Health Network, Inc Risk Management Plan (Final)

IST 6720 Spring 2022 - Professor Brough

Group Project - Part 5

Shark Attackers: Vasili Krespis, Priyanka Mago,

Daniel Marich, Nnenne Ofoegbu, Inna Tsygankova

May 15, 2022

TABLE OF CONTENTS

1 Introduction

Health Network Inc. is health services organization that has over 600 employees throughout the organization and generates $500 million USD in annual revenue. The organization has three locations and three production data centers that provide high availability across the organization's products. Health Network has three main products: HNetExchange, HNetPay, and HNetConnect.

- HNetExchange 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. HNetExchange is the main source of revenue for this organization.
- HNetPay is a web portal, hosted at Health Network production sites, that accepts various forms of payments and interacts with credit-card processing organizations.
- HNetConnect is an online directory that lists doctors, clinics, and other medical facilities to allow Health Network customers to find the right type of care at the right locations. It contains doctors' personal information, work addresses, medical certifications, and types of services that the doctors and clinics offer.

Information systems, which provide critical support for organizational missions, are a key area of risk management. Having a formal risk management plan is the foundation of effective risk management. Health Network's Risk Management Plan is out of date and a new risk management plan must be developed. The purpose of developing a Risk Management Plan for Health Network Inc. is to update the old Risk Management Plan, bring the organization within compliance and to develop an effective risk management process.

1.1 Scope

Health Network, Inc. is based in Minneapolis, Minnesota, and it has three main products that generate revenue for the organization: HNetExchange, HNetPay, and HNetConnect. The scope of this risk management plan is to create a new plan that updates the outdated risk management plan for all three of the organization's product systems and their associated computer hardware, software, production systems, and interfacing organizational networks across all three corporate office locations and three leased co-location data facilities.

The specifics to be included in the scope of this HealthNet risk management plan are the following items:

1. Product Production Systems for HNetExchange, HNetPay, and HNetConnect.

(a) Mission of HNetExchange system—Secure electronic medical messages.

(b) Mission of HNetPay system—Support the management of secure payments and billing.

(c) Mission of HNetConnect system—Online directory.

2. Organizational Data (Customer and Employee)

3. Production servers (1000 servers located at three colocation facilities)

4. Proprietary Software

5. User Devices (650 laptops and mobile devices)

6. Public-Facing Website (DMZ)

7. Backup and Recovery Systems (hardware, software, and data)

1.2 Roles and Responsibilities

Roles and Responsibilities for this risk management plan include:

- Upper Leadership—Responsible for funds and leadership.
- Chief Executive Officer—Responsible for the organization's success.
- Project Manager—Responsible for leading the team. Monitoring project progress and set deadline.
- HNetExchange system owner—Responsible for the overall operation and maintenance of a system, including any related support service or outsourced service.
- HNetPay system owner—Responsible for the overall operation and maintenance of a system, including any related support service or outsourced service.
- HNetConnect system owner—Responsible for the overall operation and maintenance of a system, including any related support service or outsourced service.
- System Administrators—Responsible for installing, supporting, and maintaining servers or other computer systems, and planning for and responding to service outages and other problems
- Human Resource—Responsible for Monitor the implementation of human resource processes. Adhere to all internal policies and legal standards. Handling people. Applying new policies.
- Chief Information Officer—Responsible for designating a senior information security officer; developing and maintain information security policies,

procedures, and control techniques; overseeing personnel; and assisting senior leaders on all security responsibilities.
- Information Owner—Responsible for statutory, management, or operational authority and the establishment of policies and procedures governing its generation, collection, processing, dissemination, and disposal.
- Senior Information Security Officer—Responsible for carrying out the chief information officer security responsibilities and serving as the primary interface between senior managers and information system owners.
- Information System Owner (ISO)—Responsible for procuring, developing, integrating, modifying, operating, and maintaining an information system.
- Information Security Architect—Responsible for ensuring that the information security requirements necessary to protect the organization's core missions and business processes are adequately addressed in all aspects of enterprise architecture.

2.1 Risk Assessment Plan for Health Network, Inc.

2.1.1 Scope of The Risk Assessment Plan

The scope of this risk assessment is to identify numerous vulnerabilities that have been identified throughout the Health Network organization. This assessment will attempt to identify potential weaknesses and create an action plan to remedy internal issues that have affected all three company product systems (as well as their associated supporting functions). This includes computer hardware, software, production systems, and interfacing company networks across all three corporate office locations (including the three co-location data facilities).

Here are the specifics that are included in the scope of our risk assessment:

- Product Production Systems for HNetExchange, HNetPay, and HNetConnect.
- Company Data (customer and employee)
- Production servers (1000 servers located at the three data center locations)
- Proprietary Software
- User Devices (650 laptops and company mobile devices)
- Public-facing website (DMZ)
- Backup and Recovery Systems (hardware, software, and data)

The goal of the risk assessment is to secure company assets and to help Health Network prepare to manage its security and privacy risks. We can achieve this by working closely with stakeholders to understand the critical business functions better. We will then assess in place controls and create an action plan to minimize vulnerabilities. Furthermore, we will develop a team to respond to and monitor/maintain

risk throughout the system development life cycle. Change management will allow us to prevent unapproved changes thus reducing risks. Let's take a closer look at Health Net's company assets.

