7-2 Project Two: Risk Management Plan

Jordan Proch

IT-313-X2318

10 December 2023

I. Importance & Purpose

The purpose of this document will be to show key stakeholders the primary risks that are at play within Health Network, Inc. and how to manage said risks. While there is a risk management plan currently, it has been deemed outdated as current risks and threats are not identified within it. This document will be critical for Health Network as certain risks and threats can put the company in jeopardy. Additionally, this plan will act as a guide for asset allocation. This plan will help reduce any liability that the company may face in the future. The following will discuss the scope of the plan, internal and external risks, physical and safety considerations, the probability and significance of risky events and how they impact Health Network, and how these risks can be mitigated.

II. Scope

The document will stay within the following bounds, listed below, that Health Network has identified via a recent risk assessment. As stated above, the scope includes internal and external risks, safety considerations, probability of significance of risks, and mitigation plans. The risks identified are as follows:

1. Potential loss of data due to inappropriate hardware decommission
2. Potential loss of protected health information (PHI) from lost or stolen company-owned assets, such as mobile devices and laptops
3. Potential data loss due to corrupt production data resulting from a systems outage
4. Internet threats from hackers and other malicious actors
5. Insider threats due to social engineering, installation of malware and spyware
6. Changes in the regulatory landscape that may impact operations

The risks and threats identified within the assessment are very real and very serious. These should NOT be taken lightly. Especially when it comes to healthcare data. These risks affect all three of Health Network's main products - being, HNetExchange, HNetPay, and HNetConnect. The plan will consider these risks based on how they affect variables such as: the three products, revenue, and geographical facilities. Implementing preventative measures will be discussed to prevent physical access to servers and databases, to prevent networking risks such as malware, and to prevent social engineering attacks. Through taking all factors into consideration, the following document will be a comprehensive Risk Management Plan that will aid Health Network in managing and mitigating risks.

III. Risks

Risks often threaten at least one of the elements of the CIA triad (Confidentiality, Integrity, and Availability) which "forms the basis for the development of security systems." (fortinet.com). This section of the Risk Management plan will serve to identify internal and external risks that threaten the elements of the CIA triad. Upholding the CIA triad will help Health Network, Inc. create a strong security posture which in turn will help them utilize and protect their assets and manage risks.

To begin, risks that are not location specific will be identified - both internal and external. The chart below will identify these risks.

Non-Location Based Risks	
Internal Risks	External Risks
Unauthorized file access	Shoulder surfing (employees viewing data by standing near another employee)
Unauthorized data access	Email phishing
Theft of company data	Credential spoofing
Employees downloading unauthorized files	DoS/DDos attacks that limit network traffic
Weak hardware security due to lack of updates	Brute force attacks on network
Weak software security due to lack of updates	Extreme events that cause power outages, or damage infrastructure
	Social engineering

By analyzing the tables, it is evident that employees are a great risk to the company. Employees are both a company's greatest risk, and greatest asset. However, most of the time when an employee creates a risky event, it is often not stemming from a place of malice. Oftentimes, it comes from a lack of education. The section 'IV: Physical and Safety Considerations' has more information regarding this. Additionally, employee based risks are not location specific. It can, and will happen regardless of region.

When it comes to extreme events, such as weather - this is also not location specific. This risk is present regardless of location. However, it would be ignorant to ignore the fact that the headquarters in Tampa, Florida and the office located in Arlington, Virginia are at

greater risk to these events. Hurricanes can often be a bit unpredictable and often affect the eastern coast of the United States. It should be expected to see power outages at these locations. Seattle, of course, does not experience hurricanes. It does, however, see quite a lot of rain throughout the year. Power outages can stem from drivers crashing into electrical infrastructure. It is imperative to ensure that lines of communication can be repaired quickly and efficiently between all of these locations in these extreme, unpredictable events.

As for network related risks, it is important to recognize the risk that comes with working alongside third-party data-centers hosting vendors. Of course, this has the desired outcome of saving money, it also makes DDoS attacks more likely. It introduces extra, and uncontrollable variables. Health Network needs to ensure that the data-centers infrastructure is adequately maintained and that they are doing everything in their power to ensure security.

IV. Physical and Safety Considerations

Following through with the risks outlined in section III, there are several key takeaways that can limit these risks. Following these considerations can and will ensure that vulnerabilities are kept to a minimum.

