THC Business Continuity Plan

!!Mock report details do not refer to any real individual or organisation!!

H,Z

June 10, 2023

Executive Summary

This report presents a business continuity management (BCM) plan for Trusted Health Clinic (THC), focusing on risk assessment, business impact analysis (BIA), and incident response planning. In the risk assessment section, various threats and vulnerabilities are identified, these include natural disasters, cyberattacks and data breaches within THC. The Business impact analysis follows the standard HB292-2006 and prioritises THC's critical business functions, such as the patient management system, Allied health and Staff management systems, and the financial management systems. The analysis considers the C.I.A triad characteristics of information security, Confidentiality, Integrity and Availability

The incident response planning details the procedures for handling various disruptive incidents to THC such as flooding, phishing attacks and ransomware. The plan includes actions taken before, during and after the incidents, by both the stakeholders, incident response teams and associated parties. The report also contains a crisis communication plan to ensure clear and effective communication with stakeholders during any given crisis. Post-incident recovery, guided by the NIST 800-184 framework is emphasised for continual improvement. These recommendations and procedures outlined aim to enhance THC's resilience for potential disruptions, and outlines recovery methods and plans.

Contents

1 Introduction **3**
- 1.1 Purpose . . . 3
- 1.2 Information Governance . . . 3
  - 1.2.1 Establish organisation-wide information security . . . 3
  - 1.2.2 Adopt a risk-based approach . . . 3
  - 1.2.3 Set the direction of investment decisions . . . 3
  - 1.2.4 Ensure conformance/compliance with internal and external requirements 3
  - 1.2.5 Ensure conformance/compliance with internal and external requirements 4
  - 1.2.6 Foster a security-positive environment . . . 4
  - 1.2.7 Review performance in relation to business outcomes . . . 4
- 1.3 Enterprise Information Security Policy . . . 4
  - 1.3.1 InfoSec Purpose and Importance . . . 4
  - 1.3.2 Roles and Responsibilities . . . 5

2 Business Impact Analysis **5**
- 2.1 Impact Assessment . . . 5

3 Incident Response Planning **8**
- 3.1 Incident Handling Procedures . . . 8
- 3.2 Flooding - Incident Handling Procedure . . . 9
- 3.3 Phishing Attacks - Incident Handling Procedure . . . 10
- 3.4 Ransomware - Incident Handling Procedure . . . 11
- 3.5 Strategic Recovery . . . 11

4 Crisis Communications **11**

A Glossary **14**
- A.1 CIA Triad . . . 14
- A.2 Risk Rating Values . . . 14
- A.3 Impact Values . . . 14
- A.4 IRACI Definitions . . . 15
- A.5 Cybersecurity Incident Response Framework . . . 15

B Selection process for Business Impact Area **16**

1 Introduction

1.1 Purpose

Business continuity management (BCM) is the process of creating and implementing a strategy to ensure that critical business functions are able to continue in the face of disaster; Strategic is relating to the most important or high-level aspects of decisions making, such as a political policy or business function, especially when the plan is decided in advance. The BCM will promote a resilient organisation that is able to effectively respond to and recover from disruptions to critical function. A disruption could be a natural disaster occurring such as a flood which damages internal hardware. Without a plan in place, THC will be disorganised in the face of a disaster, resulting in higher degrees of data loss, revenue decrease, or reputation damage.

1.2 Information Governance

The aim of information governance is to outline the set of responsibilities and practices of executive management to ensure that THC is able to meet its business objectives and maintain its value creating activities (Whitman and Mattford 2019). THC will take an action-oriented approach to governance as per ISO 27014 six principles. Creating a information governance plan will improve THC's strategic security and ensure they can address the management of patient, staff and allied service information from a broad perspective.

1.2.1 Establish organisation-wide information security

Information Security Policy, Risk Management Procedures, Incident Response Plans and Disaster Recovery should be adopted at the top levels of management to ensure that they take into account all critical business areas and are effective at maintaining business operations and mitigation of incidents.

