CYBERSECURITY RISK ASSESSMENT

Aggie Medical Center

ISTM 635 - 603

Aggie Code of Honor

An Aggie does not lie, cheat or steal or tolerate those who do.

Team

Sandheep Sridar

Harmit Jasani

Mihir Bhende

Pratik Toshniwal

Sai Subhasree Pakina

Contents

Acknowledgements 3
Executive summary 4
Asset Identification 5
Business processes: 5
Asset Identification: 5
Asset Classification 7
Classification based on Financial Impact 8
Classification based on Legal impact 10
Classification based on business operations 12
Assigning total score based on financial, legal and operational impact 14
Ranking the assets based on final score 16
Vulnerability and Threat Identification 17
PDIS 17
Router 17
FRKS 18
ECDS 20
MLS 21
Cybersecurity Risk Estimation 22
PDIS 22
Router 22
FRKS 22
ECDS 23
MLS 23
Cyber Security Risk Management Strategy 24
PDIS 24
Router 25
FRKS 26
ECDS 27
MLS 28
Appendices 29
Appendix A – Measurement scales 29

Financial impact scale 29
Operational impact scale 29
Legal impact scale 29
Appendix B 30
Brief description of technical vulnerabilities 30
Brief description of non-technical vulnerabilities 31
List of threat vectors for technical and non-technical vulnerabilities 32
Tree analysis 33
Appendix C – Measurement Scale for scoring Threat Likelihood 46
Appendix D 46
Estimation of Final Impact Value 46
Measurement Scale used for scoring FIV 47
Appendix E - Cybersecurity Risk Matrix and Risk Management Strategy for various cybersecurity risk values 47
References 48
Glossary 48
Team Work 49

Acknowledgements

We would like to take this opportunity to thank Dr. Ravi Sen for having constantly guided us throughout the entire ordeal of creating this analysis and risk assessment report. We'd also like to thank Bishvesh Pachauli (Dr. Ravi Sen's Teaching Assistant for this course, Business Information Security). He was very instrumental in resolving our doubts, queries and concerns.

Executive summary

This case study entails an exhaustive study of AMC's systems and its risk and security parameters. AMC is a College Station-based local hospital. This hospital houses a variety of employees, doctors, maintenance staff along with an in-house department that caters to the infrastructural, network and computer needs. This IT department is also responsible for facilitating various IT maintenance requests and technology upgrades that the hospital may require.

This business case is an empirical review of AMC's security status, asset analysis, risk assessment and possibility of security control additions. This case study helps us formulate and adhere to appropriate security measures and practices. The primary objective of diving into this case study was to come up with a qualitative risk assessment of AMC's security.

The team encompassed five primary steps in order to perform an exhaustive qualitative risk assessment. These steps are enlisted as follows –

1) Identifying assets
2) Classifying assets
3) Identifying vulnerabilities and threats pertaining to the most significant assets
4) Estimating risk by analyzing the likelihood and impact of threats
5) Providing risk management strategies

While analyzing this case, we identified the following to be our most critical assets (in no specific order of significance):

1) ECDS
2) FRKS
3) Router
4) MLS
5) PDIS

Most vulnerabilities associated with these assets can be countered by either resorting to official software upgrades and security patches released OTA, by the product company (Oracle – SQL Server, IBM - AIX, etc.) While there are various levels and methods to deal with risks, a broad classification can be made for risks –

1) Acceptable risks – Those that can be accepted depending on its severity
2) Avoidable risks – Those that can be avoided by getting rid of its causal factors
3) Mitigatable risks – Those that can be mitigated by:
    i. Installing software updates and security patches regularly for technical risks
    ii. Facilitating appropriate training and security drills to employees
    iii. Deploying prevention strategies like installing CCTV cameras, beefing up manual security, using safer locks, etc.
4) Transferrable the risks – Those whose management can be transferred to contractors, insurance companies, etc.
5) Shareable risks – Those that can be shared across departments in an organization

Asset Identification

The following tables show the important business processes for AMC and identifies all the assets that have direct or an indirect effect on the business operations.

Business processes:

Process code	Process name	Process description	Start	End
BP1	Patient Registration Process	The patient registration process typically starts from home PCs and ends up being registered or having a scheduled appointment through the PDIS server	Home PCs	PDIS
BP2	Patient Billing Process	Patient billing is carried out from PDIS server fetching relevant patient, appointment details and ends at the FRKS	PDIS Server	FRKS
BP3	Managing Medicine Supplies	Various units within the hospital will coalesce their records, requirements and manage medicinal supplies through the MLS	Labs/Administration/Emergency/Home PCs/Physicians' computers	MLS

Asset Identification:

Asset ID	Asset Name	Asset Description
1	Home PCs	It is the workstation from where the patient interacts with AMC System. The patient can carryout multiple task through Home PCs like registration andscheduling an appointment
2	Router	This router connects domestic personal computers to PDIS servers
3	Physician's workstations	Through these workstations, physicians can view patient data, update patient's medical records
4	Switch	This switch connects router with physician's workstations
5	PDIS Server	PDIS server stores exhaustive patient information which includes patient's records, appointment scheduler, pharmacy and billing information
6	Router	This router connects the PDIS server with various facilities in the hospital. This router is also responsible for facilitating support provided by ABC Systems
7	Switch	This switch connects router with Labs workstations
8	Labs Workstations	Patient's test records are added and modified in lab workstations. Any authorized person who has access to to these workstations can maintain record of the tests underwent by patient.
9	Emergency Care Data workstations	These machines are used to access ECDS server through a switch
10	PMS Server	A server which contains sensitive information about the personnel which includes demographics and disciplinary records

Asset ID	Asset Name	Asset Description
11	MLS Server	This server tracks the inventory for the medical centre. It tracks supplies, property, equipment and medicines
12	FRKS Server	This server tracks the finances for the medical centre. It tracks insurance, bill payments and other billing records
13	ECDS Server	This workstation contains details about the patient diagnosis, the doctor incharge and also records what treatment was given
14	Treatment Rooms' workstations	PDIS server can be accessed using workstations in the treatment rooms. These workstations are primarily used by doctors and nurses for gaining access to PDIS
15	Switch	This switch connects PDIS server through a router with treatment rooms' workstations
16	Paper Medical Records	These assets are non-electronic in nature and contain important medical records
17	Administration's workstations	These machines are used to access FRKS, PMS and MLS systems through a switch
18	Switch	This switch connects administration, (FRKS,MLS,ECDS) Servers and Emergency Data Care Systems with the router that connects to PDIS
19	Providers' Credentials	This contains identity credentials of insurance providers
20	Personnel Management Systems	This contains information about demographics, work histories, assignments, skills, disciplinary records, etc. It is connected to the PDIS via a switch and a router
21	Hand-scripted notes	The notes contain where PDIS and ECDS database information and other assets reside.

Asset Classification

After asset identification, it is imperative to classify the assets based on various factors. The assets are classified based on 3 following factors:

1. Financial impact
2. Operational impact
3. Legal impact

Financial impact includes the financial value of an asset. In financial impact, the assets are further classified based on cost to develop, maintain and replace an asset.

Operational impact includes, the value or significance of an asset based on critical business processes of the organization. Top 3 business processes are:

a. Patient Registration Process
b. Patient Billing Process
c. Managing Medicine Supplies

Legal impact includes, protection required for a particular asset based on state and federal laws

Refer the table in appendix for Asset classification for AMC

Classification based on Financial Impact

Asset ID	Asset Name	Reason for Cybersecurity Risk Assessment	Financial Impact (Develop)	Financial Impact (Maintain	Financial Impact (Replace)
1	Home PCs	Home PCs are connected to a home network and typically have low security measures, weak antivirus protection and ineffective firewalls in place. Hence they need to be assessed for cybersecurity risk.	1	1	1
2	Router	This router connects home pcs to PDIS which is the integral component of AMC as it contains data of the most important	1	2	2
3	Physician's workstations	Only authorized physicians can have access for these workstations. Any unauthorized access, physically from the workstation or remotely, could have major effect on the integrity of the data.	2	2	2
4	Switch	This switch acts as a foundation of network between the router and physician's workstation. Hence this switch must be assessed for security as any failure or intrusion will lead to authorized access in the network and potential data leaks	2	1	2
5	PDIS Server	This is the most important system in AMC application. This is a source or starting point for various critical business processes. So it is imperative to assess the PDIS server for security as any	3	4	4
6	Router	This router connects PDIS to various integral systems within AMC. This is critical point within the network as it could lead to potential break-in of threat agents within the AMC network system.	3	4	4
7	Switch	This switch acts as a foundation of network between the router and lab workstations. Critical information is stored and updated through lab workstation and any vulnerability in the switch will lead to cyber security risk	2	2	2
8	Labs Workstations	Only authorized lab workers can have access for these workstations. Any unauthorized access, physically from the workstation or remotely, could have major effect on the integrity of the data.	2	2	2
9	Emergency Care Data workstations	The administration has access to ECDS server using these workstations. If these systems are compromised, it can be difficult for the medical centre to provide treatment when a patient arrives at the ER	2	3	2
10	PMS Server	Personnel management is very critical for any organization and the organization can be sued by the employees if their personal information is hacked	4	4	4

Asset ID	Asset Name	Reason for Cybersecurity Risk Assessment	Financial Impact (Develop)	Financial Impact (Maintain)	Financial Impact (Replace)
11	MLS Server	Since all the supplies are ordered through this system, the malfunctioning of this system could put patients at risk	4	4	3
12	FRKS Server	Since all the finances are tracked through this system, the malfunctioning of this system or attack on this system through external networks could put the hospital at loss. Furthermore, the financial information of the hospital will become vulnerable to attack	4	4	4
13	ECDS Server	This system consists of sensitive data about the patients and hence it could be detrimental to the hospital if this workstation goes down.	4	4	4
14	Treatment Rooms' workstations	Sometimes, doctors and nurses may leave PDIS screens open when not in supervision which may give unauthorized people access to PDIS. Thus, this should be checked for security threats.	3	2	3
15	Switch	This router is critical to communication between PDIS server and treatment rooms. Since these may be used by employees in the treatment rooms (nurses, doctors, staff), and it gives access to PDIS, it must be assessed for security threats	2	3	2
16	Paper Medical Records	Compromising the security of these records implies the leakage of medical information and thus they need to be assessed for security	1	2	1
17	Administration's workstations	The administration has access to PMS, MLS and FRKS servers using these workstations. If these workstations have a compromised security level, it can be used to modify critical information on either of these servers.	3	2	3
18	Switch	This switch acts as a connector between several systems and if this the network fails at this point, it could break a lot of processes that depend on this node. Hence, its risk assessment is imperative	2	3	2
19	Providers' Credentials	Credentials of medical personnel are sensitive information and need to be checked for discrepancies and assessed for cybersecurity.	1	1	1
20	Personnel Management Systems	This information is crucial and requires to be protected. It includes work histories and disciplinary records, which are not meant to be accessible to outsiders, and even insiders without needed privileges. A cybersecurity assessment is needed to make sure that security is not compromised.	3	4	4
21	Hand-scripted notes	This information is physical in nature and cannot have assured security against threat agents.	1	2	1