1. Considering extreme events, such as hurricanes being a very real risk at the headquarters and the Virginia location - it is important to ensure that operations may return to normal as soon as possible. This can be done by ensuring that the nearby data-centers have offsite backups, secondary generators, UPS units, surge protectors. Additionally, this goes for both the data-centers AND the Health Network locations, thorough protocols and policies need to be in place in the event that an extreme event does happen. It is also recommended that devices at the Health Network locations also have surge protectors so that data stored locally does not become corrupted if the electricity flashes off and on.
2. In order to limit the risks that employees create - it is recommended that employee policies are audited and are kept accurate and up-to-date. Specifically, an AUP (Acceptable Use Policy) must either be created, or audited. This policy should maintain the following: BYOD (Bring Your Own Device) policies, Internet of Things (IoT) policies, training policies, etc. Training policies are likely to be most important. Employees need to be trained in identifying phishing scams, social engineering tactics, and overall internet safety. This training should be required once per year. Employees are oftentimes NOT acting maliciously, just ignorantly without fault of their own. This ignorance can be limited with training.
3. Physical access should be limited. Places like server rooms, and data-centers should only be accessible by staff with authorized access. On the same note, staff-only locations should be limited to STAFF-ONLY via keycards. In total, it

is recommended that security cameras, ID cards, mantraps, and biometric security devices be installed where necessary.

4. Hardware and software security MUST be taken seriously. This can be done by ensuring that hardware and software stay as up-to-date as possible. New security patches are released frequently and for good reason. These patches ensure that vulnerabilities are patched up. Additionally, it is recommended that Health Network purchases and maintains a Mobile Device Management (MDM) software. This will allow the company to track the usage of devices, quickly and efficiently update them, and ensure that the devices of terminated employees are returned.

V. Business Impact

The following section will analyze the risks, their probability, the impact they would have on the business, and their priority level. This will help Health Network determine an appropriate response, and which preventive measures take priority.

Business Impact Analysis			
Risk	Probability	Impact	Risk Priority
Potential loss of data due to inappropriate hardware decommission	1 (Very unlikely)	2 (Small)	2 (Tolerable)
Potential loss of protected health information (PHI) from lost or stolen company-owned assets, such as mobile devices and laptops	3 (Occasional)	3 (Moderate)	9 (Severe)
Potential data loss due to corrupt production data resulting from a systems outage	2 (Unlikely)	5 (Catastrophic)	10 (Unacceptable)
Internet threats from hackers and other malicious actors	2 (Unlikely)	4 (Critical)	8 (Severe)
Insider threats due to social engineering, installation of malware and spyware	3 (Occasional)	4 (Critical)	12 (Unacceptable)

Business Impact Analysis			
Risk	Probability	Impact	Risk Priority
Changes in the regulatory landscape that may impact operations	5 (Unlikely)	1 (Negligible)	5 (Moderate)

VI. Mitigation

The following table will list each risk from highest priority to lowest priority and will discuss mitigation tactics to limit the impact and/or probability of said risk.

Risk	Mitigation Tatic
Insider threats due to social engineering, installation of malware and spyware	As stated previously, training employees is extremely important. They're often not acting maliciously. Social engineering tactics and phishing scams are easily mitigated through training. IF social engineering tactics and phishing scams do work and malware/spyware infiltrates the network - it is important to have detection mechanisms installed that can notify IT staff. From there, IT staff will be able to remove the malware and/or spyware.
Potential data loss due to corrupt production data resulting from a systems outage	This risk primarily deals with the third-party data-center hosting vendors. This presents a unique challenge as it is slightly out of Health Networks control. However, ensuring that the vendor has backup power supplies, surge protectors, and an offsite data backup is the largest factor for redundancy.
Potential loss of protected health information (PHI) from lost or stolen company-owned assets, such as mobile devices and laptops	Once again, ensuring that employees are trained thoroughly and properly can mitigate this risk. Training can help employees develop habits to ensure that their devices do not get stolen or lost. IF a device is stolen or lost, ensuring that dual authentication protocols are implemented will mitigate this risk. Additionally, ensuring that devices that go offsite are equipped with a VPN will ensure that data is saved and backed up.

Internet threats from hackers and other malicious actors	Segmenting the network will help mitigate this risk. Segmenting the network ensures that malicious actors don't have access to the full network. Implementing a firewall on the network will make gaining access to the network for malicious actors much harder. Finally, ensuring that devices and software are maintained up-to-date will ensure that the latest security patches are installed.
Changes in the regulatory landscape that may impact operations	This risk is expected but it has a low impact. With the advancement of technology, it is almost guaranteed that regulations will change rapidly. However, staying current with the regulations and a small financial investment will ensure that the impact remain lows.
Potential loss of data due to inappropriate hardware decommission	Ensuring that before hardware is decommissioned, that a backup is first created and stored within a server.

References

What is the CIA triad and why is it important?. Fortinet. (n.d.). https://www.fortinet.com/resources/cyberglossary/cia-triad#:~:text=The%20three%20letters%20in%20%22CIA,the%20development%20of%20security%20systems.