Contents

Introduction

This report provides a cyber risk evaluation for ACME Hospitals in the context of new strategic objectives to develop 'IT enabled healthcare'. The assessment follows the ISO 31000 Risk Management Lifecycle framework (ISO, 2019) by outlining the organisational context and identifying possible risks before assessing these risks and recommending mitigations.

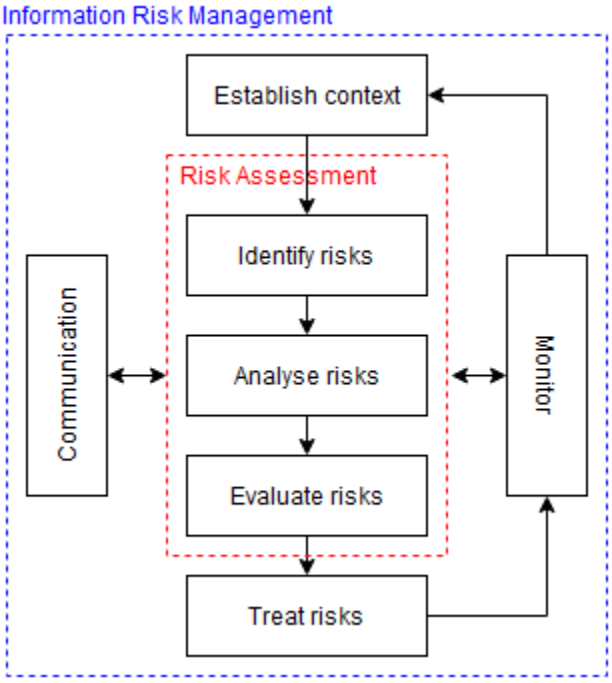


Figure 1: Information risk management process

Part 1a

Organisational Context

Overview

ACME Hospitals is a private healthcare provider. Its competitors include other private services (e.g., HCA, Nuffield Health) and the NHS, which it also partners with. A literature review of competitors highlighted that the sector is a significant target for cyber-attacks, such as the 2017 NHS WannaCry ransomware attack (Morse, 2017), which caused significant reputational damage. Therefore, investing in cybersecurity measures will both ensure ACME complies with regulations (e.g., GDPR) and maintains its critical operations.

Structure

An organisational structure is outlined in Figure 2:

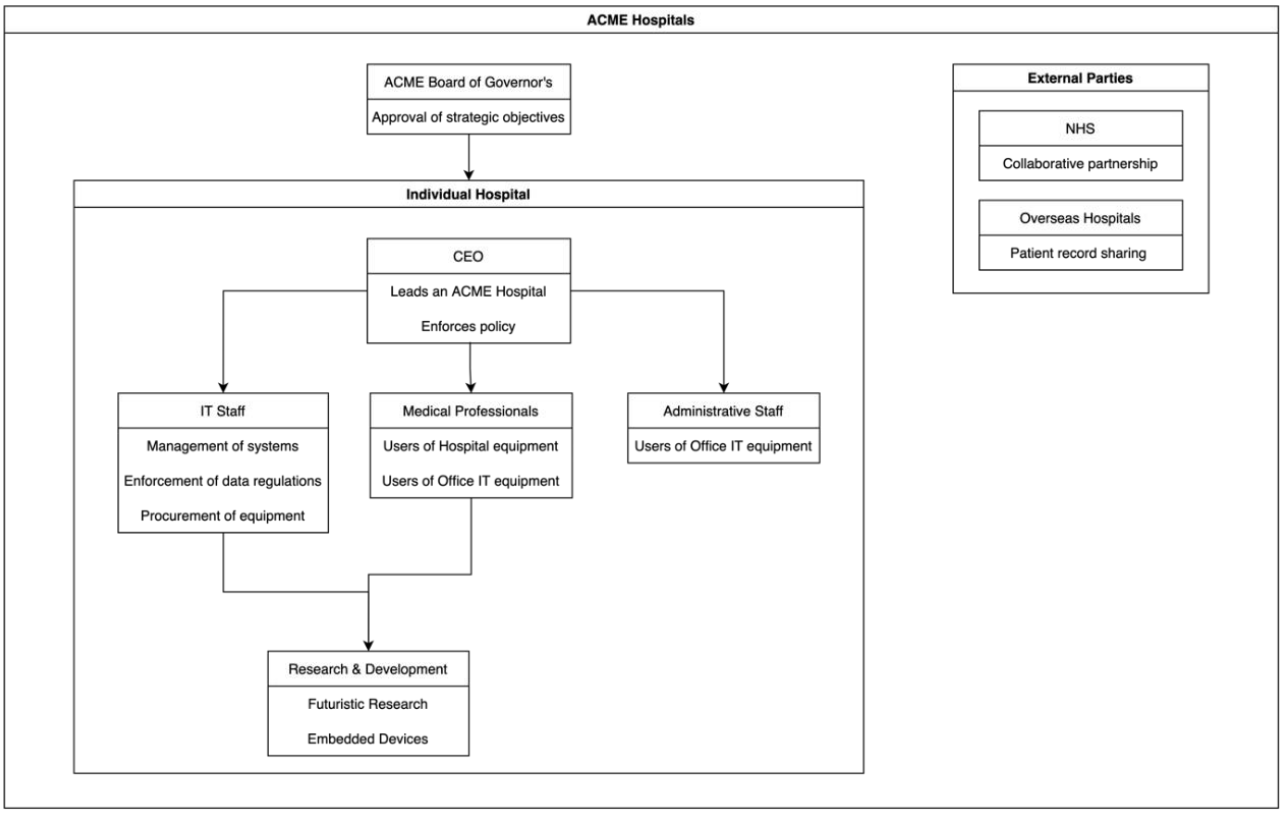


Figure 2: ACME organisational structure

Objectives

The long-term strategic objectives aim to reduce cost through insights generated from data, while providing more patient-centric care. The additions are extensions to ACME's existing IT provision, and such changes must integrate with the existing IT infrastructure. A diagram of the system environment and boundaries is presented in Figure 3:

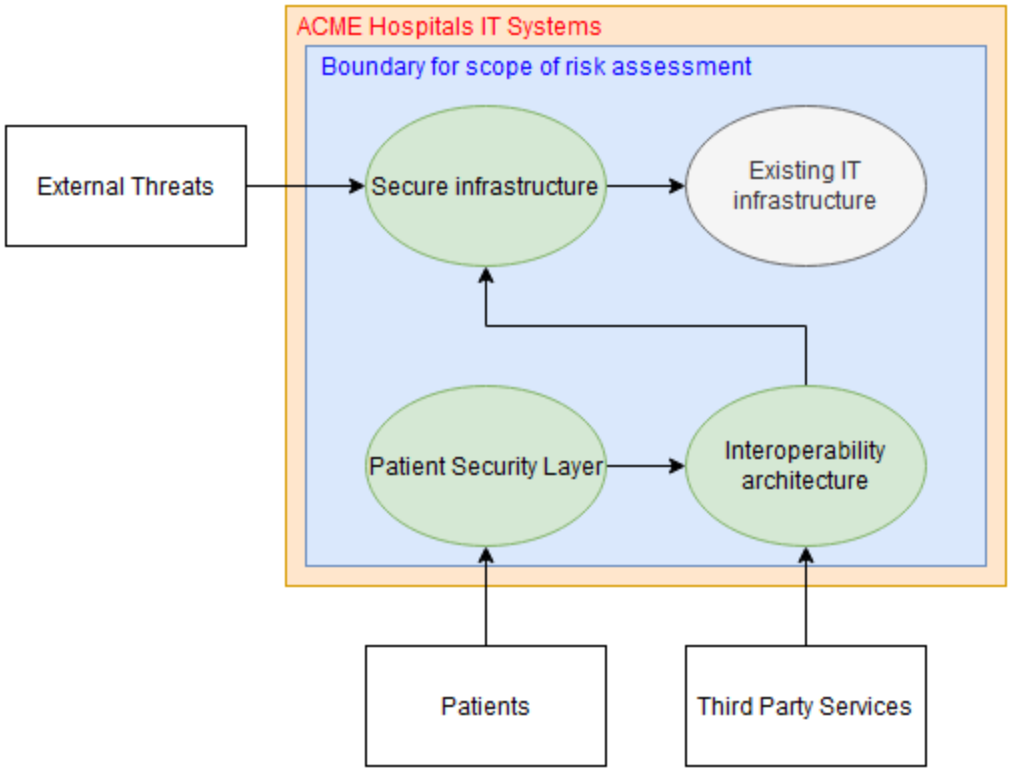


Figure 3: Context boundary diagram

The stakeholders associated with these objectives include:

- **Board of governors** – setting the strategic objectives
- **CEOs** – overseeing implementation of strategic objectives
- **Staff, patients, and third parties** – accessing systems

Since the infrastructure projects are dependent on existing infrastructure, and no cybersecurity measures are assumed other than those specified in the brief, this report evaluates the entire ACME IT system (both existing and future infrastructure).

Asset Identification and Classification

A summary of assets is presented in Table 1. Information assets are also classified in compliance with ISO 27001 Control Objective A8.2 (ISO/IEC, 2013)

Table 1: Asset table

Asset Type		Asset		Further Details	Data classification	Profit Impact
Buildings		Central HQ		Contains hardware for central database and web portal hosting.		
		ACME Hospital Sites				
		3rd Party Buildings		ACME aim to develop partnerships with the NHS and provide patient information when necessary to 3rd parties abroad.		
People	Internal	Board of Governors		Approve strategic objectives and policies		
		CEO		One per hospital		
		Employees	750 Medical Professionals			
			200 Admin Staff			
			50 IT team Staff	Manage all IT systems, enforcement of data regulations, and procurement of equipment		
		Third Party Staff		NHS, pharmacy staff, etc.		
	External	Patients		Approximately 7,000-10,000 patients per year, per hospital		
		Suppliers	General IT Hardware	Dell, HP, etc.		
			Vendor Specific hardware	Medical equipment suppliers, etc.		
Processes		Data Protection and Sharing	Sharing data internally	Procedures require to ensure data is not shared unsafely/illegally/unnecessarily. Internal data access requires a VPN to access the HQ central database.		
			Sharing data with 3rd party organisations			
			Sharing data with patients			
		Equipment Procurement				
		Implementing Policies from Board				
		Equipment Repair				
		Connecting to ACME systems		Most IT systems requires two factor authentication; a login/password and a code sent to the registered mobile phone.		

Asset Type	Asset		Further Details	Data classification	Profit Impact
Data/Information	Patient Records			Confidential	High
	Staff Records			Restricted	Medium
	Contract Information		Contracts with suppliers and third parties.	Confidential	High
	Hospital Information		Hospital layout, schedules, room allocation.	Public	Low
	Login Information	Encryption Keys		Confidential	Critical
		2FA Codes			
		Usernames /Passwords			
	Security Procedures			Confidential	Critical
	Company Objectives and Plans			Confidential	High
	Research	Data	Data protection laws must be adhered to.	Confidential	High
		Reports			
Software	Windows				
	Dedicated Embedded OS		Specialised Devices use embedded OS		
	Web Portal Front End Code and Integrity		Mark up and other code for the public facing website		
	Web Portal Back End		Back-end code managing the public facing website		
	Firewalls				
	Administrative Systems		Other software used in the hospital, for inputting patient information, accessing staff records etc.		
Hardware	Central Database		Located in central HQ		
	Web Servers		Located in central HQ		
	Equipment	General			
		Specialised			
Networking	Intranet Segmented Virtual LANs	HR			
		R&D			
		Other Traffic			
	VPN		Central HQ data sharing uses site-to-site virtual private networks		
	Public Web Portal		Provides access to information in the centralised database		
	IoT Devices		Part of organisation plan to utilise IoT devices in hospital and patient homes		
	Endpoints (e.g. PC networking)				

Asset Type		Asset		Further Details	Data classification	Profit Impact
Plans	Core Objectives	Increase data ease of availability	To Patients			
			To Clinicians			
			To Third Parties			
		Increase Research capabilities				
	New Infrastructure	Security Infrastructure	IoT integration			
			Patient interaction channels			
			Decision + monitoring services			
		New Security layer				
		An interoperability architecture				

Asset Prioritisation

Methodology

Vulnerabilities were developed and prioritised using the Delphi method. Each cyber risk expert individually compiled a list of possible vulnerabilities, each linked to an asset in Table 1. Repeated vulnerabilities were discarded.

Each expert scored each vulnerability on a 1 (low) to 5 (high) scale of importance, where importance was defined as a compromise of likelihood and impact. Scores with the most variation were discussed. Following this discussion, several vulnerabilities were added and discarded prior to the second round.

Each expert scored all vulnerabilities again, with original scores hidden to reduce confirmation bias. Following the second round the variations were deemed sufficiently low to be considered final.

