**Part 2: Risk Assessment Plan**

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

**By: Kaleb Alstott**

**Introduction**

When planning a new risk assessment for Health Network Inc, it is important to remember that a risk assessment plan is a “systematic process of identifying hazards and evaluating any associated risks within a workplace, then implementing reasonable control measures to remove or reduce them” (britsafe). What this is saying is that a risk assessment plan simply identifies which system/assets to protect and gives insight into how to implement control techniques into the possible threats. Our goal with this risk assessment plan is to demonstrate a successful understanding of the companies’ assets at risk and prioritize the risk value to implement a successful mitigation plan to lower all risk levels to a proper residual risk.

**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). With the above risk assessment plan our analysis covers all the items including servers, operating systems, company take home devices, hardware and more listed to ensure a completed project for Health Network Inc.

**Health Network Inc Assets and Activates**

Here we have rearranged Health Network Inc’s, assets and activates in which we need to assess. This diagram is implemented to easily identify the company’s assets and compare them to what activates may cause harm or damage to these assets. This is what we will focus on to mitigate to protect the company’s assets.

|  |  |
| --- | --- |
| **Assets** | **Activates** |
| Hardware – servers, desktop PC, laptops, routers, switches, firewalls | * Company equipment stolen * Hacks/breaches * Human Error |
| Software- OS (operating system), application specifics | * Updates * Service packs * Access control |
| Personal- employees, customers, stockholders | * Single point of failure * Cross training |
| Landscape | * Where you may be located at via earthquakes, tornados, tsunamis, etc. |

**Possible risk threat/vulnerabilities**

Here we have gone ahead and listed out the possible risk threat/vulnerability pairs for the company to identify what our assessment plan needs to implement and where.

* Risk: Loss of company data due to hardware being removed from production systems
  + Vulnerability: data not being backed up properly
* Risk: Loss of company information on lost or stolen company-owned assets, such as mobile devices and laptops
  + Vulnerability: non restricted company assets, can easily access unregulated information
* Risk: Loss of customers due to production outages caused by various events, such as natural disasters, change management, unstable software, and so on
  + Vulnerability: geographically being in disaster areas, lack of stronger management positions, undated and unregulated software and networks that is not properly monitored.
* Risk: Internet threats due to company products being accessible on the Internet
  + Vulnerability: unregulated company products being open source
* Risk: Insider threats
  + Vulnerability: Unprotected data, no protocols, none restricted access, unprotected passwords
* Risk: Changes in regulatory landscape that may impact operations
  + Vulnerability: location of building

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.

**Controls for Threats**

Here we have listed out the possible threats and control techniques to mitigate the loss of the company’s assets.

* Loss of data due to hardware being removed:
  + Controls: Routine database backups should be done regularly. Backups should also be stored on a cloud. Disaster Recovery should be tested frequently at least once every two weeks. Before replacing any hardware there should be a checklist of how to properly store, wipe, and destroy the data on the devices.
* Loss of data due to lost or stolen devices:
  + Controls: All devices should be encrypted with a password rest on the device every 60-90 days. Devices should have appropriate protocols assigned to employee. Devices should also have authentication protocols in place, if possible two factor authentication.
* Loss of customers due to production outages:
  + Controls: There should be in implemented disaster management and recovery plan in case of natural disasters or power outages. All data needs to be backed up properly via third party or cloud that is offsite in case of onsite problems. Software should be updated and patched as frequently as possible.
* Internet threats:
  + Strong password protected/encrypted networks using routers/firewall. Be aware of outsider attacks by training and lesson implementation. Security on all ends of the company should be practiced protecting from internet or outsider threats.
* Insider threats:
  + The insider threats can be prevented by enforcing strict password and account management, regularly monitoring employees’ online actions, and providing the employees with the least privilege protocols. Security Awareness Training should be given to all the employees. Employees should have restricted access to forms of downloading unknown files. Physical security measures such as video surveillance, biometric authentication to server rooms, man traps, and entry logs should be implemented.
* Changes in regulatory landscape:
  + Any new landscape plan needs to be dealt with in a timely manner to prevent multiple changes in the landscape. Possible thinking upon relocation if landscaping is causing a sever problem.

