Bellevue University

Eric Wellmaker

Week 12 Writing Assignment

Risk Management Studies

May 30th, 2024

Computer incident response teams, business impact analysis and business continuity plans are needed to ensure a business has the road map to operate when a disruption occurs. The project scenario for Health Network Inc. experienced several disruptions. These disruptions could have been prevented if the business had taken mitigation measures. For this final assignment, I will gather all resources for Health Network Inc and provide the business with a CIRT Plan, Business Impact Analysis and Business Continuity Plan.

CIRT Plan

The CIRT (computer incident response team) varies on each situation. CIRT members identify what is needed for their systems and use what is necessary (Wellmaker, E. (2024). The CIRT Plan below is the recommended plan that Health Network Inc. should be utilizing.

CYBER INCIDENT RESPONSE PLAN

Cyber Incident Response Plan Template., (2024).

Table of Contents

1. Authority and Review

Document Control and Review

Document Control	
Author	**Eric Wellmaker**
Owner	**Eric Wellmaker**
Date created	**6/1/2024**
Last reviewed by	**Eric Wellmaker**
Last date reviewed	**6/1/2024**
Endorsed by and date	**Eric Wellmaker 6/1/2024**
Next review due date	**6/1/2025**

Version Control

Version	Date of Approval	Approved By	Description of Change
1.01	6/1/2024	Eric Wellmaker	None

2. Purpose and Objectives

Purpose of the CIRP

The computer incident response team plan is to identify computer related incidents. Throughout this document, the questions who, what, when, where, why and how will be asked to identify vulnerabilities and methodologies for mitigation.

Objectives of the CIRP

1. Preparation
2. Detection and Analysis
3. Containment Eradication and Recover
4. Post Incident Recovery

A list of commonly used terms and definitions is provided at Appendix A.

2.1. Common Threat Vectors

The following table contains common threat vectors from the NIST Computer Security Incident Handling Guide.

Type	Description
External/Removable Media	An attack executed from removable media or a peripheral device (e.g. malicious code spreading onto a system from an infected USB flash drive).
Attrition	An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (e.g. a DDoS intended to impair or deny access to a service or application or a brute force attack against an authentication mechanism, such as passwords).
Web	An attack executed from a website or web-based application (e.g. a cross-site scripting attack used to steal credentials or a redirect to a site that exploits a browser vulnerability and installs malware).
Email	An attack executed via an email message or attachment (e.g. exploit code disguised as an attached document or a link to a malicious website in the body of an email).
Supply Chain Interdiction	An antagonistic attack on hardware or software assets utilizing physical implants, Trojans, or backdoors, by intercepting and modifying an asset in transit from the vendor or retailer.
Impersonation	An attack involving replacement of something begin with something malicious (e.g. spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation).

Improper usage	Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories (e.g. a user installs file sharing software, leading to the loss of sensitive data).
Loss or Theft of Equipment	The loss or theft of a computing device or media used by an organization (e.g. a laptop, smartphone, or authentication token).

Common Cyber Incidents

The following table provides a list of common cyber incident types and corresponding initial response activities.

Type/Description	Response
Denial of Service (DoS) and Distributed Denial of Service (DDoS): overwhelming a service with traffic, sometimes impacting availability.	Confirm the attack, implement mitigation measures (redirect network traffic, filter servers), monitor and recover.
Phishing: deceptive messaging designed to elicit users' sensitive information (such as banking logins or business login credentials) or used to execute malicious code to enable remote access.	Notify supervision, reset password(s) and change login information.
Ransomware: a tool used to lock or encrypt victims' files until a ransom is paid.	Power off infected device/unplug it from power source, disconnect other devices on network.
Malware: a Trojan, virus, worm, or any other malicious software that can harm a computer system or network.	Isolate device, identify type of infection, remove malware.
Data breach: unauthorized access and disclosure of information.	Verify the breach occurred, report breach to a supervisor, determine criminal activity of suspect(s) by asking questions to data owners.

