Tyler Hungerbuhler

Table of Contents

Risk Management Plan Page 1

Risk Assessment Plan Page 6

Risk Mitigation Plan Page 8

Business Impact Analysis Page 12

Business Continuity Plan Page 13

Risk Management Plan

Introduction

The plan includes how the organization will identify and address events or occurrences that could negatively or positively affect the success of a Health Network. Health Network, Inc has three corporate facilities located at Minneapolis Minnesota, Portland Oregon, and Arlington Virginia. With a nearby datacenter operated by a third-party data center hosting vendor. Health Network’s products are HNetExchange, HNetPay, and HNetConnect.

Threat vulnerability pairs (with costs)

|  |  |  |  |
| --- | --- | --- | --- |
| Risk | Threat | Vulnerability | Cost |
| 1 | Internal and/or external actors removing hardware losing/compromising company data. | lack of security of data centers. | Untangible because data that is lost that can’t be recovered and fines can be imposed for noncompliance. |
| 2 | Internal and/or external actors losing/compromising company data from lost devices. | Lack of GPS tracking. | the cost of replacing lost devices. |
| 3 | Internal and/or external actors losing/compromising company devices. | Lack of remote wiping of devices. | Untangible because data that is lost that can’t be recovered and fines can be imposed for noncompliance. |
| 4 | Natural disasters and other data center outages causing the shutdown of production servers. | Lack of Hot or Mobile sites to retain some operating production servers, ALE can increase if outages occur if availability if less than 99.999 of the year (up to 5 minutes, 15 seconds of unexpected downtime) achieving 99.9999 is better if the previous level of availability is achieved. | The next contract will not signed and that customer will be lost to another provider. |
| 5 | External actors from the Internet. | Lack of security and or server logs, IPS, IDS, Input Validation, Firewall Removing or changing defaults, Reducing the attack surface, keeping systems up to date, installing antivirus software, backups of servers and devices. | Untangible because data that is lost that can’t be recovered, fines can be imposed for noncompliance, the customer will be lost to another provider. |
| 6 | Internal actors from employees. | Lack of security and or server logs, surveillance of offices, Access control management. | Untangible because data that is lost that can’t be recovered, fines can be imposed for noncompliance, and the cost of replacing lost devices. |
| 7 | Changes in laws. | Lack of a team dedicated to managing compliance. | Fines can be imposed for noncompliance. |
|  | | | |

Recommendations to reduce each threat vulnerability pair (with costs)

|  |  |  |
| --- | --- | --- |
| Risk | Recommendation | Cost |
| 1 | Add a lock on production systems and server room should require authentication card. | Less than $100 per lock. |
| 2 | Provide a lock for laptops when it is not being used and implement gps tracking of all devices | Less than $30 per lock and less than $100 per device for Cell phone service for tracking. |
| 3 | Implement remote data wiping of lost devices. | Software that can wipe a device costing less than $10 per device. |
| 4 | Create Hot or Mobile sites to retain some operating production server and it can be done by making partnerships with other organizations, creating one for only Health Network, or with another third part data centre. | Creating one can cost hundreds of thousands to millions of dollars, partnering with another company is cheaper around hundreds of thousands. |
| 5 | Implement security and/or server logs on all devices, IPS, IDS, Firewall, Input Validation, Removing or changing defaults on devices and accounts, Reducing the attack surface, keeping systems up to date, installing antivirus software, backup servers and devices. | An IT team is required to review and keep the network protection active and effective; the hardware can cost thousands of dollars. |
| 6 | Implement security and/or server logs on all devices, surveillance of offices and employees, Access control management (account management and enforcement). | An IT team is required to review logs (requiring personnel costs), Security teams reviews surveillance data, User admin manages access control of all systems and data. |
| 7 | Create a team dedicated to managing compliance and giving recommendations to keep compliant. | A team of lawyers is required so costs can vary from thousands to hundreds of thousands. |
|  | | | |

Scope and Stakeholders

This document is to mitigate, manage, and eliminate the following threats on HNetExchange, HNetPay, HNetConnect

Stakeholders of this project include System Administrators, Systems security or Privacy engineer, CAO, CCO, Information owner or Steward, Senior agency official for privacy, Web development head, Third-party data center hosting vendors (System Owner)

Relevant Compliance laws

This is a list of relevant laws and regulations that Health Network must follow to remain in operation in the US. This this is not inclusive all current laws that must be followed, but it is a list of laws to start from when drafting policies, procedures, guidelines, and standards.