Delphi Table

The Delphi method results are presented in Table 2:

Table 2: Delphi table

#	Asset at Risk	Vulnerability	1-1	1-2	1-3	1-4	1-5	Ave	Var	2-1	2-2	2-3	2-4	2-5	Ave2	Var2
34	Internal People & Data/Information	Malicious ads online | Employees clicking on while using hospital equipment	2.00	1.00	2.00	3.00	1.00	1.80	0.70	2.00	1.00	1.00	2.00	2.00	1.60	0.30
39	Research Benefits	Data collection incorrect at time of collecting the data	1.00	1.00	1.00	1.00	2.00	1.20	0.20	1.00	1.00	2.00	2.00	2.00	1.60	0.30
52	Paatients & Login Information	Patients lose their credentials	3.00	2.00	3.00	1.00	1.00	2.00	1.00	2.00	2.00	1.00	1.00	2.00	1.60	0.30
57	Research Benefits	Collected Data (used to improve systems) could be misrepresented/interpreted a	2.00	1.00	2.00	1.00	2.00	1.60	0.30	1.00	2.00	2.00	2.00	1.00	1.60	0.30
25	Medical Proffesionals & Data/Information	Medical staff mistakenly share information | wrong information	4.00	3.00	4.00	3.00	2.00	3.20	0.70	3.00	2.00	1.00	1.00	2.00	1.80	0.70
32	Patients	Patients mess with equipment in their vicinity	3.00	2.00	3.00	2.00	3.00	2.60	0.30	3.00	1.00	2.00	1.00	2.00	1.80	0.70
1	ACME Hospitals	Hosptial broken into | Trespassing in standard hospital areas	3.00	2.00	3.00	3.00	2.00	2.60	0.30	2.00	2.00	2.00	2.00	2.00	2.00	0.00
3	ACME Hospitals & Hardware	Physical damage to infrastructure	2.00	2.00	2.00	2.00	2.00	2.00	0.00	2.00	2.00	2.00	2.00	2.00	2.00	0.00
30	IT Staff	IT staff hold processes only they know ransom	1.00	2.00	2.00	3.00	3.00	2.20	0.70	1.00	2.00	2.00	3.00	2.00	2.00	0.50
8	Login Information	Phone stolen for 2 factor authentication	2.00	2.00	2.00	4.00	2.00	2.40	0.80	2.00	2.00	2.00	3.00	2.00	2.20	0.20
9	Login Information	Keyboard sniffer to steal passwords	3.00	2.00	3.00	3.00	2.00	2.60	0.30	3.00	2.00	2.00	2.00	2.00	2.20	0.20
11	Internal People	Rogue Employee angry at company	2.00	2.00	1.00	2.00	2.00	1.80	0.20	2.00	2.00	2.00	3.00	2.00	2.20	0.20
18	Board of Govenors	Board of Govenors fire integral security expert	1.00	3.00	3.00	4.00	3.00	2.80	1.20	1.00	2.00	2.00	3.00	3.00	2.20	0.70
24	Medical Proffesionals & Data/Information	Medical staff misuse equipment | poor IT literacy	1.00	2.00	3.00	3.00	2.00	2.20	0.70	2.00	2.00	2.00	2.00	3.00	2.20	0.20
54	Buildings	Physical access gained by tailgating	3.00	2.00	4.00	2.00	3.00	2.80	0.70	3.00	2.00	2.00	2.00	2.00	2.20	0.20
53	Patients & Data/Information	Patients delete data they did not intend to	3.00	1.00	4.00	2.00	3.00	2.60	1.30	3.00	2.00	2.00	2.00	3.00	2.40	0.30
59	Specialised Equipment & IoT Devices	User error on patient at home devices	5.00	2.00	3.00	3.00	3.00	3.20	1.20	3.00	2.00	2.00	3.00	2.00	2.40	0.30
4	Central Database	General outages could affect ability to access information	4.00	3.00	4.00	5.00	4.00	4.00	0.50	3.00	3.00	2.00	2.00	3.00	2.60	0.30
10	Internal People	Rogue Employee bribed by competitor | 3rd Party	3.00	3.00	1.00	2.00	2.00	2.20	0.70	3.00	2.00	3.00	3.00	2.00	2.60	0.30
27	IT Staff & Data/Information	IT team underpaid and strike: no reinforcement to deal with attacks	2.00	2.00	3.00	4.00	5.00	3.20	1.70	2.00	2.00	3.00	3.00	3.00	2.60	0.30
51	Web Portal + Servers	Public facing web portal could be misused by public	3.00	2.00	2.00	1.00	2.00	2.00	0.50	3.00	2.00	3.00	3.00	2.00	2.60	0.30
20	Internal People	Disillusioned employee sabotage equipment	2.00	3.00	2.00	3.00	2.00	2.40	0.30	2.00	3.00	3.00	3.00	3.00	2.80	0.20
26	IT Staff & Data/Information	IT staff seem to all have full permissions - could set up a middle man device	1.00	3.00	4.00	4.00	3.00	3.00	1.50	2.00	3.00	3.00	3.00	3.00	2.80	0.20
40	Data/Information	Data stored locally by the medical devices themselves | being accessed	4.00	1.00	1.00	2.00	3.00	2.20	1.70	4.00	2.00	3.00	2.00	3.00	2.80	0.70
41	Web Portal + Servers	SQL injection in web forms	3.00	3.00	2.00	3.00	3.00	2.80	0.20	3.00	2.00	3.00	3.00	3.00	2.80	0.20
17	Board of Govenors	Board of Govenors make misinformed security decisions	3.00	4.00	4.00	5.00	4.00	4.00	0.50	3.00	3.00	3.00	3.00	3.00	3.00	0.00
28	General Hardware	Inherent issues/bugs/vunerabilities in windows OS	2.00	4.00	3.00	4.00	4.00	3.40	0.80	2.00	3.00	3.00	4.00	3.00	3.00	0.50
29	Login Information	Passwords leaked: not very secure passwords	4.00	4.00	4.00	4.00	3.00	3.80	0.20	4.00	3.00	3.00	3.00	2.00	3.00	0.50
12	Data/Information	Phishing emails responded to	4.00	3.00	3.00	3.00	3.00	3.20	0.20	3.00	3.00	3.00	4.00	3.00	3.20	0.20
38	Login Information	Impersonating patient to gain access to the patients own records	5.00	1.00	1.00	1.00	2.00	2.00	3.00	5.00	3.00	3.00	2.00	3.00	3.20	1.20
21	Data/Information	MITM attack (SSL stripping or cert spoofing)	3.00	3.00	2.00	2.00	3.00	2.60	0.30	3.00	4.00	3.00	4.00	3.00	3.40	0.30
31	Patients	Cloud outage which causes some services to fail	3.00	3.00	2.00	3.00	3.00	2.80	0.20	4.00	3.00	4.00	3.00	3.00	3.40	0.30
33	Internal People & Hardware	Malware enters system through USB given to an employee	4.00	4.00	2.00	4.00	2.00	3.20	1.20	4.00	4.00	4.00	3.00	2.00	3.40	0.80
35	Suppliers & Hardware & Data/Information	Vendor employee installs ransomware	1.00	4.00	4.00	5.00	4.00	3.60	2.30	2.00	3.00	4.00	4.00	4.00	3.40	0.80
37	Specialised Equipment & IoT Devices	Specialised vendor goes out of buisiness/supply issues	3.00	3.00	2.00	4.00	3.00	3.00	0.50	3.00	4.00	4.00	3.00	3.00	3.40	0.30
42	Specialised Equipment & IoT Devices	Embedded security tends to be weaker, devices are easy remote access points to	5.00	3.00	2.00	2.00	3.00	3.00	1.50	4.00	3.00	3.00	3.00	4.00	3.40	0.30
62	Data/Information	R2: Medical staff mistakenly share confidential information						N/A	N/A	5.00	4.00	3.00	2.00	3.00	3.40	1.30
5	Suppliers	General security vunerability with a specific vendor (e.g. Dell, HP)	4.00	3.00	4.00	5.00	3.00	3.80	0.70	4.00	3.00	4.00	4.00	3.00	3.60	0.30
50	VPN	VPN DoS prevents access to central database	2.00	4.00	2.00	3.00	4.00	3.00	1.00	2.00	4.00	4.00	4.00	4.00	3.60	0.80
2	ACME Hospitals & Hardware	Physical damage to essential infrastructure (e.g server room)	5.00	3.00	2.00	2.00	5.00	3.40	2.30	4.00	4.00	4.00	3.00	4.00	3.80	0.20
7	IoT Devices	Embedded devices have vunerabilities/unusable due to out of date software/hard	5.00	3.00	4.00	3.00	3.00	3.60	0.80	5.00	4.00	4.00	3.00	3.00	3.80	0.70
15	Central Database	Central database DoS through HQ power outage	3.00	4.00	4.00	4.00	5.00	4.00	0.50	4.00	3.00	4.00	4.00	4.00	3.80	0.20
16	Web Portal + Servers	Web portal servers accessed granting back end manipulation	4.00	5.00	4.00	5.00	5.00	4.60	0.30	4.00	4.00	4.00	3.00	4.00	3.80	0.20
55	Central Database	Data on central database manipulated	3.00	5.00	3.00	3.00	4.00	3.60	0.80	3.00	4.00	4.00	4.00	4.00	3.80	0.20
19	Board of Govenors	Board of Govenors choose ineffective low cost security methods	4.00	3.00	3.00	4.00	3.00	3.40	0.30	4.00	5.00	4.00	4.00	3.00	4.00	0.50
23	Web Portal + Servers	DDoS attack on any web portals (patient facing , internal portals, web systems tha	4.00	3.00	3.00	3.00	3.00	3.20	0.20	4.00	4.00	4.00	4.00	4.00	4.00	0.00
43	Web Portal & Login Information & Servers	Web portal being hacked/manipulated has potential to give out any patients data -	5.00	4.00	2.00	3.00	3.00	3.40	1.30	5.00	4.00	5.00	3.00	3.00	4.00	1.00
46	Patients	Patients share their data with malicious 3rd party	5.00	3.00	3.00	1.00	2.00	2.80	2.20	5.00	5.00	4.00	3.00	3.00	4.00	1.00
58	Specialised Equipment & IoT Devices	Devices in patients homes likely to have much less security | From a networking p	5.00	3.00	5.00	3.00	4.00	4.00	1.00	5.00	4.00	4.00	4.00	3.00	4.00	0.50
60	Hardware	R2: Foreign actor installs ransomware						N/A	N/A	5.00	4.00	4.00	4.00	3.00	4.00	0.50
6	Patient Records	3rd Party Provider has a data breach	5.00	4.00	4.00	3.00	3.00	3.80	0.70	5.00	4.00	4.00	4.00	4.00	4.20	0.20
13	Central HQ	Threat actor gains access to central HQ	3.00	3.00	3.00	3.00	4.00	3.20	0.20	4.00	4.00	4.00	5.00	4.00	4.20	0.20
48	Central Database	With access to database could manipulate encryption to have a backdoor	1.00	5.00	2.00	3.00	4.00	3.00	2.50	4.00	4.00	4.00	5.00	5.00	4.40	0.30
49	Internal People	Lack of security awareness among staff	4.00	5.00	3.00	4.00	5.00	4.20	0.70	4.00	5.00	4.00	5.00	4.00	4.40	0.30
56	VLANs	Lots of sensitive traffic through just one VLAN (IT, clinicians, etc.)	5.00	5.00	4.00	4.00	4.00	4.40	0.30	5.00	5.00	5.00	4.00	3.00	4.40	0.80
61	Thrid Parties	R2: Sensitive data unintentionally shared with third party						N/A	N/A	5.00	4.00	4.00	5.00	4.00	4.40	0.30
22	OS	Vulnerability in outdated OS	5.00	4.00	2.00	3.00	2.00	3.20	1.70	5.00	4.00	5.00	5.00	4.00	4.60	0.30
45	Specialised Equipment & IoT Devices	Threat actor could tamper with IoT devices in homes	5.00	5.00	3.00	2.00	2.00	3.40	2.30	5.00	4.00	5.00	4.00	5.00	4.60	0.30
14	Central Database	Central Database access would allow manipulation of credentials	4.00	4.00	3.00	5.00	4.00	4.00	0.50	5.00	5.00	5.00	5.00	5.00	5.00	0.00
36	Login Information	Impersonating close relative of the patient and gaining access to records	4.00	1.00	3.00	2.00	2.00	2.40	1.30						N/A	N/A
44	Web Portal + Servers	Web portal being hacked/manipulated has potential to give out any patients data -	3.00	3.00	2.00	3.00	3.00	2.80	0.20						N/A	N/A

Results

Five assets are prioritised in this report, selected as they are associated with the five most important vulnerabilities identified in the Delphi method (Table 2):

Table 3: Prioritised assets and vulnerabilities

Rank	Delphi Score	Asset	Main vulnerability
1	5.0	Central HQ database	Admin access to central database would allow for manipulation of credentials
=2	4.6	Operating systems	Outdated OS could contain security vulnerabilities
=2	4.6	Specialised equipment and IoT devices	Threat actor could tamper with medical IoT devices in homes
=4	4.4	Third parties	Sensitive data shared unintentionally with third party
=4	4.4	VLANs	Lots of sensitive data shared though just one VLAN (e.g., IT, Clinicians)

Part 1b

Threat Modelling

Vulnerabilities become threats when considered in context of how they may be exploited. To model threats posed by the vulnerabilities in Table 3, two tools are utilised. STRIDE provides a high-level overview of potential attack vectors, whereas OCTAVE is used to explore specific vulnerabilities in detail and evaluate risk.