(Cyber Incident Response Plan Template., 2024).

3. Roles and Responsibilities

This section includes details of the roles and responsibilities of core individuals and teams responsible for incident response and decision making, including the operational level Cyber Incident Response Team (CIRT) and the strategic level Senior Executive Management Team (SEMT).

All personnel listed here should be familiar with their responsibilities in this plan and practice their response.

3.1. Points of Contact for Reporting Cyber Incidents

Primary and secondary (backup) internal points of contact to report cyber incidents to over a 24/7 period.

Name	Hours of Operation	Contact Details	Role Title	Responsibilities
John Yellow	0700-1600	123-456-7890	Manager	Director

3.2. Cyber Incident Response Team (CIRT)

CIRT members responsible for managing responses to cyber incidents:

Name	Organisation Role	Contact Details	CIRT Role Title	CIRT Responsibilities
John Red	Manager	123-456-7890	**A**	Mitigation Plan Coordinator
John Blue	Supervisor	123-456-7890	**B**	Forensic Expert
John Green	Supervisor	123-456-7890	**C**	IT Specialist

(Cyber Incident Response Plan Template., 2024).

4. Containment, Evidence Collection & Remediation

4.1. Containment

Containment actions are implemented in order to minimize the damage, prevent the incident from spreading or escalating, and prevent the attacker from destroying evidence of their attack.

When planning containment actions, consider:

- Any additional impacts there could be to systems/services.
- Time and resources required to contain the incident.

- Effectiveness of the containment solution (e.g. partial vs full containment)
- Duration that the solution will remain in place (e.g. temporary vs permanent solution)

4.2. Evidence Collection and Preservation

When gathering evidence, maintain a detailed log that clearly documents how all evidence has been collected. This should include who collected or handled the evidence, the time and date (including time zone) evidence was collected and handled, and the details of each item collected (including the physical location, serial number, model number, hostname, media access control (MAC) address, IP address and hash values). See the Evidence Register template at Appendix F to capture this information.

4.3. Remediation Action Plan

A Remediation Action Plan is to be developed and implemented for eradicating and resolving the incident following successful containment and evidence collection. See Appendix G for a template.

When developing the Remediation Action Plan, consider:

4.4. Post Incident Review

A Post Incident Review (PIR) is a detailed review conducted after a cyber security incident.

Key questions to consider in the PIR:

- What were the root causes of the incident and any incident response issues?
- Could the incident have been prevented? How?
- What worked well in the response to the incident?
- How can our response be improved for future incidents?

The PIR Guide and Template with more detailed questions to consider is available at Appendix H. Recommendations that arise from the review can be documented in a corresponding Action Register. Use the template at Appendix I.

4.4.1 PPOSTTE Model

The PPOSTTE model can assist in reflecting on key elements of the incident response.

People	Roles, responsibilities, accountabilities, skills
Process	Plans, policies, procedures, protocols, processes, templates, arrangements
Organization	Structures, culture, jurisdictional arrangements
Support	Infrastructure, facilities, maintenance
Technology	Equipment, systems, standards, security, inter-operability
Training	Qualifications/skill levels, identification of required courses
***Exercise Management** *This only applies to*	Exercise development, structure, management, conduct

