**Part 1: Risk Management Plan**

**Health Network Inc. New Risk Management Plan**

**By: Kaleb Alstott**

**Introduction**

With a company such as Health Network, providing top security with minimal risk issues is a necessity, especially with a company dealing with medical records and documentation that can relate to HIPAA laws. A risk management plan is an essential document that follows an organized structure that identifies risk, threat, and vulnerabilities to allow an organization to improve their IT security overall. Our goal is to take the outdated risk management plan and to implement a new security procedure that will reassure the protection of your three biggest products: HNetExchange, HNetPay, and HNetConnect.

**Risk Management Plan Outline**

1. **Assessment** – This is a pre assessment done on the company’s current risk management plan where risk, threat, and vulnerability pairs may be discovered. In this step we identify any stakeholders involved and start to look at the scope of the overall project after the risks are identified.
2. **Risk Analysis** – The pre assessment is looked over for risks, threats, and vulnerabilities. A qualitative/quantitative assessment is done the determines the risk value of the threats found. This data is then ranked from a scale of 1-10, where 1 would indicate the least amount of impact risk on the company and 10 would indicate the most amount of impact risk.
3. **Plan Creation** – After the risk analysis is reviewed, discussed, and prioritized there is a planning of security improvements for both employees and IT security. Ideally, we start the creation of the risk management plan at the top impact risk in the risk analysis and work our way down the risk scaling.
4. **Plan Implementation** – Once created the risk management plan then starts the implementation. To do so specific head departs such as Human Resources or an IT systems administrator are contacted and relayed the new information and guidelines set for employees and system requirements.
5. **Continuous Monitoring** – In order to maintain a secure and up to date risk management plan we implement a continuous monitoring process. In this process we now observe and communicate issues to the correct departments to be resolved. We implement hotfixes, upgrades, and patches regularly to the systems when bugs or risks are noticed. We continue to properly train employees and keep a sharp eye on our network.
6. **Assessment** – Finally, we evaluate the new risk management plan that we have implemented and go over the accomplishments and goals we have completed.

***Risk Management Identification***

• Loss of company data due to hardware being removed from production systems

• Loss of company information on lost or stolen company-owned assets, such as mobile devices and laptops

• Loss of customers due to production outages caused by various events, such as natural disasters, change management, unstable software, and so on

• Internet threats due to company products being accessible on the Internet

• Insider threats

• Changes in regulatory landscape that may impact operations

In addition, other risks may be identified but we are bounded to these requests first by the company before we may deal with other arising issues that we may find.

**Scope and Boundaries:**

The scope of our project is to ensure an updated risk management plan in which it is to increase the security of the overall locations and technology that the company uses. The key locations we will include in our scope are going to be the headquarters in which is in Minneapolis, Minnesota and the two addition locations located in Portland, Oregon and Arlington, Virginia. We will be working with 600 employees who all use and work with the company technology of HNetExchange, HNetPay, and HNetConnect. HNetConnect is an online directory that can help users find health services such as doctors, clinics, medical websites, but also includes medical information such as doctors’ personal information in this database. HNetPay is an electronical online payment source the company uses to manage and handle all medical payments. “HNetExchange is the primary source is the primary source of revenue for the company. This service handles secure electronic medical messages that originate from its customers, such as large hospitals, which are then routed to receiving customers such as clinics.” (Project assignment).

**Laws and Regulations:**

When looking over Health Inc. there is two major laws and regulations we must follow as we implement the following risk management plan, one being HIPAA, and the other being PCI DSS.

**Health Insurance Portability and Accountability Act (HIPAA)** – HIPAA requires the overall protection of any health-related data rather that when handling, creating, or storing health records this must be kept confidential. The information cannot be shared with anyone unless permitted so by the employ or by another Act. HIPAA here is for dealing with the companies’ technology of HConnect, which is a transmission and directory of medical records that must be followed by the HIPAA requirements.

**Payment Card Industry Data Security Standard (PCI DSS)** – PCI DSS is a security standard for all organizations dealing with credit or debit cards that entitles the proper way of how to handle, store, process, and/or transmit cardholder data. This is for dealing with the companies’ technology of HNetPay which handles credit card information and processing. We must follow the PCI DSS criteria of handling this data to ensure the safety of the customers payments.

**Responsibilities:**

To have a successful risk management plan there will be responsibilities and teamwork that will be split up among the company. All employees working for Health Inc should be aware of current threats and vulnerabilities they will be assessing and handling. Making sure employees are following the right technique and practice in their assigned role is key here. Once we have reported the possible threats the roles and positions the company will take on to implant the risk management plan smoothly are as so:

**Chief Financial Officer (CFO):** Will look over data that is presented by IT department and the HR department. Will give financial advice to where the money should be spent and how it should be spent. Also completing a completion of a cost-benefit analysis after reviewing the data and possible constraints.

**Chief Operations Officer (COO) –** Will oversee day to day administrations of the business when implementing the risk management plan. If anything is not going as plan or is suffering to follow the risk management plan the COO will report to Chief Executive Officer (CEO).

**Chief Executive Officer (CEO)** – Will oversee the risk management plans final decision and will have the final say in the implementation of the RMP. Will also receive frequent updates form COO and COI.

**Human Resources Department (HR):** The HR department will work with the data center and report how they are storing, using, transmitting, and regulating the data ot the HIPAA laws. HR will also have to create a detailed document stating how the HIPAA laws are currently emplace and protected.

**IT Department (IT):** It is the IT’s job to provide a detailed list ranking the priority of the risk level of the threats once the current threat and vulnerability pairs are matched and described in detail. From there the IT department will recommend security methods to fix these risks as well as a cost for these solutions. On top of this I would recommend communication to the incident response team discussing how to monitor the network and discuss prevention on new and old risks that may be come up in the future.

**Project Manager (PM):** The PM will oversee the cost, funding’s, and quality of the project are handled correctly. Be aware of who stakeholders are and how they may or may not be infected in this current RMP. And overall follow the scope and boundaries of the projects reassuring the process is on point and time.

**Firm’s Legal Department (LD) -** The legal team will be involved in issues involving fraud, financial loss, policy compliance, insurance, medical care, any legal action that is required will be delt with by the LD.

**Incident response team (IRT) –** Will develop the incident response procedures, guidelines, investigate incidents, work on preventing future incidents, protection of data.

**Proposed Schedule:**

|  |  |
| --- | --- |
| **Project Stage** | **Time It Will Take** |
| Assessment (Pre) | Start: 10/03/21 - 2 weeks |
| Risk Analysis | 1 week |
| Risk management Plan Creation | 4 weeks |
| Risk management Plan implementation | 1 Month |
| Monitoring | 3-4 weeks |
| Assessment (Post) | Finished: 1/14/22 - 2-3 days |

**References**

[**https://www.e-zigurat.com/innovation-school/blog/ceo-coo-cfo-cio-cmo-cto-who-is-who/**](https://www.e-zigurat.com/innovation-school/blog/ceo-coo-cfo-cio-cmo-cto-who-is-who/)

[**https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html**](https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html)

Project part 1 samples 1-8

Project Part 1 Task Document