1.2.2 Adopt a risk-based approach

Security Policies should be based on the analysis of the highest risks to the continued operation of THC. This involves evaluation of Assets, Threats and Vulnerabilities to determine where security policies should be aimed and the extent of their coverage.

1.2.3 Set the direction of investment decisions

It is important that THC allocates a budget to security implementations. A significant amount of revenue is attributed to THC's IT assets (CKB, HealthcareOne) and the sensitive information it handles on a daily basis, THC should consider a higher investment into security than comparably sized businesses (Violino 2019). This is set out in the Enterprise Information Security Policy.

1.2.4 Ensure conformance/compliance with internal and external requirements

THC provides medical services and handles medical data from the Medicare and HICAPs systems. Thus THC must comply with relevant legislation. The handling of private and sensitive patient data requires adherence to the Australian Privacy Principles, regarding the disclosure and anonymizing of personally identifiable information for CKB licensing (Australian Information Commissioner 2022). Additionally, the in-house Healthcare One system must comply with health care record keeping to the standards outlined in Action 1.16 of the NSQHS.

1.2.5 Ensure conformance/compliance with internal and external requirements

THC provides medical services and handles medical data from the Medicare and HICAPs systems. Thus THC must comply with relevant legislation. The handling of private and sensitive patient data requires adherence to the Australian Privacy Principles, regarding the disclosure and anonymizing of personally identifiable information for CKB licensing (Australian Information Commissioner 2022). Additionally, the in-house Healthcare One system must comply with health care record keeping to the standards outlined in Action 1.16 of the NSQHS. (NSQHS 2014)

1.2.6 Foster a security-positive environment

Training and education programs are a key element in promoting a strong security policy that extends organisation wide. THC should devote itself to basic cybersecurity awareness training during their employee induction process. This will ensure a security aware workforce within THC.

1.2.7 Review performance in relation to business outcomes

It is important to frame governance in terms of the value creation of THC. Governance should promote the value creating activities of THC and increase cohesiveness between security goals and business outcomes.

1.3 Enterprise Information Security Policy

The EISP is the high-level information security policy that sets the strategic direction, scope and tone for all of an organisation's security efforts. It's important in business continuity management for THC because before implementing any strategies to ensure critical business functions, defining the whole topic of information security and its scope is important in justifying the needs for specific policies.

1.3.1 InfoSec Purpose and Importance

Establishing an overarching direction for general security with an EISP is important because it informs the information security policies and plans that go around the organisation's information assets (see figure 1). There are also the obligations of an organisation legally and ethically to implement the proper information security to protect critical information.

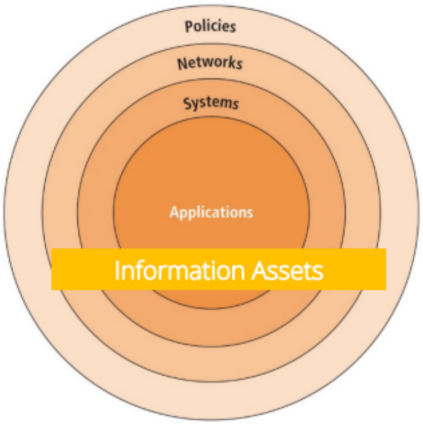

Figure 1: Bullseye Model (Whitman and Mattford 2019)

1.3.2 Roles and Responsibilities

Information Security should be managed with a top down methodology. It is the role of executive management to adopt and maintain the Information Governance strategy and Enterprise Information Security Policy.

A Chief of information security should be elected to develop specific information policies regarding at risk assets threats and vulnerabilities. These should inform information governance to ensure it maintains relevancy to the current situation context of THC. The Technical staff at THC should implement the security controls according to specific security policies (ISSP). These controls should be applied to protect critical business functions and information assets.

Incident Response Teams should be engaged during disaster recovery, and incident handling. Their role is to ensure that incident plans are carried out during a crisis, and assess the controls in place and effectiveness of response post-incident.