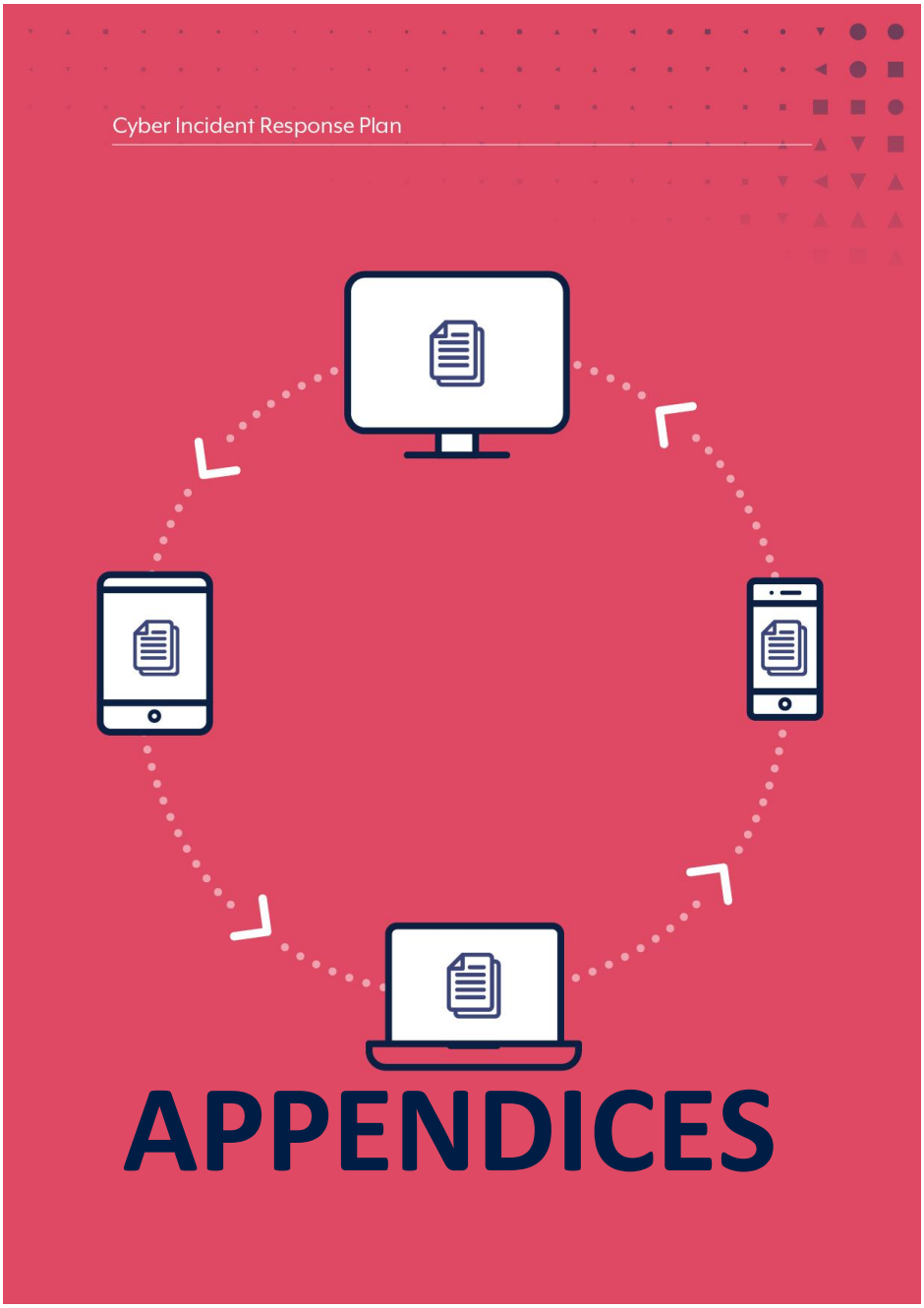
exercises	

4.5. Update and Test Cyber Incident Response Plan

The PIR may result in changes to the CIRP, Playbooks and Templates. Changes should be communicated
to the relevant personnel.

4.6. Training

Annual Computer Based Training to understand operating procedures.



