**Health Network, Inc**

Minneapolis, Minnesota

**Part 1 - Risk Management Plan**

**Introduction:**

As an IT security intern working for Health Network, Inc out of Minneapolis, Minnesota, it’s imperative to create a functioning risk management plan to ensure the security of the companies’ data, assets, and reputation. “Risk management plans help a business determine what their risks are in order to reduce their likelihood and provide a means for better decision-making in order to avoid future risk. The importance of risk management in business cannot be understated,” (Marine Agency, 2023). Not only does this apply to business but directly to information security as well. Regarding IT specifically, a risk assessment must occur that involves the “identification, classification, prioritization, and mitigation of various information technology threats,” (SolarWinds, 2023). The risk management plan for Health Network Inc will have to be tailored specifically to a medical company which comes with additional risks in the way of laws such the Health Insurance Portability and Accountability Act, HIPAA, and other laws and regulations that apply. Additionally, the plan will have to have a set scope and have boundaries in place that define what exactly is expected of the project. Key roles and responsibilities will be allocated to the appropriate people and departments as well. All of these details will closely follow a schedule to ensure resources are not wasted or misused and the project is completed efficiently.

**Scope:**

Scope is a critical part of our project because unfortunately Health Network Inc does not have an unlimited pool of resources including time and money. By setting our goals too high, we likely will end up wasting valuable resources, and by setting goals too low, we will not accomplish the goals of the risk management plan. To define the scope, it’s first necessary to define the goals as well as the deliverables, which are the outcomes of the project. In our case, we want to break down the current network architecture and dive into all current systems on that network and conduct a risk assessment which will allow us to determine what risks we are willing to accept, and which ones will need attended to as they pose to great of a risk. From there, those significant risks will be mitigated. The deliverables will be a secure network not just for the company employees, but that patients Health Network serves. In our case, the scope of this project will be limited to resources we have available in-house. There will be no outsourcing to fix any found risks beyond purchasing necessary tools, hardware, or software and hiring a compliance offer to audit our systems.

**Compliance Laws and Regulations:**

Due to the nature of being a healthcare provider, certain laws and regulations will need to be met. The largest one, HIPAA, is broken down into three rules. The first is the privacy rule which states that an individual’s health records cannot be disclosed due to it being considered protected health information. This relates to IT because it’s necessary to store patient records in our databases. Our databases must be secured appropriately to ensure that the risk of violating HIPAA remains low. The security rule “mandates that HIPAA-covered entities complete a risk assessment. A risk assessment is conducted by a compliance officer and is intended to find security risks within your company,” (Meriplex, 2023). Finally, is the breach notification rule which requires that certain parties be notified upon the occurrence of a breach of protected health information. Another regulation that is required is the quality system regulation. The QSR is “an FDA-led initiative to increase the cybersecurity of medical devices,” (Meriplex, 2023). Ransomware attacks are often targeted towards medical providers and can shut them down for extended periods of time. QSR mandates that databases encrypt their data and require additional authentication to access devices. Lastly, the National Institute of Standards and Technology (NIST) Cybersecurity Framework is not mandatory but is a widely practiced and used framework for cybersecurity. Making use of it would be wise.

**Roles and Responsibilities:**

The roles and responsibilities will begin with a project manager overlooking the project to guarantee the process will run smoothly and efficiently. Under the project manager will be a team of the best suited individuals to aid in the process of developing a risk management plan. Part of this team will be our IT Risk Manager who currently is responsible for mitigating risk and providing fixes for vulnerabilities discovered. His actions are based upon the companies’ goals, financial capabilities, as well as the level of risk a threat poses. The information security team will be responsible for applying patches and fixes that are identified. The risk owner will be tasked with ensuring the risk is properly managed and mitigated.

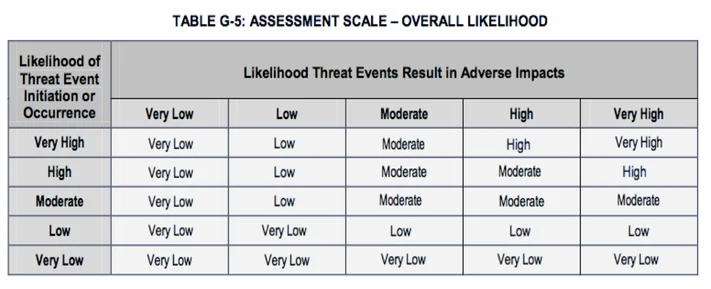
**Schedule:**

Ultimately, a risk management plan is one that is always adapting to the current times and changes based upon the companies’ evolving goals and situation. However, a base risk management plan needs to be constructed and the overall project should take no longer than 30 days. The schedule can be broken down into four phases. One being the risk assessment conducted by a professional, second being to formulate a course of action based upon their findings, third to implement the fixes discussed, and fourth to monitor and assess the situation indefinitely to be able to revisit prior phases as need be. On a deeper level, the schedule should follow the NIST framework.