2 Business Impact Analysis

Business impact analysis (BIA) is a process that helps an organisation identify, analyse and evaluate potential impacts of a disruption to the business operations. The BIA process also involves identifying critical business functions and processes to analyse the potential consequence that a disruption will have on the business.

A disruption scenario is any event or incident which could disrupt an organisation's operations. The role of disruption scenarios and disruption scenario planning in BCM is to look at the level above individual risks and more at the critical business functions at the operational level, coming up with scenarios which could potentially interrupt those functions and planning around them. For THC, centering BCM and BIA around disruption scenarios keeps the objectives at the business impact level and forces the organisation to determine what are the most critical business units in their operation.So that in the event of a crisis, the business is able to manage the disruption and return to operation efficiently.

2.1 Impact Assessment

To begin a BIA the first major task is to analyse the prioritisation of business processes (this document also refers to them business priority areas) within the organisation (Whitman and Mattford 2019). THC must collect critical information about each of its business units and select which business function must be sustained in order to continue business operations. One problem in this process are the potential internal conflicts about priority (one manager might feel that their function is more critical than another), and it is the role of senior management to arbitrate these problems with the goal of following the mission of business continuity and resilience.

Table 1 shows a list of the top 3 business priority areas within THC with any related information assets of those processes. These business areas are important to THC as they constitute the primary methods of value creation for the organisation. Without the ability to accept patients, employ staff, and fund their employees and supplies. THC would not be able to maintain business continuity.

The three conceived disruption scenarios in table 2 broadly cover the C.I.A triad characteristics of information security that protects data and services, that is confidentiality, integrity

Table 1: Business Priority Areas

Critical Business Functions	**Description**	**Related Information Assets**
Patient Management	The system responsible for maintaining patient information and diagnosis information, as well as private client information such as addresses.	Patient Information, Insurance information, Imaging information
Allied Health & Staff Management	The allied health system is responsible for storing and assisting in diagnosis for patients, and staff information including personal identifiers, ID numbers and other valuable information.	Employee Information, Clinical Knowledge base, Healthcare one Assets
Financial Resolutions	The system responsible for payment processing, staff payroll and patient accounts, as well as insurance information and payment.	Banking, Payroll managers, Insurance Accounts, 3rd Party Accounts

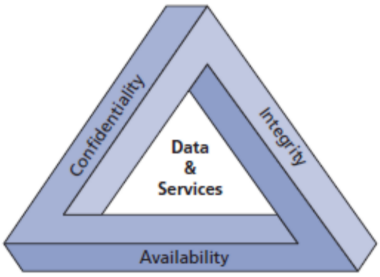

Figure 2: The CIA Triad (Whitman and Mattford 2019)

and accessibility (see figure 2. In this way we cover a diverse range of possible disruptions that can affect THC.

1. The disclosure of sensitive details can be mapped to confidentiality which limits access to information to only those authorised and need it.

2. The deletion or modification of data can be mapped to integrity, an attribute of data that is whole, complete, and uncorrupted.

3. The lack of access to IT systems can be mapped to the availability of information to users.

Table 2: Business Impact Analysis

Disruption Scenario	Lack of access to IT systems	Disclosure of sensitive details	Deletion or Modification of Data
Critical Business Function	Allied Health & Staff Management	Patient Management	Financial Resolution (CKB Licensing & payroll)
Information Asset at Risk	CKB & HealthCare One Application and Payroll System	Patient Data stored in the CKB & Healthcare One and Staff Payrolls.	CKB, HealthCare One and Payroll System
Business Impact	THC can't operate as a clinic as they will not be able to access internal servers for patient records or upload new information	THC's reputation to stakeholders is damaged. Externally to the patients and internally to staff.	THC can't operate as a clinic for patients and can't pay record and manage staff payment
Overall Impact Level	1	2	2
MTD	24 hours	12 hours	24 hours
RTO/RPO	Regain access to IT systems within 48 hours of a loss incident	Regain complete control over what caused the disclosure of data within 24 hours	Reinstate function of IT systems by 48 hours. Reinstate complete backups from remote location by 7 days

See Appendix for more information on Impact level and Risk Rating

Table 3 compares the consequences and likelihood of a disruption scenario and assigns an impact level (used in table 2) and risk rating to them. The risk rating for each disruption scenario is taken from the average risk ratings in the appendix for threat events that constitute a disruption scenario of that type.