Appendix A

Terminology and Definitions

Use of consistent and pre-defined terminology to describe incidents and their effects can be helpful during a response. In your CIRP, include commonly used terms used in your organization. ACSC defines cyber threats, events, alerts, and incidents as follows:

Cyber threat

A cyber threat is any circumstance or event with the potential to harm systems or information. Other threats are listed on cyber.gov.au. Organizations can include a list of cyber threats of concern. The ACSC Annual Cyber Threat Report (2021) outlines the following threat environment and key cyber security trends:

- COVID-19 themed malicious activity including phishing emails and scams.
- Ransomware
- Exploitation of security vulnerabilities
- Software supply chain compromise
- Business Email Compromise
- Cybercrime

Cyber security event

A cyber security event is an occurrence of a system, service or network state indicating a possible breach
of security policy, failure of safeguards or a previously unknown situation that may be relevant to security.

A cyber security event has the potential to become, but is not confirmed to be, a cyber incident.

Examples of cyber security events include (but are not limited to):

- A user has disabled the antivirus on their computer.
- A user has deleted or modified system files.
- A user restarted a server.
- Unauthorized access to a server or system.

Cyber security alert

A cyber security alert is a notification generated in response to a deviation from normal behavior. Cyber security alerts are used to highlight cyber security events.

Cyber incident

A cyber incident is an unwanted or unexpected cyber security event, or a series of such events, that have
a significant probability of compromising business operations. A cyber incident requires corrective action.

Examples of cyber security incidents include (but are not limited to):

- Denial-of-service attacks (DoS)
- Unauthorized access or attempts to access a system
- Compromise of sensitive information
- Virus or malware outbreak (including ransomware).

Appendix B

Cyber Incident Response Readiness Checklist

This checklist is to aid your organization's initial assessment of its readiness to respond to a cyber security incident. This checklist is not an exhaustive list of all readiness activities.

PREPARATION	
☐	Your organization has a cyber security policy or strategy that outlines your organization's approach to prevention, preparedness, detection, response, recovery, review, and improvement. • For example, does your organisation have a position on, for example, paying ransom, reporting incidents to government, publicly acknowledging cyber incidents, sharing information about incidents with trusted industry and government partners?
☐	A Cyber Incident Response Plan has been developed, which: • Aligns with your organization's operating environment and other processes, including emergency management and business continuity processes. • Has been reviewed or tested in an exercise to ensure it remains current and responsible personnel are aware of their roles, responsibilities, and processes. • Templates have been prepared, for example Situation Reports.
☐	Staff involved in managing an incident have received incident response training.
☐	Up-to-date hard copy versions of the Cyber Incident Response Plan and playbooks are stored in a secure location (in case of electronic or hardware failure) and are accessible to authorized staff members.
☐	Specific playbooks to supplement the Cyber Incident Response Plan have been developed, that define step-by-step guidance for response actions to common incidents, and roles and responsibilities.
☐	A Cyber Incident Response Team (CIRT) and a Senior Executive Management Team (SEMT) – or equivalents - have been formed to manage the response, with approved authorities.

☐	All relevant IT and OT Standard Operating Procedures (SOPs) are documented and have been reviewed or tested in an exercise to ensure they remain current and responsible personnel are aware of their roles, responsibilities, and processes.
☐	Arrangements for service providers, including cloud and software as a service, to provide and retain logs have been established and tested to ensure these include useful data and can be provided in a timely manner.
☐	Log retention for critical systems have been configured adequately and tested to confirm that they capture useful data. Refer to the ACSC publications including Windows Event Logging and Forwarding for specific guidance.
☐	Your organization has internal or third party arrangements and capabilities to detect and analyze incidents. If these capabilities are outsourced, your organization has an active service agreement/contract.
☐	Critical assets (data, applications and systems) have been identified and documented.
☐	Standard Operating Procedures (SOPs) have been developed, and roles and responsibilities assigned for use of facilities and communications technologies in response to cyber incidents, and these resources are confirmed as available. This includes for alternative/back-up ICT-based channels.
☐	Incident logging/records and tracking technologies used to manage a response are confirmed as available and have been tested.
☐	Role cards have been developed for each person involved in the CIRT and the SEMT. Individual actions will depend on the type and severity of the incident. Example role card is available at Appendix J.
☐	Your organization has internal or third-party arrangements and capabilities to monitor threats. Situational awareness information is collected from internal and external data sources, including: • Local system and network traffic and activity logs • News feeds concerning ongoing political, social, or economic activities that might impact incident activity. • External feeds on incident trends, new attack vectors, current attack indicators and new mitigation strategies and technologies.
DETECTION, INVESTIGATION, ANALYSIS AND ACTIVATION	
Standard Operating Procedures (SOPs) have been developed, and roles and responsibilities assigned for:	