STRIDE

Based on the description of ACME hospitals IT infrastructure and the desired strategic objectives, a data flow diagram is produced:

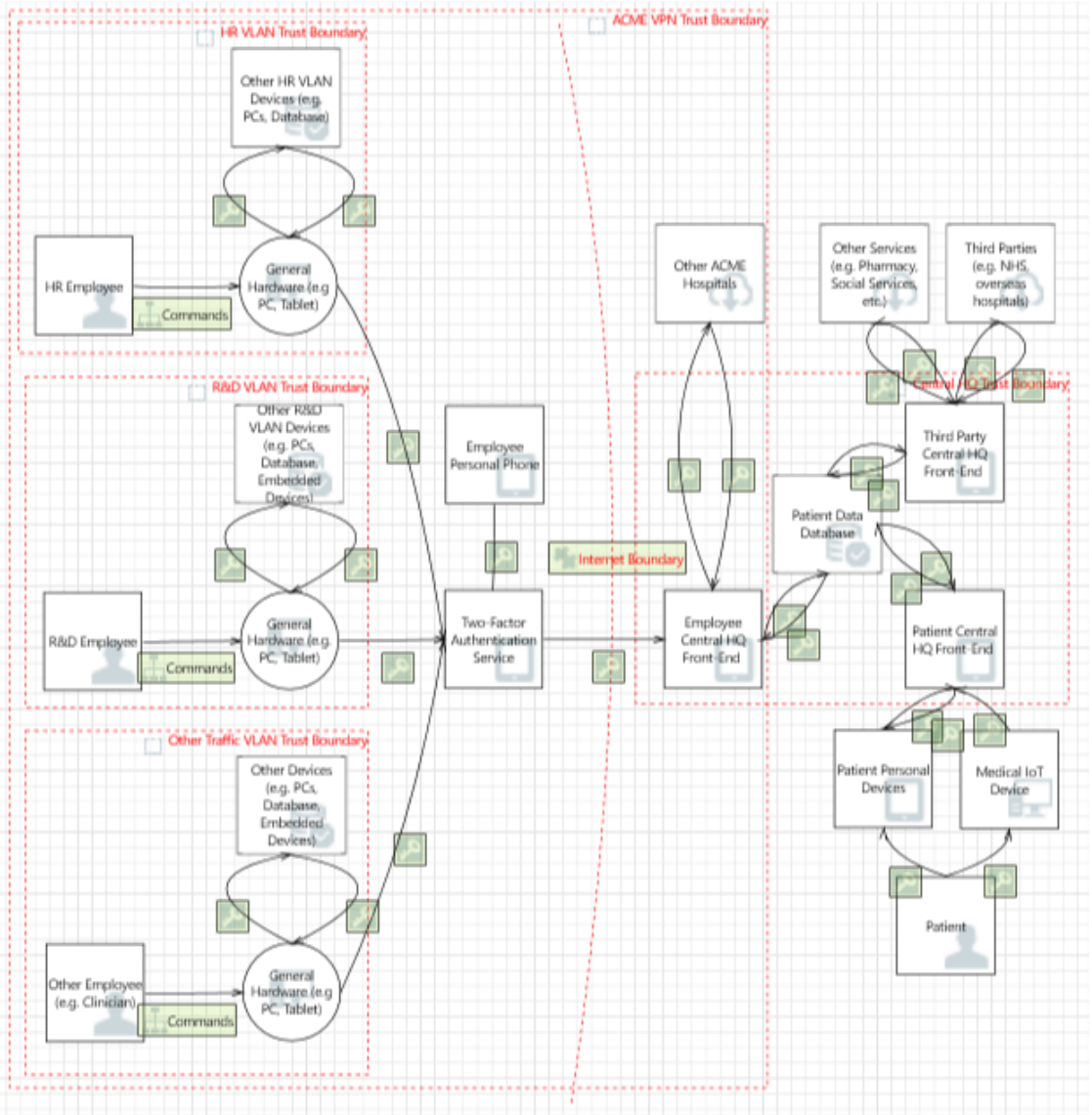


Figure 4: Data flow diagram

Due to the large number of elements, STRIDE per Interaction is chosen to limit the model complexity. The following interactions are identified and categorized by threat type:

Table 4: STRIDE table

Element	Interaction	S	T	R	I	D	E
Medical IoT Device	Collect sensor data and store on device		X			X	
	Send data to central HQ database	X	X	X	X	X	
General Hardware (e.g. PC, Tablet)	General user access local device information	X	X	X	X		
	Request and send data to/from other VLAN devices	X	X	X	X		
	Request and send data to/from central HQ database	X	X	X	X		
	Request and send data to/from other ACME hospitals	X	X	X	X		
	As a privileged user (e.g. R&D, clinician), request and send GDPR patient data to/from central HQ database	X	X	X	X		X
Employee Personal Phone	Authenticate user login	X	X			X	
Other Health Services (e.g. Pharmacy, Social Services)	Request and send data to/from central HQ database	X	X	X	X		
Third Parties (e.g. NHS, Overseas Hospitals)	Request and send data to/from central HQ database	X	X	X	X		
Central HQ Database	Respond to data requests from sources	X	X	X	X	X	
	As a privileged user (e.g. IT), access database admin and logs	X	X	X	X	X	X

This model provides an overview of the most prevalent threats. Tampering threats are likely widespread due to the wide variety of devices and vendors. Conversely, the use of a centralised database limits the number of elements subject to denial of service and elevation of privilege threats; however, this data flow structure may present a significant point of failure. It is notable that accessing the central database presents threats in all six categories, reinforcing its selection as a prioritised asset.

OCTAVE Allegro

OCTAVE Allegro presents a formal eight step process for threat modelling:

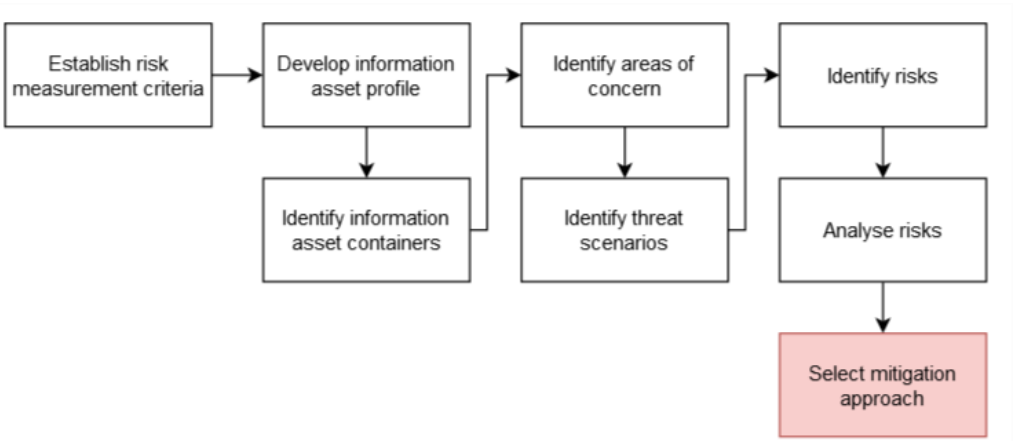


Figure 5: OCTAVE Allegro process

Figures 6, 7, 8, 9, and 10 establish the risk measurement criteria across a range of impact areas, to enable standardised comparison between threats. Some impact areas are more critical to ACME than others, therefore Figure 11 prioritises impact areas from 5 (highest) to 1 (lowest), ensuring the threat model is tailored to ACME's circumstances.

An information asset profile has been established previously in Table 1 (Abrishami, 2019). It was determined that patient records should be the critical information asset in Figure 12, since loss could result in significant reputational damage, GDPR-related sanctions, or harm to the patient. Containers for patient data are identified and owners assigned in Figures 13 and 14

Each of the five prioritised vulnerabilities in Table 3 is evaluated as an area of concern in Figures 15, 16, 17, 18 and 19. The impact area prioritisation is used to produce a relative risk score, which considers the likelihood and severity of the threat.

Allegro Worksheet 1	RISK MEASUREMENT CRITERIA – REPUTATION AND CUSTOMER CONFIDENCE		
Impact Area	**Low**	**Moderate**	**High**
Reputation	Reputation is minimally affected; little or no effort or expense is required to recover.	Reputation is damaged, and some effort and expense is required to recover.	Reputation is irrevocably destroyed or damaged.
Customer Loss	Less than 2 % reduction in customers due to loss of confidence	2 to 5 % reduction in customers due to loss of confidence	More than 5 % reduction in customers due to loss of confidence
Other: Occupancy rates	Reduction of hospital occupancy rates of less than 2%	Reduction of the hospital occupancy rates of 2% - 5%	A reduction of the hospital occupancy rate of more than 5%

Figure 6: Risk measurement criteria – reputation and customer confidence

Allegro Worksheet 2	RISK MEASUREMENT CRITERIA – FINANCIAL		
Impact Area	**Low**	**Moderate**	**High**
Operating Costs	Increase of less than 2 % in yearly operating costs	Yearly operating costs increase by 2 to 5 %.	Yearly operating costs increase by more than 5 %.
Revenue Loss	Less than 10 % yearly revenue loss	10 to 40 % yearly revenue loss	Greater than 40 % yearly revenue loss
One-Time Financial Loss	One-time financial cost of less than $ 100K	One-time financial cost of $ 100K to $ 1M	One-time financial cost greater than $ 1M

Figure 7: Risk measurement criteria – financial

Allegro Worksheet 3	RISK MEASUREMENT CRITERIA – PRODUCTIVITY		
Impact Area	**Low**	**Moderate**	**High**
Staff Hours	Staff work hours are increased by less than 10 % for More than 1 day	Staff work hours are increased between 10 % and 20 % for More than 1 day	Staff work hours are increased by greater than 20 % for More than 1 day
Other: Staff unable to work while system is down (productivity impact)	System down for less than 1 hour	System down for 1 - 2 hours	System down for more than 2 hours

Figure 8: Risk measurement criteria – productivity

Allegro Worksheet 4	RISK MEASUREMENT CRITERIA – SAFETY AND HEALTH		
Impact Area	**Low**	**Moderate**	**High**
Life	No loss or significant threat to customers' or staff members' lives	Customers' or staff members' lives are threatened, but they will recover after receiving medical treatment.	Loss of customers' or staff members' lives
Health	Minimal, immediately treatable degradation in customers' or staff members' health with recovery within four days	Temporary or recoverable impairment of customers' or staff members' health	Permanent impairment of significant aspects of customers' or staff members' health
Safety	Safety questioned	Safety affected	Safety violated And significant regulatory response resulting in investigation

Figure 9: Risk measurement criteria – safety and health

Allegro Worksheet 5	RISK MEASUREMENT CRITERIA – FINES AND LEGAL PENALTIES		
Impact Area	**Low**	**Moderate**	**High**
Fines	Fines less than $ 5000 are levied.	Fines between $ 5000 and $ 10000 are levied.	Fines greater than $ 10000 are levied.
Lawsuits	Non-frivolous lawsuit or lawsuits less than $ 5000 are filed against the organization, or frivolous lawsuit(s) are filed against the organization.	Non-frivolous lawsuit or lawsuits between $ 5000 and $ 10000 are filed against the organization.	Non-frivolous lawsuit or lawsuits greater than $ 10000 are filed against the organization.
Investigations	No queries from government or other investigative organizations	Government or other investigative organization requests information or records (low profile).	Government or other investigative organization initiates a high-profile, in-depth investigation into organizational practices.

