**Final Course Project: Risk Management Plan**

Alice Mace

Cybersecurity, Bellevue University

CYBR 610: Risk Management Studies

Professor Erich Krueger

November 18, 2022

[TABLE OF CONTENTS](#_Toc118668102)…………………………………………………………………………………………….2

**RISK MANAGEMENT PLAN**……………………………………………………………...……….………………3

Introduction…………………………………………………………………………………………….……3

Scope………………………………………………………………………………………………………..3

Laws & Regulations………………………………………………………………………………………..4

Roles & Responsibilities…………………………………………………………………………………..6

Schedule……………………………………………………………………………………………………6

**RISK ASSESSMENT & MITIGATION PLAN**…………………………………………………………………….7

Introduction………………………………………………………………………………………………….7

Scope………………………………………………………………………………………………………..7

Risk Analysis Overview……………………………………………………………………………………8

Risk Mitigation Overview…………………………………………………………………………………..9

Risks/Mitigations………………………………………………………………………………………….12

Roles & Responsibilities………………………………………………………………………………….21

Process…………………………………………………………………………………………………….21

**BUSINESS IMPACT ANALYSIS**…………………………………………………………………………………23

Overview…………………………………………………………………………………………………...23

Purpose…………………………………………………………………………………………………….23

System Description……………………………………………………………………………………….24

BIA Data Collection……………………………………………………………………………………….25

Process & System Criticality…………………………………………………………………...25

Outage Impacts………………………………………………………………………………….26

Estimated Downtime……………………………………………………………………………27

Resource Requirements……………………………………………………………………….28

Recovery Priorities……………………………………………………………………………..29

**BUSINESS CONTINUITY PLAN**…………………………………………………………………………………31

Purpose/Scope……………………………………………………………………………………………31

Recovery Priorities………………………………………………………………………………………..31

Relocation Strategies…………………………………………………………………………………….32

Recovery Phases…………………………………………………………………………………………32

Disaster Occurrence…………………………………………………………………………….32

Plan Activation…………………………………………………………………………………...33

Alternate Site Operation………………………………………………………………………..33

Transition to Primary Site………………………………………………………………………33

Records Backup…………………………………………………………………………………………..33

Restoration Plan…………………………………………………………………………………………..33

Recovery Teams………………………………………………………………………………………….34

Testing Recovery Procedures…………………………………………………………………………...34

**REFERENCES**……………………………………………………………………………………………………...36

**RISK MANAGEMENT PLAN**

**Introduction**

A risk management plan identifies and addresses potential risks for an organization and assists in determining mitigation efforts, cost, and procedures for integrating improvements to the organization. (Gibson, 2020) Health Network, Inc is a health services organization headquartered in Minneapolis, Minnesota with two additional locations in Portland, Oregon and Arlington, Virginia. They have experienced some issues with data loss and the senior management has requested an update to their risk management plan.

The purpose of this plan is to ensure security of data and compliance with Health Insurance Portability and Accountability Act (HIPAA) regulations. This plan will review applicable laws and regulations, identify roles and responsibilities, define schedule, identify threats and vulnerabilities, detail risk reduction/mitigation recommendations, develop a Business Impact Analysis (BIA), and outline a Business Continuity Plan (BCP).

**Scope**

In line with the purpose of this plan to ensure Health Network’s security of data and compliance with HIPAA, the scope includes identifying key data to protect; data storage, use, and collection; hardware/software security; and secure payment information. Stakeholders for this project include Health Network’s Senior management, Chief Information Officer (CIO), and data center managers. It will focus specifically on the three services Health Network manages: HNetExchange, HNetPay, and HNetConnect. HNetExchange primarily handles secure medical messages between various customers and clinics. HNetPay assists customers in billing and payments. HNetConnect is a directory of doctors, clinics, and medical facilities for customers to research doctors for their care.

**Laws & Regulations**

* Health Insurance Portability and Accountability Act (HIPAA) – “A U.S. law passed in 1999 that mandates the protection of health information.” (Gibson, 2020)
* Payment Card Industry Data Security Standard (PCI DSS) – “An international standard used to protect credit card data whose requirements are set by the PCI Security Council.” (Gibson, 2020)
* General Data Protection Regulation (GDPR) – “A legal framework that sets guidelines to collect and process the personal information of individuals who live in the EU and the European Area.” (Gibson, 2020)
* Control Objectives for Information and Related Technology (COBIT) – “A framework of good practices for IT management and governance and helps link business goals with IT goals.” (Gibson, 2020)
* International Organization for Standardization (ISO) 27002 – “A set of guidelines and principles used for security management derived from the British Standard 7799. It includes practices related to security policy, organization of information security, asset management, human resources security, physical and environmental security, access control, incident management, business continuity, and compliance.” (Gibson, 2020)
* Health Information Technology for Economic and Clinical Health (HITECH) Act – “An act enacted in 2009 expands HIPAA, and provides certain health IT compliance standards for the adoption of electronic health records (EHR).” (Symplr, n.d.)
* CMS Interoperability and Patient Access Final Rule – “The Interoperability and Patient Access final rule (CMS-9115-F) put patients first by giving them access to their health information when they need it most, and in a way, they can best use it. This final rule focused on driving interoperability and patient access to health information by liberating patient data using CMS authority to regulate Medicare Advantage (MA), Medicaid, Children's Health Insurance Program (CHIP), and Qualified Health Plan (QHP) issuers on the Federally-facilitated Exchanges (FFEs).” (Policies and Technology for Interoperability and Burden Reduction | CMS, n.d.)
* Hospital Price Transparency – “This helps Americans know the cost of a hospital item or service before receiving it. Starting January 1, 2021, each hospital operating in the United States will be required to provide clear, accessible pricing information online about the items and services they provide in two ways: 1. As a comprehensive machine-readable file with all items and services. 2. In a display of shoppable services in a consumer-friendly format.” (Hospital Price Transparency | CMS, n.d.)