Table 3: Assessed Impact Level for Disruption Scenarios

Disruption	Consequence	Likelihood	Risk Rating	Impact Level
Lack of access to IT systems	High	Low	15	1
Disclosure of sensitive details	High	Medium	17	2
Deletion or modification of data	High	Medium	17	2

See Appendix for more information on Impact level and Risk Rating

3 Incident Response Planning

3.1 Incident Handling Procedures

Throughout the incident response planning process, IR procedures, also referred to as standard operating procedures (SOPs) are created in response for handling each identified disruption scenario. The incident-handling procedures cover the steps to perform in response to incidents before, during, and after the incident occurs (3 phases). The procedures outlined encompass the recovery steps for both THC's stakeholders, that is patients and staff as well as an incident response team (IRT) that will guide THC through the IR process with predefined responses. IR procedures are vital because they enable organisations to react to detected incidents quickly and efficiently, reducing wasted time in confusion and increasing the THC's operational resilience to unforeseen events.

3.2 Flooding - Incident Handling Procedure

The region that THC is located in, is an at risk area for seasonal flooding. These floods could vary in severity where a minor flood may only cause minor damages to the building and its flooring, or it may be a high severity flood which damages the building structure and any IT systems. Additionally the back up facility is located in the same region, and thus it may also be subject to similar damages. It is advised that backups should be located in a remote facility so that they do experience damages and the same time as THC.

Table 4: Flood Incident-Handling Procedure

Disruption Scenario: Loss of Access to IT		
Before An Attack	During An Attack	After An Attack
Stakeholders: • Partake in flood warning training, with regard to procedures in the event of a minor vs major flood event. • Monitor forecasting and flood warnings. • Identify procedures to conduct work remotely	**Stakeholders:** • If the flood is minor, board up the building with sandbags. • If the flood is major, engage evacuation procedures.	**Stakeholders:** • File insurance claim. • Begin remote work and services, until the building is repaired and usable
IR Team: • Ensure critical network infrastructure is located in a water sealable room. • Maintain a store of sandbags and other emergency supplies. • Test evacuation plans. • Ensure IT systems are located on elevated racks and tables, to avoid damage during a minor flood event. • Maintain backups in a remote location.	**IR Team:** • Turn off UPS, Servers and Workstations , to avoid electrocution dangers. • Lock critical IT assets in the water sealable room. • Continue to monitor forecasts for escalation of the flood event and assess the need for evacuation.	**IR Team:** • Take stock of Assets, Building, and Damages. • Assess Incident Response Effectiveness • Assess Evacuation Procedures • Assess warning times and adjust incident handling to accommodate

3.3 Phishing Attacks - Incident Handling Procedure

Phishing attacks are a vessel of delivery for any malware or ransomware. Phishing takes the form of a human psychological attack where the attacker poses themselves as a legitimate body to lure people into revealing personally identifiable information (PII) such as account credentials, financial data or medical records. Phishing attempts are usually done through emails, text messages or links. The table below provides a set of recommended procedures that can be undertaken in the event of a phishing attack causing the disclosure of sensitive data in THC.

Table 5: Phishing Incident-Handling Procedure

Disruption Scenario: Disclosure of Sensitive Details		
Before An Attack	During An Attack	After An Attack
Stakeholders: • View unsolicited emails, links and text messages with high caution. • Don't share credentials to other entities without verifying their integrity. • Don't click on suspicious links or email attachments.	**Stakeholders:** • Report to senior staff and the CSIRT of the event immediately when detected. • Decide whether or not to inform external stakeholders of the event.	**Stakeholders:** • Learn from the mistakes that occurred and increase awareness for better practices.
IR Team: • Provide awareness and training to staff on proper use of email systems and safe cybersecurity practices. • Enable two factor authentication.	**IR Team:** • Implement containment strategies that lock down the account affected or shutdown the system temporarily. Change passwords. • Notify other users internally that a phishing attack has occurred. • Deploy a response team to inspect other users' systems.	**IR Team:** • Conduct an incident recovery investigation. • Train stakeholder awareness on phishing tactics and how to avoid them. • Identify weaknesses in training content. Evaluate incident response actions and effectiveness.