☐	Detection mechanisms which can be used to identify potential information security incidents, such as scanning, senses and logging mechanisms. These mechanisms require monitoring processes to identify unusual or suspicious activity, for example behavior and logging, commensurate with the impact of an incident. Common monitoring techniques include: a) network and user profiling that establishes a baseline of normal activity which, when combined with logging and alerting mechanisms, can enable detection of anomalous activity. b) scanning for unauthorised hardware, software, and changes to configurations. c) sensors that provide an alert when a measure breaches a defined threshold(s) (e.g. device, server and network activity). d) logging and alerting of access to sensitive data or unsuccessful logon attempts to identify potential unauthorised access; and e) users with privileged access accounts subject to a greater level of monitoring considering the heightened risks involved.[1]
☐	Incident detection, including self-detected incidents, notifications received from service providers or vendors, and notifications received from trusted third parties (e.g. ACSC).
☐	Incident analysis, including how incidents are to be categorized, classified and prioritized, and controls related to how data is stored and transmitted (i.e. if out-of-band transmission is required).
☐	Activating a Cyber Incident Response Team (CIRT) to manage critical incidents, with roles and responsibilities assigned.
☐	Activating a Senior Executive Management Team (SEMT) to manage critical incidents, with roles and responsibilities assigned.
CONTAINMENT, EVIDENCE COLLECTION AND REMEDIATION	
☐	Standard Operating Procedures (SOPs), playbooks and templates, have been developed, and roles and responsibilities assigned for containment, evidence collection and remediation. These can be included as appendices to the Cyber Incident Response Plan.
☐	A secure location is available for storing data captured during an incident, which could be used as evidence of the incident and the adversary's tradecraft, and ready to be provided to third-party stakeholders if needed.
COMMUNICATIONS	
☐	Policy, plans, Standard Operating Procedures (SOPs) and templates have

	been developed to support communicating with: • Internal stakeholders (e.g. Board, staff) • External stakeholders (e.g. stakeholders to assist with the response and stakeholders with an interest in the response)
☐	Policy, plans, Standard Operating Procedures (SOPs) and templates for media and communications professionals have been developed, and roles and responsibilities assigned, to support public and media messaging.
☐	You organization has assigned a public and media spokesperson, who is supported by subject matter experts.
☐	Staff have been trained to implement the communications processes and execute their roles and responsibilities.
☐	Staff who are not involved in managing incidents are cognizant of your organization's policy and processes and their responsibilities when an incident occurs (e.g. exercising discretion, using approved talking points, referring enquiries to the designated officer).
INCIDENT NOTIFICATION AND REPORTING	
☐	Processes and contact details are documented to support the organization to meet its legal and regulatory requirements on cyber incident notification, reporting and response, with roles and responsibilities within your organization are assigned. This includes the processes for obtaining authority to release and share information.
☐	Processes are documented for insurance requirements.
POST INCIDENT REVIEW	
☐	A process is documented to conduct Post Incident Reviews (PIR) following conclusion of an incident and PIR reports with recommendations are submitted to management for endorsement.
☐	A process is documented to ensure actions following incidents and/or exercises are tracked and completed (e.g. Action Register).

(Cyber Incident Response Plan Template., 2024).

Business Impact Analysis (BIA) for Health Network Inc.

1. Overview

This Business Impact Analysis (BIA) is developed as part of the contingency planning process for the *{Health Network}.* It was prepared on {*6/1/2024*}.