Figure 10: Risk measurement criteria – fines and legal penalties

Allegro Worksheet 7	IMPACT AREA PRIORITIZATION WORKSHEET
PRIORITY	IMPACT AREAS
5	**Reputation and Customer Confidence**
1	**Financial**
3	**Productivity**
2	**Safety and Health**
4	**Fines and Legal Penalties**

Figure 11: Prioritization of impact areas

Allegro Worksheet 8	CRITICAL INFORMATION ASSET PROFILE		
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*	
Patient records	Records of patients personal data and medical history is important as this information affects any procedures that might be carried out. For example, a chronic health condition could affect treatment plans	This information contains personal identification data such as names, home addresses, NI numbers, insurance details, payment data, treatment history, medical data, and criminal records.	
(4) Owner(s) *Who owns this information asset?*			
ACME			
(5) Security Requirements *What are the security requirements for this information asset?*			
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	Clinical staff involved in treatment Patients: their own data Administrative staff: limited access R&D: access to medical data but not personal identification data	
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	Clinical staff involved in treatment Administrative staff: limited access	
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	Clinical staff Administrative staff	
	This asset must be available for 24 hours, 7 days/week, 52 weeks/year.	Procedures happen at any time of day, 7 days a week	
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:		
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*			
❑ Confidentiality	☑ Integrity	❑ Availability	❑ Other

Figure 12: Critical information asset profile

Allegro Worksheet 9a	INFORMATION ASSET RISK ENVIRONMENT MAP (TECHNICAL)
INTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1. Database servers, web servers, Windows OS, HP, Dell	Hospital IT Department
2. Internal network, VPN, virtual LANS, central HQ site	Hospital IT Department
3. Hospital workstations	Hospital IT Department
4.	
EXTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1. Internet: patients access their information through an online portal	Unknown
2. NHS cloud database: NHS owned or an external company	NHS/External
3. Patients' personal devices	Patients
4.	

Figure 13: Information asset risk environment map (technical)

Allegro Worksheet 9b	INFORMATION ASSET RISK ENVIRONMENT MAP (PHYSICAL)	
INTERNAL		
	CONTAINER DESCRIPTION	**OWNER(S)**
1.	Paper copies of patients' personal information and medical records	Admin staff
2.	Paper: written data for R&D	R&D
3.	Printed scans, eg. X-rays and ultrasound scans	Clinicians
		Patients
4.		
EXTERNAL		
	CONTAINER DESCRIPTION	**OWNER(S)**
1.	Letters sent to patients with confidential information regarding treatment or medical history	Patients
		R&D
2.		
3.		
4.		

Figure 14: Information asset risk environment map (technical)

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Information Asset	Patient records		
	Area of Concern	Central database would allow manipulation of credentials		
Threat	(1) Actor *Who would exploit the area of concern or threat?*	Malicious attacker, either internal or external		
	(2) Means *How would the actor do it? What would they do?*	The attacker would change credentials enabling unauthorised persons to have access to confidential data		
	(3) Motive *What is the actor's reason for doing it?*	This could be to gain access to confidential data in order to sell it, destroy it, or modify it with malicious intent		
	(4) Outcome *What would be the resulting effect on the information asset?*	☑ **Disclosure** ☑ **Destruction** ☑ **Modification** ☐ **Interruption**		
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Information asset could have been modified, destroyed, or seen by people who should not have access		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	☐ **High**	☑ **Medium**	☐ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Patient records and treatment information being erased or modified could result in incorrect treatment for the patients, especially if data has been modified without the clinicians knowledge. This could result in injury or death	Reputation & Customer Confidence	3	15
	Financial	1	1
Legal fines for patient information being leaked	Productivity	3	9
	Safety & Health	3	6
Reputation of company affected: loss of customers	Fines & Legal Penalties	2	8
	User Defined Impact Area		
	Relative Risk Score		34

Figure 15: Information asset risk – central database manipulation

Allegro - Worksheet 10	Information Asset Risk Worksheet			
Information Asset Risk	Information Asset	Patient Records		
	Area of Concern	Outdated operating system		
	Threat (1) Actor *Who would exploit the area of concern or threat?*	Hackers; malicious attacks may result in data being stolen to sell on the black market.		
	Threat (2) Means *How would the actor do it? What would they do?*	IoT medical equipment with outdated software with security gaps allow hackers to easily access equipment databases with patient records. Ransomware may also be installed.		
	Threat (3) Motive *What is the actor's reason for doing it?*	Access patients' personal and medical data to sell on the darknet, which may be used for identity fraud or other purposes.		
	Threat (4) Outcome *What would be the resulting effect on the information asset?*	☒ Disclosure ☐ Destruction ☐ Modification ☐ Interruption		
	Threat (5) Security Requirements *How would the information asset's security requirements be breached?*	Privacy breach - unauthorised access to patient data.		
	Threat (6) Probability *What is the likelihood that this threat scenario could occur?*	☒ High	☐ Medium	☐ Low

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
- Loss of patients due to mistrust	Reputation & Customer Confidence	2	10
	Financial	3	3
- Legal fees if patients sue	Productivity	1	3
	Safety & Health	1	2
- Loss of data if attacker deletes records (this could potentially result in health risks to patients as diagnoses and treatment may not be given correctly).	Fines & Legal Penalties	2	8
	User Defined Impact Area		
		Relative Risk Score	26

Figure 16: Information asset risk – OS vulnerabilities

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Information Asset	Patient Records		
	Area of Concern	Threat actor tampers with Embedded IoT medical devices in homes		
Threat	(1) Actor *Who would exploit the area of concern or threat?*	The actor may be a corrupt member of staff, someone who appears to be visiting the hospital or patients themselves.		
	(2) Means *How would the actor do it? What would they do?*	Data may be read from embedded devices without adequate encryption, or if debug ports are left exposed, an actor may access data.		
	(3) Motive *What is the actor's reason for doing it?*	Access patients' personal and medical data to sell on the darknet, which may be used for identity fraud or other purposes. The actor may attempt to change medical records such that a patient receives different treatment.		
	(4) Outcome *What would be the resulting effect on the information asset?*	☒ Disclosure ☒ Destruction ☒ Modification ☐ Interruption		
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Privacy breach - unauthorised access to patient data.		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	☐ High	☒ Medium	☐ Low

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
- Fines	Reputation & Customer Confidence	2	10
	Financial	2	2
- Legal fees and reputation if actor is hospital staff or if data is stolen and sold	Productivity	1	9
	Safety & Health	2	4
- Loss of data if actor deletes records (this could potentially result in health risks to patients as diagnoses and treatment may not be given correctly).	Fines & Legal Penalties	3	12
	User Defined Impact Area		
		Relative Risk Score	37

Figure 17: Information asset risk – IoT devices tampering

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET		
Information Asset Risk	Information Asset	Patient Records	
	Area of Concern	Hospital shares data with third parties	
Threat	(1) Actor *Who would exploit the area of concern or threat?*	The third party may be a company the hospital intentionally sends data to, or a malicious attacker obtaining data by spoofing.	
	(2) Means *How would the actor do it? What would they do?*	Data is sent directly to third party, intentionally.	
	(3) Motive *What is the actor's reason for doing it?*	Data may be sold, used for fraudulent purposes, as a means to blackmail the hospital or for business purposes (steal customers).	
	(4) Outcome *What would be the resulting effect on the information asset?*	☒ Disclosure ☐ Destruction ☐ Modification ☐ Interruption	
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Privacy breach - unauthorised access to patient data.	
	(6) Probability *What is the likelihood that this threat scenario could occur?*	☐ High	☒ Medium ☐ Low

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
- Fines	Reputation & Customer Confidence	3	15
	Financial	3	3
- Legal fees and reputation if actor is hospital staff or if data is stolen and sold	Productivity	1	3
	Safety & Health	1	2
- Reputation damage due to privacy breach, which may result in further financial burden.	Fines & Legal Penalties	3	12
	User Defined Impact Area		
		Relative Risk Score	35

Figure 18: Information asset risk – Data sharing with third parties

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk / Threat	Information Asset	Patient records		
	Area of Concern	Traffic going through a single virtual LAN		
	(1) Actor *Who would exploit the area of concern or threat?*	Malicious attacker, either internal or external Staff: unintentional		
	(2) Means *How would the actor do it? What would they do?*	The actor would access, modify or delete data through the virtual LAN either intentionally or accidentally		
	(3) Motive *What is the actor's reason for doing it?*	To access confidential data, or by accident		
	(4) Outcome *What would be the resulting effect on the information asset?*	☑ **Disclosure** ☑ **Destruction** ☑ **Modification** ☐ **Interruption**		
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Information asset could have been modified, destroyed, or seen by people who should not have access		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	☐ **High**	☑ **Medium**	☐ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Patient records and treatment information being erased or modified could result in incorrect treatment for the patients, especially if data has been modified without the clinicians knowledge. This could result in injury or death	Reputation & Customer Confidence	3	15
	Financial	1	1
Legal fines for patient information being leaked	Productivity	1	9
	Safety & Health	3	6
Reputation of company affected: loss of customers	Fines & Legal Penalties	1	8
	User Defined Impact Area		
	Relative Risk Score		34

Figure 19: Large amount of traffic through single VLAN

Risk Analysis

Cause consequence diagrams (CCA) are employed for each prioritised vulnerability to evaluate possible attack vectors and consequences.