2.1.2 Company Assets

We have worked closely with stakeholders to identify assets and critical business functions. The three main assets are Health Networks products: HNetExchange, HNetPay, and HNetConnect. Additional assets include 1,000 production servers at the three data center co-locations, 650 corporate laptops and company-issued mobile devices, company/customer data, proprietary software, physical controls (including DMZ and firewall), as well as the internal network including backup hardware. Let's look at the threats, vulnerabilities, and in place controls.

2.1.3 Vulnerability, Threats, and Controls

Vulnerabilities	Threats	In Place Controls	NIST Control List	Likelihood of Threat Event Occurrence	Likelihood of Threat Event Resulting in Adverse Impacts	CVSS score
Lack of patch management	Bad actors may take advantage of unsecured software.	Automated patch management system	CM-2 (Baseline Configuration)	Very High	Very High	8.6
Public-Facing Website	Bad actors may enter an unsecured system and cause damage to company assets.	Multi-Factor authentication	IA-2 (Identification and Authentication-organizational users)	Very High	Very High	9.2
Lack of inventory control	Loss of company data due to	Asset Monitoring and tracking	PE-20, CM-8, (Asset	Very High	Very High	9.0

	hardware being removed from production systems.		Monitoring and Tracking, System Component Inventory)			
Lack of system redundancy	Loss of customers & data due to power outage	System backup	CP-9, (System Backup)	High	Very High	8.0
Lost/stolen company devices	Loss of company info on lost or stolen company assets (cell phones & laptops)	Mobile devices sign out	AC-19, AC-7(2), (Access Control for mobile devices, Purge/wipe mobile device)	Very High	Very High	9.6
Lack of hardware maintenance	Changes in the regulatory landscape that may impact operations	Procedural maintenance & up-keep	MA-6(1), (Timely/preventative maintenance)	High	Very High	8.6
Lack of employee exit policies	Former disgruntled employees w/ unauthorized access	Employee access removal procedure	PS-4, Personnel Termination	High	Very High	7.9

2.1.4 Type of Controls (in place controls)

Establishing security controls to detect and limit damage to critical business functions is essential to restore business capabilities in the event of a disaster. Controls aim to protect against unauthorized behavior and minimize the likelihood of impact resulting in

harm or loss. Security controls will protect the Health Network across all three organization tiers. We will use the Risk Management Framework in the selection of controls to safeguard assets throughout the system development life cycle.

2.1.5 Users/ Stakeholders

- Chief Information Officer - CIO at Health Network is the stakeholder that oversees the operation of the data technology department and consults with other C-level personnel on technology-related needs and purchasing decisions.
- IT Security Analyst - The Information Security Analyst at Health Network are the stakeholders that work on planning, implementing, analyzing, and monitoring security protocols to protect the PHI (Patient Health Information) data of Hospitals and clinics which are the primary customers.
- Doctors - Doctors are one of the key stakeholders and users of the system who maintain information in their profiles. Doctors work to proactively prevent situations that can result in losses, harm, or liability. These risks can include patient privacy breaches, medical errors, hazardous conditions, financial and personal liability, and non-compliance with governing healthcare agencies.
- Hospital Administrators - Hospital admin are the users to track the calls from patients for doctor's appointments that get routed to the clinic with the secured medical messages such as patient health information, type of services, or treatment required.
- Clinic Administrators - Clinic Administrators are also the users of the system who maintains the patient's information, billing, payments, and appointment schedule. They oversee day-to-day operations and work closely with the medical staff.
- Patients - Recipients of health care services that are performed by healthcare professionals and pay their bills after receiving the services.
- Practitioners like Nurses - They provide acute and primary care to patients across the healthcare continuum who also use the system (on behalf of doctors) for updating the information about clinics, doctors, and patients.
- Human Resources - Responsible for both the clinical and non-clinical staff that delivers services to the patients, and for policy implementation.
- System Administrators - Responsible for organizing and overseeing the health services and daily activities of a hospital or any healthcare facility.

Healthcare data is owned by the patient by law, but providers, payers, pharma, and others know far more about how the data is being shared than the consumer. System admin users are the Hospital admin staff who manages the system of record of all 3 products: HNetExchange, HNetPay, and HNetConnect.In this case, Data custodians are Health Network because a system like the HNetPay web portal, hosted at Health

Network production sites, accepts various forms of payments, and interacts with credit-card processing organizations.