1.1 Purpose

The purpose of the BIA is to identify Health Network Inc. data centers critical business functions, critical resources, Maximum acceptable outage (MAO) and impact. And its recovery point objective (RPO) and recovery time objective (RTO).

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 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, Inc.}* 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.

2. System Description

The Health Network Inc. (Health Network) is comprised of three main products. HNetExchange is the primary source of money for the business. HNetPay is a web portal which facilitates secure payments and billing for HNetExchange Customers. Finally, there's HNetConnect which is an online directory which provides doctors personal information to include certifications, work addresses, and types of services offered which can help customers find the correct level of care.

The Health Network Inc. (Health Network) infrastructure operates three data centers. Each data center has an estimated 1,000 production servers, to include 650 company issued laptops and mobile devices.

3. BIA Data Collection

Data collection can be accomplished through individual/group interviews, workshops, email, questionnaires, or any combination of these.

3.1 Determine Process and 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
HNetExchange	*Secure electronic medical messages from customers like Hospitals which are routed to clientele*
HNetPay	Web portal for secure payments and billing
HNetConnect	Online directory listing Hospital staff, medical facilities, and medical personnel certifications & personal information

If criticality of mission/business processes has not been determined outside of the BIA, the following subsections will help to determine criticality of mission/business processes that depend on or support the information system.

3.1.1 Identify Outage Impacts and Estimated Downtime

This section identifies and characterizes the types of impact categories that a system disruption is likely to create in addition to those identified by the FIPS 199 impact level, as well as the estimated downtime that the organization can tolerate for a given process. Impact categories should be created, and values assigned to these categories in order to measure the level or type of impact a disruption may cause. An example of cost as an impact category is provided. Organizations could consider other categories like harm to individuals and ability to perform mission. The template should be revised to reflect what is appropriate for the organization.

Outage Impacts

Impact categories and values should be created in order to characterize levels of severity to the organization that would result for that particular impact category if the mission/business process could not be performed. These impact categories and values are samples and should be revised to reflect what is appropriate for the organization.

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

> ***Example impact category = Cost***
>
> - ***Severe*** *- temp staffing, overtime, fees are greater than $1 million*
> - ***Moderate*** *– fines, penalties, liabilities potential $550k*
> - ***Minimal*** *– new contracts, supplies $75k*

Impact category: {*Health Network, Inc.*}

Impact values for assessing category impact:

- Severe = {*Over $1 Million*}
- Moderate = {*$500K*}
- Minimal = {*$50k*}

The table below summarizes the impact on each mission/business process if *{Health Network Inc.}* were unavailable, based on the following criteria:

Mission/Business Process	**Impact Category**				
	{Minimal}	***{Moderate}***	***{Severe}***	**{}**	**Impact**
Vendor Invoice					
HNetExchange		x			Moderate

Mission/Business Process	Impact Category				
	{Minimal}	***{Moderate}***	***{Severe}***	**{}**	**Impact**
HNetPay		x			Moderate
HNetConnect			x		Severe

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 amount of time which can be tolerated before a business's recovery is considered compromised. This means if the MAO is exceeded than the survival of the business is no longer guaranteed.

- **Maximum Tolerable Downtime (MTD).** The MTD represents the total amount of time leaders/managers are willing to accept for a mission/business process outage or disruption and includes all impact considerations. Determining MTD is important because it could leave continuity planners with imprecise direction on (1) selection of an appropriate recovery method, and (2) the depth of detail which will be required when developing recovery procedures, including their scope and content.

- **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 MTD, RTO, and RPO (as applicable) for the organizational mission/business processes that rely on *{Health Network Inc.}*. *Values for MTDs and RPOs are expected to be specific time frames, identified in hourly increments (i.e., 8 hours, 36 hours, 97 hours, etc.).*

Mission/Business Process	MTD	RTO	RPO	MAO
Pay vendor invoice	*72 hours*	*48 hours*	*12 hours (last backup)*	*12 hours*
HNetExchange			***x***	***x***
HNetPay		***x***		
HNetConnect			***x***	***x***

HNetExchange RPO & MAO 12 hours downtime before operations are affected by lack of services.