**Roles & Responsibilities**

The HR department is responsible for identifying health information held by Health Network, all health information sources, existing HIPAA policies currently in place and awaiting implementation, recommended solutions, and costs associated with implementation, potential risks/fines if not in compliance, and inspection results for all data sources regarding HIPAA compliance.

The IT department is responsible for identifying all hardware health data is stored on or could be accessed through, identifying access controls to get to the data, recommended solutions and cost associated with their implementation, and implementing the solutions in conjunction with HR at each data center once the solution has been chosen by senior management and the CIO.

All management and personnel are to make known any issues or concerns regarding recommended solutions or implementation and will assist in the implementation once decided upon, as necessary.

**Schedule**

Weeks 1-3 – Study foundations and research risk management

Week 4 – Generate outline and planning portions

Week 5 – Assess, identify, and rank risks

Weeks 6-7 – Determine risk mitigations, implementation, roles, and timelines

Weeks 8-10 – Develop BIA and BCP

Weeks 9-12 – Finalize risk management plan

**RISK ASSESSMENT & MITIGATION PLAN**

**Introduction**

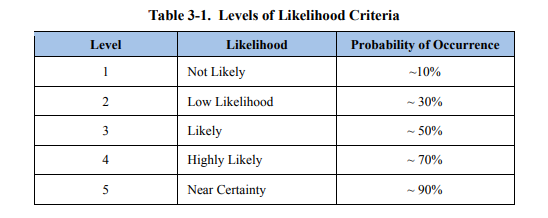
A risk assessment is “a process used to identify and evaluate risks based on an analysis of threats and vulnerabilities to assets. Risks are quantified based on their importance or impact severity. These risks are then prioritized.” (Gibson, 2020) Mitigations are put in place for each risk/vulnerability, as applicable. “Mitigation is also known as risk reduction. Vulnerabilities are reduced by implementing controls, or countermeasures.” (Gibson, 2020) The purpose of this plan is to identify, assess, rate risks, and provide mitigation strategies based on their likelihood of occurrence and consequence to Health Network. Rating criteria and matrices will use the Department of Defense Risk Management Guide for Defense Acquisition Programs model, as shown in the Threats and Vulnerabilities section below.

**Scope - Assets, Activities, & Controls**

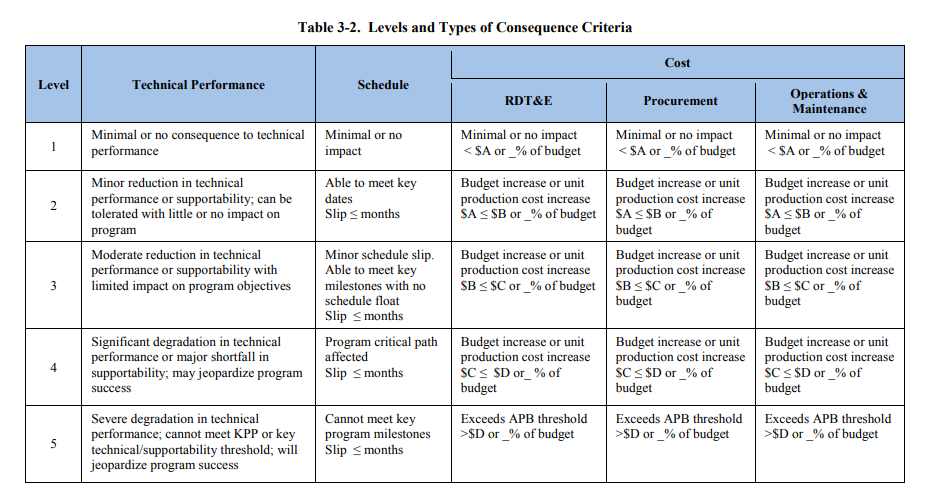
This plan will focus specifically on threats and vulnerabilities regarding the three services Health Network manages: HNetExchange, HNetPay, and HNetConnect. A qualitative risk assessment will be performed, which is defined as “a subjective method used for risk assessment that uses relative values based on opinions from experts.” (Gibson, 2020) Hardware vulnerabilities, such as laptops and mobile devices, and their configurations, connections with networks, and physical handling will be detailed in this plan. Potential risks to new or non-compliant policies and activities of Health Network employees will also be assessed. Risk mitigations have been added and will be implemented into Health Networks processes and procedures. Mitigations will not change the consequence rating of risks, but may reduce the likelihood of occurrence.