Classification based on Legal impact

Asset ID	Asset Name	Reason for Cybersecurity Risk Assessment	Legal Protection Requirement
1	Home PCs	Home PCs are connected to a home network and typically have low security measures, weak antivirus protection and ineffective firewalls in place. Hence they need to be assessed for cybersecurity risk.	0
2	Router	This router connects home pcs to PDIS which is the integral component of AMC as it contains data of the most important	0
3	Physician's workstations	Only authorized physicians can have access for these workstations. Any unauthorized access, physically from the workstation or remotely, could have major effect on the integrity of the data.	0
4	Switch	This switch acts as a foundation of network between the router and physician's workstation. Hence this switch must be assessed for security as any failure or intrusion will lead to authorized access in the network and potential data leaks	0
5	PDIS Server	This is the most important system in AMC application. This is a source or starting point for various critical business processes. So it is imperative to assess the PDIS server for security as any	1
6	Router	This router connects PDIS to various integral systems within AMC. This is critical point within the network as it could lead to potential break-in of threat agents within the AMC network system.	0
7	Switch	This switch acts as a foundation of network between the router and lab workstations. Critical information is stored and updated through lab workstation and any vulnerability in the switch will lead to cyber security risk	0
8	Labs Workstations	Only authorized lab workers can have access for these workstations. Any unauthorized access, physically from the workstation or remotely, could have major effect on the integrity of the data.	0
9	Emergency Care Data workstations	The administration has access to ECDS server using these workstations. If these systems are compromised, it can be difficult for the medical centre to provide treatment when a patient arrives at the ER	0
10	PMS Server	Personnel management is very critical for any organization and the organization can be sued by the employees if their personal information is hacked	1

Asset ID	Asset Name	Reason for Cybersecurity Risk Assessment	Legal Protection Requirement
11	MLS Server	Since all the supplies are ordered through this system, the malfunctioning of this system could put patients at risk	0
12	FRKS Server	Since all the finances are tracked through this system, the malfunctioning of this system or attack on this system through external networks could put the hospital at loss. Furthermore, the financial information of the hospital will become vulnerable to attack	1
13	ECDS Server	This system consists of sensitive data about the patients and hence it could be detrimental to the hospital if this workstation goes down.	1
14	Treatment Rooms' workstations	Sometimes, doctors and nurses may leave PDIS screens open when not in supervision which may give unauthorized people access to PDIS. Thus, this should be checked for security threats.	0
15	Switch	This router is critical to communication between PDIS server and treatment rooms. Since these may be used by employees in the treatment rooms (nurses, doctors, staff), and it gives access to PDIS, it must be assessed for security threats	0
16	Paper Medical Records	Compromising the security of these records implies the leakage of medical information and thus they need to be assessed for security	1
17	Administration's workstations	The administration has access to PMS, MLS and FRKS servers using these workstations. If these workstations have a compromised security level, it can be used to modify critical information on either of these servers.	0
18	Switch	This switch acts as a connector between several systems and if this the network fails at this point, it could break a lot of processes that depend on this node. Hence, its risk assessment is imperative	0
19	Providers' Credentials	Credentials of medical personnel are sensitive information and need to be checked for discrepancies and assessed for cybersecurity.	1
20	Personnel Management Systems	This information is crucial and requires to be protected. It includes work histories and disciplinary records, which are not meant to be accessible to outsiders, and even insiders without needed privileges. A cybersecurity assessment is needed to make sure that security is not compromised.	1
21	Hand-scripted notes	This information is physical in nature and cannot have assured security against threat agents.	0

Classification based on business operations

Asset ID	Asset Name	Reason for Cybersecurity Risk Assessment	Impact on BP1	Impact on BP2	Impact on BP3
1	Home PCs	Home PCs are connected to a home network and typically have low security measures, weak antivirus protection and ineffective firewalls in place. Hence they need to be assessed for cybersecurity risk.	3	1	1
2	Router	This router connects home pcs to PDIS which is the integral component of AMC as it contains data of the most important	3	1	1
3	Physician's workstations	Only authorized physicians can have access for these workstations. Any unauthorized access, physically from the workstation or remotely, could have major effect on the integrity of the data.	1	1	3
4	Switch	This switch acts as a foundation of network between the router and physician's workstation. Hence this switch must be assessed for security as any failure or intrusion will lead to authorized access in the network and potential data leaks	1	1	5
5	PDIS Server	This is the most important system in AMC application. This is a source or starting point for various critical business processes. So it is imperative to assess the PDIS server for security as any	5	5	5
6	Router	This router connects PDIS to various integral systems within AMC. This is critical point within the network as it could lead to potential break-in of threat agents within the AMC network system.	1	5	5
7	Switch	This switch acts as a foundation of network between the router and lab workstations. Critical information is stored and updated through lab workstation and any vulnerability in the switch will lead to cyber security risk	1	1	3
8	Labs Workstations	Only authorized lab workers can have access for these workstations. Any unauthorized access, physically from the workstation or remotely, could have major effect on the integrity of the data.	1	1	3
9	Emergency Care Data workstations	The administration has access to ECDS server using these workstations. If these systems are compromised, it can be difficult for the medical centre to provide treatment when a patient arrives at the ER	1	3	1
10	PMS Server	Personnel management is very critical for any organization and the organization can be sued by the employees if their personal information is hacked	1	1	1

Asset ID	Asset Name	Reason for Cybersecurity Risk Assessment	Impact on BP1	Impact on BP2	Impact on BP3
11	MLS Server	Since all the supplies are ordered through this system, the malfunctioning of this system could put patients at risk	1	1	5
12	FRKS Server	Since all the finances are tracked through this system, the malfunctioning of this system or attack on this system through external networks could put the hospital at loss. Furthermore, the financial information of the hospital will become vulnerable to attack	1	5	2
13	ECDS Server	This system consists of sensitive data about the patients and hence it could be detrimental to the hospital if this workstation goes down.	2	2	2
14	Treatment Rooms' workstations	Sometimes, doctors and nurses may leave PDIS screens open when not in supervision which may give unauthorized people access to PDIS. Thus, this should be checked for security threats.	1	4	1
15	Switch	This router is critical to communication between PDIS server and treatment rooms. Since these may be used by employees in the treatment rooms (nurses, doctors, staff), and it gives access to PDIS, it must be assessed for security threats	1	1	1
16	Paper Medical Records	Compromising the security of these records implies the leakage of medical information and thus they need to be assessed for security	1	1	1
17	Administration's workstations	The administration has access to PMS, MLS and FRKS servers using these workstations. If these workstations have a compromised security level, it can be used to modify critical information on either of these servers.	1	4	4
18	Switch	This switch acts as a connector between several systems and if this the network fails at this point, it could break a lot of processes that depend on this node. Hence, its risk assessment is imperative	1	3	3
19	Providers' Credentials	Credentials of medical personnel are sensitive information and need to be checked for discrepancies and assessed for cybersecurity.	1	1	1
20	Personnel Management Systems	This information is crucial and requires to be protected. It includes work histories and disciplinary records, which are not meant to be accessible to outsiders, and even insiders without needed privileges. A cybersecurity assessment is needed to make sure that security is not compromised.	1	1	1
21	Hand-scripted notes	This information is physical in nature and cannot have assured security against threat agents.	1	1	1

Assigning total score based on financial, legal and operational impact

Asset Name	Reason for Cybersecurity Risk Assessment	Total impact
Home PCs	Home PCs are connected to a home network and typically have low security measures, weak antivirus protection and ineffective firewalls in place. Hence they need to be assessed for cybersecurity risk.	8
Router	This router connects home pcs to PDIS which is the integral component of AMC as it contains data of the most important	10
Physician's workstations	Only authorized physicians can have access for these workstations. Any unauthorized access, physically from the workstation or remotely, could have major effect on the integrity of the data.	11
Switch	This switch acts as a foundation of network between the router and physician's workstation. Hence this switch must be assessed for security as any failure or intrusion will lead to authorized access in the network and potential data leaks	12
PDIS Server	This is the most important system in AMC application. This is a source or starting point for various critical business processes. So it is imperative to assess the PDIS server for security as any	27
Router	This router connects PDIS to various integral systems within AMC. This is critical point within the network as it could lead to potential break-in of threat agents within the AMC network system.	22
Switch	This switch acts as a foundation of network between the router and lab workstations. Critical information is stored and updated through lab workstation and any vulnerability in the switch will lead to cyber security risk	11
Labs Workstations	Only authorized lab workers can have access for these workstations. Any unauthorized access, physically from the workstation or remotely, could have major effect on the integrity of the data.	11
Emergency Care Data workstations	The administration has access to ECDS server using these workstations. If these systems are compromised, it can be difficult for the medical centre to provide treatment when a patient arrives at the ER	12
PMS Server	Personnel management is very critical for any organization and the organization can be sued by the employees if their personal information is hacked	16

Asset Name	Reason for Cybersecurity Risk Assessment	Total impact
MLS Server	Since all the supplies are ordered through this system, the malfunctioning of this system could put patients at risk	18
FRKS Server	Since all the finances are tracked through this system, the malfunctioning of this system or attack on this system through external networks could put the hospital at loss. Furthermore, the financial information of the hospital will become vulnerable to attack	21
ECDS Server	This system consists of sensitive data about the patients and hence it could be detrimental to the hospital if this workstation goes down.	19
Treatment Rooms' workstations	Sometimes, doctors and nurses may leave PDIS screens open when not in supervision which may give unauthorized people access to PDIS. Thus, this should be checked for security threats.	14
Switch	This router is critical to communication between PDIS server and treatment rooms. Since these may be used by employees in the treatment rooms (nurses, doctors, staff), and it gives access to PDIS, it must be assessed for security threats	10
Paper Medical Records	Compromising the security of these records implies the leakage of medical information and thus they need to be assessed for security	8
Administration's workstations	The administration has access to PMS, MLS and FRKS servers using these workstations. If these workstations have a compromised security level, it can be used to modify critical information on either of these servers.	17
Switch	This switch acts as a connector between several systems and if this the network fails at this point, it could break a lot of processes that depend on this node. Hence, its risk assessment is imperative	14
Providers' Credentials	Credentials of medical personnel are sensitive information and need to be checked for discrepancies and assessed for cybersecurity.	7
Personnel Management Systems	This information is crucial and requires to be protected. It includes work histories and disciplinary records, which are not meant to be accessible to outsiders, and even insiders without needed privileges. A cybersecurity assessment is needed to make sure that security is not compromised.	15
Hand-scripted notes	This information is physical in nature and cannot have assured security against threat agents.	7

Ranking the assets based on final score

Asset ID	Asset Name	Asset Description	Total impact
5	PDIS Server	PDIS server stores exhaustive patient information which includes patient's records, appointment scheduler, pharmacy and billing information	27
6	Router	This router connects the PDIS server with various facilities in the hospital. This router is also responsible for facilitating support provided by ABC Systems	22
12	FRKS Server	This server tracks the finances for the medical centre. It tracks insurance, bill payments and other billing records	21
13	ECDS Server	This workstation contains details about the patient diagnosis, the doctor incharge and also records what treatment was given	19
11	MLS Server	This server tracks the inventory for the medical centre. It tracks supplies, property, equipment and medicines	18

Vulnerability and Threat Identification

In this section, 4 vulnerabilities of each top ranked asset are identified. For each asset, 2 technical vulnerabilities and 2 non-technical vulnerabilities are identified and later classified based on likelihood.