2.1.6 HealthNet Risk Assessment Schedule

The HealthNet Risk Assessment schedule is broken up into three stages: Preparation, Assessment Test, and Post-Assessment. The Preparation stage is a four-week process that includes but is not limited to: asset and business function identification, finalizing scope and critical areas, building an assessment team, developing vulnerability/threat

HealthNet Risk Assessment Plan Schedule

Group 3 - Shark Attackers

Timetable

Day 1	Week 1	Week 2	Week 3	Week 4	Day 1 Tests	Day 2 Tests	Week 5
Stage 1 - Preparation					Stage 2 - Assessment Test		Stage 3 - Post Assessment
Announce Tentative Security Assessment Date to Stakeholders (first weekend after the four-week preparation stage)	Begin Asset Identification Process	Finalize Asset Identification	Conduct Vulnerability Assessment	Rate Threat/Vulnerability pairs	Conduct Assessment Testing Plan (Exploitation Assessment)		Organized and Confirm Risk Assessment Results
Begin Selecting Assessment Team Members with Stakeholder Input	Begin Business Functions Identification Process	Finalize Business Functions	Identify Threat and Vulnerability Pairs	Develop Assessment Test Plan (transaction test, penetration test, disaster simulation, etc....)	Gather Results		Conduct Likelihood/Impact Analysis based on Risk Assessment Findings
		Finalize Scope and Critical Areas	Conduct Threat Modeling	Prepare Assessment Team for Weekend test period.			Finalize Risk Assessment Report
		Finalize Assessment Team	Identify Controls In-Place	Plan and Confirm Backup/Restore Procedures for Worst-Case Scenarios.			Make Risk Assessment Presentation to Stakeholders
		Confirm and Announce Assessment Date		Begin Code Freeze			

pairs, and identifying in place controls to be assessed. The actual assessment will be conducted over two days during the first weekend after the four-week Preparation stage. This assessment will be precluded by a one-week code freeze where no

development or system changes are to be made. The Post-Assessment will confirm the results from the assessment, conduct a likelihood/impact analysis, and finalize a report based on the results.

2.2 Risk Mitigation Plan for Health Network, Inc

2.2.1 Scope

The scope of this risk mitigation plan is to address the top four CSVV-rated vulnerabilities as presented in the results of the Healthnet risk assessment These four vulnerabilities if exploited could impact any or all of Healthnet's product line systems; therefore, they should be mitigated as soon as possible. All other vulnerabilities identified in the risk assessment have either been mitigated since the risk assessment has been completed, will be mitigated in a separate mitigation plan later, or represent a level of risk that is considered acceptable.

The four vulnerabilities that this mitigation will address are:

1) **Lost or Theft of Mobile Devices** (Threat of PII Data being Accessed)
2) **Malicious Login Attempts to Public-Facing Production Systems**
3) **Lack of Inventory Control** (Servers, Firewalls, Switches, Workstations/Laptops, Network Devices. Mobile Devices)
4) **Lack of Patch Management** (Devices are not updated in a timely manner)

The focus of this mitigation plan is to provide HealthNet with a process to implement controls that will mitigate the four identified vulnerabilities to the critical areas of concern: PII data servers, public-facing production system client access, network infrastructure, and all physical devices. Implementation of controls will follow three stages: Planning, Testing, and Implementation with a fourth continuous stage of continuous monitoring of the process. Once approved any changes to this mitigation plan must be approved by the CIO.

2.2.2 Risk Assessment Plan Results:

The risks which were identified were "Loss of company data, theft, production outages, as well as internal/external threats."

- The loss of company data can be avoided by enforcing strict surveillance and by also applying full data encryption so that the data cannot be leaked. The budget must be approved in case new hardware is needed.

- The loss of consumer data by production outages and other factors like natural disasters or by system errors can be avoided by updating it regularly and recovery mechanisms can be enforced.
- Also, if the data is not received due to any reason, all the clients must be informed by clearly mentioning the reason for data loss and what all attempts were made by the company to recover the data.
- All the laptops must be protected by the passwords and all the disks must be encrypted.
- If the employees update the laptops timely, which is also advised to them, the devices can be escaped from the high attacks as the devices are outdated if not updated.
- When it comes to internal threats, employees should be given appraisals and trained regularly as there is a possibility that they may abuse the company's business secrets. The authority for data access has to be restricted and sanctions must be required for approaching critical data.
- It is also crucial to implement the services in cloud computing.
- If there are internet threats, backup internet must be installed ignoring its cost.

2.2.3 Areas of Concern

We have identified several critical business areas of concern throughout Health Networks' internal infrastructure including

- **User Domain** - By implementing strong security control policies and awareness training for all employees we can efficiently raise user awareness. Furthermore, we can utilize an AUP to help guide employee behavior. Employees that lose or steal mobile devices will be liable to replace the equipment. Disciplinary action will be taken to ensure that employees are following policy and procedures.
- **LAN Domain** - the local area network components including hardware such as routers, switches, hubs, and access points should be periodically reviewed and updated to ensure both functionality and security from attacks. Servers should be secured, and regularly scanned, and unused ports should remain closed. The LAN domain can be subjected to significant risk if an attacker has unrestricted access. Internal routers should use an ACL to control traffic. Furthermore, redundancy and backup power supplies should be utilized to ensure network availability in the event of an outage. Documentation should be updated when changes to the network components have been made.
- **Workstation Domain** - We want to ensure that antivirus software is installed and regularly updated. Operating systems must be kept up to date and security patches should be deployed when needed. We will incorporate a patch management system to ensure that all devices are updated in a timely manner.