**Risk Analysis Overview**

“Risk analysis is the activity of examining each identified risk to refine the description of the risk, isolate the cause, and determine the effects to aid in subsequent risk mitigation. It refines each risk in terms of its likelihood and consequence, and its relationship to other risk areas or processes.” (Department of Defense, 2014) The tables below define the criteria that will be used in rating the risks for Health Network. Once each risk has been assigned a likelihood and consequence, it will be depicted in the matrix at the end of this section. “Risk likelihood is the assessed probability that a risk event will occur given existing conditions.” “When assessing the consequence magnitude, the program team evaluates each risk as if it were going to occur. The impact is assessed qualitatively on a scale of 1 to 5, using the guidelines in the table.” (Department of Defense, 2014)



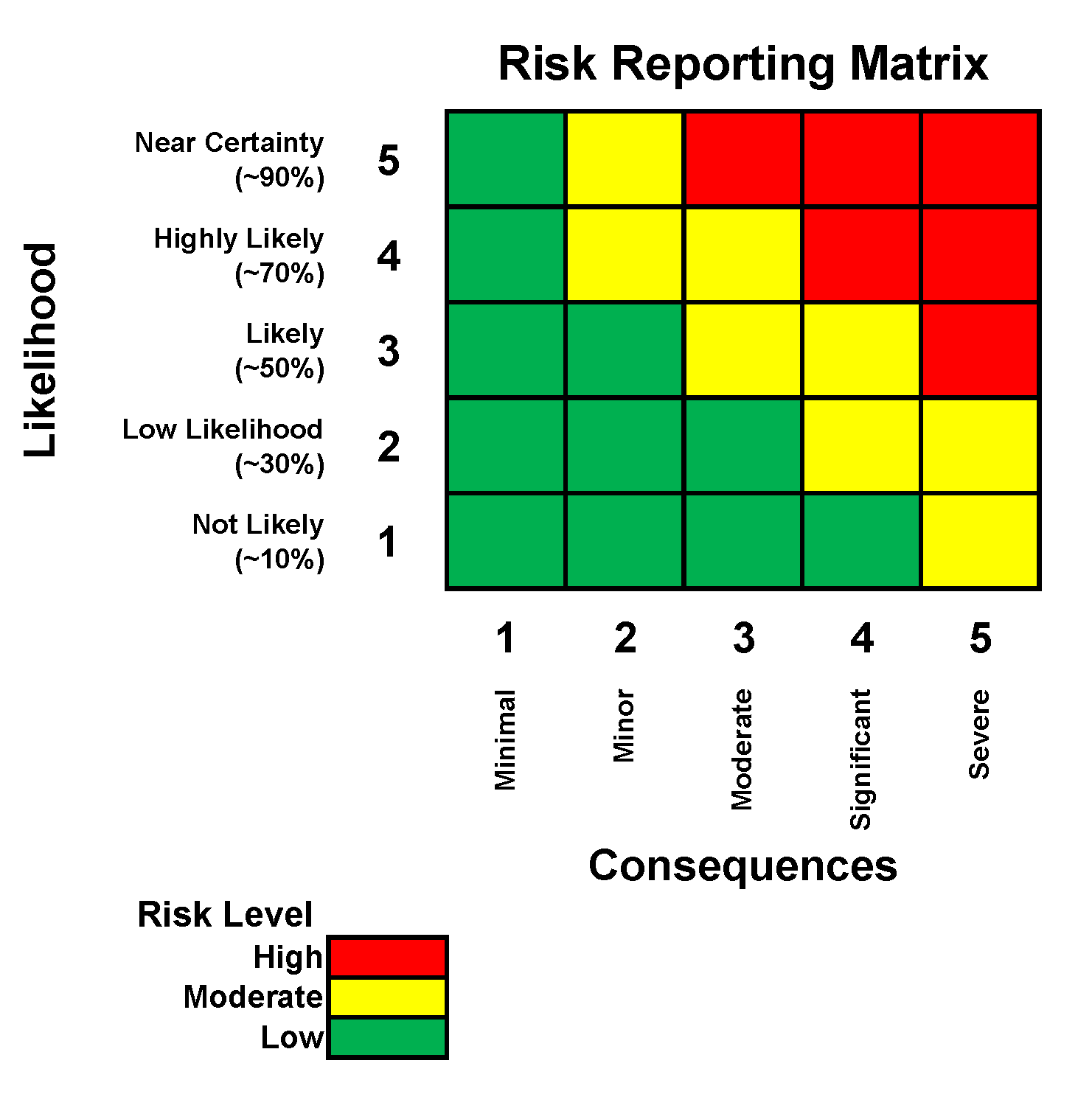
(Department of Defense, 2014)

****(Department of Defense, 2014)

**Risk Mitigation Overview**

“Risks can be characterized as high, moderate, or low based on rating thresholds. Risk mitigation incorporates a strategic approach to addressing risks. A risk mitigation approach answers the question, *What is the plan?*” (Department of Defense, 2014) The below table and matrix depict the mitigated risk ratings for each risk/vulnerability identified to Health Network. A detailed description of the risks and their mitigation strategies is in the following section.