PDIS

Asset	Threat Statement Label	CIA	Gap in Technical controls	Gap in Administrative controls	Gap in Physical Controls	Exploit	Threat Agent (insider)	Threat Agent (outsider)
PDIS	A1	IA	CVE-2017-15535 -MongoDB 3.4.x before 3.4.10, and 3.5.x-development, has a disabled-by-default configuration setting, networkMessageCompressors (aka wire protocol compression), which exposes a vulnerability when enabled that could be exploited by a malicious attacker to deny service or modify memory.	behind patches, updates	N/A	Attackers can exploit this issue to cause denial-of-service conditions or modify memory. Due to the nature of this issue, code execution may be possible but this has not been confirmed.	Any employee using the system	Any user with access to the server
	A2	A	CVE-2017-14227 - In MongoDB libbson 1.7.0, the bson_iter_codewscope function in bson-iter.c miscalculates a bson_utf8_validate length argument, which allows remote attackers to cause a denial of service (heap-based buffer over-read in the bson_utf8_validate function in bson-utf8.c), as demonstrated by bson-to-json.c.	N/A	N/A	MongoDB libbson is prone to a heap-based buffer-overflow vulnerability because it fails to adequately bounds-check user-supplied data before copying it into an insufficiently sized buffer. (https://bugzilla.redhat.com/show_bug.cgi?id=1489355 has the details of the exploit)	Unauthorized lab technicians or employees with priviledged access to the server	N/A
	A3	I	N/A	Missing data validation	N/A	System has incorrect data	Staff member	N/A
	A4	CIA	N/A	N/A	PDIS screen is left unattended by the doctor after using or entering the data	Someone can fetch, enter or modify existing data and that will flow into the system and could result in incorrect medical treatment	Staff member or personnel working at AMC	A patient, patient's relatives, friends, delivery people

Router

Asset	Threat Statement Label	CIA	Gap in Technical controls	Gap in Administrative controls	Gap in Physical Controls	Exploit	Threat Agent (insider)	Threat Agent (outsider)
Router	B1	A	CVE-2013-6701 - A process which is being executed in the router is allowing the hackers to gain remote access and lodge a denial of service attack	The router is not updated	N/A	The hackers to gain remote access and lodge a denial of service attack	Untrained staff memeber who can fall victim to phishing link	Anyone who has the router information
	B2	C	CVE-2013-1241 - An ISM module on the router does not handle authentication packets allowing hackers to bypass the authentication remotely and cause a Denial of Service attack	Consult with service providers to find a workaround	N/A	The exploit is in the authentication headers allowing hackers to bypass the authentication remotely and cause a Denial of Service attack	Untrained staff memeber who can fall victim to phishing link	Anyone who has the router information
	B3	CIA	N/A	N/A	The router is placed in a location with no physical security mechanisms to prevent anyone from accessing it	Since there are no physical controls for the router access, an intruder could reset or tamper with the router	Staff member with access to router location	Anyone who knows router location
	B4	CIA	N/A	The default SSID and passwords of the Cisco 2951 router has to be changed	N/A	The default passwords of Cisco 2951 is available on internet and any outsider could gain access to the network	N/A	Anyone who knows router's SSID

FRKS

Asset	Threat Statement Label	CIA	Gap in Technical controls	Gap in Administrative controls	Gap in Physical Controls	Exploit	Threat Agent (insider)	Threat Agent (outsider)
FRKS	C1	CIA	CVE-2012-1675 - The TNS Listener of Oracle 10g is vulnerable to remote command execution by attackers by allowing service registration which can be initiated by any remote host. This vulnerability is called as the TNS Poison. https://nvd.nist.gov/vuln/detail/CVE-2012-1675 (AV): N (AC): L (AU): N (C): P (I): P (A): P	Administrators are not restricting the TNS Listener access to unaothrized users	None	The attacker exploits this vulnerability by initiating a service registration followed by illicitly directing the data from the database server to the attacker's system. After getting the access, he can create database instances and launch man-in-the-middle, session hijacking and denial of service attacks.	Satff Members	Hacker
	C2	C	CVE-2005-4884 - An error in the Oracle Server 10g causes a vulnerability which can be used to bypass authentication. The error exists in the /dav_portal/portal directory which exposes the database resources. https://nvd.nist.gov/vuln/detail/CVE-2008-2138 (AV): N (AC): L (AU): N (C): P (I): N (A): N	Administrators do not properly secure the portal directory with strong authentication mechanisms.	None	Attackers exploit the vulnerability by sending a HTTP request with characters like "%0A" and thus bypassing the portal authentication by using the same session ID of the HTTP request. In this way, the attacker gains access to the /dav portal and the confidential information is disclosed to him. This directory may also reveal confidential information which can be used by attackers to launch further attacks.	Staff members	Skilled Hacker
	C3	CI	N/A	None	Credentials are being disclosed verbally or in some written form without encryption.(This vulnerability is an important area of concern for the senior management as said in the case) (AV): P (AC): L (AU): N (UI): N (S): U (C): H (I): H (A): N	Attackers can hack into the FRKS server using the stolen credentials and manipulate the billing information of patients or steal their financial sensitive information.They can even delete records or bills where the AMC will incur losses.	Friends and family	Outside attackers
	C4	C	N/A	None	No installtion of physical security where FRKS server is kept. (This vulnerability is an important area of concern for the senior management as said in the case) (AV): P (AC): L (AU): N (UI): N (S): U (C): H (I): N (A): N	Attackers can exploit this vulnerability by posing as staff members or patients and walking into the FRKS server room and he can just see the sensitive information by shoulder surfing or recording the monitor as there is no physical barrier.	Saff members	Outside attackers

ECDS

Asset	Threat Statement Label	CIA	Gap in Technical controls	Gap in Administrative controls	Gap in Physical Controls	Exploit	Threat Agent (insider)	Threat Agent (outsider)
ECDS	D1	CI	CVE-2018-8273: This vulnerability allows remote execution of a code on an affected system. it is a buffer overflow vulnerability		N/A	Any user can exploit the vulnerability since the system is already having the vulnerability. The user should know how to excute a code.	Highly skilled staff member	Highly skilled attacker
	D2	CI	CVE-2018-8527: This vulnerability discloses information when parsing a malicious XEL file containing a reference to an external entity in SSMS aka "SQL Server Management Studio Information Disclosure Vulnerability."		N/A	Any user can exploit this vulnerability by parsing the XEL file	Trained internal staff members	Expert hacker or someone with sound programming knowledge
	D3	CIA	N/A	Staff does not understand security issues. Entering incorrect medications for the patient	N/A	Staff members when they overlook their security issues, end up exposing the machines to possible attacks	Employees	Hackers
	D4	CI	N/A	No action taken if a policy is violated by someone working in the organization. Security is not a priority for the hospital	N/A	A user can misuse systems if the organization does not take necessary action and will keep on exploiting	Employees	Hacker impersonating himself as a staff member physically or digitally

MLS

Asset	Threat Statement Label	CIA	Gap in Technical controls	Gap in Administrative controls	Gap in Physical Controls	Exploit	Threat Agent (insider)	Threat Agent (outsider)
MLS Server	E1	C	CVE-2018-1655 - A software vulnerability in the rmsock command that exposes the kernel and it affects the confidentiality of the system	N/A	N/A	An attacker can exploit this issue to gain access to sensitive information that may lead to further attacks. The following products and versions are vulnerable: AIX 5.3, 6.1, 7.1, 7.2 VIOS 2.2.x	Internal staff	Highly skilled attacker
	E2	CIA	CVE-2018-1383 - A software logic bug creates a vulnerability in an AIX 6.1, 7.1, and 7.2 daemon which could allow a user with root privileges on one system, to obtain root access on another machine.	N/A	N/A	IBM AIX and Virtual I/O Server are prone to an unspecified remote privilege-escalation vulnerability. A remote attacker can exploit this issue to bypass certain restrictions and execute arbitrary code with root privileges. The following products are vulnerable: IBM AIX 6.1, 7.1 and 7.2 IBM VIOS 2.2.x	Internal staff	Highly skilled attacker
	E3	CI	N/A	N/A	Sharing passwords could compromise the security of MLS server. Solaris has a vulnerability for remote logins and when there is no control over the user, the system could be compromised using a simple phishing attack	Multiple users sharing one system leading to mismanagement of files and emails, one user can compromise the whole system by clicking a phishing link	Internal staff	N/A
	E4	CIA	N/A	N/A	There is no physical security in the room where FRKS is located. Since FRKS and MLS server are accessed via the same switch, an experienced intruder can remotely gain access to the inventory system	A one time visitor or an espionage agent could use his or her expertise to navigate from MLS server and access FRKS system.	Insider involved in espionage	Intruder

Cybersecurity Risk Estimation

The following tables are depiction of the risks that may be caused by the vulnerabilities identified in the previous sections. The risk estimation table shows the threat vector and the corresponding impact score, exploitable score, asset value and its Final impact value. Refer Appendix D to identify FIV calculation.

PDIS

Asset	Threat Statement Label	Threat Vector	Impact score	Exploitable score	Asset value score	FIV score	Likelihood	FIV	Risk
PDIS	A1	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	5.9	3.9	9.64	7.77	Possible	Severe	Medium High
	A2	AV:L/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:N	1.4	0.3	9.64	5.52	Very unlikely	Significant	Medium
	A3	AV:P/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N	4	0.9	9.64	6.82	Very unlikely	Significant	Medium
	A4	AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N	5.8	0.9	9.64	7.72	Unlikely	Severe	Medium high

Router

Asset	Threat Statement Label	Threat Vector	Impact score	Exploitable score	Asset value score	FIV score	Likelihood	FIV	Risk
Router	B1	AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H	3.6	1.2	3.93	3.765	Very unlikely	Minor	Low
	B2	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	3.6	3.9	3.93	3.765	Unlikely	Minor	Low med
	B3	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	5.9	3.9	3.93	4.915	Unlikely	Moderate	Low med
	B4	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	5.9	3.9	3.93	4.915	Unlikely	Moderate	Low med

FRKS

Asset	Threat Statement Label	Threat Vector	Impact score	Exploitable score	Asset value score	FIV score	Likelihood	FIV	Risk
FRKS	C1	(AV): N (AC): L (AU): N (C): P (I): P (A): P	6.4	10	6.79	6.595	Very likely	Significant	High
	C2	(AV): N (AC): L (AU): N (C): P (I): N (A): N	2.9	10	6.79	4.845	Very likely	Moderate	Medium high
	C3	(AV): P (AC): L (AU): N (UI): N (S): U (C): H (I): H (A): N	5.2	0.9	6.79	5.995	Very unlikely	Significant	Medium
	C4	(AV): P (AC): L (AU): N (UI): N (S): U (C): H (I): N (A): N	3.6	0.9	6.79	5.195	Very unlikely	Significant	Medium