3.4 Ransomware - Incident Handling Procedure

Ransomware is a type of attack designed to block access to a computer system till a ransom is paid. Typically in a ransom attack, there is a threat that data can be deleted or modified; the data is then generally attacked if the ransom isn't paid.

Table 6: Ransomware Incident-Handling Procedure

Disruption Scenario: Deletion or Modification of Data		
Before An Attack	During An Attack	After An Attack
Stakeholders: • Have recent backups • Be trained on how to save data to an offsite location • Don't delete information	**Stakeholders:** • Detect attack quickly • Report the incident to the IT team	**Stakeholders:** • Load backups • Analyse the effectiveness of procedures
IR Team: • Verify backup storage and safety • Implement safeguards	**IR Team:** • Isolate affected systems • Log out all devices	**IR Team:** • Determine what has been modified • Determine the attack vector

3.5 Strategic Recovery

While the incident handling procedures will help aid THC in tactically responding to disruption events it is also important for the organisation to focus on the strategic recovery phase post incident. It is recommended that THC evaluate the impacts of an incident and conduct a review to improve on what could be better next time in the planning or procedures. One framework that can be adopted to help guide this process is NIST 800-184 "Guide for Cybersecurity Event Recovery" (2016) which breaks up the recovery process into five stages (see Appendix).

4 Crisis Communications

A Crisis Communication Plan provides the roles and responsibilities for communicating with stakeholder, incident response teams and the public during a crisis. THC needs a crisis communication plan to present a line of authority and a clear message to the public when incident handling procedures are engaged. This way THC can keep the confidence of their patients and other stakeholders during disastrous events. This communication plan is developed based on the IRACI Model from HB292. Definitions for each of the columns in the table can be found in the Appendix - IRACI Definitions.

Table 7: IRACI Crisis Communication Plan

General Crisis Communication Plan					
Com.	Intervention	Responsibility	Accountability	Consult	Inform
1	Brad Hill	Angelique Farelli	Angelique Farelli, Practice Manager	IR Team,Systems Admin	Patients, Public, Donors
2	Angelique Farelli	Brad Hill	HR Manager	IR Team, Systems Admin	Internal Staff, Allied Health
3	Angelique Farelli and Brad Hill	Head of IR Team IR Team	Systems Admin, HR Manager	Practice Manager	Executive Management
4	Head of IR Team	IR Team	IR Team	Emergency Services, Systems Admin	IR Team, Directors, Systems Admin
General Crisis Communication Details					
Com.	Description		Key Message	Format	Frequency
1	Message to the public and patients during crisis.		Under Control. Where to seek services during downtime.	Press release, Social Media, Local News	Daily, or Weekly
2	Internal communications, to staff to update on status.		What progress has been made,Current procedures to take, Working remotely	Email,Meetings	Daily or Weekly
3	Communication to management.		Updates on Status,What needs to be done.	Email, SMS, Meetings	Daily or Hourly
4	Communication between IR Team and Directors during an emergency affecting traditional communication.		Updates on status, Progress to restoring proper communication.	Radio phones	Hourly

References

NSQHS (2014). *Action 1.16 Australian Commission on Safety and Quality in Health Care*. Safetyandquality.gov.au. URL: https://www.safetyandquality.gov.au/standards/nsqhs-standards/clinical-governance-standard/patient-safety-and-quality-systems/action-116 (visited on 03/22/2023).