|  |  |
| --- | --- |
| **Risk** | **Mitigated Risk Rating** |
| 1. Loss of Company/Patient Data |  |
| 1a. Hardware being removed from production systems | LOW |
| 1b. Lost or stolen company-owned assets | MODERATE |
| 1c. Misconfiguration of devices | LOW |
| 2. Loss of customers due to production outages |  |
| 2a. Natural disasters | LOW |
| 2b. Change management | LOW |
| 2c. Unstable software | LOW |
| 3. Internet threats due to company products being accessible on the Internet |  |
| 3a. Payment information | MODERATE |
| 3b. PII/PHI | MODERATE |
| 4. Insider threats |  |
| 4a. Intentional release/sharing of PII/PHI | MODERATE |
| 4b. Intentional interruption of services | MODERATE |
| 5. Changes in regulatory landscape that may impact operations |  |
| 5a. New policies | LOW |
| 5b. Network administration | LOW |



**1b 3a**

**5a**

**3b**

**1c**

**2a 5b**

**1a 2c**

**4a 4b**

**2b**

**Mitigated Risk Ratings**

**Risks/Mitigations:**

1. Loss of Company/Patient Data
   1. Hardware being removed from production systems – When assets have to be disconnected from the system for repairs or software updates, it can cause problems and patient data could be lost. The consequence of this could pose a moderate risk to the company due to patient data being lost; there is a low likelihood that this could occur. The unmitigated rating of this risk is LOW.

As a preventative measure, all patient data, medical messages, and payment information will be backed up on an external drive before any planned system outages or hardware replacements occur. This reduces the likelihood of patient data being lost due to hardware being removed from production systems to NOT LIKELY.

Estimated costs to implement this mitigation is approximately $1k per site for the hard drives and labor.

* 1. Lost or stolen company-owned assets (such as mobile devices and laptops) – Employees may take or keep devices even after employment with Health Network has ceased. The consequence of these assets being taken and unauthorized access or data being released could pose significant risk to the company; it is likely that this could occur. The unmitigated rating of this risk is MODERATE.

All company-owned devices must be returned upon out processing from Health Network. The company has the right to involve law enforcement to obtain possession of their devices and/or withhold the employees last paycheck until all company owned devices are returned. This reduces the likelihood of employees keeping company owned devices and the risk of unauthorized access or data being released from them to a LOW LIKELIHOOD.

There is no immediate cost associated with implementing this mitigation, only policy change. Potential legal fees should be taken into account and fees for a retainer should be available of a minimum of $5k.

* 1. Misconfiguration of devices - If devices are not configured to a defined security policy regarding software, virus/malware protection, and accessibility, it could introduce greater risk of compromise and loss of data. The consequences could pose significant risk to the company; it is likely that this could occur. The unmitigated rating of this risk is MODERATE.

A security policy will be developed and implemented for all company owned devices. Updates will be installed regularly to ensure compliance with the latest standards in accordance with the policy. Accessibility will be limited to content applicable to Health Network and its services. The implementation and upkeep of the security policy lowers the likelihood of occurrence to NOT LIKELY.

Estimated costs for implementing this control is primarily associated with monitoring and obtaining updated software and is approximately $5k annually.

1. Loss of customers due to production outages
   1. Natural disasters – Winter storms are common in all three of Health Network’s locations. These could cause power outages and potential hardware failures resulting in the loss of customers due to services not being available. The consequence of this could pose minor risks to the company; there is a low likelihood that this could occur. The unmitigated rating of this risk is LOW.

Health Network will install Uninterruptable Power Supplies in their server rooms that provide online access to customers. They will also have backup servers that can substitute if a server fails to maintain customer access. This reduces the likelihood of customer loss to NOT LIKELY.

Estimated costs to implement this mitigation for uninterruptible power supplies and servers is approximately $3k per location.

* 1. Change management – Hardware or software changes and updates could require the system to be offline for a period of time. The consequence of this could pose minor risk to the company by loss of customers due to services not being available; it is likely that this could occur. The unmitigated rating of this risk is LOW.

Backup servers will be utilized, when possible, to maintain access for customers. If this is not possible, outages will be scheduled and socialized with all customers holding accounts on any of Health Network’s services informing them of the outage and when services are expected to return. This reduces the likelihood of customer loss to NOT LIKELY.

If other mitigations are implemented that cover the cost of servers, then there is no additional cost associated with this mitigation. Otherwise, it is estimated to cost approximately $1k per site.

* 1. Unstable software – Software not thoroughly tested out or that does not have patches implemented could cause an outage due to failure. The consequence of this could pose a moderate risk to the company by loss of customers due to services not being available; there is a low likelihood that this could occur. The unmitigated rating of this risk is LOW.

The security policy will document approved software types authorized for all Health Network devices. It will also identify patches or updates and provide a timeframe they will be put in place once made available. This reduces the likelihood of customer loss to NOT LIKELY.

There is no cost associated with the security policy but the estimated cost for identifying patches/updates and incorporating them is approximately $5k annually. This cost may be covered in other mitigations, if implemented.

1. Internet threats due to company products being accessible on the Internet
   1. Payment information – If the HNetPay is breached it could allow the release of client’s payment methods and other information. The consequence of this could pose significant risk to the company; it is likely that this could occur. The unmitigated rating of this risk is MODERATE.

Stored payment information will use encryption algorithms to ensure security of data. Firewalls will also be in place to prevent internet threats from accessing the encrypted data from the servers. This reduces the likelihood of exposure of client’s payment and other private information to a LOW LIKELIHOOD.

The estimated cost for implementing this mitigation to cover firewalls and encryption software is approximately $5k per site.