**Part 2 - Risk Assessment Plan**

**Qualitative Risk Assessment Plan:**

This approach to risk assessment does not utilize numbers and other statistics that you would see with a quantitative risk assessment. Quantitative risk assessment determines risk accurately by analyzing precise numbers but unfortunately not all risks are quantifiable. Therefore, for this risk management plan, a qualitative approach will best suit us. Qualitative is much more judgment based and look at through a scientific approach. Many thoughts will be gathered to determine risk and input should come from higher ups at the company as well as all employees. “ A qualitative risk assessment provides a general picture of how risks affect an organization’s operations,” (Stevenson, 2022). Due to lack of statistical data provided by Health Network Inc, a qualitative approach is not only preferred but required. The plan will consist of five total steps and begin with identifying all risks at hand. Severity should not be taken into consideration at this point as we are just gathering information. Risks to consider are internal and external risks, technical risks, organizational risks, and management risks. Stakeholders should be involved in this process to weigh their concerns along with staff. Step two requires analyzing likelihood, or how likely a risk is to become a problem. This step will enable Health Network Inc to establish a hierarchy of priority for their risks. To easily grade likelihood, NIST recommends using their scale which combines two factors. The first is how likely the threat is to take place. The second is how likely that event will result in adverse effects. This scale has values of very low, low, moderate, high, and very high. The two values will then determine the final likelihood value through the matrix NIST provides. For example, if the threat initiation risk was moderate and the impact risk was very high, the overall outcome would be a high-level risk.



Step three involves viewing the risks impact from a business perspective. The question to answer is how is this going to affect the company’s current and long-term goals? This could take into consideration the company’s reputation or financial stability among other factors. As a general rule, Health Network Inc should assume to the worst as this leaves much less room for risks to become problems. Step four is to create a hierarchy of the risk you’ve identified based upon their levels of risk as well as the company’s level of risk appetite, or willingness to take on risk. Finally, step five will include formulating a plan to mitigate and respond to the problems identified. Additionally, solutions should be implemented to monitor the situation and make future decisions based upon the initial response in order to further mitigate any risks that appear. Risk assessment and risk management is an ongoing process.

**Scope:**

The scope of this part of the risk management plan will consist of developing a plan that assesses and defines current risks that might be found within the organization. A list will be created of all risks and likelihood ratings will be assigned. Following that, a hierarchy will be created of the risks we as a company deem to be of most urgent concern. Finally, a plan will be created to find solutions to the found flaws.

**Data Center Assets to be Assessed:**

The assets that must be included in this assessment are all servers, computers, mobile devices, databases, and especially all pieces of hardware that contain HIPAA related information. As a medical organization, HIPAA is of highest priority to us. Threats to systems with patient information must be viewed as very high risk.

**Relevant Threats and Vulnerabilities:**

* Ransomware (Medical center are notorious for being targets of this malware)
* Physical Security Flaws (Restricted areas, cameras, keycards, tailgating)
* Phishing (Most are easily fooled by genuine looking emails)
* Social Engineering (People are the most vulnerable part of a network)
* Denial of Service (Have to be able to reliably access our networks)
* SQL Injections (Could allow hackers to steal HIPAA data from databases)
* Most threats are External and on an individual or organizational level.

**Types of Controls to Assess:**

* Elimination- Can the risk at hand be entirely removed from the organization or system it effects.
* Substitution- Some risks cannot be entirely removed and only can be kept under control to reduce its risk. By changing or substituting software, hardware, policy or other factors, risk can be decreased.
* Staff Oversight- If a risk cannot be adequately resolved, a staff member can be tasked with overseeing and monitoring the risk to allow for hasty resolution should threats arise.
* Administrator Policies- Admin should create policies to enforce and guide employee’s ensuring risks don’t create themselves.

**Roles and Responsibilities:**

Roles and Responsibilities will closely follow and resemble that of the mitigation plan so that there is minimal confusion as to what is being asked of whom. The project manager will ensure the project carries out smoothly and within issues. The one additional piece that was absent from the mitigation roles and responsibilities will be the inclusion of employees as well as stakeholders. Their input will be necessary for conducting qualitative risk assessment. A member of the project managers’ team will be responsible for keeping track of the concerns of the employees and stakeholders as the project team meets with them.