Central HQ Database

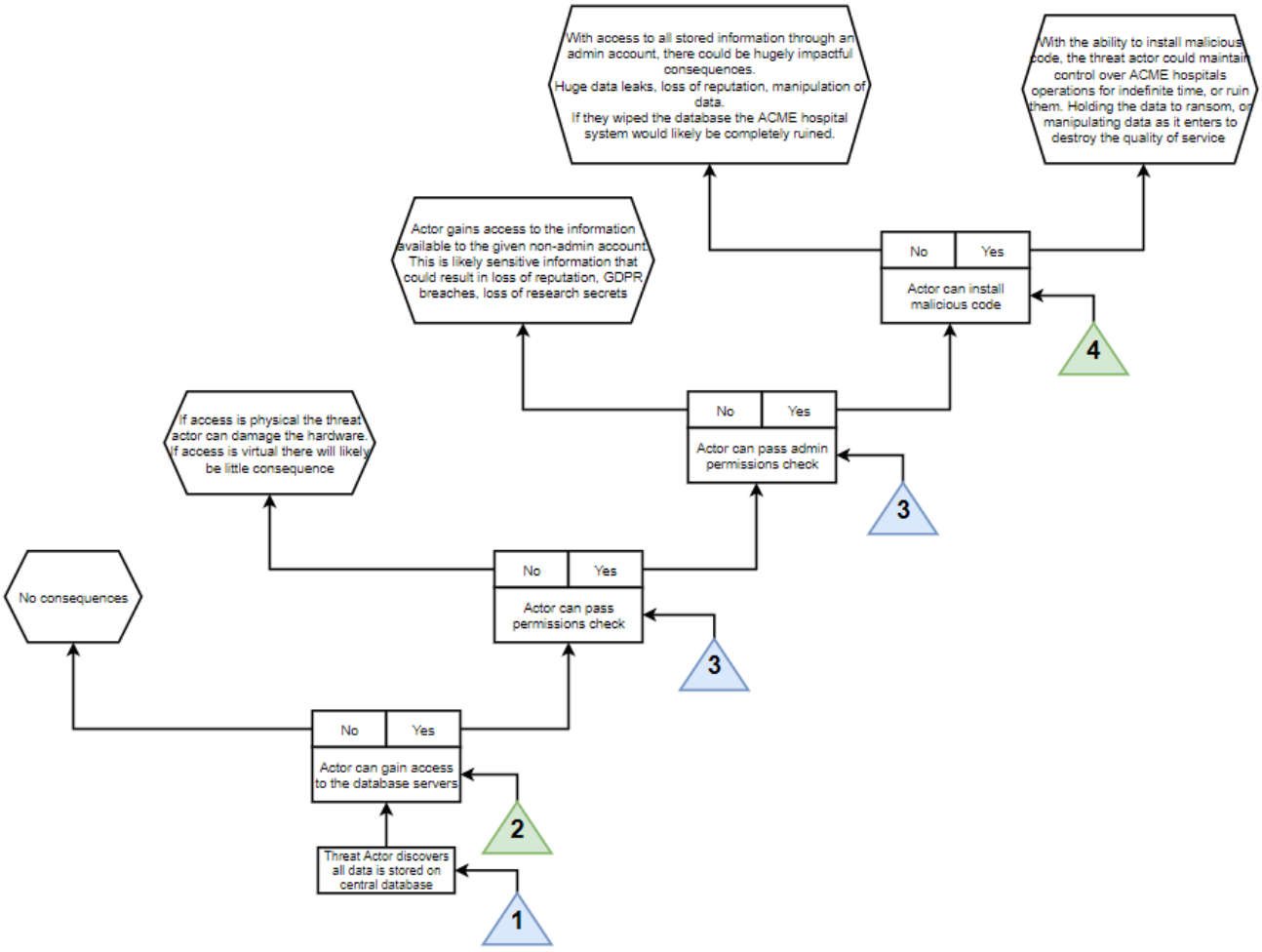


Figure 20 - CCA for central HQ database

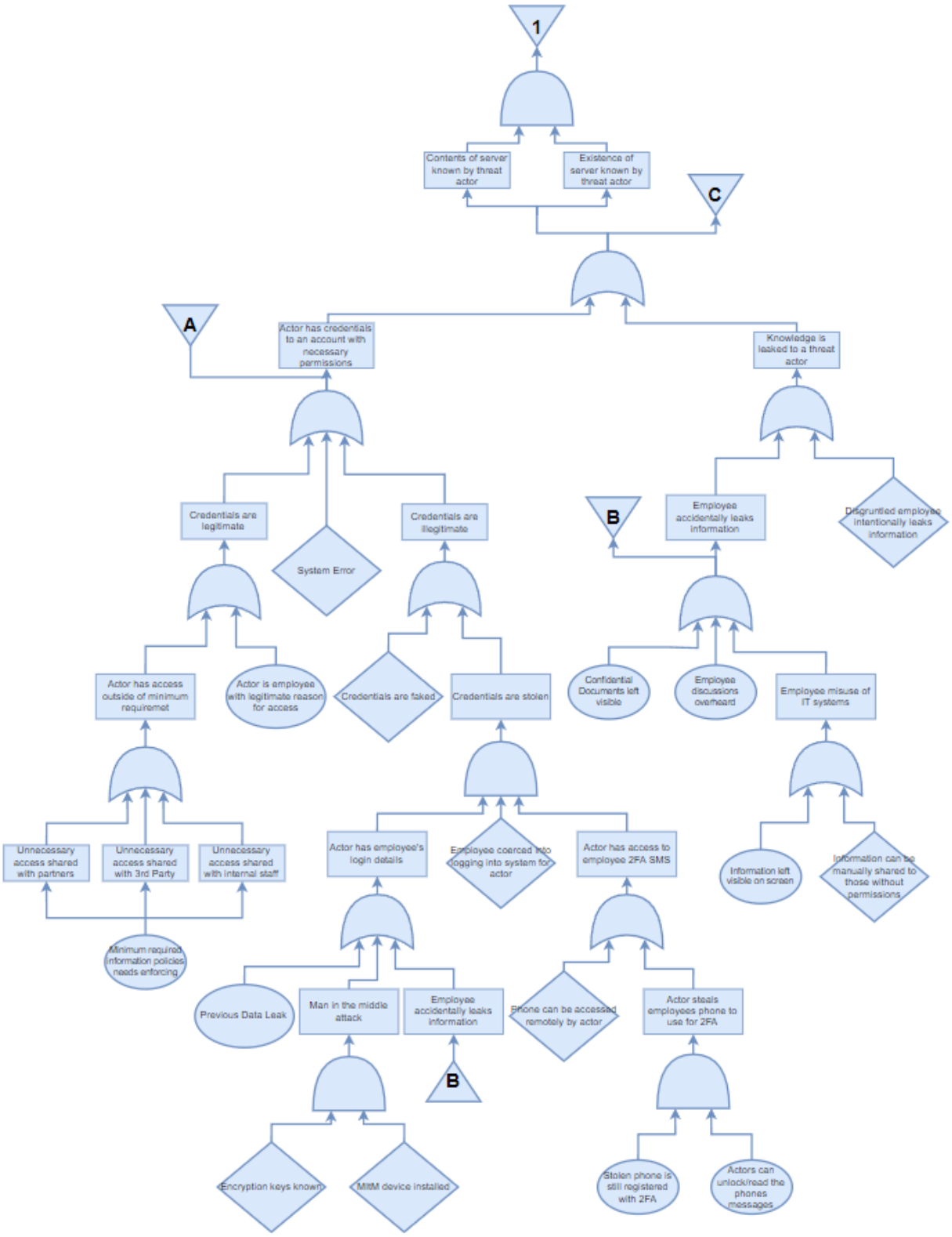


Figure 21: Fault tree 1

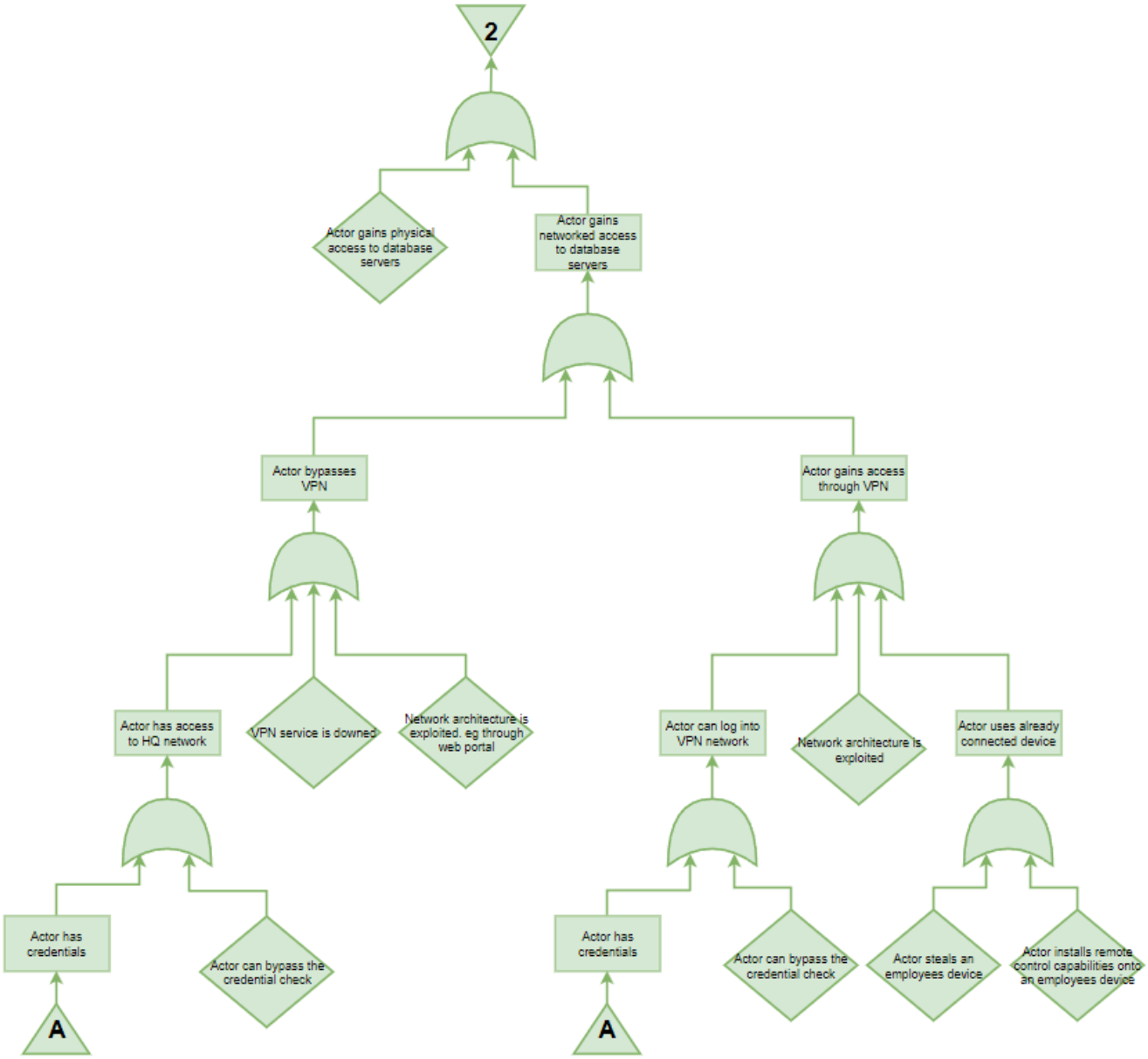


Figure 22: Fault tree 2

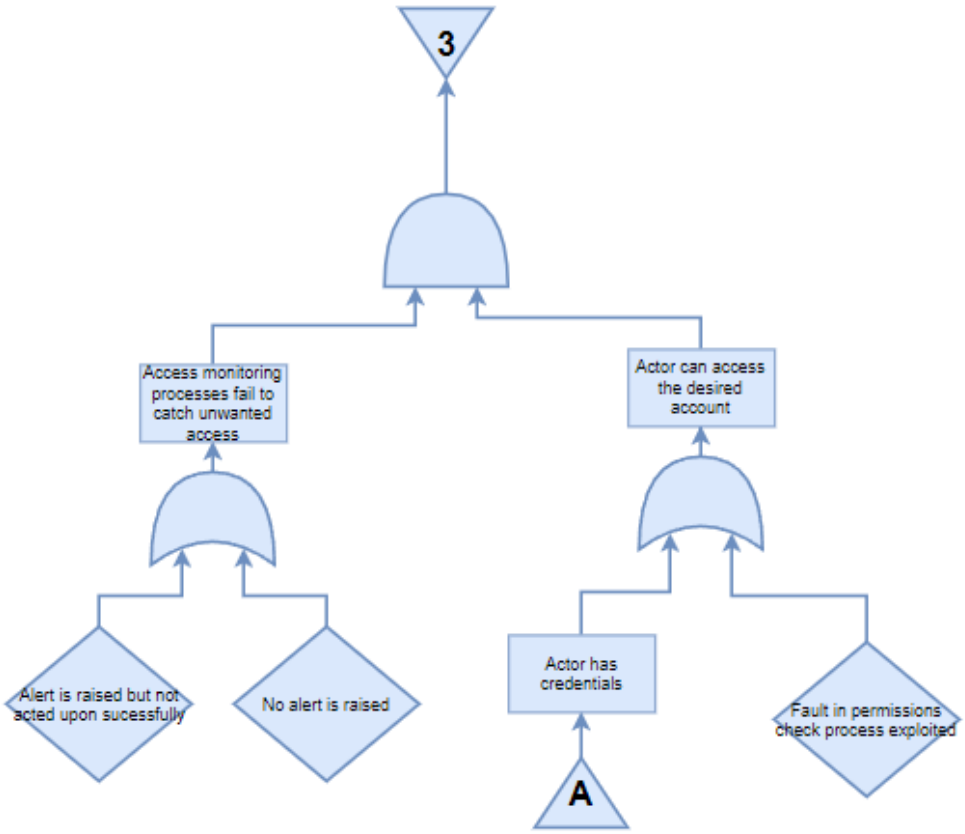


Figure 23: Fault tree 3

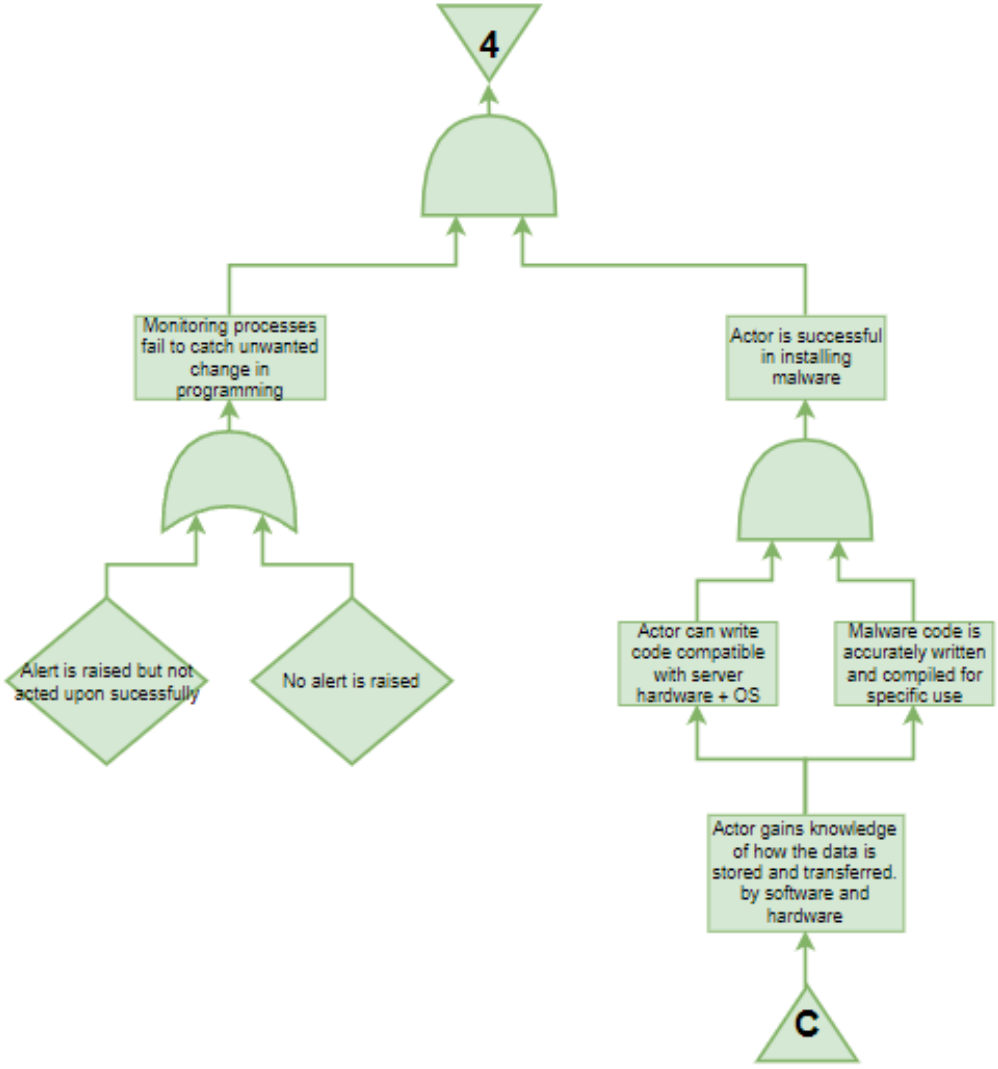


Figure 24: Fault tree 4

Operating Systems