* 1. PII/PHI – If the HNetExchange is breached it could allow the release of personally identifiable information and/or personal health information. The consequence of this could pose a severe risk to the company; there is a low likelihood that this could occur due to the secure messaging functions in place. The unmitigated rating of this risk is MODERATE.

Stored PII/PHI will use encryption algorithms to ensure security of data. Firewalls will also be in place to prevent internet threats from accessing the encrypted data from the servers. This, in addition to the secure messaging functions already in place, does not change the likelihood of exposure of client’s PII/PHI; it remains a LOW LIKELIHOOD.

The estimated cost for implementing this mitigation to cover firewalls and encryption software is approximately $5k per site. This cost could be covered by other mitigations, if incorporated.

1. Insider threats
   1. Intentional release/sharing of PII/PHI – Insider threats with access to PII/PHI could release this data to cause harm to Health Network. The consequence of this could pose a severe risk to the company; it is not likely that this could occur. The unmitigated rating of this risk is MODERATE.

Employees are aware of consequences of potential loss of job and/or credentials if they intentionally release client PII/PHI as is documented in their HR paperwork and device user agreements. The likelihood of this risk remains as NOT LIKELY.

There is no immediate cost associated with implementing this mitigation. Potential legal fees should be taken into account and fees for a retainer should be available of a minimum of $5k.

* 1. Intentional interruption of services – Insider threats could intentionally inject Health Network systems with a digital attack rendering the network unusable for a period of time. The consequence of this could pose a severe risk to the company; it is not likely that this could occur. The unmitigated rating of this risk is MODERATE.

Administrator privileges are limited to system administrators, preventing general employees from accessing the database in ways that would allow such digital attacks to occur. System administrators are thoroughly vetted before hire and are aware of employment and legal repercussions that could occur if they abuse their access. The likelihood of this risk remains NOT LIKELY.

There are no associated costs with these current mitigations.

1. Changes in regulatory landscape that may impact operations
   1. New policies – If new policies are put in place or enforced that require changes to the system, it could require the system to go offline for a period of time. The consequence of this could pose a minor risk to the company; it is highly likely that this could occur. The unmitigated rating of this risk is MODERATE.

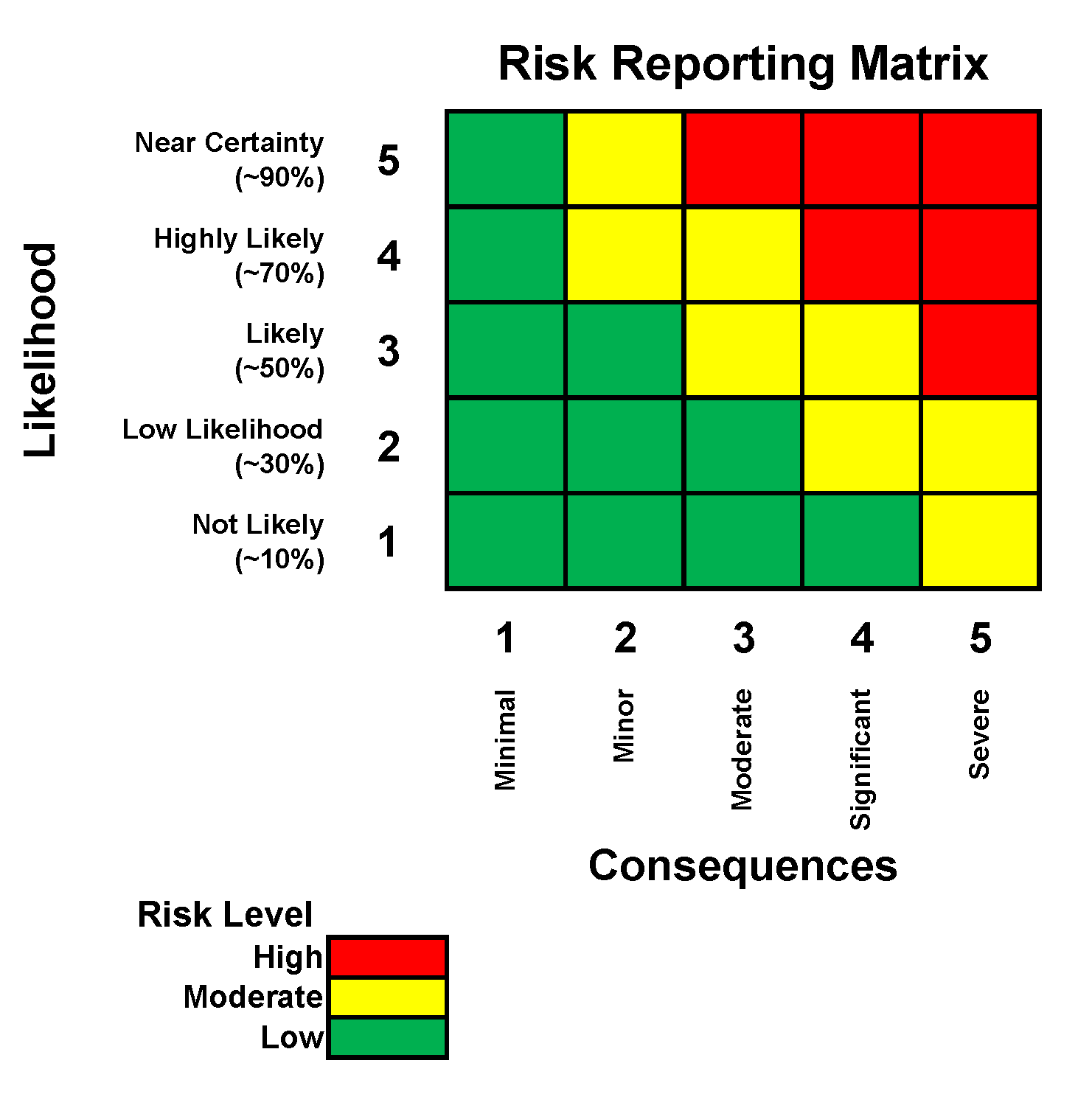
Backup servers will be utilized, when possible, to maintain access for customers. If this is not possible, outages will be scheduled and socialized with all customers holding accounts on any of Health Network’s services informing them of the outage and when services are expected to return. This reduces the likelihood of impact to a LOW LIKELIHOOD.