Violino, Bob (Aug. 2019). *How much should you spend on security?* CSO Online. URL: https://www.csoonline.com/article/3432138/how-much-should-you-spend-on-security.html%5C#:%5C~:text=As%5C%20a%5C%20rule%5C%20of%5C%20thumb.

Whitman, Michael E and Herbert J Mattford (2019). *Management of information security*. 6th ed. Cengage Learning.

Australian Information Commissioner, Office of the (2022). *Australian Privacy Principles quick reference*. OAIC. URL: https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-quick-reference (visited on 03/22/2023).

A Glossary

A.1 CIA Triad

Confidentiality An attribute of information that describes how data is protected from disclosure or exposure to unauthorised individuals or systems.

Integrity An attribute of information that describes how data is whole, complete, and uncorrupted.

Availability An attribute of information that describes how data is accessible and correctly formatted for use without interference or obstruction.

A.2 Risk Rating Values

Critical (21-25) The event has a 85% chance of happening or incurs significant financial or reputational damages

High (16-20) The event has a 75% chance of happening or incurs major financial damages and a weeks outage of business operation

Medium (11-15) The event has 50% chance of happening or incurs moderate financial damages and a day outage to business operation

Low (6-10) The event has 15% chance of happening or incurs minor financial damages and temporary outage to some business operation

Trivial (1-5) The event will rarely occur or incurs negligible financial damages and only inconveniences to business operation

A.3 Impact Values

Assess the consequence, likelihood and risk prioritisation of a disruption scenario and assign a business impact level to that to be used in a business impact analysis. The table below qualitatively explains the arbitrary scaling levels of business impact that a disruption scenario may cause to critical business functions.

Impact 1 Business functions are mission-critical and must be available during all business hours. Online systems must be available 24 hours a day, seven days a week.

Impact 2 Business processes can survive without the business function for a short amount of time.

Impact 3 Business processes can survive without the business functions for a longer period of time.

Impact 4 Business processes can survive without the business functions for extended periods without the collapse of the business.

A.4 IRACI Definitions

Intervention This identifies who has ultimate control over communication. This allows for communication to be vetoed or altered or monitored. Particularly in the event that the communication is misinterpreted, dishonest or does not hold the values of the organisation.

Responsibility: This identifies who is responsible for initiating and conducting the communication. THey are liable for ensuring the communication reaches its intended audience.

Accountability Accountability is about who can authorise the communication and its content.

Consult This identifies the individuals or groups who may need to be consulted during the communication. This is not the audience of the communication, but may include specialised individuals who may be able to specify the technical details in the content of the communication.

Inform This is the intended audience of the communication. Who needs to be made aware of the content in the communication.

In addition to the IRACI model the following additional columns are used to specify additional components of the communication:

Key Message What is the key component of the content of the communication.

Format In what manner and media should the communication be released.

Frequency How often should the communication take place?