ECDS

Asset	Threat Statement Label	Threat Vector	Impact score	Exploitable score	Asset value score	FIV score	Likelihood	FIV	Risk
ECDS	D1	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	5.9	3.9	6.43	6.165	Possible	Significant	Medium high
	D2	AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N	3.6	1.8	6.43	5.015	Unlikely	Significant	Medium
	D3	AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	5.9	0.9	6.43	6.165	Very unlikely	Significant	Medium
	D4	AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N	5.2	2.5	6.43	5.815	Unlikely	Moderate	Low med

MLS

Asset	Threat Statement Label	Threat Vector	Impact score	Exploitable score	Asset value score	FIV score	Likelihood	FIV	Risk
MLS Server	E1	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	3.6	1.8	7.5	5.55	Very unlikely	Significant	Medium
	E2	AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H	6	2.3	7.5	6.75	Unlikely	Significant	Medium
	E3	AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N	5.2	1.2	7.5	6.35	Very unlikely	Significant	Medium
	E4	AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	5.9	1.2	7.5	6.7	Very unlikely	Significant	Medium

Cyber Security Risk Management Strategy

PDIS

Asset	Threat Label	Risk Management Strategy	Controls Required	Cost of Control
PDIS	A1	Risk Mitigation: Oracle Critical patch update was issued to keep a track of risks such as denial of service attack and data modification by the outside user	Oracle Critical patch update	Control can be found at: http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
	A2	Risk Mitigation: Oracle Critical patch update is issued to keep track of the risks associated with threat to counter the escalation of priviledges to other outside users.	Oracle Critical patch update	The security update and explanation is available at http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
	A3	Risk Mitigation: The staff members entering data into the system should crosscheck the entries of the data. Also there should be authentication of data at another level which is checked another person	Training session and corrective measures	Free of cost training and awareness must be spread among staff members regarding criticality of correct data
	A4	Risk Mitigation: Unauthorized access to the system must be blocked so that no outside user could access the system	Training session and corrective measures	Free of cost training and awareness must be spread among staff members regarding criticality of correct data

Router

Asset	Threat Label	Risk Management Strategy	Controls Required	Cost of Control
Router	B1	Risk Mitigation: Administrators should allow only authorized users to access the network and only the trusted users can modify the system preferences.	Access controls	No cost
	B2	Risk Mitigation: The authentication header should be carefully tracked to avoid denial of service attack. cisco-upgrade-latest patch should be deployed for better management of authentication packets.	cisco-upgrade-latest patch	The update and fix is free and can be found at https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20130507-CVE-2013-1241
	B3	Risk Mitigation - The router should be placed in such a location that it cannot be accessed by anyone physically. Physical barriers should be installed, the router can be put in the lock box or security case.	Security case or lock box/ biometric access control	The cost of security case or lock box is pretty low. Another option could be biometric access controls which is available at various range of prices
	B4	Risk Mitigation - The default password and SSID should be changed. All rules for setting a strong password should be followed	Password authentication	No cost

FRKS

Asset	Threat Label	Risk Management Strategy	Controls Required	Cost of Control
FRKS	C1	Risk Mitigation - TNS Listener Checker module can be installed which sends the TNS Listener registration request packet to server and gets an error packet in response. If it doesn't, then the adminstrator can check for illicit registrations.	TNS Listener Checker Module	The source code for the module is freely available online
	C2	Avoid Risk - Administrators should enforce stronger authentication mechanisms for the /dav portal directory so that attackers do not access it easily. Risk Mitigation - Trend Micro Deep Security software protects Oracle 10g from attacks resulting from these kind of vulnerabilities. So, AMC can install this software in FRKS.	Trend Micro Deep Security DPI Rule Number: 1002514	Trend Micro Deep Software charges an hourly rate of 1, 3 or 6 cents
	C3	Risk Mitigation - Employees should be given a proper training on security mechanisms like strong passwords and about sharing of passwords to anyone. They should be educated and even given some hands-on training on how not to divulge confidential information.	Training session and activities	The training activities do not incur much charges or cost.
	C4	Risk Avoidance - This threat can be avoided by installing a physical security mechanism in the room where FRSK server is kept. The door should have a biometric or RFID lock using which only authorized users can gain access to the room.	Biometric/RFID lock on FRKS server room door	The cost of installing the locks ranges from $50 - $500

ECDS

Asset	Threat Label	Risk Management Strategy	Controls Required	Cost of Control
ECDS	13	Risk Mitigation: This threat can be nullified by installing Microsoft's latest security update. To perform this exploit, the exploiter would have to submit a custom-built query on to an infected SQL Server. This security update alters the manner in which the database engine deals with memory objects.	Microsoft SQL Server Remote Code Execution Vulnerability Security Update	The security update is available for free download at https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8273
	14	Risk Mitigation: This threat can be nullified by installing Microsoft's latest security update. To perform this exploit, the exploiter would have to lure a user to open a specially made XEL file on an infected SQL Server. This security update alters the manner in which SSMS parses XML inputs.	SQL Server Management Studio Information Disclosure Vulnerability Security Update	The security update is available for free download at https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8527
	15	Risk Avoidance: This threat can be avoided by educating the hospital staff about security precautions and training them to prescribe correct medications to the patients.	Training session	Employing training sessions to educate hospital staff can be conducted without incurring any cost
	16	Risk Avoidance/Mitigation: This threat can be remedied by enforcing strict action on employees working on the inside or outsiders who try to exploit SSMS by posing as insiders. Implementation of stringent security would discourage malpratices and reduce chances of future exploits.	Corrective measures	Deploying disciplinary measures would not cost anything.

MLS

Asset	Threat Label	Risk Management Strategy	Controls Required	Cost of Control
MLS	17	Risk Mitigation: This threat can be nullified by subscribing to IBM Authorized Program Analysis Reports (APARs). These reports are unique to specific vulnerabilities. IBM will share these reports over email and will contain the status of the APAR and a link that will allow the user to download the software fix whenever it becomes available. Moreovere, the fixes have now been made available without the use of APAR subscription.	APARS subscription/AIX fix	Free (can be found at http://www-01.ibm.com/support/docview.wss?uid=isg3T1027880)
	18	Risk Mitigation: This threat can be nullified by subscribing to IBM Authorized Program Analysis Reports (APARs). These reports are unique to specific vulnerabilities. IBM will share these reports over email and will contain the status of the APAR and a link that will allow the user to download the software fix whenever it becomes available. Moreovere, the fixes have now been made available without the use of APAR subscription.This fix will negate the logic bug that maliciously provides root access to a user to procure root access on another machine.	APARS subscription/AIX fix	Free (can be found at http://www-01.ibm.com/support/docview.wss?uid=isg3T1026948)
	19	Risk Mitigation: Improve storage and efficiency to make login time faster/ encourage employees to use separate systems	Introduce several systems	~$600 per workstation
	20	Risk Mitigation: Biometrics/RFID systems should be implemented to limit people accessing the rooms	RFID/Biometric Systems	~ $200 per biometric lock

Appendices

Appendix A – Measurement scales

Financial impact scale

Financial Impact		
Most expensive -4	>50k	Failure of the asset will have financial impact of more than 50k
Somewhat expensive - 3	>25k	Failure of the asset will have financial impact of more than 25k
Inexpensive - 2	>10k	Failure of the asset will have financial impact of more than 10k
Least expensive - 1	<5k	Failure of the asset will have financial impact of less than 5k

Operational impact scale

Operational Impact	
Very high - 5	Process failure
High - 4	Critical and indirect effect on process
Medium - 3	Process delayed
Low - 2	Process affected but not critical
None - 1	No impact on process

Legal impact scale

Legal Impact	
Yes-1	Failure will result in lawsuits
No-0	No legal implication

Appendix B

Brief description of technical vulnerabilities

Asset	Threat Statement Label	CVE ID	CVE link
PDIS	A1	CVE-2017-15535	https://nvd.nist.gov/vuln/detail/CVE-2017-15535
	A2	CVE-2017-14227	https://nvd.nist.gov/vuln/detail/CVE-2017-14227
Router	B1	CVE-2013-6701	https://nvd.nist.gov/vuln/detail/CVE-2013-6701
	B2	CVE-2013-1241	https://nvd.nist.gov/vuln/detail/CVE-2013-1241
FRKS	C1	CVE-2012-1675	https://nvd.nist.gov/vuln/detail/CVE-2012-1675
	C2	CVE-2005-4884	https://nvd.nist.gov/vuln/detail/CVE-2005-4884
ECDS	D1	CVE-2018-8273	https://nvd.nist.gov/vuln/detail/CVE-2018-8273
	D2	CVE-2018-8527	https://nvd.nist.gov/vuln/detail/CVE-2018-8527
MLS Server	E1	CVE-2018-1655	https://nvd.nist.gov/vuln/detail/CVE-2018-1655
	E2	CVE-2018-1383	https://nvd.nist.gov/vuln/detail/CVE-2018-1383

Brief description of non-technical vulnerabilities

Asset	Threat Statement Label	CIA	Gap in Administrative controls	Gap in Physical Controls	Exploit
PDIS	A3	I	Missing data validation	N/A	System has incorrect data
	A4	CIA	N/A	PDIS screen is left unattended by the doctor after using or entering the data	Someone can fetch, enter or modify existing data and that will flow into the system and could result in incorrect medical treatment
Router	B3	CIA	N/A	The router is placed in a location with no physical security mechanisms to prevent anyone from accessing it	Since there are no physical controls for the router access, an intruder could reset or tamper with the router
	B4	CIA	The default SSID and passwords of the Cisco 2951 router has to be changed	N/A	The default passwords of Cisco 2951 is available on internet and any outsider could gain access to the network
FRKS	C3	CI	None	Credentials are being disclosed verbally or in some written form without encryption.(This vulnerability is an important area of concern for the senior management as said in the case)	Attackers can hack into the FRKS server using the stolen credentials and manipulate the billing information of patients or steal their financial sensitive information.They can even delete records or bills where the AMC will incur losses.
	C4	C	None	No installtion of physical security where FRKS server is kept. (This vulnerability is an important area of concern for the senior management as said in the case)	Attackers can exploit this vulnerability by posing as staff members or patients and walking into the FRKS server room and he can just see the sensitive information by shoulder surfing or recording the monitor as there is no physical barrier.
ECDS	D3	CIA	Staff does not understand security issues. Entering incorrect medications for the patient	N/A	Staff members when they overlook their security issues, end up exposing the machines to possible attacks
	D4	CI	No action taken if a policy is violated by someone working in the organization. Security is not a priority for the hospital	N/A	A user can misuse systems if the organization does not take necessary action and will keep on exploiting
MLS Server	E3	CI	N/A	Sharing passwords could compromise the security of MLS server. Solaris has a vulnerability for remote logins and when there is no control over the user, the system could be compromised using a simple phishing attack	Multiple users sharing one system leading to mismanagement of files and emails, one user can compromise the whole system by clicking a phishing link
	E4	CIA	N/A	There is no physical security in the room where FRKS is located. Since FRKS and MLS server are accessed via the same switch, an experienced intruder can remotely gain access to the inventory system	A one time visitor or an espionage agent could use his or her expertise to navigate from MLS server and access FRKS system.