If other mitigations are implemented that cover the cost of servers, then there is no additional cost associated with this mitigation. Otherwise, it is estimated to cost approximately $1k per site.

* 1. Network administration – If network administrations change or decide to implement new procedures, it could impact the function of Health Network’s systems or potentially require the system to go offline for a period of time. The consequence of this could pose a minor risk to the company; there is a low likelihood that this could occur. The unmitigated rating of this risk is LOW.

Backup servers will be utilized, when possible, to maintain access for customers. If this is not possible, outages will be scheduled and socialized with all customers holding accounts on any of Health Network’s services informing them of the outage and when services are expected to return. This reduces the likelihood of impact to a NOT LIKELY.

If other mitigations are implemented that cover the cost of servers, then there is no additional cost associated with this mitigation. Otherwise, it is estimated to cost approximately $1k per site.



**5a**

**2b**

**1b 1c**

**3a**

**1a 2c**

**2a 5b**

**3b**

**4a 4b**

**Unmitigated Risk Ratings**

**& Mitigation Strategies**

**Roles & Responsibilities**

The HR department is responsible for identifying health information held by Health Network, all health information sources, existing HIPAA policies in place and that need to be implemented, recommended solutions and cost associated with their implementation, potential non-compliance risks/fines, and inspection results for all data sources regarding HIPAA compliance.

The IT department is responsible for identifying all hardware health data is stored on or could be accessed through, identifying access controls to get to the data, recommended solutions and cost associated with their implementation, and implementing the solutions in conjunction with HR at each data center once the solution has been chosen by senior management and the CIO. They are also responsible for communicating if/when any new hardware/software needs to be installed and a management plan for if/how long systems will be down to incorporate it.

All management and personnel are to communicate any additional risks not previously mentioned and/or any factors that could impact the consequence or likelihood of occurrence not captured in their present ratings.

**Process**

* Define scope of assessment – Completed before the start of the assessment and briefed to all participants to identify boundaries
* Identify risks – First phase of assessment. Can be completed in parallel with the next step of analyzing the risk and may be done in multiple meetings/forums. Requires subject matter experts in relevant topics defined in the scope.
* Analyze risks – Second phase. Requires subject matter experts for each relevant topic defined in the scope. Typically where subcategories of risks are determined and can be done in parallel with risk ratings.
* Rate risks (likelihood/consequence) – Third phase. Requires subject matter experts for each relevant topic defined in the scope. Use organization’s definitions of likelihood and consequence. Only identify unmitigated ratings.
* Create Risk Matrix – Fourth phase. Use the rating from the previous step to plot each risk on the matrices and summarize if a high, moderate, or low overall risk rating.
* Mitigation phase – Note strategies and actions that can be implemented to reduce the likelihood of occurrence of each risk. Note changes on the risk matrix.

**BUSINESS IMPACT ANALYSIS**

**Overview**

This Business Impact Analysis (BIA) is developed as part of the contingency planning process for data centers owned by Heath Network, Inc*.* It was prepared on November 6, 2022.

**Purpose**

The purpose of the BIA is to identify and prioritize system components by correlating them to the mission/business process(es) the data centers support, and using this information to characterize the impact on the process(es) if the data centers were unavailable.

The BIA is composed of the following three steps:

1. **Determine mission/business processes and recovery criticality.** Mission/business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime. The downtime should reflect the maximum amount of time that an organization can tolerate while still maintaining the mission.
2. **Identify resource requirements.** Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes and related interdependencies as quickly as possible.  Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records.
3. **Identify recovery priorities for system resources.** Based upon the results from the previous activities, system resources can more clearly be linked to critical mission/business processes. Priority levels can be established for sequencing recovery activities and resources.

This document is used to build the Health Network data center Information System Contingency Plan (ISCP) and is included as a key component of the ISCP. It also may be used to support the development of other contingency plans associated with the system including, but not limited to, the Disaster Recovery Plan (DRP) or Cyber Incident Response Plan.