**Schedule:**

The risk assessment could take some time due to the availability of scheduling meetings with employees and stakeholders. Once meetings have been conducted the project team can begin the qualitative risk assessment and carry out the outlined steps to do so. Following the interviewing process, the risk assessment should take no longer than a week and a half and ideally be completed in one.

**Part 3 - Risk Mitigation Plan**

**Risk Mitigation Plan:**

The first part of a mitigation plan is to understand how it’s different than a management plan or assessment plan. Risk management involves “identifying risks and developing plans to avoid them or lessen their impact,” (Jones, 2023). Risk assessment outlines and analyzes the risks that currently exist and involves developing a plan to fix the risks. Risk mitigation on the other hand, deals with taking a course of action that ensures risks cannot develop in the first place. Mitigation involves four aspects which are avoidance, reduction, transference, and acceptance. Avoidance is the usual desired outcome and optimal solution if it’s possible. This plan allows the risk to be completely controlled prior to its occurrence. “For example, you may face a risk where you won’t be able to complete a task for an important project due to a lack of specialists. To avoid this risk, you could hire multiple specialists in case one got sick or wasn’t available,” (Wojno, 2023). In the case of Health Network Inc, an avoidance plan might entail purchasing biometric or keycard scanners to restrict server rooms. This mitigates and avoids the risk of someone not authorized walking in. The second type of plan is reduction. Reduction does not entirely rule out the risk occurring, but greatly reduces it. If the company had a security breach due to a software vulnerability, they could update the software and hire someone to keep systems up to date. It’s still possible an update could introduce more vulnerabilities and therefore this is reductions as opposed to avoidance. Up to date systems are much safer than out-of-date systems. The third plan is transference. This plan accepts that the risk can’t be controlled on their own so the company places that risk elsewhere. In many cases this type of risk plan comes in the way of insurance. You pay someone to cover damages for something that may occur. That third party company is assuming the risk on your behalf for a fee. Fourth and finally is acceptance. Acceptance is the least ideal scenario and requires the company to assume the risk and take a chance it’s not going to cause problems. Based on a company’s tolerance for risk, some companies may be able to accept more than others. In some cases, risks have to be accepted due to lack of resources to solve them. Risks that fall under acceptance must be monitored, especially closed, so they can be addressed if they become a problem. As for a mitigation plan, Health Network Inc should review the risks identified in their risk assessment and categorize the risks into these four categories to determine how they will all be handled if at all.

**Threats and Mitigation Plan:**

* Ransomware (Reduction)- Threat will always exist but employees can be trained, and systems well maintained to reduce the risk.
* Physical Security Flaws (Avoidance)- Proper security measures with locks, cameras, and guards can fully avoid this risk.
* Phishing (Reduction)- Employee training can help but some phishing emails will always be successful.
* Social Engineering (Reduction)- Employee training can help again, but some will always be victims of social engineering.
* Denial of Service (Transference)- Consider hosting systems in the cloud, the provider will handle denials of service for a fee.
* SQL Injections (Avoidance)- Hiring expert developers can create systems to remove this risk.

**Factors and Resources Involved:**

The most common factors and resources involved with risk as a whole are time, skills, money, and tools, (Asana, 2022). With a company there are only so many of these resources to go around and these resources are used not just in managing risk. These resources belong to the company as a whole and have to be allocated accordingly so the company can achieve its goals. Health Network Inc should allocate ample resources to solve their risk concerns due to their nature of being a health organization. Unfortunately, not all of the risks can be addressed, therefore, the most severe have to take priority. If Health Network can utilize their resources to secure things like HIPAA data, and protect against severe malware attacks, they can afford to take on the risk of say a physical threat in the way of an attacker walking into a restricted area. This of course is not ideal, but the best solution considering the resources at hand.

**Part 4 – BIA and BCP Plan**

**BIA Plan:**

The goal of the Business Impact Analysis is to allow Health Network Inc to review potential disruptions of their ongoing and future processes within their data centers This plan will detail the critical business functions, critical resources, the maximum acceptable outage (MOA) and impact, and recovery point objective (RPO) and recovery time objective (RTO)

Critical Business Functions for Health Network Inc mostly include their data centers. These must be identified specifically to construct a proper BIA. Data storage itself and well as the ability to retrieve that data reliably is the most critical aspect of the business. Patient information has to constantly and accurately be retrieved so that patients can retrieve proper treatment and so their records can be accurately kept. Access to this database must be uninterrupted. While this function considers availability, we still have to account for confidentiality and integrity. Therefore, another critical function comes in the form of proper encryption. Data has to be secure not only for the privacy of patients and employees but because it is legally required under HIPPA. The business cannot function without proper encryption. Sticking with secure practices, the security of the entire network is also critical because data does not solely reside in the database as it’s transferred all around the network to where it needs to go.

