threat(Ways) will exploit the system vulnerability(Means) and create a detrimental effect(Ends) to the system. There are critical cyber security risks involving healthcare organizations. Zombie Health System(ZHS) a not for profit healthcare organization that has over 25 000 patients, and its staff is around 3,000 altogether including medical personnel, administrative and IT teams. In this regard, the board of directors of ZHS has decided to support research for new ways to protect our employees and patients records. This document is an initial risk assessment of the cyber security risks of ZHS.

The Governance Risk and Compliance team, using the NIST made an assessment of all identified risk register items(I) and suggested NIST controls to mitigate them(II). We identified five risks, presented in a qualitative model, rated very high, high, and moderate.

[1] https://www.techtarget.com/searchsecurity/definition/What-is-risk-management-and-why-is-it-important#:~:text=Risk%20management%20is%20the%20process,errors%2C%20accidents%20and%20natural%20disasters.

I- Cyber security risk assessment for Zombie Health System

Risk is an essential part of everyday life and risks are unavoidable in any complex program[2]. A common definition of risk is “the chance of something happening that will have an impact on the achievements of the states organizational objectives“[3]. Risk assessments are used to identify, estimate and prioritize risk to organizational operations, assets, resulting from the operations and use of information systems[4]. We will identify the cyber risk for ZHS(I-A), then we will assess each one of them(I-B).

I-A. Identification of the risks

Healthcare has different priorities and will conduct risk assessment differently than other organizations like the financial one.

The Risk analysis in healthcare involves consideration of the sources of risk, their consequences and the likelihood that those consequences may occur with patient safety, persons involved in providing healthcare, the organization itself, in an effort to distinguish minor acceptable risks from unacceptable major risks and to provide data to assist the subsequent evaluation and treatment of risks[5]. We identified five major risks that threatening the cyber environment of ZHS:

1- Physical damage of the IT Infrastructure

2- Data Breach

3- Data Loss

4- System disruption

5-Compliance failure

[2] Arimbi H, Puspasari M, Syaifullah D. Hazard identification, risk assessment and risk control in a woodworking company. *IOP Conf Ser: Mater Sci Eng*. 2019;505:012038. doi: 10.1088/1757-899X/505/1/012038 [CrossRef] [Google Scholar] [Ref list]

[3] Health Service Executive. Risk assessment tool and guidance; 2008. Available from: https://www.hse.ie/eng/about/who/oqr012-20081210-v4-risk-assessment-tool-and-guidance-incl-guidance-on.pdf. Accessed November 3, 2019.

[4] https://docs.google.com/document/d/1qPCibhJKeis-KBN7n_VXH8HRTnlzuEcYQxW-kOPcajk/edit

[5] Strametz R. Requirements on clinical risk management systems in hospitals; 2017. Available from https://www.aps-ev.de/wp-content/uploads/2017/03/Clinical-Risk-Management-Systems-1.pdf. Accessed January 10, 2020. doi: 10.21960/201707/E [CrossRef] [Google Scholar] [Ref list]

I-B. Risk Analysis of the identified risks

1-Physical damage of the IT Infrastructure

Physical damage is any damage to an organization's hardware assets, such as its servers, laptops and network devices. For healthcare organizations, physical damage can lead to loss of protected personal healthcare information (PHI), system outages and inability to provide medical services. In some critical cases, it can be a direct threat to patients' lives and well-being: if critical equipment is out of order, patients might not get the level of care they urgently need[6].

Threats that lead to physical damage include natural disasters, improper storage environment, inadequate hardware maintenance or careless handling, employees mistakes and purposeful attacks by attackers. Physical damage is the type of incident that organizations experienced most frequently over the past year. Again, the regular users are one of the most dangerous for physical damage of IT infrastructure. It can be from employees' mistakes(50% of the cases). It can be negligence from employees, caused by work overload, in particular for small IT groups. Thus, we need to pay close attention to that, because ZHS has a relatively small IT and security team for a network of almost 30 000 employees and patients.

2- Data Breach

A data breach is a confirmed security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an unauthorized individual. In the case of the healthcare industry, data breaches often involve the compromise of Protected Health Information (PHI), but some cases include other types of data, such as payment information or Personally Identifiable Information (PII). Consequences of a data breach include massive leaks of extremely sensitive data, which can be easily sold on the black market or used for extortion and fraud, as well as lawsuits from enraged customers, substantial compliance fines and reputational damage.
Unfortunately, the healthcare industry is not a stranger to data breaches. Recent headline-making breaches include the Premera Blue Cross and Anthem incidents, both in 2015. 68% of healthcare organizations named data breaches their top priority among IT risks. Mostly, password sharing is considered as the most dangerous threat pattern, about 79%. But, in reality, most breaches were caused by human errors, such as unintended disclosure or clicking on a phishing links[7]. Hackers often smuggle in malware by tricking employees into opening malicious attachments in phishing emails, or take advantage of poor corporate practices like password sharing. Half of data breaches involve activity by regular business users, followed by IT team members (33%) and mid-level managers(24%).