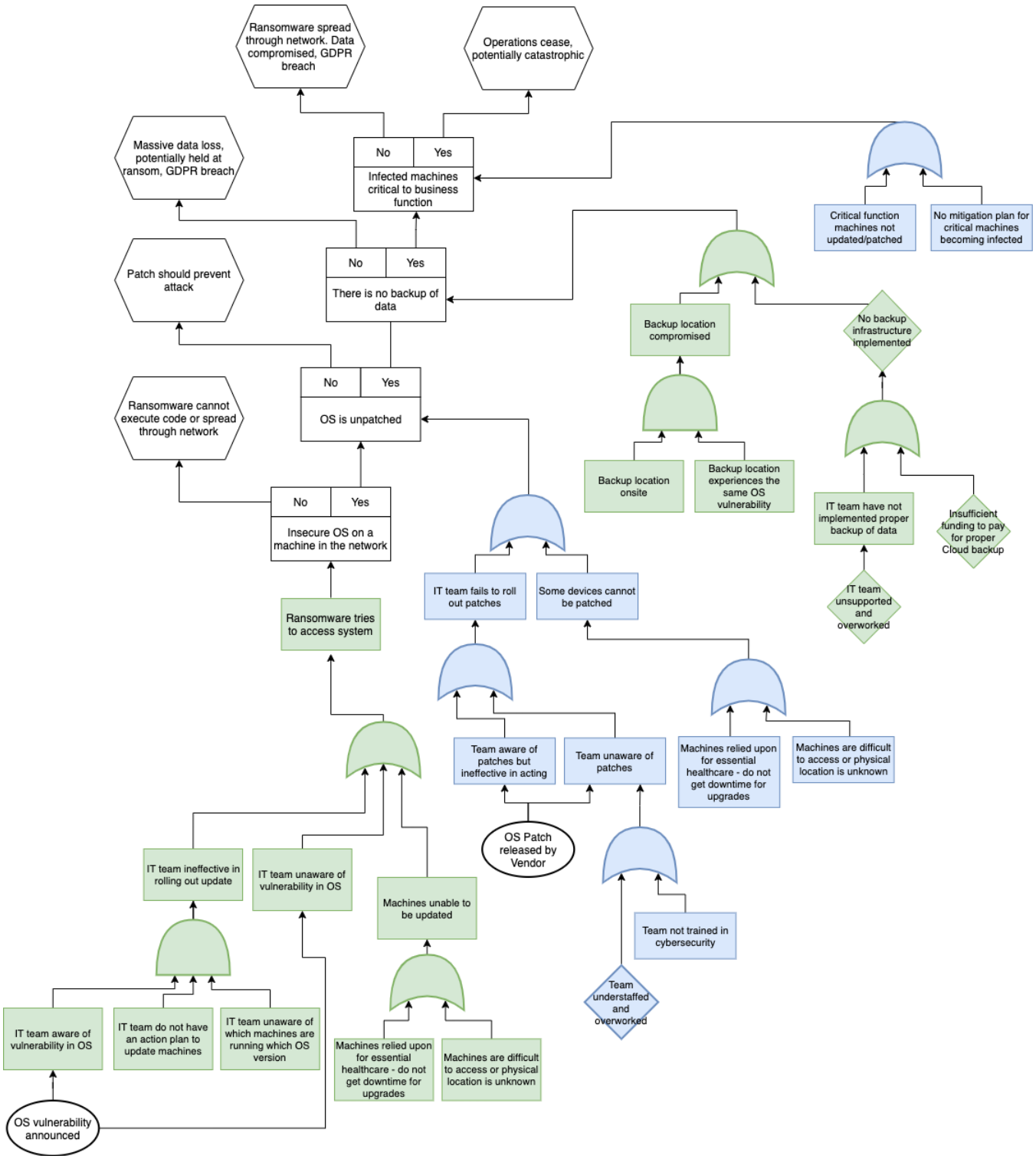


Figure 25: CCA for operation system vulnerabilities

VLANs

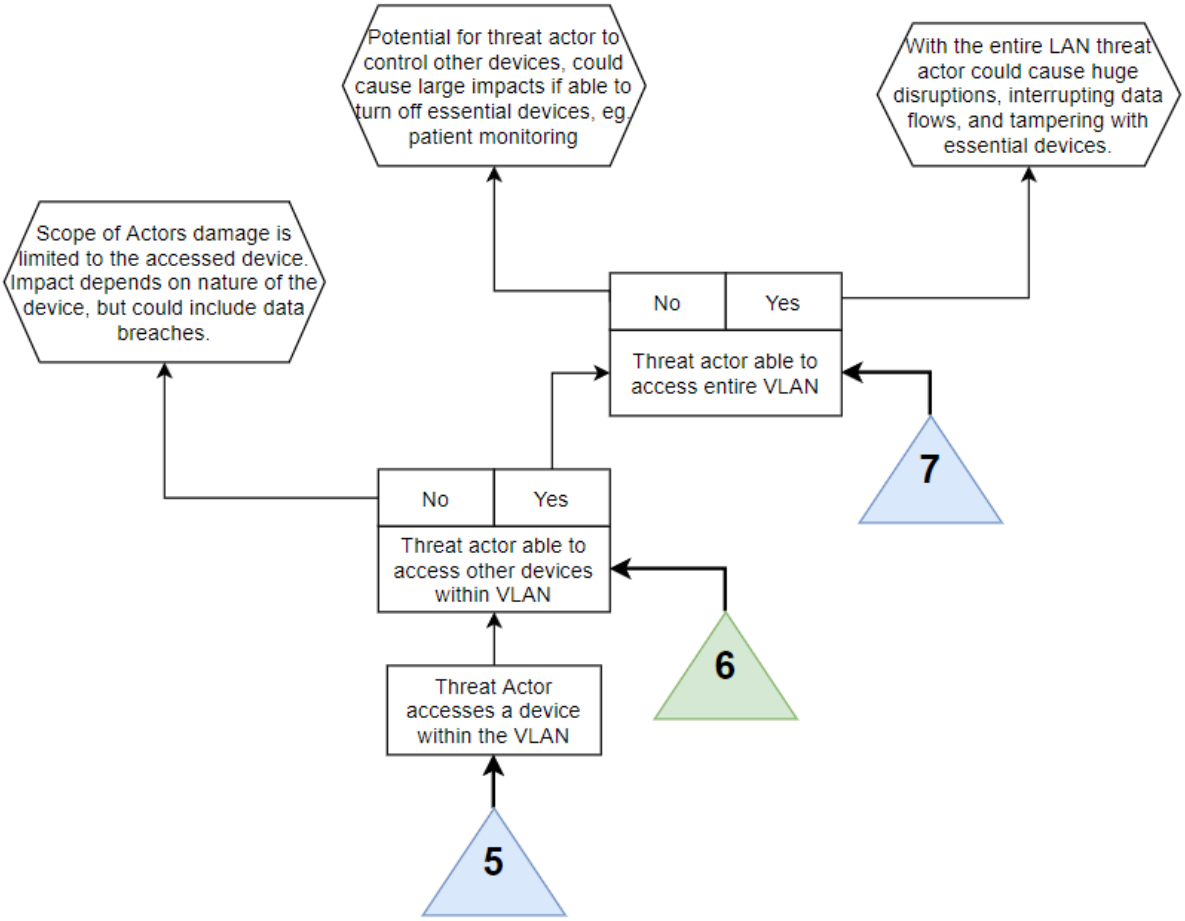


Figure 26: CCA for VLAN vulnerabilities

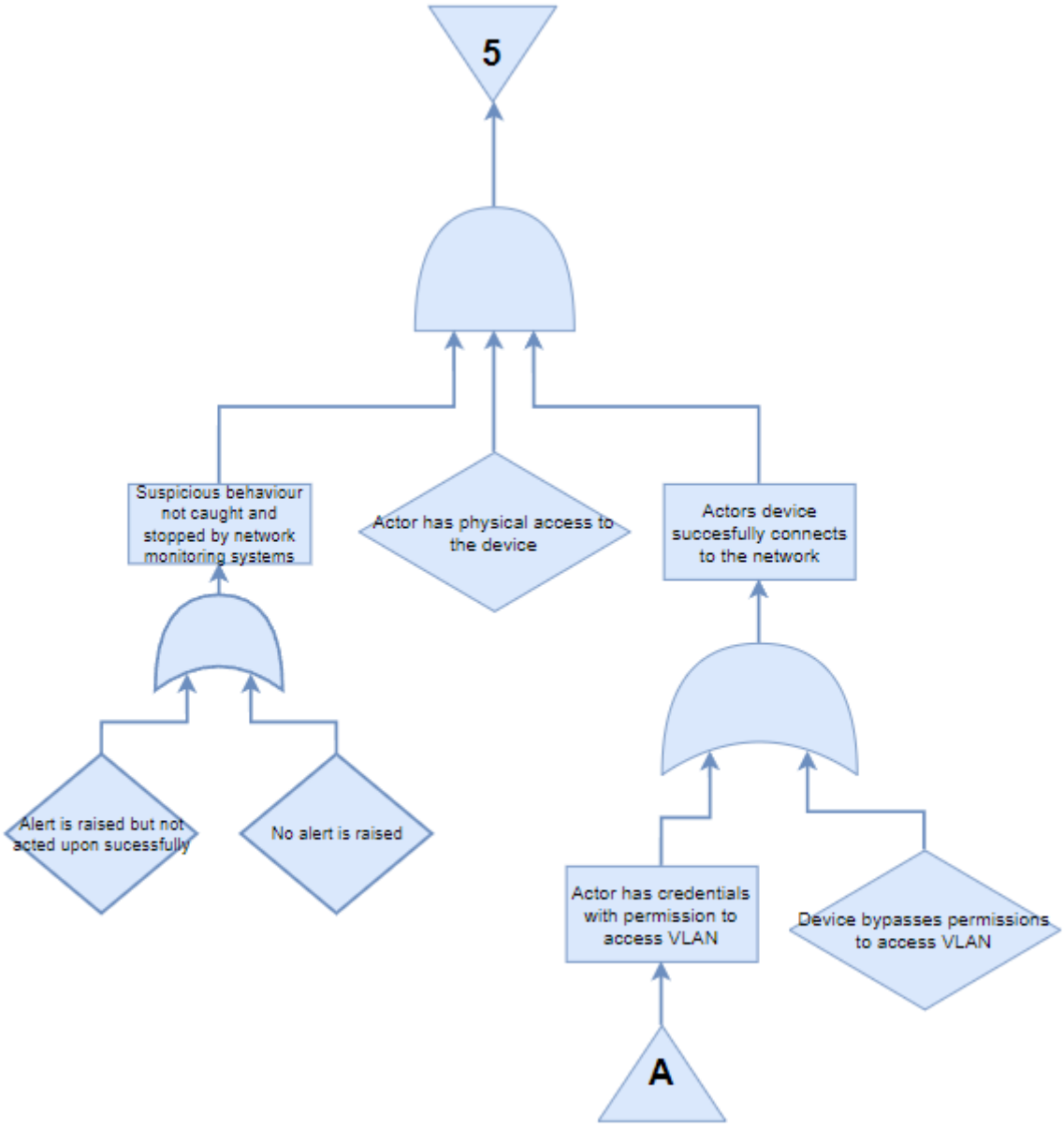


Figure 27: Fault tree 5

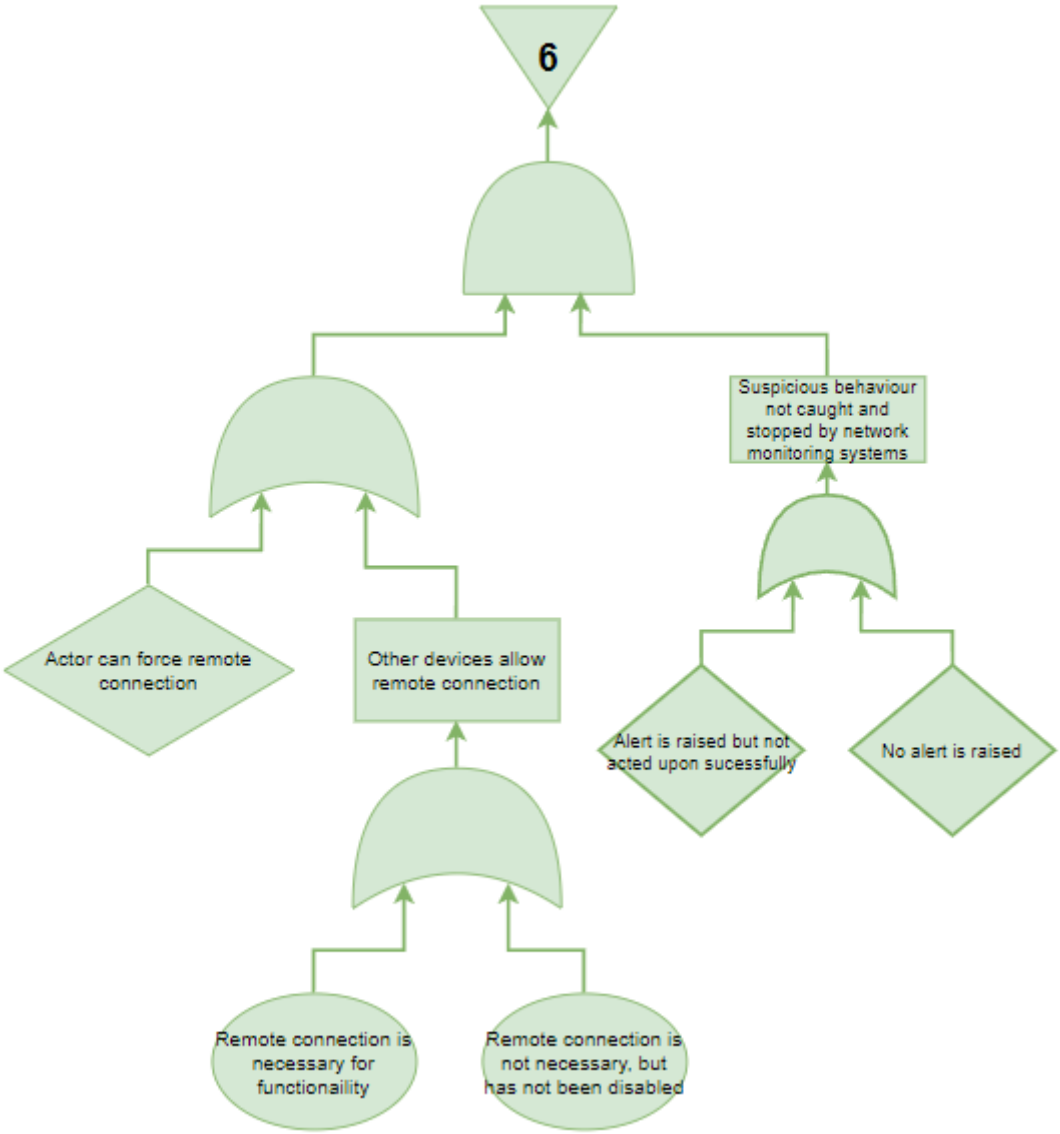


Figure 28: Fault tree 6

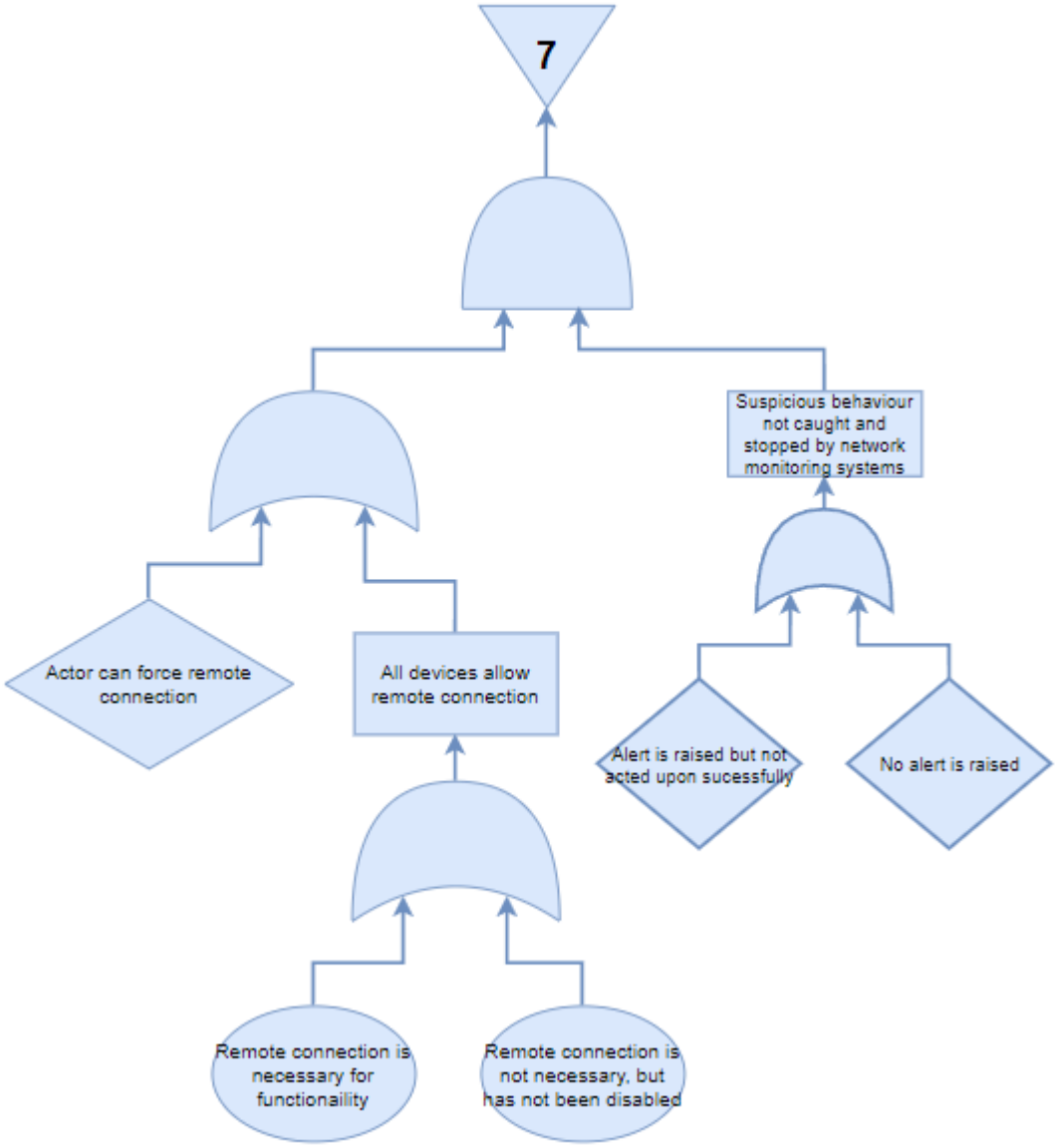


Figure 29: Fault tree 7

Specialized equipment and IoT devices