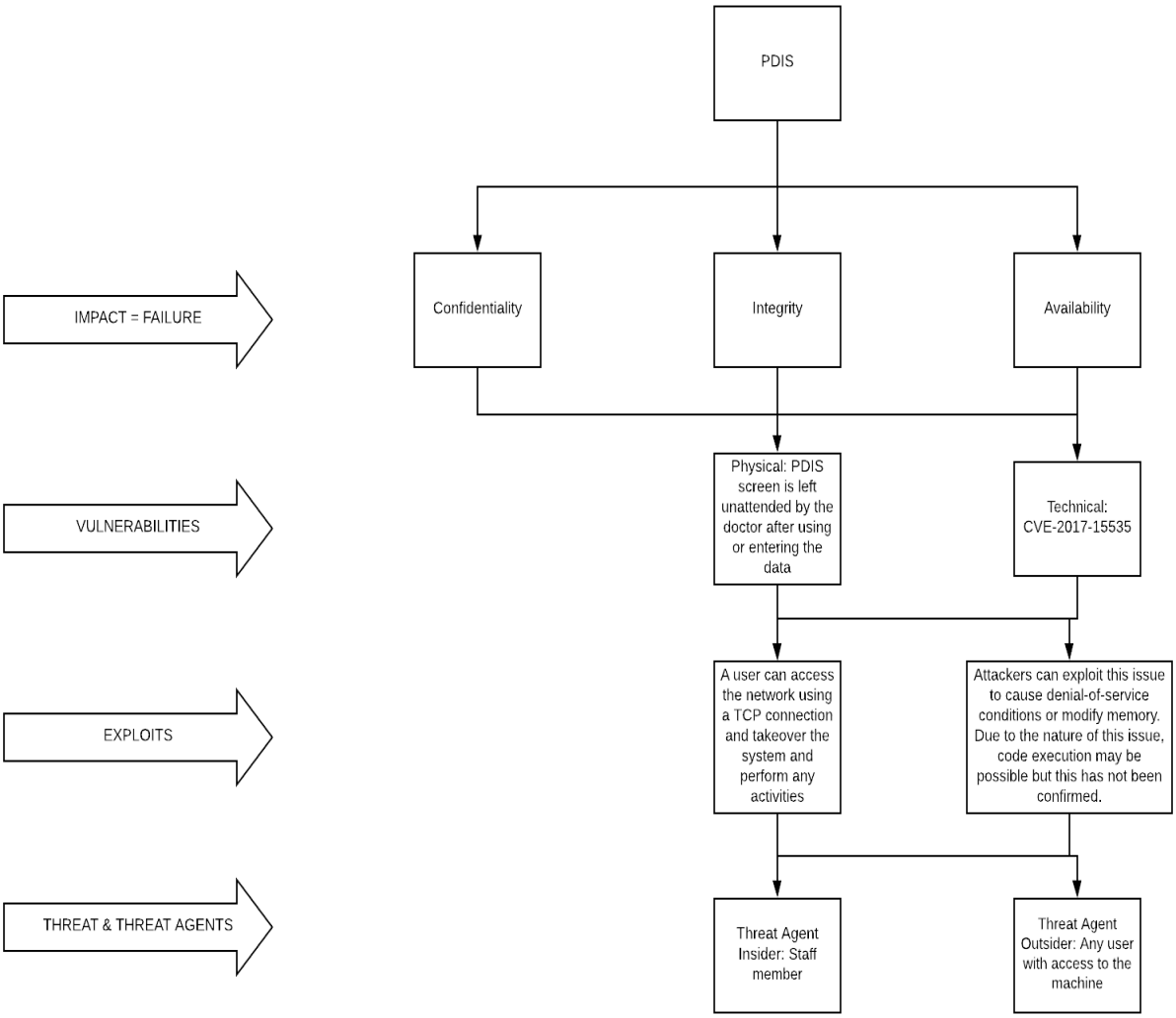
List of threat vectors for technical and non-technical vulnerabilities

Asset	Threat Statement Label	Threat Vector
PDIS	A1	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
	A2	AV:L/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:N
	A3	AV:P/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N
	A4	AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N
Router	B1	AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H
	B2	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
	B3	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
	B4	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
FRKS	C1	(AV): N (AC): L (AU): N (C): P (I): P (A): P
	C2	(AV): N (AC): L (AU): N (C): P (I): N (A): N
	C3	(AV): P (AC): L (AU): N (UI): N (S): U (C): H (I): H (A): N
	C4	(AV): P (AC): L (AU): N (UI): N (S): U (C): H (I): N (A): N
ECDS	D1	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
	D2	AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
	D3	AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
	D4	AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
MLS Server	E1	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
	E2	AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
	E3	AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N
	E4	AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