We will use policies to delegate duties and automation to help keep systems up to date.

- **LAN to WAN** - We want to ensure that the boundaries where the private and public network meet is secured. Proper firewall installation/implementation is critical to help protect against several types of internet attacks. Administrators may need additional training regarding the management and maintenance of the firewall.
- **WAN** - Includes all systems accessible through the internet. We will utilize a DMZ as a primary method of protection. The DMZ can help limit an attacker's access to public-facing servers. Proper upkeep and maintenance should be reviewed regularly.
- **SYSTEM/APPLICATION DOMAIN -** All server-based applications require proper maintenance and configuration. Administrator training and knowledge are critical to keeping these systems up to date and secure.

Critical Business Functions

- **Internet access** - If internet access fails, customers cannot access the webserver.
- **Web server availability** - If the web server fails, customers cannot complete purchases.
- **Database server availability**- The database server must be available to record transactions, this may contain sensitive customer information, products purchased, as well as payment information. If the database server fails, this may result in an incomplete transaction.

2.2.4 Vulnerabilities to be Mitigated by This Plan:

Vulnerability	CVSS Score	In-Place Control	Planned Control	Owner
Lost/stolen company devices	9.6	Mobile devices signed out	AC-7(2) – Purge/wipe the mobile device after 10 unsuccessful login attempts	System Administrator

Public Facing Website	9.2	Password Log-in with forced password change every 90 days.	IA-2(6) Implement multi-factor authentication for remote access to public-facing privileged accounts where one of the factors is provided by a device separate from the system gaining access.	Web Development Team
Lack of inventory control	9.0	Asset Monitoring and tracking	PE-20 Employ asset location technologies to track and monitor the location and movement of hardware devices.	Inventory Manager

Lack of patch management	8.6	Manual Patch management system	CM-3(3) Implement changes to the current system baseline and deploy the updated baseline across the installed base using an automated patch management system.	Patch Manager

2.2.5 Roles and Responsibilities:

- **Chief Information Officer** - CIO at Health Network is the stakeholder that oversees the operation of the data technology department and consults with other C-level personnel on technology-related needs and purchasing decisions. The chief information officer (CIO) oversees the people, processes, and technologies within the company's IT department to ensure they deliver outcomes that support the goals of the business.
- **System Administrator** - He would organize, install, and support the organization's computer systems. These include local area networks (LAN), wide area networks (WAN), and other data communication systems such as intranets or internet cafes within their company. The system administrator is responsible for managing, troubleshooting, and proactively updating hardware and software assets to prevent downtime or zero-day exploits from occurring. In this mitigation planning role, the System administrator would be responsible for Password and identity management, Patch firmware, and software, verifying that peripherals are working properly, and Monitor system performance
- **Web Development Team -** The Web Developers create and maintain the organizations' websites. They will typically spend time creating coding languages like HTML5, which powers many modern mobile devices and manages the site's technical aspects, such as its performance and capacity to handle traffic without crashing. The Web Developer oversees ensuring websites look good and function properly. The team collaborates with website and graphic designers,

monitors website traffic, troubleshoots website problems when they arise, and updates websites as necessary.

- **Inventory Manager** - The inventory manager oversees the inventory levels of the business. He is responsible for devising ways to optimize inventory control procedures through daily monitoring and evaluation.
- **Patch Manager -** He is responsible for controlling the deployment of updates to the operating system and 3rd party applications on network endpoints. He would manage the vulnerability by remotely deploying operating system updates and automatically applying updates to groups of tagged endpoints.

2.2.6 Cost-Benefit Analysis of Planned Mitigation Controls

Lost/stolen company devices		Countermeasure AC-7(2)
Loss before countermeasure	Loss after countermeasure	Projected Benefit
$1,500,000	$13,000	$1,487.000
Projected benefit	Cost of countermeasure	Countermeasure value
$1,487,000	$5,000	$1,482.000
Countermeasure is recommended		