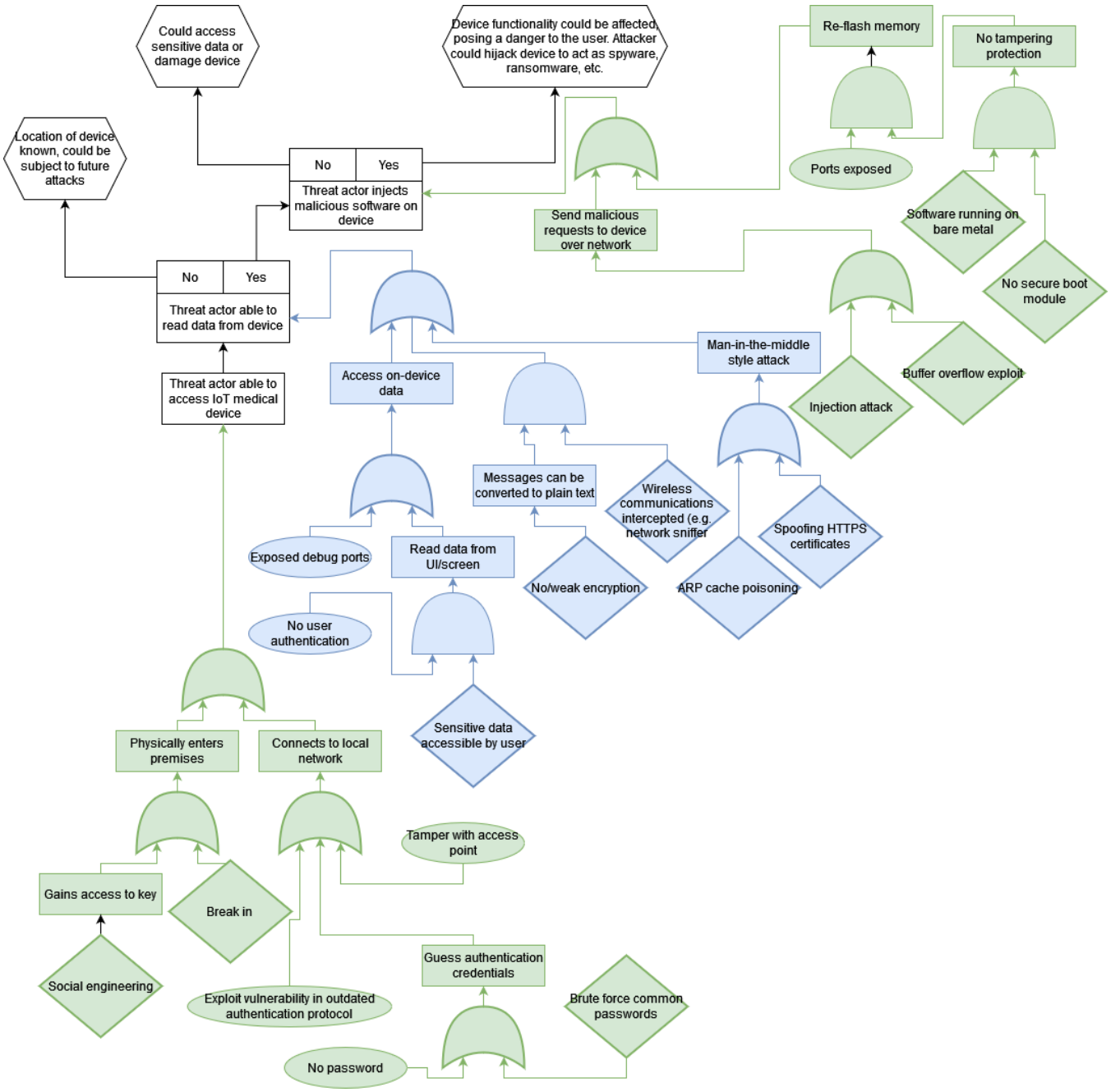


Figure 30: CCA for specialised equipment and IoT devices

Third Parties

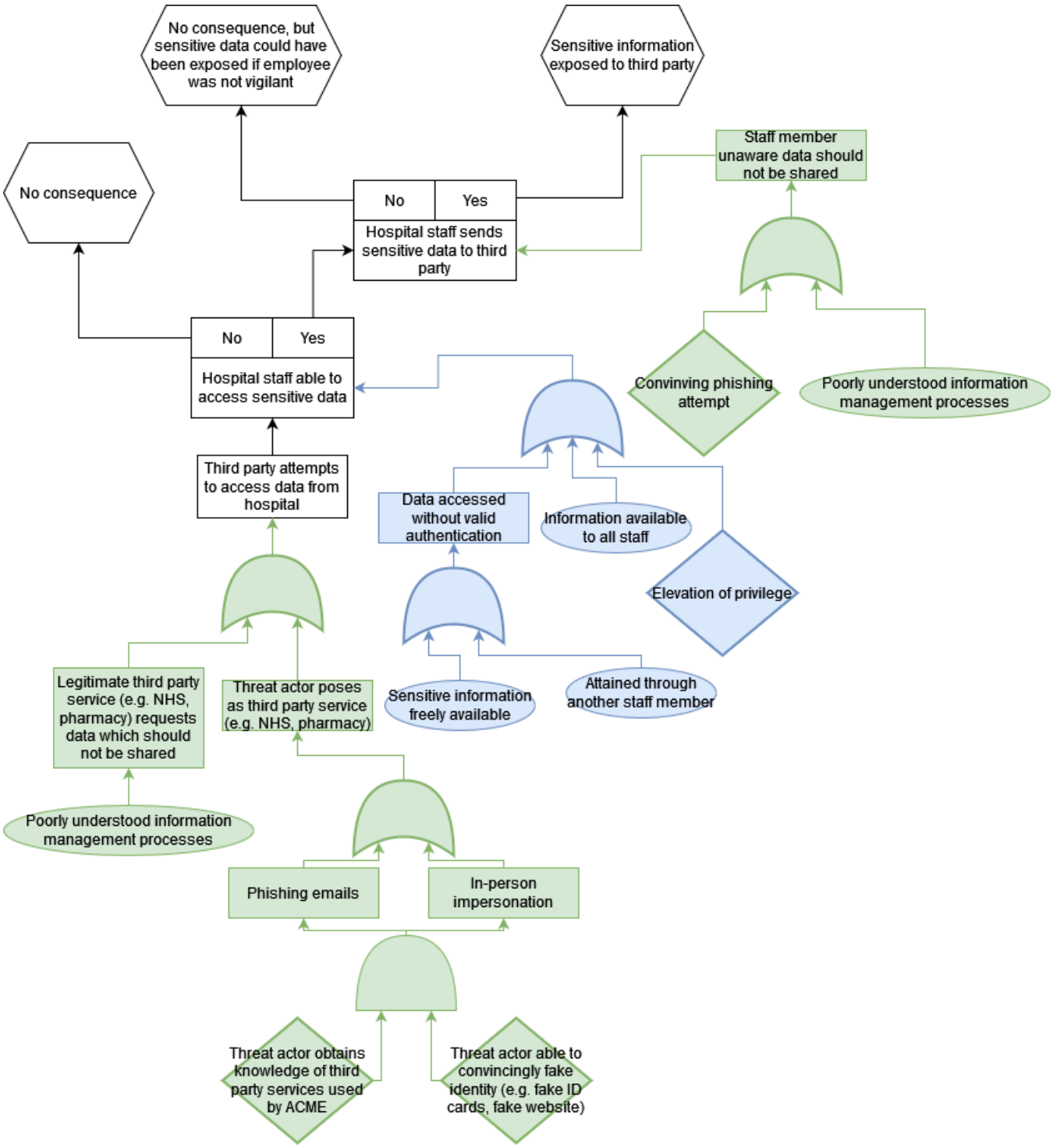


Figure 31: CCA for sending data to third parties

Risk Prioritisation

Based on the risk analysis conducted on the vulnerable assets identified in Table 3, the following risks can be categorized by the likelihood and consequence rating:

Table 5: Risk likelihood and consequence rating

Risk ID	Risk Summary	Raised by	Affected Asset	Risk Owner	Risk Statement	Risk Likelihood	Risk Consequence	Risk Rating
I001	Compromised HQ Database	Adam Holwell	All data and files accessible from Central Database	Head of IT	There are no methods of restoration and limited prevention for a threat actor can manipulating data in the central database,	C (Possible)	5 (Catastrophic)	Very High
I002	Insecure Operating Systems	Alex Hudson	All data and files accesible from machines with insecure OS'	Head of IT	If ransomware accesses the system through an insecure OS, all data and files accessible from that machine and it's network are at risk.	B (Probable)	5 (Catastrophic)	Critical
I003	Tampering with IoT devices	Matthew Beaton	IoT devices in patients homes	Head of R&D, approved by Board of Governors	Patient monitoring devices may be tampered with in the field, leading to data or functionality loss	D (Improbable)	4 (Major)	High
I004	Data sharing with Third Parties	Matthew Beaton	Patient Data	CEO	Patient data may be shared without authorization, via third party partners or spoof actors	C (Possible)	4 (Major)	Very High
I005	VLANs	Adam Holwell	Sensitive network traffic, including clinician data	Head of IT	Current segmentation leaves a large amount of traffic on a single VLAN that can be comprimised simultaneously	C (Possible)	4 (Major)	Very High

Part 1c

Control Selection

Through Control measures are proposed for each identified risk:

Compromised HQ Database

- Migrate data storage to cloud PaaS solution
    - Transfers risk
    - Can store server back-ups outside ACME environment on independent servers to ensure lost data can be retrieved
    - May also improve uptime, mitigating denial of service threats
- Minimum Requirement Necessary (MRN) policies
    - Restrict the access of data to only those necessary for limited duration
    - Reduces opportunity for data to be accessed by unauthorised personnel
- Access monitoring
    - Passive monitoring software to track database activity
    - Server attacks or accidental deletions can be caught automatically and traced

Several controls have also been identified from the ISO27001 framework:

- A5.1.1 – Policies for information security
- A6.1 – Internal Organisation Information Security
- A7.2.2 - Information security awareness, education, and training
- A9 – Access Control
- A12.3.1 – Information Backup
- A13.2.1 - Information transfer policies and procedures
- A16 – Information security Incident Management
- A18.2 – Information security reviews

Insecure Operating Systems

- Patch Management
    - Ensures OS always running latest security updates
- Measures to limit malware proliferation
    - Blocking executable email attachments
    - Only allow IT-issued devices on network
- Develop Reaction Plan
    - Sufficient incident planning limits impact on business functions
    - Includes identifying critical assets, understanding, and documenting how these services can be restored from offline backups.

Several controls have also been identified from the ISO27001 (ISO/IEC, 2013) framework:

- A12.2.1 – Controls against Malware
- A12.5.1 – Controls of Operational Software: Installation of Software on Operating Systems
- A12.6.1 – Technical Vulnerability Management
- A12.6.2 – Restrictions on software installation

Tampering with IoT devices

- Install hardware security module
    - Contains non-erasable digital signature to detect inauthentic software
    - Additionally, run a basic RTOS rather than bare metal code for some in-built security enhancements
- Enable OTA updates
    - Ensures security flaws discovered post-release may be patched
- Remove developer ports from consumer devices
- Store as little personal data as possible locally.
- Keep device source code secret
    - Ensures bad actors cannot research system for vulnerabilities

Several controls have also been identified from the ISO27001 framework:

- A9.4.5 Access control to program source code
- A11.2.3 - Cabling security
- A11.2.6 - Security of equipment and assets off-premises

Data sharing with third parties

- Develop robust policies, to be approved by the CEO, for information transfer
    - Organise regular policy review
- Deliver Data Management and Policy training for all staff.
- Train staff to recognise phishing attacks
- Set up agreements and NDAs with the NHS and third-party hospitals

Several controls have also been identified from the ISO27001 framework:

- A5.1.1 – Policies for information security
- A5.1.2 – Review of the policies for information security
- A7.2.2 – Information security awareness, education, and training
- A13.2.1 – Information transfer policies and procedures
- A13.2.2 – Agreements for information transfer
- A13.2.4 – Confidentiality and non-disclose agreements (NDA’s)

VLANs

- Increased Segmentation
    - Consider a VLAN for each department, not just R&D and HR
- Limited Remote Access to Connected Devices
    - Ensure remote access of devices can only be achieved from within ACME trust boundary
    - Minimises damage a threat actor can do by accessing the network through a standard device
    - This can also follow an MRN policy
- Traffic Monitoring
    - Automatic detection and prevention of unusual traffic, e.g., DoS incidents
    - Improves server uptime and productivity

Several controls have also been identified from the ISO27001 framework:

- A5.1.1 – Policies for information security
- A6.1 – Internal Organisation Information Security
- A7.2.2 - Information security awareness, education, and training
- A9 – Access Control
- A13 Communications Security
- A16 – Information security Incident Management
- A18.2 – Information security reviews

Risk Treatment Strategy

An overview of the risk treatment strategy is presented in Table 6

Table 6: ISMS Table

Risk ID	Risk Summary	Raised by	Affected Asset	Risk Owner	Risk Statement	Risk Likelihood	Risk Consequence	Risk Rating	Risk Treatment Decision	Risk Treatment Summary	ISO Control Measures	Treated Residual Risk Likelihood	Treated Residual Risk Consequence	Treated Residual Risk
I001	Compromised HQ Database	Adam Holwell	All data and files accessible from Central Database	Head of IT	There are no methods of restoration and limited prevention for a threat actor can manipulating data in the central database,	C (Possible)	5 (Catastrophic)	Very High	Transfer + Mitigate	Transfer risks of server hosting to dedicated company, implement policies to control access to the data and allow for restoration	A5.1.1 A6.1.x A9.x A12.3.1 A13.2.1 A16.x A18.2.x	D (Improbable)	2 (Low)	Low
I002	Insecure Operating Systems	Alex Hudson	All data and files accesible from machines with insecure OS'	Head of IT	If ransomware accesses the system through an insecure OS, all data and files accessible from that machine and it's network are at risk.	B (Probable)	5 (Catastrophic)	Critical	Mitigate	Implement a patch management framework which tracks OS version and enables rollout of patches. Create a ransomware reaction plan to enable quick reaction to stop ransomware spreading.	A12.2.1 A12.5.1 A12.6.1	D (Improbable)	4 (Major)	High
I003	Tampering with IoT devices	Matthew Beaton	IoT devices in patients homes	Head of R&D, approved by Board of Governors	Patient monitoring devices may be tampered with in the field, leading to data or functionality loss	D (Improbable)	4 (Major)	High	Mitigate	Keep device source code secret. Build devices with a RTOS and hardware security module. Allow for OTA patches post-deployment. No exposed ports. Minimal local data.	A9.4.5 A11.2.3 A11.2.6	E (Rare)	3 (Moderate)	Low
I004	Data sharing with Third Parties	Matthew Beaton	Patient Data	CEO	Patient data may be shared without authorization, via third party partners or spoof actors	C (Possible)	4 (Major)	Very High	Mitigate	Develop policies for information securityand processes for regular reviews. Implement data management training for staff. Set up agreements and NDA's with partners.	A5.1.1 A5.1.2 A7.2.2 A13.2.1 A13.2.2 A13.2.4	D (Improbable)	3 (Moderate)	Medium
I005	VLANs	Adam Holwell	Sensitive network traffic, including clinician data	Head of IT	Current segmentation leaves a large amount of traffic on a single VLAN that can be comprimised simultaneously	C (Possible)	4 (Major)	Very High	Mitigate	Further segmentmentation into VLANs, MRN policies for access between dives on a network, monitoring traffic to detect and prevent dangerous behavious, such as hugely increased requests from a device fro DoS attacks	A5.1.1 A6.1.x A7.2.2 A9.x A12.3.1 A13.2.1 A16.x A18.2.x	C (Possible)	2 (Low)	Low

Due to the high initial consequence ratings of the risks selected, it was decided that all risks should be mitigated or transferred by the controls outlined. The database risk may additionally be transferred, expanding resources internally to implement other controls.

It is assumed that medium an acceptable risk level. Following the implementation of controls, it is expected that the residual risk will be acceptable for four out of five risks. Insecure operating systems maintains high risk due to the possibility of a significant malware attack resulting in significant financial and reputational damage. However, its likelihood is improbable, and its overall rating has decreased from critical.

It is recommended that the IT department carry out a statement of applicability for the ISO270001 controls identified in this report to formally document the controls to be implemented and provide justification for controls which will not be.

Monitoring risk

Monitoring is a key stage in the ISO 31000 framework. It is recommended that the organisation carry out regular audits of the identified assets and risks, and flag for review any circumstances which may have changed the risk level. Processes should be in place for recording and reporting newly identified risks in a timely manner. Additionally, the board of directors should regularly review the acceptable risk tolerance for the organisation, as this may affect the amount of funding required.

Conclusion

While providing IT enabled healthcare presents many risks for the organisation, at a reputational, financial, and legal level, this report has shown that by employing formal risk assessment techniques and strategically layering defence mechanisms to mitigate or transfer risks, these impacts can be brought within an acceptable level of likelihood and severity. ACME Hospital’s should strive to implement the recommended processes and controls, especially for monitoring residual risk in an ever-changing landscape of threats and vulnerabilities.

References

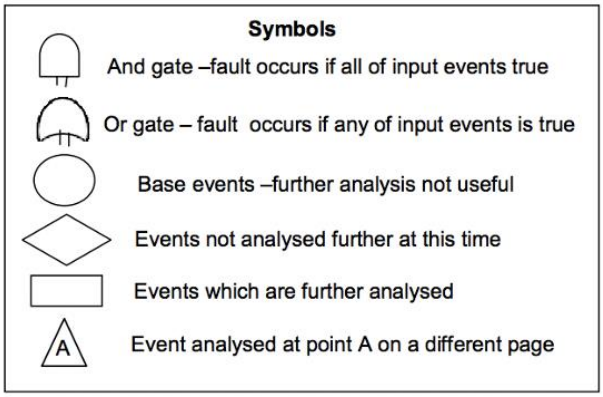
Abrishami, B. e. (2019). *OCTAVE Allegro Risk Assessment: The George Washington University Hospital.* Retrieved November 4, 2021, from University of Warwick Moodle: https://moodle.warwick.ac.uk/mod/resource/view.php?id=1518696

ISO. (2019). *ISO 31000 - Risk management.* Retrieved November 6, 2021, from https://www.iso.org/iso-31000-risk-management.html>

ISO/IEC. (2013, October). *ISO/IEC 27001:2013.* Retrieved November 13, 2021, from https://www.iso.org/standard/54534.html

Morse, A. (2017, October 24). *Investigation: WannaCry cyber attack and the NHS.* Retrieved November 12, 2021, from National Audit Office: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

Appendix



Appendix A - Cause-Consequence Analysis Key