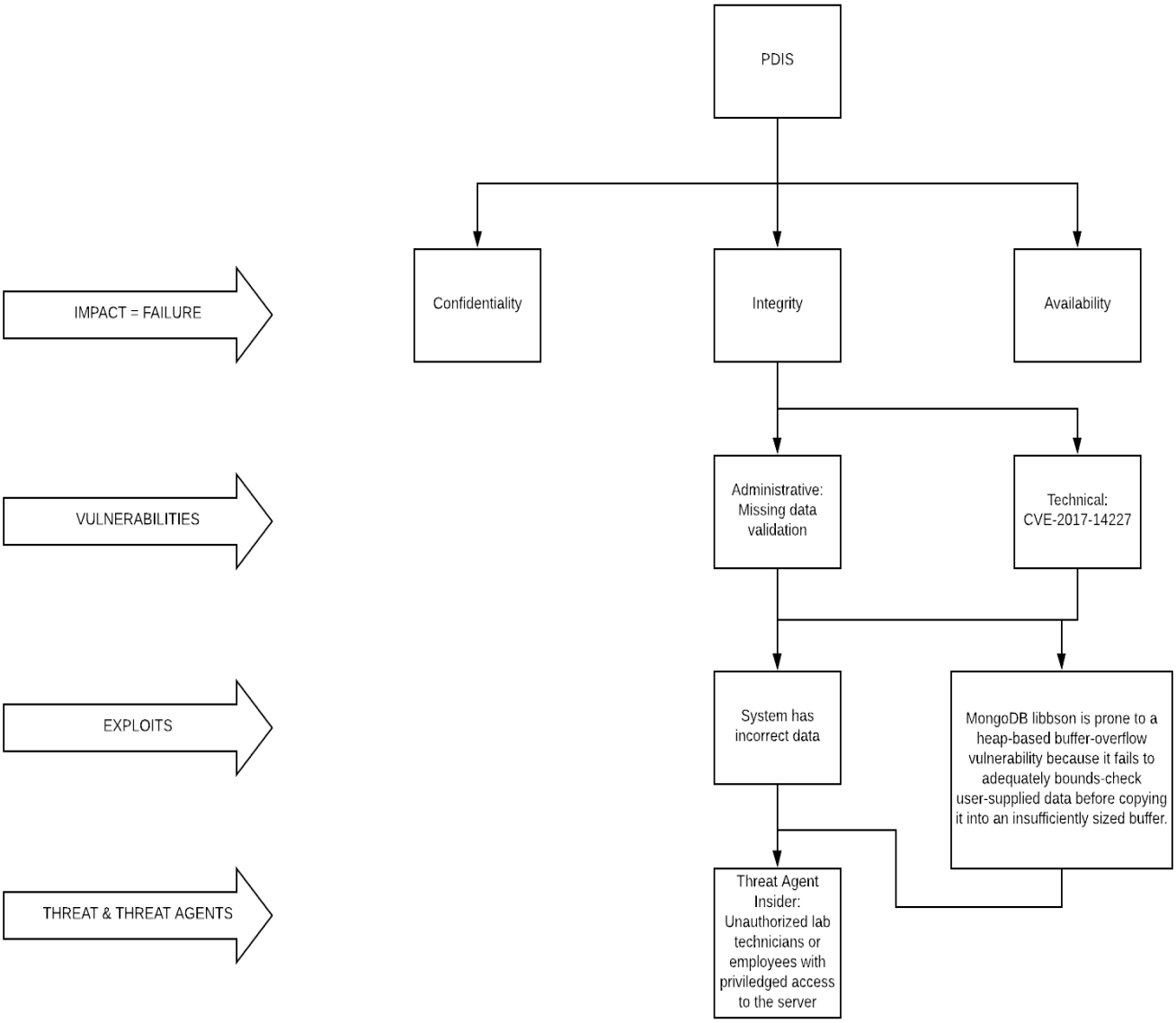
Tree analysis

PDIS

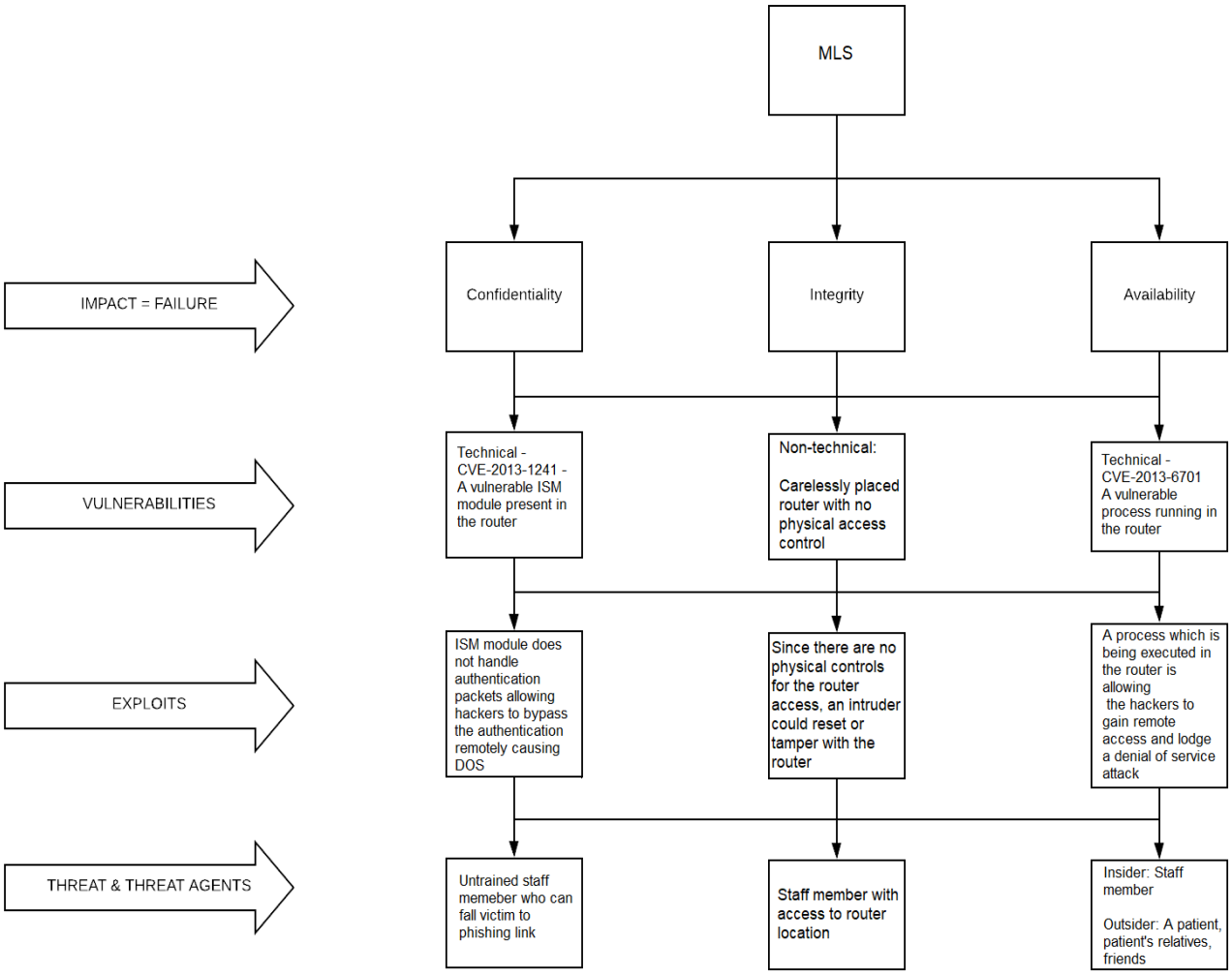
PDIS tree analysis - 1



PDIS tree analysis – 2

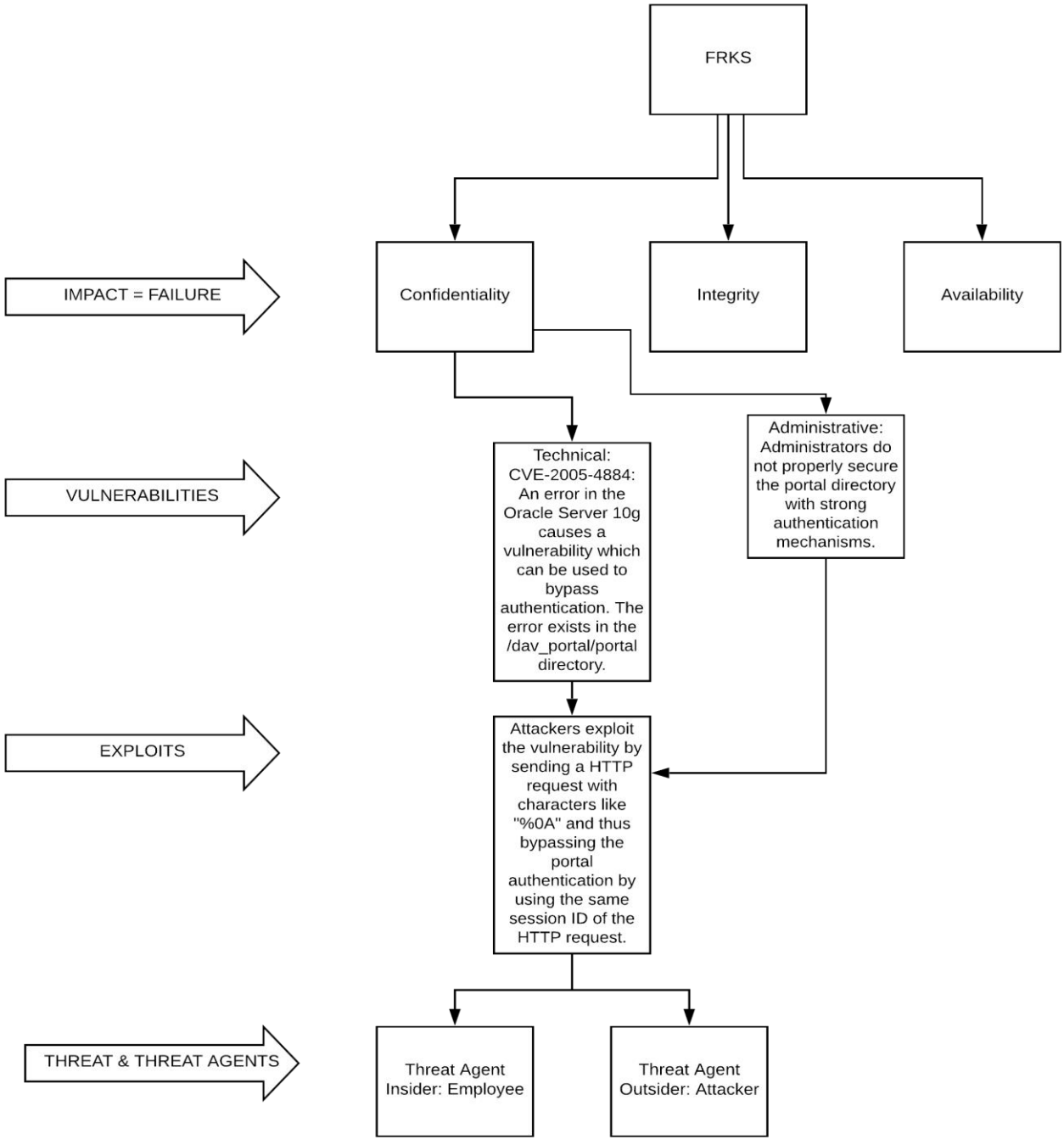


Router

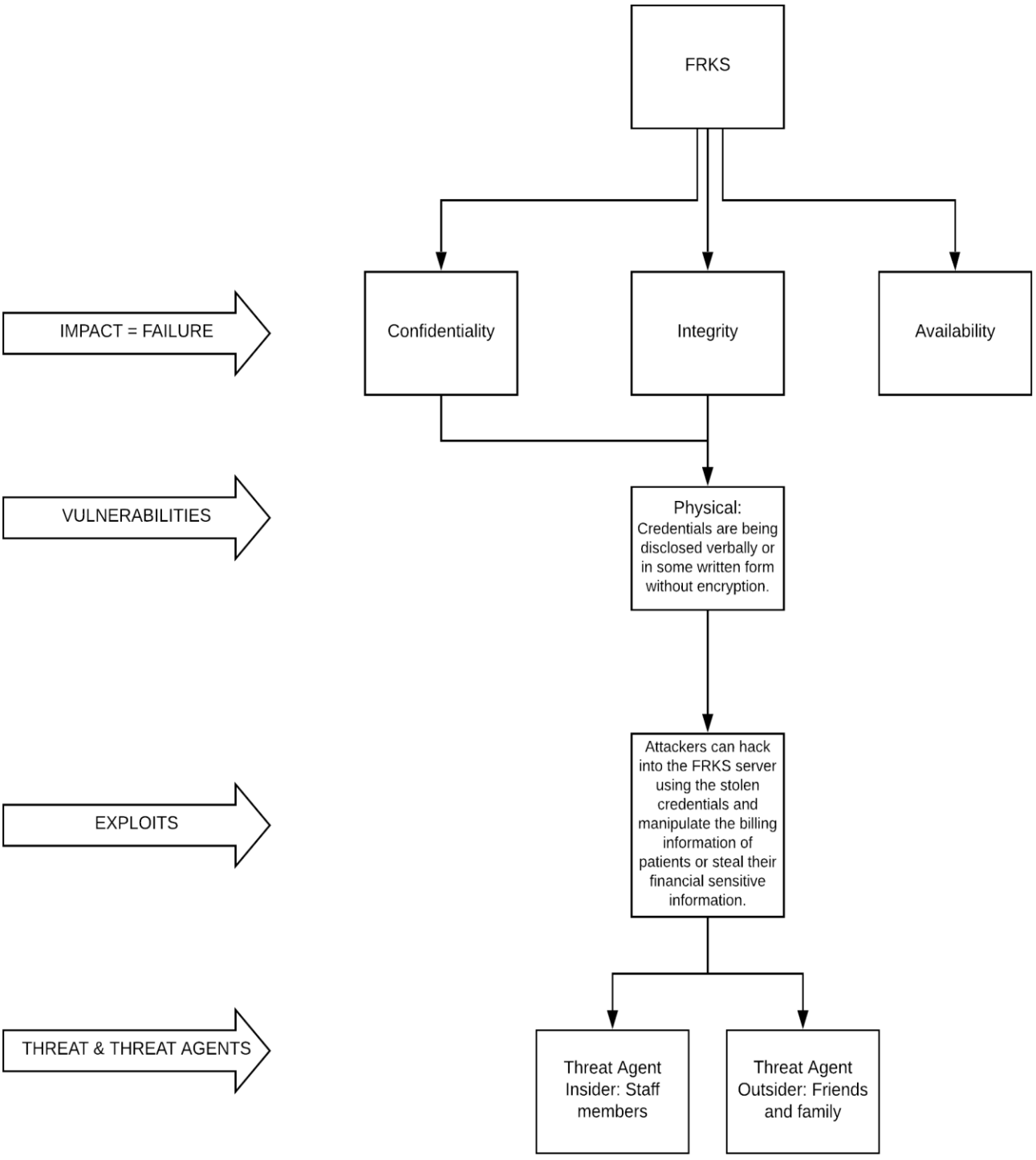

MLS
IMPACT = FAILURE
Confidentiality
Integrity
Availability
VULNERABILITIES
Technical - CVE-2013-1241 - A vulnerable ISM module present in the router
Non-technical: Carelessly placed router with no physical access control
Technical - CVE-2013-6701 A vulnerable process running in the router
EXPLOITS
ISM module does not handle authentication packets allowing hackers to bypass the authentication remotely causing DOS
Since there are no physical controls for the router access, an intruder could reset or tamper with the router
A process which is being executed in the router is allowing the hackers to gain remote access and lodge a denial of service attack
THREAT & THREAT AGENTS
Untrained staff memeber who can fall victim to phishing link
Staff member with access to router location
Insider: Staff member
Outsider: A patient, patient's relatives, friends