From a recent report of security incidents from data breaches analyzed in the healthcare sector 61% of the data breaches were found perpetrated by external actors, while the static is 39 % for insiders. Without appropriate authorization policies and procedures and access controls, hackers, workforce members, or anyone with an Internet connection may have impermissible access to the health data, including protected health information (PHI), that HIPAA regulated entities hold[8]. The attackers might have gotten access to customers' clinical information, banking account numbers, Social Security numbers, birth dates and more. According to the Verizon 2018 DBIR, the most frequent threat pattern for breaches in healthcare is miscellaneous errors, mainly in the form of misdelivery and unintended disclosure.The result is also of a failure of compliance of HIPAA requirement and could potentially lead to fine.

[6] ttps://blog.netwrix.com/2018/11/15/infographics-it-risks-for-the-healthcare-industry-expectations-vs-reality/#:~:text=The majority of survey respondents,or clicking on phishing links.

[7] https://blog.netwrix.com/2018/11/15/infographics-it-risks-for-the-healthcare-industry-expectations-vs-reality/#:~:text=The majority of survey respondents,or clicking on phishing links.

[8] https://www.hhs.gov/sites/default/files/controlling-access-ephi-newsletter.pdf

3- Data Loss

Data loss usually happens when information is destroyed by failures during storage, processing or transmission. Data loss can be deliberate (e.g., erasure, session hijacking, malware infiltrations and IoT exploits), or the result of human mistakes. Another scenario is when a portable device with access to sensitive data is lost or stolen. The consequences of such incidents for healthcare organizations can be severe. If the extremely sensitive data of their clients and employees, which includes personal information, financial data and results of clinical examinations, ends up in the wrong hands, it might be used for phishing attacks, blackmail or fraud. Even if patient data is lost rather than stolen, vital healthcare procedures might be delayed and important decisions might be less well informed. In either case, the company might experience loss of customer loyalty, decrease in business velocity or even bankruptcy.

In 2018, the U.S. Department of Health and Human Services' Office for Civil Rights announced its fourth largest HIPAA violation penalty, issued to the University of Texas MD **Anderson Cancer Center.** The case stems from three incidents in 2012 and 2013: An employee's laptop was stolen and two thumb drives went missing; all of the devices stored electronic protected health information (ePHI) of MD Anderson patients. In total, the PHI of 34,883 patients was lost and might have been exposed to unauthorized individuals. Analysis revealed that the portable devices containing ePHI were not encrypted, which was a direct violation of HIPAA. Due to their failure to implement security controls required by HIPAA, MD Anderson was ordered to pay $4,348,000 in penalties.

Although the departing employees are considered as the primary threat for data loss, it seems that most data loss in the healthcare industry is caused by regular users(54%)[9]. It happens mostly by human error from regular users involving data loss(e.g., hardware failures and lost/stolen devices). Intentional erasure is one of the threats but not the principal one.

4- System disruption

A system disruption (or service interruption) is the failure of certain systems to provide or perform their primary function for a period of time. Common reasons include system failures (including power outages), natural disasters, malicious techniques used by both outsiders and insiders (e.g., Distributed Denial-of-Service(DDoS) attacks, sabotage and ransomware), and human mistakes. For healthcare organizations, unplanned downtime means that they cannot function effectively, since the disruption might affect every aspect of their operations, from patient care to admissions to supply chain and more. For example, a system disruption might prevent an organization that relies on electronic health record (EHR) systems from registering patients, scheduling appointments and accessing test results. System disruptions also create problems for organizations that provide clinical healthcare to patients from a distance using IT (telemedicine)[10]. It seems that power outages are leading the cause of system disruption, with 48% of the cases, while human mistakes place second 45%. Also, there is ransomware by hackers. They are also responsible for 33% of power outages leading to system disruption. They take advantage of human mistakes and leverage gaps in cyber security (e.gSystem vulnerabilities and unpatched systems) to perform ransomware and DDos attacks.

[9] https://blog.netwrix.com/2018/11/15/infographics-it-risks-for-the-healthcare-industry-expectations-vs-reality/#:~:text=The majority of survey respondents,or clicking on phishing links.

[10] https://blog.netwrix.com/2018/11/15/infographics-it-risks-for-the-healthcare-industry-expectations-vs-reality/#:~:text=The majority of survey respondents,or clicking on phishing links.