HIPAA, PCI DSS, The Durbin Amendment, IRS Mandate (Section 6050W), PA-DSS, CCPA, CPRA, CalOPPA, ADA

Plan of Action and Milestone

|  |  |  |
| --- | --- | --- |
| Risk | Tasks | Assigned member |
| 1 | Identify threats, vulnerabilities, recommendations and implement the recommendations. | System Owner |
| 2 | Identify threats, vulnerabilities, recommendations and implement the recommendations. | Systems security or Privacy engineer |
| 3 | Identify threats, vulnerabilities, recommendations and implement the recommendations. | System Administrators |
| 4 | Identify threats, vulnerabilities, recommendations and implement the recommendations. | System Administrators |
| 5 | Identify threats, vulnerabilities, recommendations and implement the recommendations. | System Administrators |
| 6 | Identify threats, vulnerabilities, recommendations and implement the recommendations. | System Administrators |
| 7 | Identify threats, vulnerabilities, recommendations and implement the recommendations. | CCO and Information Owner |
|  | | | |

Risk Assessment Plan

Scope

This document is to mitigate, manage, and eliminate the following threats on HNetExchange, HNetPay, HNetConnect.

Critical areas

Things that are needs for the organization to run are Electricity, Internet, Web server, Database server, Internet firewall, IPS, IDS, personnel, production servers, corporate laptops and devices.

Stakeholders

System Administrators, Systems security or Privacy engineer, CAO, CCO, Information owner or Steward, Senior agency official for privacy, Web development head, Third-party data center hosting vendors (System Owner).

Type

This will be a Qualitative and Quantitative risk assessment; Risk 1, 3, 5, 6, and 7 are Qualitative because the trust and customers lost is intangible. Risk 2 and 4 are Quantitative because they deal with the replace assets that have a SLE and can be put into an ALO.

1. Risk 1. Probability is medium, and Impact is very high
2. Risk 2. SLE is around $1000, ARO is around 12, ALO is around $12, 000
3. Risk 3. Probability is medium, and Impact is low
4. Risk 4. SLE is in the millions, ARO is around 2-3 times, ALO is in the multi-millions
5. Risk 5. Probability is very high, and Impact is very high
6. Risk 6. Probability is medium, and Impact is very high
7. Risk 7. Probability is high, and Impact is very high

Best Practice

Teams should always have the required number of members as much as possible, with the right experience. A risk assessment should be done regularly with the same methodology. All controls should block anything not required for normal operations and if exceptions need to be made, they must only be for a limited amount of time, and then blocked to prevent a vulnerability in security.

Asset Identification

* 1000 production servers; Owned by third party
* Products HNetExchange, HNetPay, and HNetConnect; Owned by Health Network
* Security to protect the servers form the internet; Owned by third party
* 650 company-issued laptops and mobile devices; Owned by Health Network
* Health Network website and IP; Owned by Health Network
* 600 employees; Employees of Health Network
* 3 corporate locations across the US; Owned by Health Network

Risk Mitigation Plan

Identified Threats

HNetExchange, HNetPay, and HNetConnect all must be resilient enough to protect them from the following threats: Tornadoes, Hurricanes, Earthquakes, Blackout, Blackhat hacker, DoS and DDoS attack, Port scanning, Session hijack, SYN flooding and attack, Spoofing or Poisoning MAC addresses, SQL injection, man-in-the-middle attack, Social Engineering, Automated Running of Scripts without Malware/Virus Checks, Smurf attack, Ping flooding attack, URL poisoning, Cross-Site Scripting attack

Identified Vulnerabilities

HNetExchange, HNetPay, and HNetConnect all must built to prevent the use of the following vulnerabilities from being exploited: Telnet, SMTP, TFTP, HTTP, WEP, WPA, FTP, lack of access control (account management and enforcement), weak passwords, lack of 2 factor authentication, communication methods of executives and security managers on public facing websites. Lack of encryption on files, poorly configured firewalls, insecure Wi-Fi access points which use default settings, Operating System vulnerabilities, lack of file and information encryption when not in use or being transmitted, Admin Privileges for accounts who do not need Admin Privileges.

Identified Exploits

HNetExchange, HNetPay, and HNetConnect all must be resilient enough to protect them from the following exploits: Trojan, Spyware, Virus, Worm, Ransomware, Botnet, Hidden Backdoor Programs.

Current vs result of planned control of each risk

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  |  | **Impact** | | | | | |  |  | 1=Very low | 2=Low | 3=Medium | 4=High | 5=Very high | | **Likelihood** | 5=Very high | 5 | 10 | 15 | 20 | 25(Pre 5) | | 4=High | 4 | 8 | 12 | 16 | 20(Pre 4,7) | | 3=Medium | 3 | 6(Pre 3) | 9 | 12(Pre 2) | 15(Pre 1,6) | | 2=Low | 2(Post 2,3) | 4(Post 5) | 6 | 8 | 10 | | 1=Very low | 1(Post 4,7) | 2(Post 1,6) | 3 | 4 | 5 |   Legend:   |  |  | | --- | --- | |  | Risks can be accepted; contingency plans may be developed. | |  | Risks cannot be accepted, a risk response strategy should be developed (avoid, reduce, transfer/ share) | |  | Unacceptable – immediate risk reduction or avoidance response | |  | Risk appetite | |