FRKS

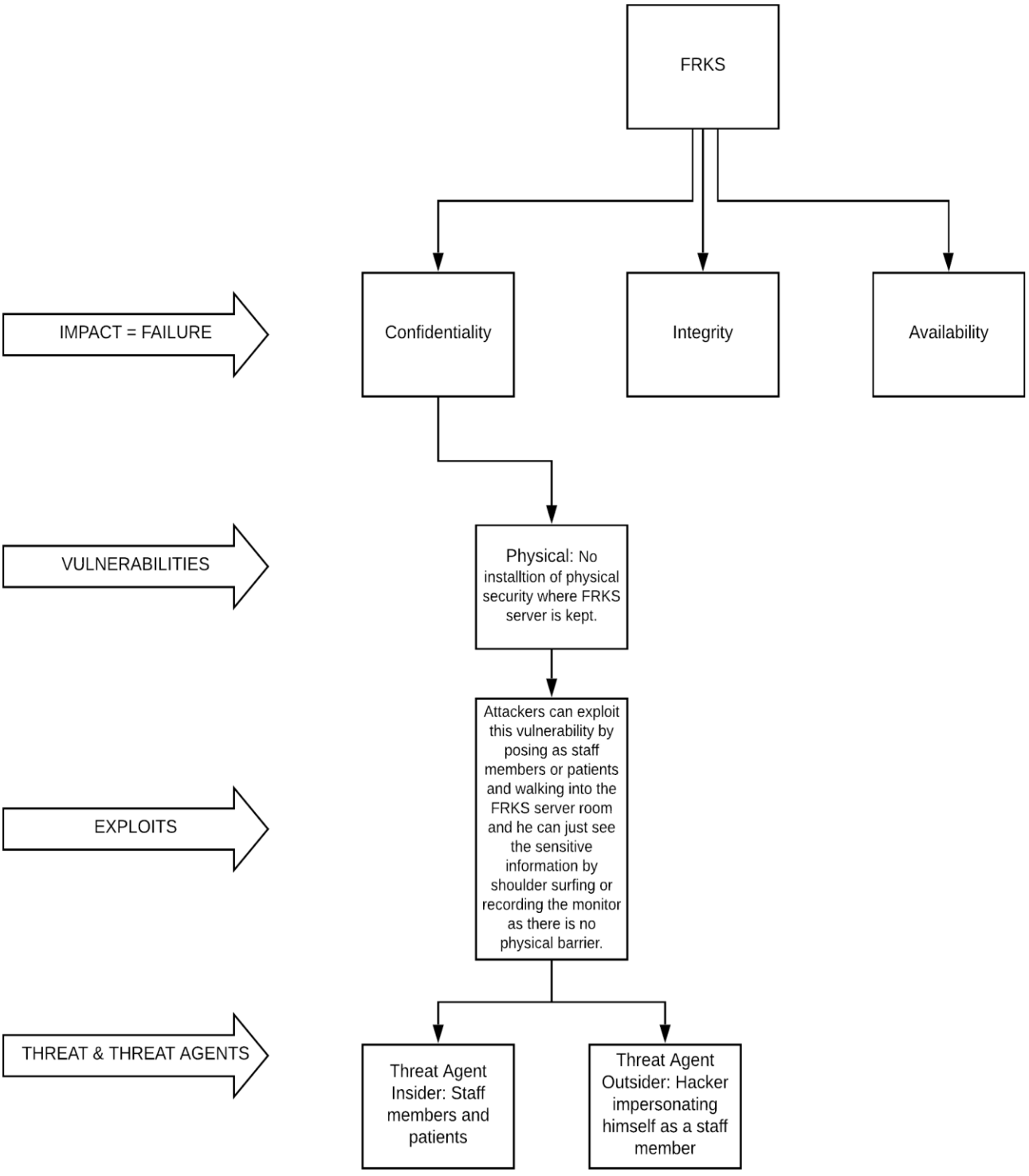
FRKS tree analysis 1



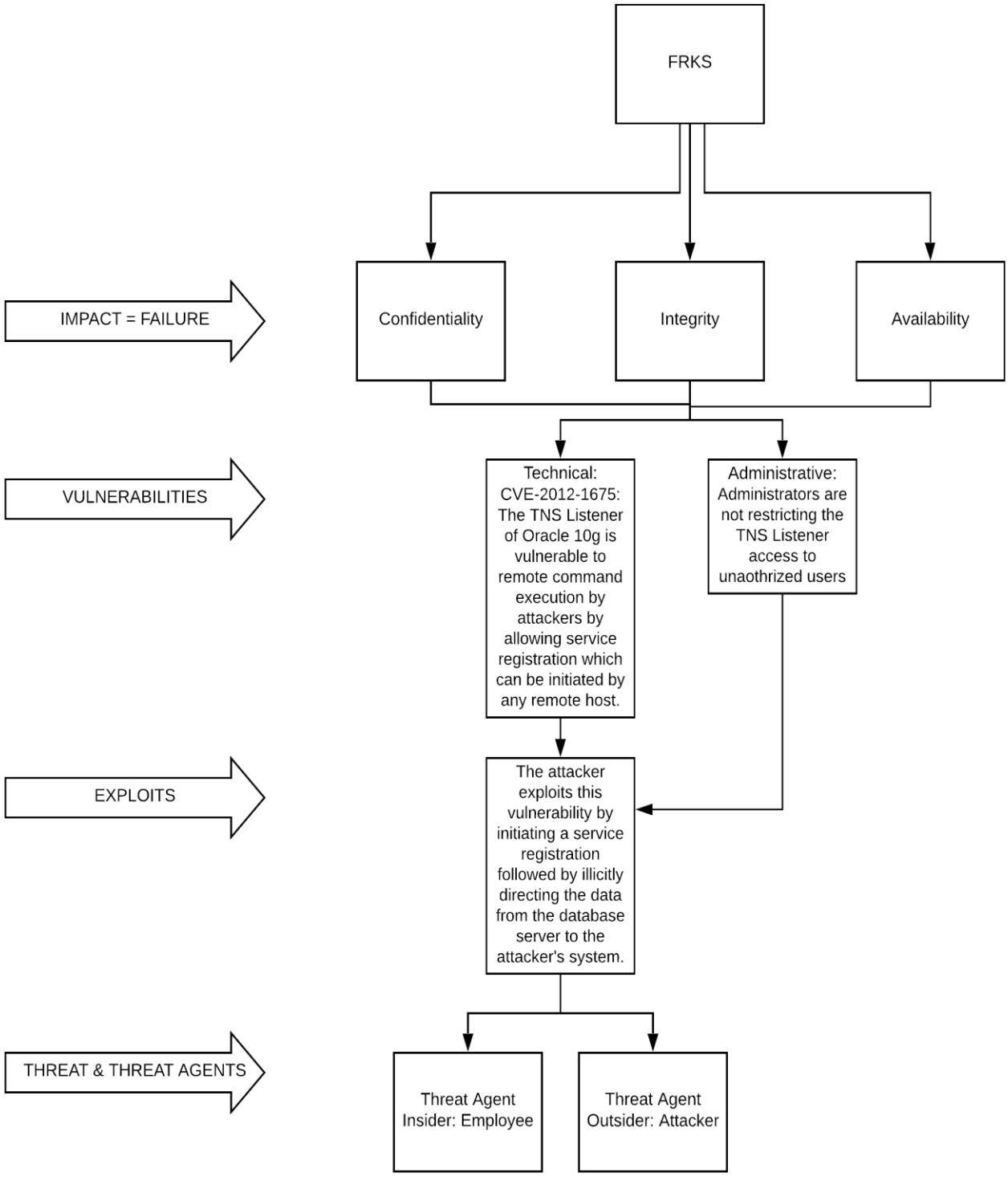
FRKS tree analysis 2



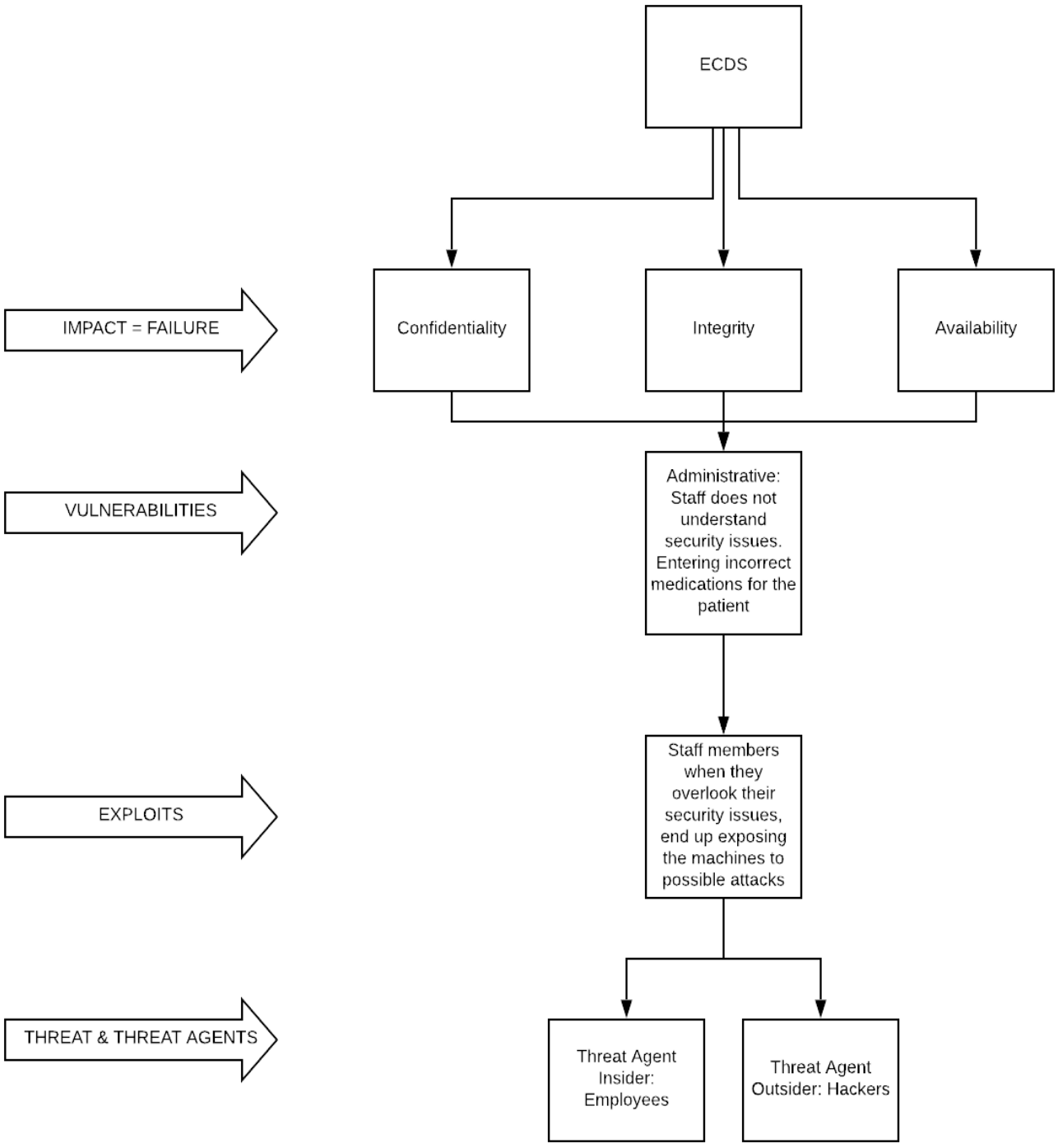
FRKS tree analysis 3