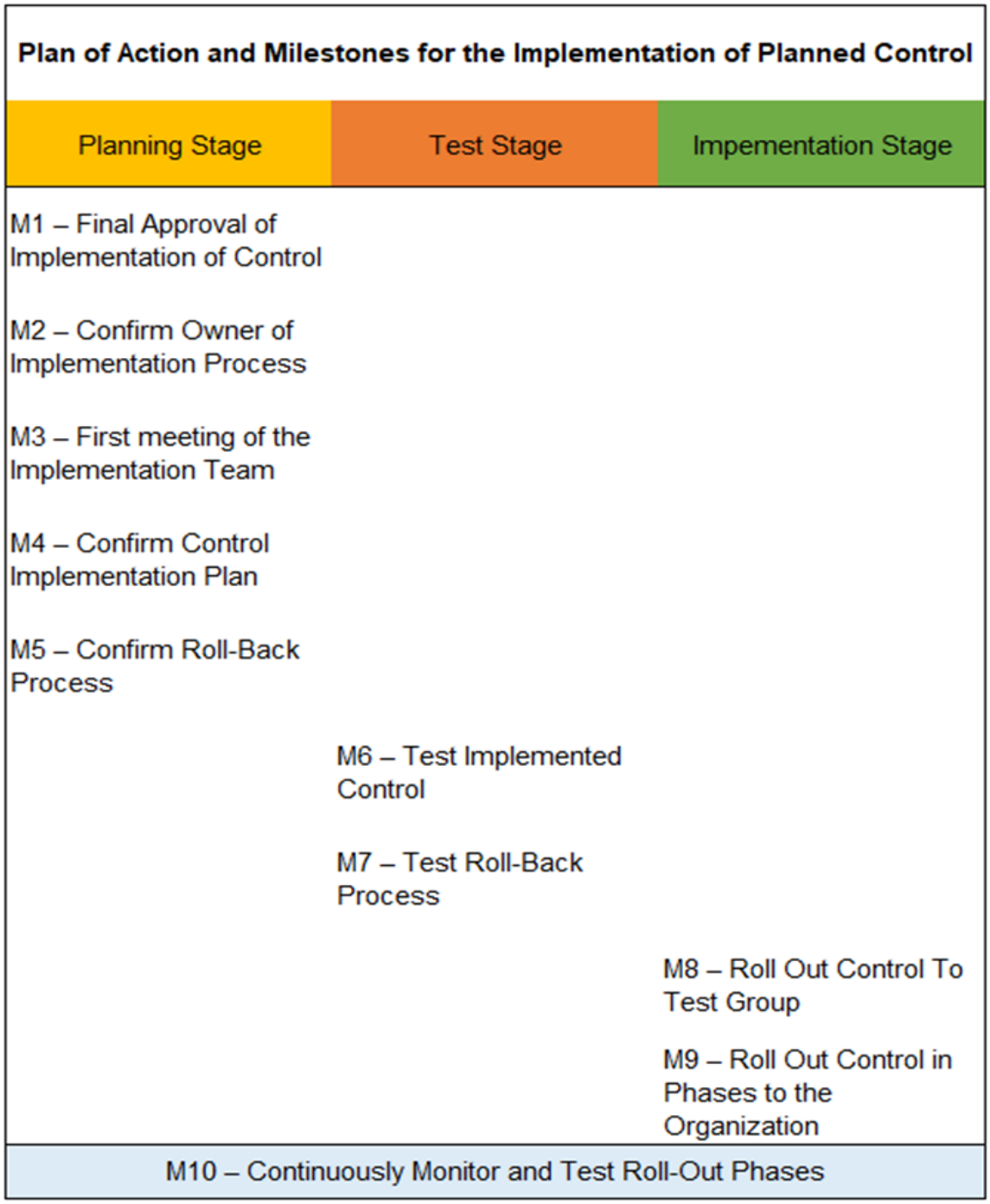
Public-Facing Website	Countermeasure IA-2(6)

Loss before countermeasure	Loss after countermeasure	Projected Benefit
$800,000	$120,000	$680,000
Projected benefit	Cost of countermeasure	Countermeasure value
$680,000	$40,000	$640,000
Countermeasure is recommended		

Lack of inventory control		Countermeasure PE-20
Loss before countermeasure	Loss after countermeasure	Projected Benefit
$700,000	$15,000	$685,000
Projected benefit	Cost of countermeasure	Countermeasure value
$685,000	$25,000	$660,000
Countermeasure is recommended		

Lack of patch management		Countermeasure CM-3(3)
Loss before countermeasure	Loss after countermeasure	Projected Benefit
$550,000	$45,000	$505,000
Projected benefit	Cost of countermeasure	Countermeasure value
$505,000	$100,000	$405,000
Countermeasure is recommended		

2.2.7 Plan of Action and Milestones for the Implementation of Planned Controls at Healthnet



2.3 Health Network Business Impact Analysis – Data Center Disruption

Health Network Inc. is a health services organization that has three main products: HNetExchange, HNetPay, and HNetConnect. These three product lines are supported by three data centers located in the vicinity of each of the three corporate office locations: Minneapolis, Minnesota; Portland, Oregon; and Arlington, Virginia. Senior management at Health Network Inc. would like to prepare for the possibility of the loss of one of the three data centers. To assess the impact of the loss of a data center on Health Network operations, a business impact analysis (BIA) will be required. This business impact analysis should be conducted on all three Health Network product lines. This document will provide the scope of this analysis, the data collection process, and a BIA for all three product lines.