HNetPay RTO 48 hour downtime before operations are affected by lack of services.

HNetConnect 12 hours downtime before operations are affected by lack of services.

HNetExchange secondary processing would be normal billing through postal services.

HNetPay secondary procedures in event of interruption will be visiting site directly for all payments and billing.

HNetConnect secondary action is printing out a map of facilities to include the types of services provided.

3.2 Identify Resource Requirements

The following table identifies the resources that compose *{Health Network Inc.}* including hardware, software, and other resources such as data files.

System Resource/Component	Platform/OS/Version (as applicable)	Description
Web Server 1	***Optiplex GX280***	***Web Site Host***

It is assumed that all identified resources support the mission/business processes identified in Section 3.1 unless otherwise stated.

Note: Information for this section should be available from the system's System Security Plan (SSP) and can be copied from the SSP, or reference the applicable section in the SSP and attach the latest version of the SSP to this contingency plan.

3.3 Identify Recovery Priorities for System Resources

The table below lists the order of recovery for *{Health Network, Inc.}* resources. The table also identifies the expected time for recovering the resource following a “worst case” (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 MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD.

Priority	System Resource/Component	Recovery Time Objective
Web Server 1	*Optiplex GX280*	*24 hours to rebuild or replace*

A system resource can be software, data files, servers, or other hardware and should be identified individually or as a logical group.

Alternative strategies for RTOs include backing up physical media for HNetConnect. This data will contain medical locations, business address, and type of services for each facility. HNetPay will have a backup server in place to keep operations going in the event of a disruption. HNetExchange will also have backup servers and cloud storage so it is easily accessible in the event of a disruption.

Health Network Inc. Business Continuity Plan (BCP).

Summary Report.

VERSION HISTORY

BUSINESS CONTINUITY PLAN

HEALTH NETWORK
999 Health Network LN
Atlanta, GA and 12345

VERSION 1.2.2

06/1/2024

VERSION	APPROVED BY	REVISION DATE	DESCRIPTION OF CHANGE	AUTHOR
1.0.0	Eric Wellmaker	5/12/2024	No Changes	Eric Wellmaker
1.2.2	Eric Wellmaker	6/1/2024	Consolidated Text, Items and Descriptions.	Eric Wellmaker

PREPARED BY	Eric Wellmaker	**TITLE**	BCP Manager	**DATE**	06/1/2024
APPROVED BY	Eric Wellmaker	**TITLE**	BCP Manager	**DATE**	06/1/2024

TABLE OF CONTENTS

M. Testing 7.

1. 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.

In the event of a disruption, here are the critical areas of infrastructure of Health Network. The data center hosts an estimated 1,000 servers and the company also maintains 650 company issued laptops. In the event of a disruption, these items need to be moved to a secure location and all assets need to be accounted for.

2. RELOCATION STRATEGY

Depending on the service disruption. Assets can be flown out by air, truck, boat or rail. Assets will be accounted for with a manifest and sent to alternate location site.

Inventory all items and networking equipment.

Create an emergency Action Checklist including IT members, and Vendor Help Desk.

Backup servers and have physical copies.

3. 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. This strategy should include both short-term and long-term relocation sites in the case of both types of disruptions.

The alternate business site will be at a location what is favorable to the systems and personnel needed to continue operations at the alternate site.

4. RECOVERY PLAN

The recovery plan will be able to perform business functions at the lowest level required to keep the business running. Keep mind that the lowest level means only core operating components performing basic functions needed for Health Network to keep operating.

5. 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:

A. DISASTER OCCURRENCE

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

B. PLAN ACTIVATION

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

C. ALTERNATE SITE OPERATION

This phase continues until Health Network can restore the primary facility.