Critical resources allow the critical functions to operate as needed. These resources include but are not limited to human resources, financial resources, and physical or hardware resources. Humans or employees’ biggest resource is their time and skills and those must be appropriately applied to systems to allow them to function at the highest level. Finances determine how many employees can be hired and determine the quality of hardware and software that can be implemented. Finally, the hardware limits just how secure the network and database can be. More expensive equipment can provide more security for the critical functions. The main takeaway of critical resources is how they relate to the critical functions. They relate because the critical functions can only operate at a level that the available resources allow them to.

The maximum acceptable outage and impact will closely monitor data center outage, application down time as well as financial impact. Data center outage is the most significant impact and the highest risk because it entirely negates the health network’s ability to conduct business. Any downtime for the data center must be serviced in a quick manner and should last no more than an hour and should be done during hours of the day when data center usage is at its lowest point. Application downtime should follow the same practice as the data centers are no good if they can’t be accessed by the applications being run on the local machines. Both of these impacts create a severe financial impact for the company that needs to be mitigated significantly as the company can’t afford to have its data centers down.

The Recovery Point Objective looks at minimizing data loss. It is the maximum amount of data that Health Network Inc is willing to accept in the event of a disruption. The RPO in this case will be determined by the outcomes of the risk assessment and take into consideration other business impacts. For the health network, I would estimate that the RPO should be around 4-6 hours. A short RPO would suggest that backups occur frequently which costs more money, however they do need to be relatively frequent due to the nature of the data. As for the recovery time objective, this the longest amount of time critical functions should be offline for. Once again shorter RTO’s can be more expensive. A reasonable RTO could be in the 3–6-hour range but leaning more towards three. Both RTO and RPO have to align with each other and work together to be most beneficial. It’s important to note that these values can and should change depending on the state of the business, therefore they should be reviewed regularly.

**BCP Plan:**

A business continuity plan is a “document that outlines how a business will continue operating during an unplanned disruption in service. It’s more comprehensive than a disaster recovery plan and contains contingencies for business processes, assets, human resources, and business partners – every aspect of the business that might be affected,” (Kyndryl, 2023). For the purpose of Health Network, we will be looking only at the data centers for this plan. The first step of the BCP is to identify critical business functions that might need to be recovered. Many of these should already have been defined in the BIA. As for managing access to data centers in the event of a disaster, there should be alternative methods to access the data. This could be accomplished by implementing backups in the cloud that can be accessed in emergency situations. Data still must be accessed not only in emergencies but while maintenance is occurring as well. The next step is to implement recovery procedures. How will Health Network Inc respond during planned or unplanned downtime? Immediately upon data centers going down, access to the cloud must be enabled and all traffic necessary should be routed there. The procedure must also establish a secure way to do this and ensure only trusted users can access this emergency cloud. In order to ensure the plan works and is effective step three will involve testing. Periodically, tests will be run to ensure in the case of a real disaster this procedure functions as intended with no glaring security vulnerabilities. It’s important to note that this procedure should also undergo a risk assessment and undergo risk mitigation as necessary. Finally, documentation should be kept on the testing to allow for improvements to be made over time and allow for easier risk mitigation, (Arcserve, 2023).

**Part 5 – Conclusion**

**Strengths of Plan:**

The strengths of this plan are found in its in-depth effort to encourage those who use the plan to understand the risks before working to mitigate them, as well as its clear definitions of the scope and limitations, and finally, its ability to work within laws and regulations as required. By pushing the understanding of risks before acting, those involved can better solve issues by having strong knowledge of internal and external risks, risks and different levels of the company, and risks associated with laws and regulations. The plan clearly defines laws, specifically HIPAA and QSR, as well as acknowledges frameworks like the NIST Cybersecurity Framework that allow not only legal compliance but also the proper security standards to be met efficiently. By defining the specific scope and limitations of the project, the company can be confident that resources will not be wasted. The project limits the scope to in-house resources meaning that outsourcing for contractors or other goods will be limited and only done as necessary. This way, the resources on hand can be used before spending money elsewhere. Overall, the plan is strong and should allow Health Network Inc. to manage risk effectively.