The cyber attack wannaCry in 2017 severely disrupted the British National Health Service(NHS). Hospitals and General Practitioners(GPs) surgeries in England and Scotland were among at least 16 health service organizations hit by the ransomware attack, which used malware called Wanna Decryptor to encrypt data. The demand for payments of $300 to $600 to restore access was the least of the problems — the attack caused major disruptions to surgery schedules in the UK. Since the attack affected key systems, including telephones, staff were forced to revert to pen and paper and use their own mobiles for daily operations. They also had to turn away patients and cancel appointments; patients were advised to seek medical care only in emergencies[11].

5- Compliance failure

Compliance is not in itself an IT risk, however, they are a major concern for healthcare organizations. Healthcare organizations have to comply not only with standards specific to their industry like the Health Insurance Portability and Accountability Act(HIPAA) and the Health Information Technology for Economic and Clinical Health(HITECH) Act, but also with standards like Payment Card Industry Data Security Standard (PCI DSS) if they accept credit card payments, The most obvious consequence of non-compliance is huge amount of fine[12]. Compliance standards require organizations to prove that PHI and other personal data of patients and employees are thoroughly protected at all times. Compliance with industry standards depends on the fulfillment of certain IT requirements. But not exactly an IT risk. Failure to respond to IT requirements can lead to compliance failures.

In December 2014, hackers compromised a database owned by Anthem, the second largest health insurer in the U.S. The compromise wasn't discovered until January 27, 2015, after a database administrator discovered his credentials being used to run a suspicious query. In the interim, hackers stole the data of 78 million plan members, including their names, addresses, dates of birth, medical identification numbers, employment information, email addresses and Social Security numbers.

In 2018, Anthem agreed to pay a $16 million fine for the 2015 data breach and to undertake a robust corrective action plan to address the compliance issues discovered by Office of Civil Rights (OCR) during the investigation. This fine is more than triple the previous record HIPAA breach settlement amount of $5.55 million, levied against Advocate Health Care in 2016.

II-Controls to apply to the identified risks

In the healthcare space, entities (covered entities and business associates) regulated by the Health Insurance Portability and Accountability Act(HIPAA) must comply with the HIPAA Security Rule to ensure the confidentiality, integrity, and availability of electronic protected health information (ePHI) that they create, receive, maintain, or transmit. This crosswalk document identifies "mappings" between the Cybersecurity Framework and the HIPAA Security Rule. The organization must see the appropriate mitigation of the compliance failure (A), while identifying the residual risk left after applying the controls (B).

II-A. Mitigation for the identified risks

[11] https://blog.netwrix.com/2018/11/15/infographics-it-risks-for-the-healthcare-industry-expectations-vs-reality/#:~:text=The majority of survey respondents,or clicking on phishing links.

[12] https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996

To mitigate the risk the organization needs to understand what risks pose the biggest threat and be able to prioritize the security efforts to ensure that you use the resources to maximum effect. However, a critical issue is the danger of giving preference to a few security controls and neglecting others. To avoid this, we will see each risk separately.

1- Physical damage of IT infrastructure

- **Improve the protection of hardware.**Around 60% of respondents patch software and update user passwords once a quarter. But 20% of organizations rarely or never get rid of stale and unnecessary data or classify the data they store. Organizations also fail to control shadow IT — only 21% review the software that employees use on quarterly basis[13].

- Keep an eye on hardware agenda operating and storage conditions.
- Patch software regularly
- Unpredictability of hardware failure or employee mistakes that lead to the damage.

2- Data Breach

Improve the detection and protection aspects of their Security policies.

- Determine privileged access and non privileges access when accessing sensitive data.
- Also, incur encryption of sensitive data of the patients as well as the employees.
- Employees training
- Limited the access from external email accounts inside the company to prevent malware infiltration.

- Implementing a mechanism to automatically terminate an electronic session after a period of inactivity reduces the risk of unauthorized access when a user forgets or is unable to terminate their session. Failure to implement automatic logoff not only increases the risk of unauthorized access and potential alteration or destruction of ePHI, it also impedes an organization's ability to properly investigate such unauthorized access because it would appear to originate from an authorized user.

- **Encryption:** encrypted in a manner consistent with NIST Special Publication 800-111 (Guide to Storage Encryption Technologies for End User Devices) (SP 800-111). It is not considered unsecured PHI and therefore is not subject to the Breach Notification Rule. Encrypting ePHI in this manner is an excellent example of how implementing an effective encryption solution may not only fulfill an organization's encryption obligation under the Access Control standard, but also provides a means to leverage the Breach Notification Rule's safe-harbor provision.

Monitoring access control

- is a technical safeguard required from covered entities to allow access to ePHI only to those approved in accordance with the organization's information Access Management Process. Susch access can include, role-based access, user-based access, attribute-based access, or any other access control mechanisms the organization deems appropriate. along with some further

[13] https://blog.netwrix.com/2018/10/29/Netwrix-2018-it-risks-report-summary-and-key-takeaways/

technical access to limits computers systems, Firewalls, network segmentation, and Network Access Control (NAC)[14].