D. TRANSITION TO PRIMARY SITE

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

6. RECORDS BACKUP

Backup all records on hard copies. If utilizing a third-party vendor, use cloud services and ensure data records are kept up to date and can be extracted in a timely manner.

7. 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. The teams periodically back up and store the most critical files at an offsite location.

This measure can be accomplished by keeping frequent data backups that can be restored in the event of data loss, intentional or accidental deletion, and data destruction.

8. 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.

A. TEAM ROLES

Team Leader, Backup Team Leader, Team Member

B. TEAM CONTACTS

Stored in the Contact List Appendix

C. TEAM RESPONSIBILITIES

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

D. DEPARTMENTAL RECOVERY TEAMS

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

5

9. RECOVERY PROCEDURES

Health Network details the specific activities or tasks needed to recover normal and critical business operations. It describes each strategy by enumerating the specific set of activities and tasks needed to recover appropriately.

This is where the TRT (technical recovery team) restores, repairs, and recovers damaged systems and components.

BCDR (Business Continuity Disaster Recovery) team that reduces the effects of disruptions for Health Network.

A. POTENTIAL RECOVERY PROCEDURE

i. Disaster Occurrence

ii. Notification of Management

iii. Preliminary Damage Assessment

iv. Declaration of Disaster

v. Plan Activation

vi. Relocation to Alternate Site

vii. Implementation of Temporary Procedure

viii. Establishment of Communication

ix. Restoration of Data Process and Communication with Backup Location

x. Commencement of Alternate Site Operations

xi. Management of Work

xii. Transition Back to Primary Operations

xiii. Cessation of Alternate Site Procedures

xiv. Relocation of Resources Back to Primary Site

(Marker, A., 2018), (Wellmaker, E., 2024)

10. testing

Health Network must identify any inconsistencies with the drafted business continuity plan. The business must also devise ways to address solutions to the BCP as well. All personnel must have a common goal for the plan to operate efficiently, as well as be knowledgeable on the BCP procedures (Quinn, A., 2022).

This is where the testing takes place and is recommended to be completed at least

annually. The procedures of the BCP should be done line by line. The purpose for testing is to identify discrepancies with the BCP, its steps, personnel responsibilities, or resources and resolve them as soon as possible (Gibson, D., & Igonor, A., 2022).

BCP Test will show how the BCP will operate.

Tabletop Exercises: Will bring all Health Network members together to discuss the BCP process and the BCP coordinator will present a scenario to solve.

Functional Exercise: Members will rate functions within the BCP. This type of exercise can be used at an alternate site to see if the BCP can restore and recover critical components of the business.

Full-Scale Exercises: This type of exercise offers more realism due to it simulating actual disruptions. Health Network members would be taking action, and following the drafted BCP in order to see how members would react in an emergency situation.

(Gibson, D., & Igonor, A., 2022).

The CIRT, BIA and BCP from this final plan identifies what is needed to prevent a cybersecurity threat. If Health Network Inc, can implement the recommended mitigation measures, then if a disruption were to occur, the business can continue to operate without worrying about a major disruption or business failure.

References

Cyber Incident Response Plan Template. (2024). Cyber.gov.au. https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Cyber-Incident-Response-Plan-Template.docx

Gibson, D., & Igonor, A. (2022). *Managing Risk in Information Systems* (3rd ed.).

Marker, A. (2018). Free Business Continuity Plan Templates. Smartsheet. https://www.smartsheet.com/business-continuity-templates

Sheldon, R., Kirvan, P., & Sliwa, C. (2024). *Business Impact Analysis (BIA)*. TechTarget. https://www.techtarget.com/searchstorage/definition/business-impact-analysis

Quinn, A. (2022). WHAT IS BCP TESTING? Continuity2. https://continuity2.com/blog/what-is-bcp-testing

Wellmaker, E. (2024). Modified Business Continuity Plan Templates. Smartsheet.