2.3.1 Scope of the business impact analysis

This business impact analysis (BIA) aims to provide HealthNet management with the information needed to determine the impact of a power outage or disruption of service to one of its data centers on all three of its product line systems: HnetExchange, HnetPay, and HnetConnect. This BIA will identify the critical business functions, the critical resources, the maximum acceptable outage (MAO) time, impact, and recovery requirements for each of the respective systems.

This business impact analysis focuses exclusively on the three main product lines as it pertains to a data center outage. It does not reflect the impact on business operations at any of the three office locations other than concerning access to the data centers.

2.3.2 Data Collection Process

To conduct the BIA for a scenario involving the complete outage/disruption at one of the three data center locations leased by Healthnet, this BIA gathered information and data required over one month using a questionnaire, group meetings with key stakeholders, and one-on-one interviews with staff at different levels of the organization. All participants in the data collection process were given between one to two weeks before the actual questionnaire and/or interviews were conducted to give the stakeholders time to consider how the loss of a data center would disrupt their ability to do their job.

Once the data was completed, the information will be correlated and organized by specific product lines. From these three data sets, a Business Impact Analysis will be conducted for each of HealthNet's three product lines to determine the impact a data center disruption would have on each respectively.

2.3.3 Business Impact Analysis – HnetExchange

HNetExchange 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.

Critical Business Functions

- Customer access HnetExchange medical messages application server
- HnetExchange application server sends medical messages to recipients
- HnetExchange access to the Internet to send messages to recipients
- HnetExchange server access HnetExchange database server to log message transaction
- HnetExchange database server access Healthnet billing system to provide billing information

Critical Resources

- Internet Access
- Health Network Infrastructure
- HnetExchange application Server
- HnetExchange Database server
- HnetExchange Firewall
- HnetExchange Load Balancer

Maximum Acceptable Outage and Impact

- MAO is 10 minutes
- Impact of Outage is Severe (5 out of 5)

Recovery Requirements

- RTO 5 minutes
- RPO 5 minutes

2.3.4 Business Impact Analysis – HnetPay

HNetPay is a web portal used by many of the company's HNetExchange customers to support the management of secure payments and billing. The HNetPay web portal, hosted at Health Network production sites, accepts various forms of payments and interacts with credit-card processing organizations.

Critical Business Functions

- HNetPay secure payment system
- HNetPay online payments facilitate instant payments
- HNetPay payment switch server – channel of funds transfers among banks and other institutions
- HNetPay systems clients' access to manage their secure payment accounts.
- HNetPay credit card payment system turns checks into electronic payments that can be made anywhere

Critical Resources

- Internet Access
- Health Network Infrastructure
- HnetPay Payment switch server
- HnetPay Database server
- HnetPay Client-server
- HnetPay Webserver
- HnetPay Credit card payment system

Maximum Acceptable Outage and Impact

- MAO is 10 minutes
- Impact of an outage is Critical (5 out of 5)

Recovery Requirements

- RTO 5 minutes
- RPO 5 minutes

2.3.5 Business Impact Analysis – HnetConnect

HNetConnect is an online directory that lists doctors, clinics, and other medical facilities to allow Health Network customers to find the right type of care at the right locations. It contains doctors' personal information, work addresses, medical certifications, and types of services that the doctors and clinics offer. Doctors are given credentials and can update the information in their profiles.

Critical Business Functions

- Health Network customer access to HNetConnect directory application server

- Doctor web access to HNetConnect director application server to update profile
- HNetConnect application server connects to the HNetConnect database server
- HNetConnect server access from application administrators access to update the directory

Critical Resources

- Internet Access
- HNetConnect Network Infrastructure
- HNetConnect application Server
- HNetConnect Database server
- HNetConnect Firewall
- HNetConnect Load Balancer

Maximum Acceptable Outage and Impact

- MAO is 120 minutes
- Impact of an outage is medium (3 out 5)

Recovery Requirements

- RTO 60 minutes
- RPO 12 hours

2.4 Health Network Business Continuity Plan for Arlington County, VA Location

Health Network has a corporate office located in Arlington, VA, affected by winter storms that have made it extremely difficult for employees to reach the offices in a safe and timely manner during these weather events. Recently, the closure of the Arlington office had an impact on operations that senior management has found to be unacceptable, and the lack of a business continuity plan (BCP) was a primary reason. Therefore, senior management at Health Network Inc. has requested that a complete business continuity plan be created that will be implemented in the event of a future weather disruption that results in the closure of operations at the Arlington location. This document will provide the scope of the BCP, the BIA of the closure of the Arlington offices, the roles, and responsibilities of those tasked with implementing the BCP, the phases of the BCP, and the testing, training, and maintenance of the BCP.

2.4.1 Scope of the business continuity plan

The scope of this business continuity plan is to provide a strategy to maintain business continuity if there is a complete shutdown of business operations at the Arlington County, Virginia corporate offices. This business continuity plan will use the information from a business impact analysis to determine the critical business functions and resources associated with the Arlington corporate offices. Using the results from the BIA this business continuity plan will prioritize what business functions and resources are needed to maintain continuity, what are the roles and responsibilities of the continuity plan when it should be implemented and terminated, and how it will be tested and maintained.