**System Description**

Health Network’s Arlington office is the primary location for business units, such as Finance, Legal, and Customer Support. Some of the corporate systems, such as the payroll and accounting applications, are located only in the corporate offices. Each corporate facility is located near a co-location data center, where production systems are located and managed by third-party data center hosting vendors. Health Network operates in three production data centers to assist in availability of their products. The data centers host about 1,000 production servers, and Health Network maintains 650 corporate laptops and company-issued mobile devices for its employees. Health Network is currently developing/updating their security plan to encompass backup procedures of the corporate systems and the interconnectedness to all three production center servers for redundancy in case of site outages. Each corporate location can access the other two, and remote virtual private networks (VPNs) exist between each production data center and the corporate locations.

**BIA Data Collection**

**Process & System Criticality**

**Step one of the BIA process** - Working with input from users, managers, mission/business process owners, and other internal or external points of contact (POC), identify the specific mission/business processes that depend on or support the information system.

| **Mission/Business Process** | **Description** |
| --- | --- |
| Customer/Patient data protection | Ensuring HIPAA & PII/PHI law compliance for all customer data |
| Secure messages | Secure electronic medical messages from customers to other organizations |
| Secure billing/payments | Payment processing and billing interactions for customers |
| Online directory | List of doctors, clinics, and other medical facilities for customers to find care locations/providers |

**Identify Outage Impacts and Estimated Downtime**

**Outage Impacts**

The following impact categories represent important areas for consideration in the event of a disruption or impact.

Impact category: Legal

Impact values for assessing category impact:

* Severe = Revocation business license/Legal fees in excess of $1 mil
* Moderate = Fines/Penalties in excess of $500k
* Minimal = Mandated new infrastructure/personnel

Impact category: Cost

Impact values for assessing category impact:

* Severe = Network upgrades/replacements in excess of $1 mil
* Moderate = Network upgrades/replacements in excess of $500k
* Minimal = Network upgrades/replacements less than $500k

Impact category: Customers

Impact values for assessing category impact:

* Severe = Loss of greater than 10%
* Moderate = Loss of greater than 5%
* Minimal = Loss of less than 5%

The table below summarizes the impact on each mission/business process if Health Network’s data centers were unavailable, based on the following criteria:

| **Mission/Business Process** | **Impact Category** | | | |
| --- | --- | --- | --- | --- |
| **Legal** | **Cost** | **Customers** | **Impact** |
| Customer/Patient data protection | Severe | Severe | Severe | Severe |
| Secure messages | Minimal | Moderate | Severe | Moderate |
| Secure billing/payments | Moderate | Moderate | Severe | Moderate |
| Online directory | Minimal | Minimal | Moderate | Minimal |

**Estimated Downtime**

Working directly with mission/business process owners, departmental staff, managers, and other stakeholders, estimate the downtime factors for consideration as a result of a disruptive event.

* **Maximum Acceptable Outage (MAO).**  The MAO represents the total amount of time a system or service can be down before affecting a company’s mission. The MAO directly affects the required recovery time, which means that a system must be recoverable before the MAO time has been reached. (Gibson, 2022)
* **Recovery Time Objective (RTO).** RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD.
* **Recovery Point Objective (RPO**). The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data must be recovered (given the most recent backup copy of the data) after an outage.

The table below identifies the MAO, RTO, and RPO (as applicable) for the organizational mission/business processes that rely on Health Network’s data centers.

| **Mission/Business Process** | **MAO** | **RTO** | **RPO** |
| --- | --- | --- | --- |
| Customer/Patient data protection | 0 hours | 0 hours | 0 hours |
| Secure messages | 12 hours | 2 hours | 1 hours |
| Secure billing/payments | 24 hours | 4 hours | 1 hours |
| Online directory | 48 hours | 24 hours | 12 hours |

**Identify Resource Requirements**

The following table identifies the resources that compose Health Network’s data centers including hardware, software, and other resources such as data files.

|  |  |
| --- | --- |
| **System Resource/Component** | **Description** |
| Production Servers | Hosts all data for Health Network and maintained by third-party venders |
| Customer/Patient Files | Health, personal, and payment information of all customers/clients |
| Virtual Private Networks (VPNs) | Allow for remote connection between production data centers and corporate locations |
| Firewall/Router | Provides protection against potentially harmful data entering or exiting the network |
| Anti-Malware/Anti-Virus | Scans for, identifies, and mitigates potential malware/virus threats in the network |

It is assumed that all identified resources support the mission/business processes identified in the previous section unless otherwise stated.

**Identify Recovery Priorities for System Resources**

The table below lists the order of recovery for Heath Network’s data centers. The table also identifies the expected time for recovering the resource following a “worst case” (i.e., complete rebuild/repair or replacement) disruption.

* **Recovery Time Objective (RTO)** - RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MAO. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MAO.

| **Priority** | **Recovery Time Objective** |
| --- | --- |
| Production Servers | 72 hours to rebuild or replace |
| VPNs | 48 hours to reestablish/secure |
| Firewall/Router | 24 hours to replace if HW/config on site |
| Customer/Patient Files | 12 hours to recover all files |
| Anti-Malware/Anti-Virus | 6 hours to reinstall on all devices |

**BUSINESS CONTINUITY PLAN**

# Purpose/Scope

The purpose of this BCP is to ensure that mission critical elements of Health Network continue to operate after any disruption and will be in place until normal operations are restored. This plan is primarily focused on recovering business operations is access to a facility is unavailable due to weather and/or natural disasters. The current focus is in response to a winter storm affecting access to the Arlington, VA offices.