A.5 Cybersecurity Incident Response Framework

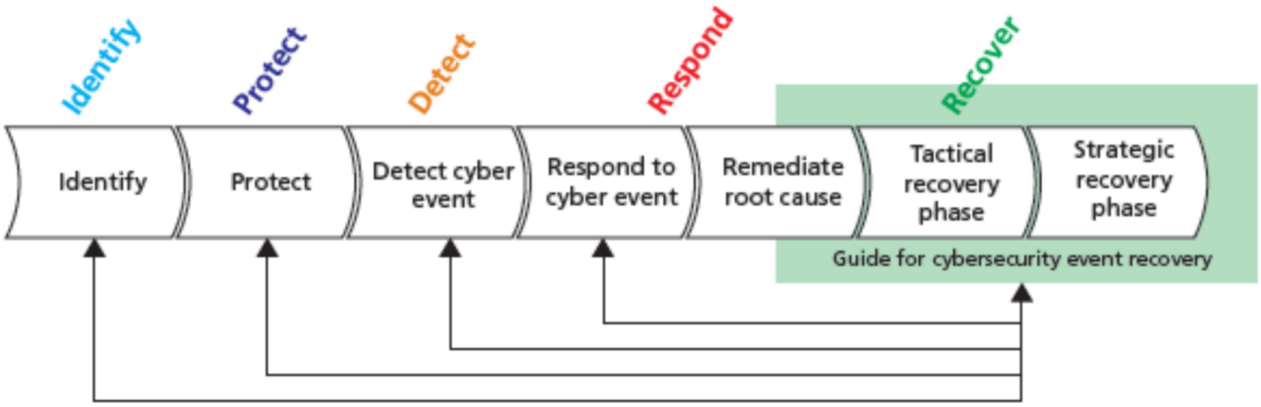

Figure 3: NIST 800-184 from (Whitman and Mattford 2019)

B Selection process for Business Impact Area

Table 8 documents the decision making process for the critical Business Functions and Disruption Scenarios. This is based on a previous risk assessment conducted for THC which prioritised risks of certain Threats to Assets and their Vulnerabilities. From this we can see that Patient Management, Allied Health & Staff Management, and Financial Resolutions are the most at risk business functions and should be prioritised. This table also identifies disruption scenarios that should be considered based on the types of threat events common to each critical business function.

Table 8: Expanded BIA Selection Process

Asset	**Threat Event**	**Risk Rating**	**Associated Business Function**	**Disruption Scenario**
CKB (Application)	Power outage	12	Call-in and Resolution Services	Loss of access to IT systems & data
CKB (Datastore)	Data Breach	20	Patient Treatment Services	Disclosure of sensitive details. Reputational Harm
CKB (Datastore)	Ransomware	20	Patient Treatment Services, CKB IP Leasing	Loss of access to IT systems & data, Deletion or Modification of Data
CKB (Datastore)	Destructive Virus	15	Patient Treatment Services, CKB IP Leasing	Deletion or Modification of Data
CKB (Program Code)	Data Breach	20	CKB IP Leasing	Disclosure of sensitive details
Internal Server	Flood of building	10	Patient Treatment Finance Resolution, Allied Health Communication	Loss of access to IT systems & data
Internal Server	Power Outage	15	Patient Treatment, Finance Resolution, Allied Health Communication	Loss of access to IT systems & data

Continued on next page

Table 8: Expanded BIA Selection Process *Continued*

Asset	**Threat Event**	**Risk Rating**	**Associated Business Function**	**Disruption Scenario**
HealthCare One (Application)	Software Faults	12	Finance Resolution, Patient Management, Allied Health & Staff Management	Loss of access to IT systems & data
HealthCare One (Datastore)	Data Breach, Phishing	20	Finance Resolution, Patient Management, Allied Health & Staff Management	Disclosure of sensitive details
HealthCare One (Datastore)	Ransomware	20	Finance Resolution, Patient Management, Allied Health & Staff Management	Loss of access to IT systems & data, Deletion or Modification of Data
HealthCare One (Datastore)	Destructive Virus	15	Finance Resolution, Patient Management, Allied Health & Staff Management	Deletion or Modification of Data
Patient Data	Data Breach	12	Patient Management	Disclosure of sensitive details, Reputational Harm
Patient Data	Ransomware	12	Patient Management	Loss of Access to IT systems & data, Reputational Harm, Deletion or Modification of Data
Patient Data	Human Error (Incorrect Entry)	9	Patient Management	Deletion or Modification of Data

Continued on next page

Table 8: Expanded BIA Selection Process *Continued*

Asset	**Threat Event**	**Risk Rating**	**Associated Business Function**	**Disruption Scenario**
Allied Health Professional Data	Data Breach	10	Allied Health & Staff Management	Disclosure of sensitive details
Patient Call-Records	Data Breach	15	Patient Management, Call-in and Resolution Services	Disclosure of sensitive details, Reputational Harm
Supply lists	Data Breach	20	Finance Resolutions	Disclosure of sensitive details
Staff Data	Data Breach	20	Finance Resolutions, Allied Health & Staff Management	Disclosure of sensitive details
Website	DoS Attack	12	Marketing and Advertising, Patient Management (Bookings)	Loss of access to IT systems & data