**Future Risks of Plan:**

While the plan will be effective in the short term, the plan will likely need to be tweaked in the future to account for new risks. This is not due to a lack of detail in the plan but rather due to the constant evolution of technology in the computer science world. All good risk management plans leave room for additions and revisions to be made as necessary. One aspect that could be addressed but was not, is zero-day threats. Zero-day threats are new attacks that have never been seen before. It’s nearly impossible to prevent them outright, but good plans can mitigate them and at the very least have solutions in place to recover from them when they occur. Technological and software advances not only aid hackers in developing new attacks but can also aid in the fight against them. For this reason, the plan stresses the ability to understand risk before acting. Companies have to stay active in reading up on the newest threats to implement solutions to account for those threats. A future revision to the plan could certainly detail a specific course of action for never-before-seen threats that take place.

**Lessons Learned:**

Overall, this project when incredibly beneficial in learning and understanding what it takes to develop a strong risk management plan. Learning from a book or videos is certainly a viable method to learn about cyber-related topics, but getting a hands-on approach allows you to make mistakes and learn what works and what does not. Throughout this project, I discovered that managing risk is no easy task. There are so many aspects that need to be accounted for. There are many frameworks to learn, laws and regulations to follow, and many different angles attackers can take advantage of to exploit a company or individuals. Pulling this all together to form one comprehensive plan takes significant time and research. While it all seems overwhelming, the best part is that frameworks are not there to overwhelm or overcomplicate matters but are there to simplify and make plans easier to construct by following what are essentially instructions. I’m certainly looking forward to utilizing these learned skills in the future and hope they can prove to be as beneficial as I expect they will be.

References

Arcserve. (2023, November 28). *6 steps for developing a business continuity plan*. https://www.arcserve.com/blog/6-steps-developing-business-continuity-plan

Asana, T. (2022, November 8). *7 common project risks and how to prevent them [2023] • asana*. <https://asana.com/resources/project-risks>

*Business continuity plan*. Kyndryl. (n.d.). https://www.kyndryl.com/nz/en/learn/plan#:~:text=A%20key%20component%20of%20a,business%20needs%20can%20be%20met.

Cote, R. (2023, September 13). *Why do companies need A risk management plan?*. Marine Agency. <https://marineagency.com/reasons-why-every-company-should-implement-a-risk-management-plan/#:~:text=Risk%20management%20plans%20help%20a,in%20business%20cannot%20be%20understated>.

Gonzalez, E. (2022, August 5). *A beginner’s Guide to Qualitative Risk Analysis*. The Motley Fool. https://www.fool.com/the-ascent/small-business/project-management/articles/qualitative-risk-analysis/

HASpod. (2021, March 18). *5 best risk assessment control measures with examples*. HASpod. https://www.haspod.com/blog/paperwork/5-best-risk-assessment-control-measures

*How project scope management can save you time: The workstream*. Atlassian. (n.d.). https://www.atlassian.com/work-management/project-management/project-scope

*It risk manager: Skills and roles & responsibilities*. InfosecTrain. (2022, August 24). https://www.infosectrain.com/blog/it-risk-manager-skills-and-roles-responsibilities/#:~:text=IT%20Risk%20Manager’s%20roles%20and%20responsibilities,-An%20IT%20Risk&text=There%20are%20various%20duties%20and,company%20or%20organization%20may%20face

Jones, A. (2023, March 28). *Risk mitigation VS risk management*. AWA International. https://awainfosec.com/blog/risk-mitigation-vs-risk-management/#:~:text=Risk%20management%20is%20all%20about%20identifying%20risks%20and%20developing%20plans,occurring%20in%20the%20first%20place.

*Meet Healthcare Cybersecurity Regulations*. Meriplex. (2023, October 22). https://meriplex.com/how-to-meet-healthcare-cybersecurity-regulations/#:~:text=The%20Privacy%20Rule%20limits%20the,which%20are%20vulnerable%20to%20cyberthreats.

*revised table g-5*. (n.d.). Fairinstitute. Retrieved November 17, 2023, from https://www.fairinstitute.org/hs-fs/hubfs/revised%20table%20g5.jpg?width=711&height=289&name=revised%20table%20g5.jpg.

Stevenson, R. (2022, July 21). *6 types of risk assessment methodologies + how to choose - drata*. Drata. https://drata.com/blog/risk-assessment-methodologies

*What is it risk management? - it glossary*. SolarWinds. (2023). https://www.solarwinds.com/resources/it-glossary/it-risk-management

Wheeler, E. (2023, March 23). *Risk management team roles: Who takes care of project risk?*. MIGSO. https://www.migso-pcubed.com/blog/risk-management/risk-management-team-roles/

Wojno, R. (2023, November 23). *4 practical risk mitigation strategies for your business*. monday.com Blog. https://monday.com/blog/project-management/risk-mitigation/#:~:text=What%20are%20the%20four%20risk,reduction%2C%20transference%2C%20and%20acceptance.