# Business Function Recovery Priorities

Disaster recovery teams use this strategy to recover essential business operations at an alternate location site. The information system and IT teams restore IT functions based on critical business functions.

| **Mission/Business Process** | **Description** |
| --- | --- |
| Customer/Patient data protection | Ensuring HIPAA & PII/PHI law compliance for all customer data |
| Secure messages | Secure electronic medical messages from customers to other organizations |
| Secure billing/payments | Payment processing and billing interactions for customers |
| Online directory | List of doctors, clinics, and other medical facilities for customers to find care locations/providers |

# Relocation Strategy/Alternate Business Site

An organization uses the alternate business site and relocation strategy in the event of a disaster or disruption that inhibits the continuation of the business processes at the original business site.

With Health Network’s three locations, if one site is down, the other two are able to cover the majority of operations from their location. If network connectivity is still available at any site, VPNs can also be used to access production center data and employees can work remotely in the short term. For longer term facility access issues, a mobile site can be set up near the original office that is down to allow employees to begin integrating into that location. It will likely take 3-5 days for the site to be operational once the best location for set up is determined and all equipment is verified functional.

# Recovery Phases

These are the activities most needed for the business to continue, and the recovery plan should target these essential business functions. The recovery plan should proceed as follows:

## Disaster Occurrence

Health Network CEO or CIO declares a disaster and makes the decision to activate the rest of the recovery plan.

## Plan Activation

During this phase, Health Network BCP Manager puts the business continuity plan into effect. This phase continues until the company secures the alternate business site/operations plan and/or relocates the business operations.

## Alternate Site Operation

This phase continues until Health Network can restore the primary facility

## Transition To Primary Site

This phase continues until Health Network can appropriately move business operations back to the original business site.

# Records Backup

Currently the corporate systems are not being backed up but Health Network is in the process of developing/updating their security plan to encompass backup procedures for corporate and production data centers. There will be servers at all three locations for both the data center and corporate locations to ensure no data is lost even if one facility at a location goes down.

# Restoration Plan

Disaster recovery/IT teams maintain, control, and periodically check on all the records that are vital to the continuation of business operations and that would be affected by facility disruptions or disasters.

Upon restoration of the location to the network, the data centers will sync with the corporate sites and the other locations will be able to access the data generated at the corporate sites during the data center down time. Health Network will work with the third-party organization that manages the data center to ensure routine backups of their servers are conducted. These would be used in the event of a server failure to ensure substantial amounts of data is not lost.

# Recovery Teams

The company establishes recovery teams and divides the participants into appropriate groups based on job role and title. The organization designates a team leader for each team. It assigns a specific role or duty to each remaining member of the team.

## Team Roles

Team Leader, Backup Team Leader, Team Member

## Team Responsibilities

Incident Commander, HR/PR Officer, Information Technology, Finance/Admin, Legal/Contacts

## Departmental Recovery Teams

Business Continuity Coordinator, EOC Communications Team, EOC Human Resources Team, EOC Administration Team, Emergency Response Team, Information Technology Recovery Team

# Testing Recovery Procedures

Health Network at each site will test out their recovery procedures no less than bi-annually. This will include ensuring equipment is functional, individuals are familiar with their roles and responsibilities, and ensuring connectivity from remote or alternate sites functions appropriately. Any issues discovered in testing will be documented and mitigations/repairs will be incorporated and this BCP updated accordingly.

## Overarching Recovery Procedure

* + 1. Disaster Occurrence
    2. Notification of Management
    3. Preliminary Damage Assessment
    4. Declaration of Disaster
    5. Plan Activation
    6. Relocation to Alternate Site
    7. Implementation of Temporary Procedure
    8. Establishment of Communication
    9. Restoration of Data Process and Communication with Backup Location
    10. Commencement of Alternate Site Operations
    11. Management of Work
    12. Transition Back to Primary Operations
    13. Cessation of Alternate Site Procedures
    14. Relocation of Resources Back to Primary Site

**REFERENCES**

Department of Defense. (2014, December). *Department of Defense Risk Management Guide for Defense Acquisition Programs*. www.acqnotes.com. Retrieved October 2, 2022, from https://www.acqnotes.com/wp-content/uploads/2014/09/DoD-Risk-Mgt-Guide-v7-interim-Dec2014.pdf

Gibson, D., & Igonor, A. (2020b). *Managing Risk in Information Systems (Information Systems Security & Assurance)* (3rd ed.). Jones & Bartlett Learning.

*Hospital Price Transparency | CMS*. (n.d.). Retrieved September 25, 2022, from https://www.cms.gov/hospital-price-transparency

Marker, A. (n.d.). *Free Business Continuity Plan Templates*. Smartsheet. Retrieved November 6, 2022, from https://www.smartsheet.com/business-continuity-templates

*Policies and Technology for Interoperability and Burden Reduction | CMS*. (n.d.). Retrieved September 25, 2022, from https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index#CMS-Interoperability-and-Patient-Access-Final-Rule

Symplr, B. (n.d.). *Healthcare Compliance: All You Need To Know | symplr*. Retrieved September 25, 2022, from https://www.symplr.com/blog/healthcare-compliance-all-you-need-to-know#:%7E:text=The%20Health%20Information%20Technology%20for%20Economic%20and%20Clinical,file%20a%20false%20claim%20to%20a%20federal%20payer.