This scope does present the critical steps in the recovery process and the BCP's relationship with the disaster recovery plans for the critical business functions and supporting resources. This scope does not present detailed disaster recovery plans, but the information presented here should be reflected within the creation of DRPs for critical business functions and supporting resources.

2.4.2 Business Impact Analysis of Closure of Arlington County, VA Location

Critical Business Functions

- Payroll processing to calculate payment compensation to employees including withholdings to third parties.
- Accounting operations for financial reporting, financial control and compliance, bookkeeping, and payroll tracking.
- The internal email system ensures communication between employees, customers, and third parties.
- Sever sale system to provide accurate billing and customer service information to customers.
- Database server connectivity to access customer information to assist with billing and payment processing.

Critical Resources

- Internet Access
- VPN Access
- IP phone system
- Workstations
- Server Hosting Cloud
- Database server
- Credit card system to accept payments.

Maximum Acceptable Outage and Impact

- MAO is 8 hours
- Impact of Outage is Moderate (3 out of 5)

Recovery Requirements

- RTO 2 hours
- RPO 12 hours

2.4.3 Roles and Responsibilities

Director of Operations, Arlington Location - This position is responsible for authorization of the BCP within the established chain of command and consultation with the BCP Program Manager and the BCP Coordinator. The director of operations will be a member of the BCP Team and oversee the Technical Recovery Team while the BCP coordinator implements and maintains the BCP until its deactivation.

BCP Program Manager – This position will be responsible for Healthnet BCPs, and they will oversee the execution of the BCP by the BCP Coordinator and the BCP Team. This position directly reports to the Health Network CIO, and they are responsible for the creation of all Health Network BCPs.

BCP Coordinator – This position will manage the specific business continuity plan once it has been authorized to be implemented. The BCP Coordinator will be responsible for the development and completion of this specific BCP prepared for a complete shutdown of business operations at the Arlington County, Virginia corporate offices.

BCP Team – Managed by the BCP Coordinator, the BCP team the complete shutdown of business operations at the Arlington County, Virginia corporate offices will be the Director of Operations, Arlington Location, Network administrator, Arlington location, Application System Administrator, Arlington location, and Healthnet Cloud Service Coordinator.

Amazon Web Services – This vendor should be aware of the increased bandwidth and processing required to implement the BCP. All communications with this critical vendor should be the responsibility of the Healthnet Cloud Service Coordinator.

Healthnet Cloud Service Coordinator **–** This position is responsible for managing all cloud service vendor contracts which are specifically set up to help maintain business continuity in the event of corporate outages/disruptions. For this specific, BCP all business applications will need to be accessed via a cloud system that will sync the data with application servers and database servers in the Arlington corporate offices.

Order of Succession

- Healthnet CEO
- Healthnet CIO
- Healthnet Vice President of Operations
- Healthnet Director of Operations, Arlington Location
- Healthnet Assistant Direct of Operations, Arlington Location

2.4.4 Business Continuity Plan for Arlington, VA Corporate Offices Phases

Notification Phase—Phase declared by the BCP coordinator who is the Healthnet Director of Operations, Arlington Location. During the notification and activation phase, all personnel needs to respond as quickly as possible

Time Frame to Respond to Winter Storm

- 24hr before a forecasted winter storm
    - Review steps and responsibilities checklist for the Notification Phase
    - Ensure that the Personnel Location Control Form and Vendor Location Form are up to date

- 12hr before a forecasted winter storm
    - Organization-wide notification SMS is activated to update personnel and notify personnel of the BCP plan activation
    - Ensures that all needed supplies are on hand
    - Test backup generators
    - Release personnel to take care of their homes and families

Recovery Phase—Technical Recovery Team Lead oversees this phase and keeps the EMT lead and BCP coordinator informed of the progress. Appropriate personnel had tested the DRPs and kept them up to date

MAO-8 hrs., RTO-2hrs

- Activate DRP for CBF of Payroll processing
- Activate DRP for CBF of Accounting operations
- Activate DRP for CBF of Internal email system
- Activate DRP for CBF of Sever sale system
- Activate DRP for CBF of the Database server

Reconstitution Phase—Technical Recovery Team will perform the primary work. The least critical functions should be moved first.

- Plan Deactivation Checklist
- Move CBF off cloud

2.4.5 Training, Testing, and Simulation Exercises

Training - Teaching personnel details about the BCP

- Training session for all personnel
- Emergency management team training
- Damage assessment team training
- Technical recovery team training

Testing - Verifying that the BCP will work as planned

- Testing individual steps within each phase of the BCP
- Testing all disaster recovery plans
- Locating and testing alternate resources

Simulation Exercises - Demonstrating how the BCP will work. BCP exercises should not affect normal operations.