Procedural controls

Risk 1. Implement policies and procedures for Authentication and Identification of personnel, Get bonding insurance

Risk 2. Implement policies and procedures for Locking device and don’t leave it unattended, Get bonding insurance

Risk 3. Implement policies and procedures for Locking device and don’t leave it unattended, Get bonding insurance

Risk 4. Get Insurance for equipment and buildings

Risk 5. Implement policies and procedures for reviewing logs, Encryption, changing defaults of all devices, Reducing the attack surface, keeping systems up to date, installing and maintaining antivirus software, and backing up servers and devices,

Risk 6. Implement policies and procedures for reviewing logs, Authentication, and Identification of personnel

Risk 7. Create group that monitors for new laws and once those laws pass, they make changes in the policies and procedures

Technical controls

Risk 1. N/A

Risk 2. Implement GPS tracking of devices

Risk 3. Implement Session time-out, Remote wiping, and GPS tracking of devices, backups of devices

Risk 4. Monitor production servers and switch to external site at the sign of trouble, backups of servers

Risk 5. Implement security, server, system, and audit logs, Encryption of data at rest and transmitted, changing defaults of all devices, Reducing the attack surface, keeping systems up to date, installing antivirus software, backups of servers and devices, creating Input Validation for all fields

Risk 6. Implement Logon identifier, Session time-out, security, server, system, and audit logs

Risk 7. Monitor production servers and company devices to ensure compliance with laws

Physical controls

Risk 1. Implement Locks and keypads on doors, access logs, and closed-circuit television

Risk 2. Use locks

Risk 3. Use locks

Risk 4. Create or partner with other Hot or Mobile sites

Risk 5. Implement IPS, IDS and Firewall

Risk 6. Implement Locks and keypads on doors, access logs, and closed-circuit television

Risk 7. N/A

Business Impact Analysis

Scope & Critical business functions

HNetExchange, HNetPay, and HNetConnect are the products coved in this analysis.

HNetExchange must be as resilient as possible because it is the primary revenue source of Health Network, Inc and it is likely to hold HIPPA protected information.

Critical Resources

These are the resources needed to conduct businesses operations for customers. HNetExchange, HNetPay, and HNetConnect all require these resources.

* Internet access
* Web server
* Web application
* Databases
* Network connectivity between servers
* Firewall, IDS and IPS on the Internet side of the DMZ and IDS, IPS on the LAN side of the DMZ
* Power
* Heating and air-conditioning

Maximum acceptable outage (MAO) and Impact

HNetExchange: MAO: 30 minutes. In addition, any outage will have an almost immediate massive negative impact on the business relationship with customers.

HNetPay: MAO: 12 hours. In addition, if the outage lasts more than a day, it will have a negative impact on the business relationship with customers.

HNetConnect: MAO: 24 hours. In addition, if the outage lasts more than a day, it will have a minor negative impact on the business relationship with customers.

Recovery Requirements

HNetExchange: RTO: 20 minutes, RPO: 99.99999% of data must be recovered.

HNetPay: RTO: 10 hours, RPO: 99.999% of data must be recovered.

HNetConnect: RTO: 20 hours, RPO: 99.99% of data must be recovered.

Business Continuity Plan

Assumptions and Planning Principles

Assume operations under Business Continuity Plan (BCP) need to continue for at least a few days to a week. A hot or warm site must be prepared for the usage of BCP in the days before the expected disaster with some parts of the site ready to implement the plan in an hour or less with the rest of the site following soon after. Backup resources should be staged nearby the site and additional personal on call to help with managing business functions. This provides for business operation to continue during and after nearly any disaster, including natural disasters and attacks against Heath Network. Incident response teams must monitor how the disaster or attack is progressing and manage the remaining resources to keeping only the most critical systems online. Data that is at risk of being damaged should have addition protection added depending on the disaster type.

System description and architecture

Systems and products that are to remain operational should be prioritized with remaining resources are. Any systems and data not being used should be protected by any means available so that the systems and data can be recovered and used.

The following is systems and products that are to be prioritized: HNetExchange, Communications between disaster incident response teams and employees distributing resources, Internet links between Health Network and its customers.

Notification and activation phase

A BCP coordinator declares the notification and activation phase as soon as possible. If the disaster or attack is already occurring the incident response teams must meet and coordinate actions, but if it likely to occur the plans must be implemented for the coming disaster. The plans must be implemented as quickly as possible, and communication should occur in the planned communication method.

Recovery phase

Following the end of the Disaster or attack systems must be restored to operational status, this can take from weeks to months, but plans should have it limited to a couple of weeks at most. The recovery priority is as follows HNetExchange, HNetPay, then HNetConnect. System damage should be documented during disaster or attack so only the damaged systems and data need to be replaced or recovered instead of the whole system and its data. The Recovery Goal is for all systems to be restored to pre-disaster operation status within two weeks with HNetExchange being fully restored within days or less of the disaster.