**Risk Analysis**

After performing an in-depth assessment of the qualitative and quantitative data for the company’s possible risk, threat, and vulnerabilities we have come up with a risk assessment chart. In this chart we have identified the occurrence in which a risk may happen annually, the risk impact level, and finally the importance of the risk. The risk importance rank will be from a 1-10 identifying the least important risk at 1 and the most important risk at 10. The risk impact levels will be identified as low, medium, high, and critical meaning of the severity of the risk at hand. The highest impact level being critical, meaning this risk will cause the most damage, and the lowest being low meaning the risk will cause low to no damage. The risk level will overall take into consideration of the annual occurrence and the risk impact to form a single number to identify the seriousness of a risk.

|  |  |  |  |
| --- | --- | --- | --- |
| **Risks, Threats, and Vulnerabilities** | **Probability of Occurrence Annually** | **Risk Impact Level** | **Risk Importance Rank**  **(1 Least Worry – 10 High Importance)** |
| **Loss of data due to hardware being removed** | **10%** | **Low** | **3** |
| **Loss of data due to lost or stolen devices** | **25%** | **High** | **7** |
| **Loss of customers due to production outages** | **40%** | **Critical** | **9** |
| **Internet threats:** | **70%** | **Critical** | **10** |
| **Insider threats** | **18%** | **Medium** | **6** |
| **Changes in regulatory landscape** | **10%** | **Low** | **1** |

After looking over the risk assessment chart our next goal would be to assign each risk with a project team or individual to assure the risks are being dealt with correctly. For each of the risks available we have a handful of approaches to mitigate the risk as best as we can. Our approaches to the risks our

* Avoid- eliminate the threat by eliminating the cause of it.
* Mitigate- Identify possible ways of reducing the impact of the risk as close to 0% as we can
* Accept- nothing will be done. You have accepted the risk and loss.
* Third party/Transfer- another party will be transferred the responsibility of the risk

For each risk that will be dealt with, these techniques will help our teams or individuals to reduce or prevent the probability of said risk occurring again. For each project dealt with it is key for employees to document and to continue monitoring these risks. Continuous monitoring can help your company catch possible threats and fix risks easier and more frequently if you are staying up to date with your technology and assets. It is key for these roles to continue monitorization to mitigate these risks as the company’s life cycle goes on.

**Risk Assessment Schedule**

The below the schedule is in order from the most relevant threat that is ranked highest on our risk assessment chart down to the lowest threat and the time it would take each project.

|  |  |
| --- | --- |
| **Risks, Threats, and Vulnerabilities** | **Time (Starting today 10/24)** |
| Internet threats | 1-2 months |
| Loss of customers due to production outages | 1-2 months |
| Loss of data due to lost or stolen devices | 2 weeks |
| Insider threats | 2 weeks |
| Loss of data due to hardware being removed | 1 week |
| Changes in regulatory landscape | Take time on each landscape remodeling one at a time. Possibly will take all year but must only have 1 project at a time.  Estimated time per project 2-3 months  Finish date 4/15/22 |

**References**

[**https://www.britsafe.org/training-and-learning/find-the-right-course-for-you/informational-resources/risk-assessment/**](https://www.britsafe.org/training-and-learning/find-the-right-course-for-you/informational-resources/risk-assessment/)

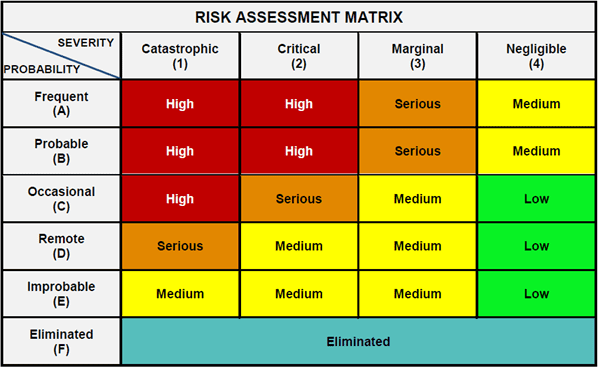
**<https://www.e-zigurat.com/innovation-school/blog/ceo-coo-cfo-cio-cmo-cto-who-is-who/>**

[**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

Writing assignment part 2



<https://sageshield.com/services/conducting-risk-assessment-provide-control-options-for-mitigation-of-risks/>