- Tabletop Exercises
- Functional Exercises
- Full-Scale Exercises

2.4.6 BCP Summary

Health Network Inc. is a health services organization that has three main products: HNetExchange, HNetPay, and HNetConnect. To address the request by senior management regarding the impact of a data center outage a business impact analysis was required. It was determined that each product line should have its own Business Impact Analysis (BIA) conducted to properly budget and configure the Business Continuity Plans and the Disaster Recovery Plans which are outside the scope of this business impact analysis.

Health Network has a corporate office located in Arlington, VA, affected by winter storms that have made it extremely difficult for employees to reach the offices in a safe and timely manner during these weather events. Senior management has requested that a BCP be created to prepare the Arlington offices for future extreme weather events. To that end, this document presents a BIA of an outage on the Arlington offices. Although

the Arlington offices do not contain critical business function assets, there are many supporting resources at that location where an outage would impact company operations. Consequently, the BIA analysis concluded that the MAO is 8 hours, the impact is Moderate (3 out of 5), RTO should be 2 hours, and the RPO should be 12 hours. Based on that analysis the BCP in this document was created. As presented above, the supporting business functions would be moved to a cloud environment to allow employees to work remotely during the closure of the Arlington offices. This BCP proposes the use of an off-site backup data location to help maintain continuity when data cannot be accessed at the Arlington facility. While the BCP is being implemented and maintained by the BCP Coordinator, the Director of Operations will oversee implementing the DRPs required to get the Arlington office operational after the conclusion of the weather event and safe to return to work.

After a thorough analysis and interviews with stakeholders, the following table summarizes the results.

Product Line	MAO	Impact	RTO	RPO
HNetExchange	10 minutes	Severe (5 of 5)	5 minutes	5 minutes
HNetPay	10 minutes	Severe (5 of 5)	5 minutes	5 minutes
HNetConnect	120 minutes	Medium (3 of 5)	60 minutes	12 hours

3 Executive Summary

Health Network Inc. is health services organization that has over 600 employees throughout the organization and generates $500 million USD in annual revenue. The organization has three locations and three production data centers that provide high availability across the organization's products. Health Network has three main products: HNetExchange, HNetPay, and HNetConnect.

In order to protect the company long term viability, it is highly recommended that this proposed risk management plan be accepted and implemented as soon as possible. Not only does it address the protecting of Health Networks company assets, critical business functions, it also address any concerns associate with being in compliance with all industry regulations and laws.

RISK MANAGEMENT PLAN APPROVAL

The undersigned acknowledge they have reviewed the **Risk Management Plan** for the **Health Network, Inc.** project. Changes to this Risk Management Plan will be coordinated with and approved by the undersigned or their designated representatives.

Signature: _____ Date: _____
Print Name: _____
Title: _____
Role: _____

Signature: _____ Date: _____
Print Name: _____
Title: _____
Role: _____

Signature: _____ Date: _____
Print Name: _____
Title: _____
Role: _____

Signature: _____ Date: _____
Print Name: _____
Title: _____
Role: _____

RESEARCH

HIPPA—Summary of the HIPAA Privacy Rule - A major goal of the Privacy Rule is to assure
that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high-quality health care and to protect the public's
health and well-being.
https://www.hhs.gov/hipaa/for-professionals/security/lawsregulations/index.html

GLBA—Gramm Leach Bliley Act –Safeguards Rule- Companies must have a security plan to
protect customer information, which should ensure data is not released without authorization and
ensure data integrity. Companies are responsible for ensuring risk management plans are used.
All employees must be trained on security issues. PG 140 textbook.

PCI-DSS – (Mandatory for merchants using specific credit cards).
The Payment Card Industry Data Security Standard (PCI DSS) is an international security
standard. The purpose is to enhance the security of credit card data. The goal is to thwart the theft of
credit card data. Fraud can occur if a thief gets certain data. PG 155 textbook.

GDPR—Sites must protect that data from misuse and exploitation and notify
users of any data breach. Sites also must respect the privacy rights of data owners.
https://eurlex.
europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

ECPA—Electronic Communications Privacy Act of 1986—protects wire, oral, and electronic
communications while those communications are being made, are in transit, and when they are
stored on computers. The Act applies to email, telephone conversations, and data stored
electronically.
https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285

CFAA—Computer Fraud and Abuse Act—prohibits intentionally accessing a computer without
authorization or in excess of authorization, but fails to define what "without authorization"

means. https://www.nacdl.org/Landing/ComputerFraudandAbuseAct

REFERENCES

NIST 800-30

NIST SP 800-53rev5 control catalog

Gibson, D., & Igonor, A. (2022). *Managing risk in information systems*. Jones & Bartlett Learning.

NIST RMF: https://www.nist.gov/system/files/documents/2018/03/28/vickie_nist_risk_management_framework_overview-hpc.pdf

NIST risk assessment guidance: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

NIST contingency planning guidance: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

Business Impact Analysis: https://www.ready.gov/business-impact-analysis

Business Continuity Plan (Ready.gov): https://www.ready.gov/business-continuity-plan