- This solution can limit not only insider threats, but also form hackers to gain access to the ZHS 's network or impede the ability of a hacker already in the network from accessing other information systems- especially systems containing sensitive data.

Information Access Management is an administrative safeguard for ePHI and Access Control is a technical safeguard for ePHI, together, they ensure that organizations implement policies and procedures and technical controls that limit access to ePHI to only authorized persons or software programs that have been granted access rights[15].

3-Data Loss

- **Identify what is lost and way to restore data as soon as possible**
- Monitor activities of employees:

Almost half of respondent 44% either do not know or are unsure of what their employees are doing with sensitive data and have very little control over the unauthorized activity of employees[16].

- **Ensure visibility into what users are doing and how they deal with sensitive data.**

4-System disruption

- Monitoring of users activities
- Patch systems regularly
- Ensure alternative sources of energy are available and systems can transit to it automatically.

5- Compliance failures

Identify security risks that could lead to compliance failures
Conduct regular risk assessment compliance with the Security Rule and improve their ability to secure ePHI and other critical information and business processes. Also, ensure security of medical devices.

Addressable implementation specifications require HIPAA regulated entities to assess whether an implementation specification is a reasonable and appropriate safeguard in its environment, and if so to implement it. If a particular implementation specification is not reasonable and appropriate, entities must document why, and implement equivalent alternative measures if reasonable and appropriate.

-Information access management standard:
requires HIPAA covered entities and business associates to "implement policies and procedures for authorizing access to [ePHI] that are consistent with the applicable requirements of [the HIPAA Privacy Rule].
Access authorization : to focus on the policies and procedures that govern how the ZHS will grant access to electronic Protected Health Information (ePHI) within the organization. It may include how access to each information containing ePHI is requested, authorized, and granted, who is responsible for authorizing access requests, and criteria for granting access. Those parameters would reflect what information access is necessary for workforce members to do their job.For example, a billing clerk role may not need access to medical images on a Pictures Archiving and Communication System (PACS) server in order to carry out their billing responsibilities.

[14] https://www.hhs.gov/sites/default/files/controlling-access-ephi-newsletter.pdf

[15] https://www.hhs.gov/sites/default/files/controlling-access-ephi-newsletter.pdf

[16] https://blog.netwrix.com/2018/10/29/Netwrix-2018-it-risks-report-summary-and-key-takeaways/

The Acces Establishment and modification implementation specifications focuses on the procedural aspects about how such access is established, documented, reviewed, and modified[17].

The Access Control standard includes four implementation specifications for limiting access to only authorized users and software programs. The first, Unique User Identification, is a required implementation specification and is a key security requirement for any system, but particularly those containing ePHI.

I-B. Residual risk

Human mistake: when people forget to lock their computer screen.

Download of sensitive data to a flash drive to work from home or on the weekend.

because shared usernames and passwords can become widely known, it may be difficult to know whether the person responsible was an authorized user.

How workforce members can securely access ePHI during periods of increased teleworking should be part of an organization’s Emergency Access Procedures. Appropriate procedures should be established beforehand for how to access needed ePHI during an emergency.

Conclusion

ZHS like any healthcare organization is vulnerable to cyber security risks. The risks may be the physical damage of IT infrastructure which can be catastrophic for the operations and more importantly on the lives of patients. It may also be data breach which is very frequent in the healthcare industry. It might also be data loss; system disruption, and compliance failure. We proposed some steps to mitigate these risks from monitoring access control, patch systems regularly and have a larger team of IT and Security for the Organization. However, these measures wont erase these risks, there are still some residual risks, like human error that persist as a challenge to deal with after we take action to control the big effect.

[17] https://www.hhs.gov/sites/default/files/controlling-access-ephi-newsletter.pdf

Appendices:

Risk Register :
The risk register is the repository for all registered risks.

Refnce No.	Priority	Risk Name	Risk Description	Cause	Dependent Systems	Risk Owner (POC)	Priority (Impact/Likelihood)	Cost	Risk Treatment	Control	Residual Risk	Accepted Y/N
1	Very High	Physical damage of IT infrastructure	Physical damage is any damage to an organization's hardware assets, such as its servers, laptops and network devices.	natural disaster; inadequate storage; employers mistakes	IT	Opéra tions	High					N
2	High	Data Breach	A data breach is a confirmed security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an unauthorized		Security team		High					N

			individual.									
3		Data Loss	Data loss usually happens when information is destroyed by failures during storage, processing or transmission.		Security Team		High					N
4	High	System Disruption	A system disruption (or service interruption) is the failure of certain systems to provide or perform their primary function for a period of time.		Opérations		Moderate					N
5	High	Compliance failure			GRC		High					