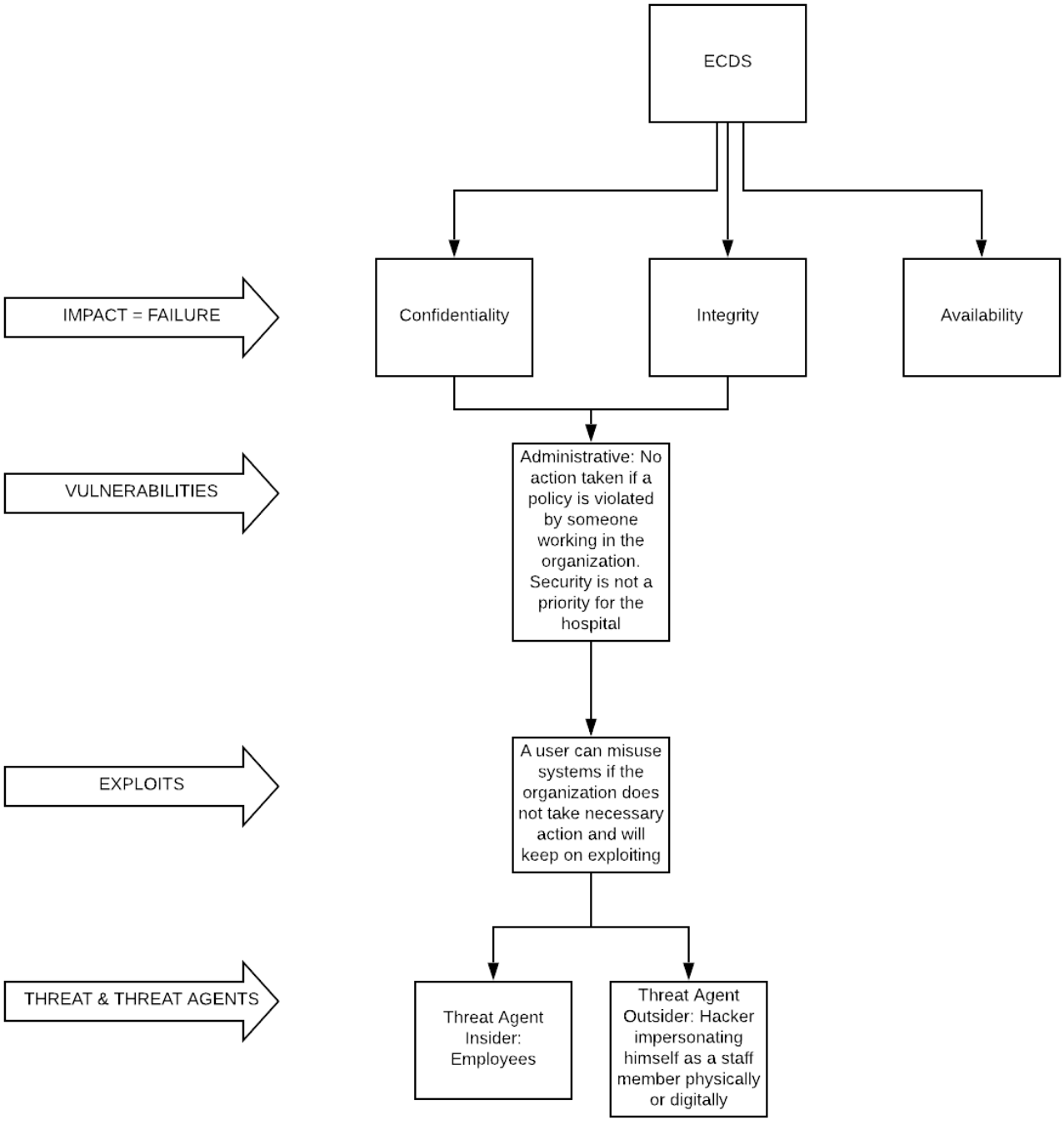
FRKS tree analysis 4



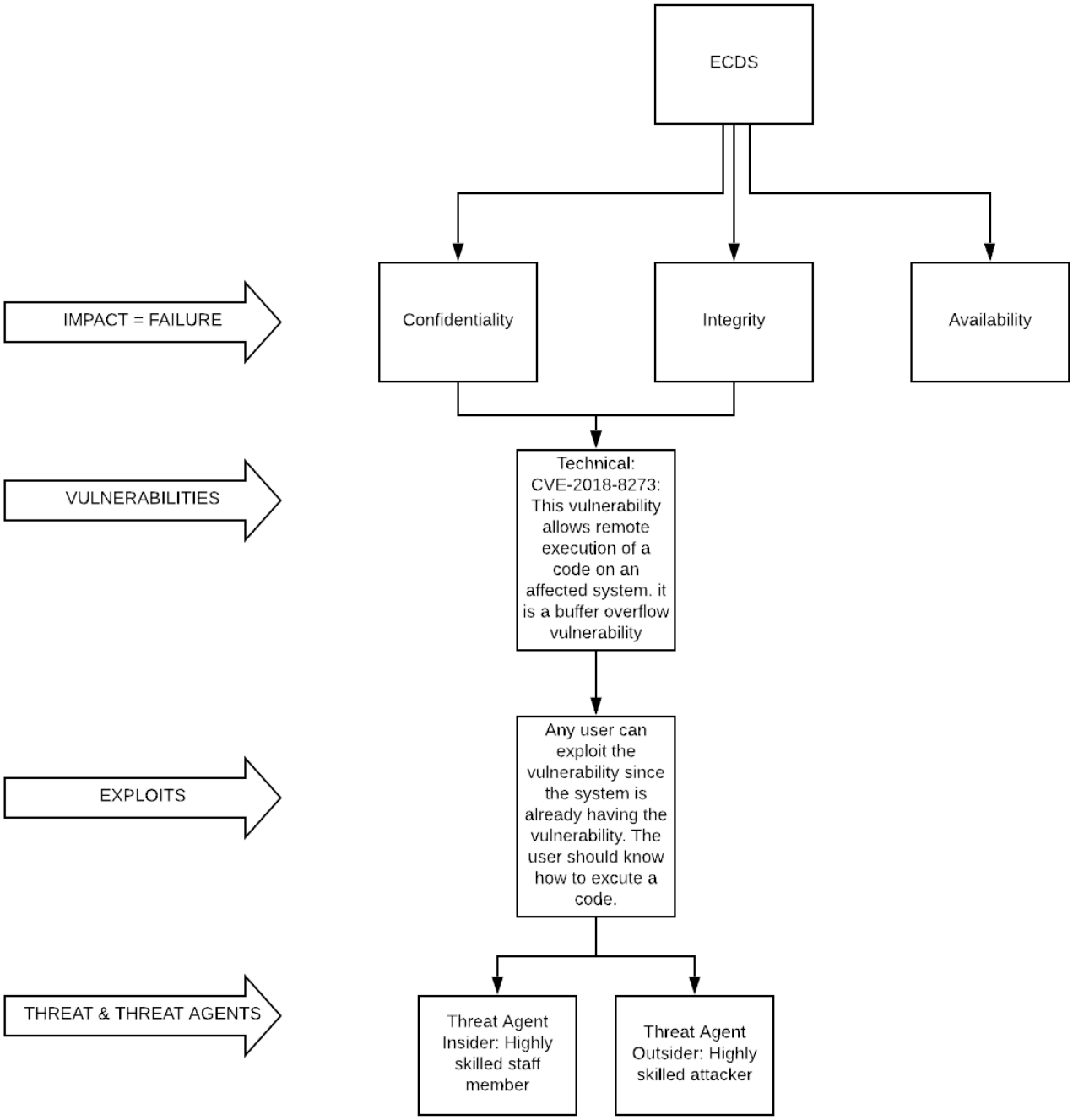
ECDS tree analysis 1



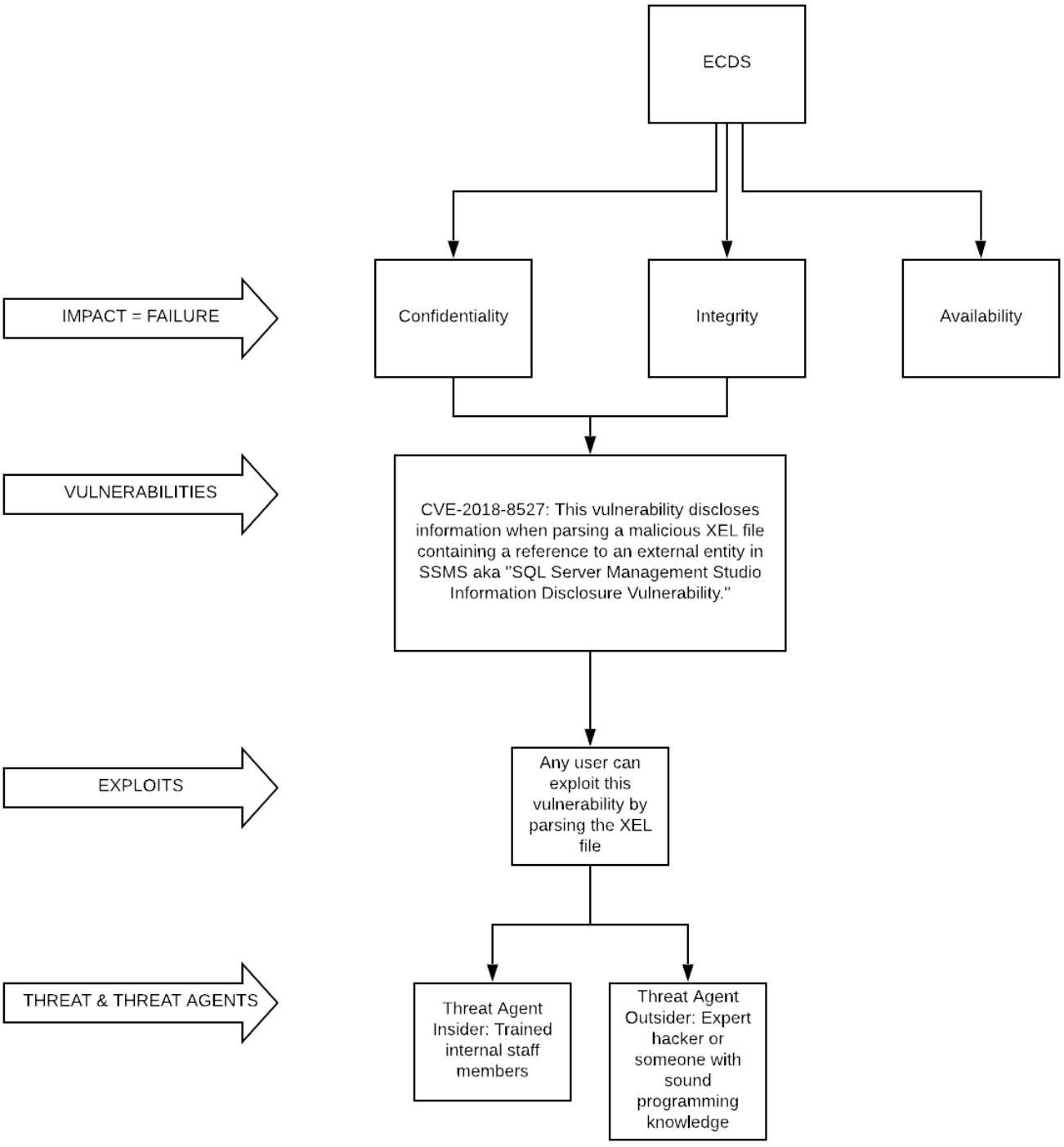
ECDS tree analysis 2



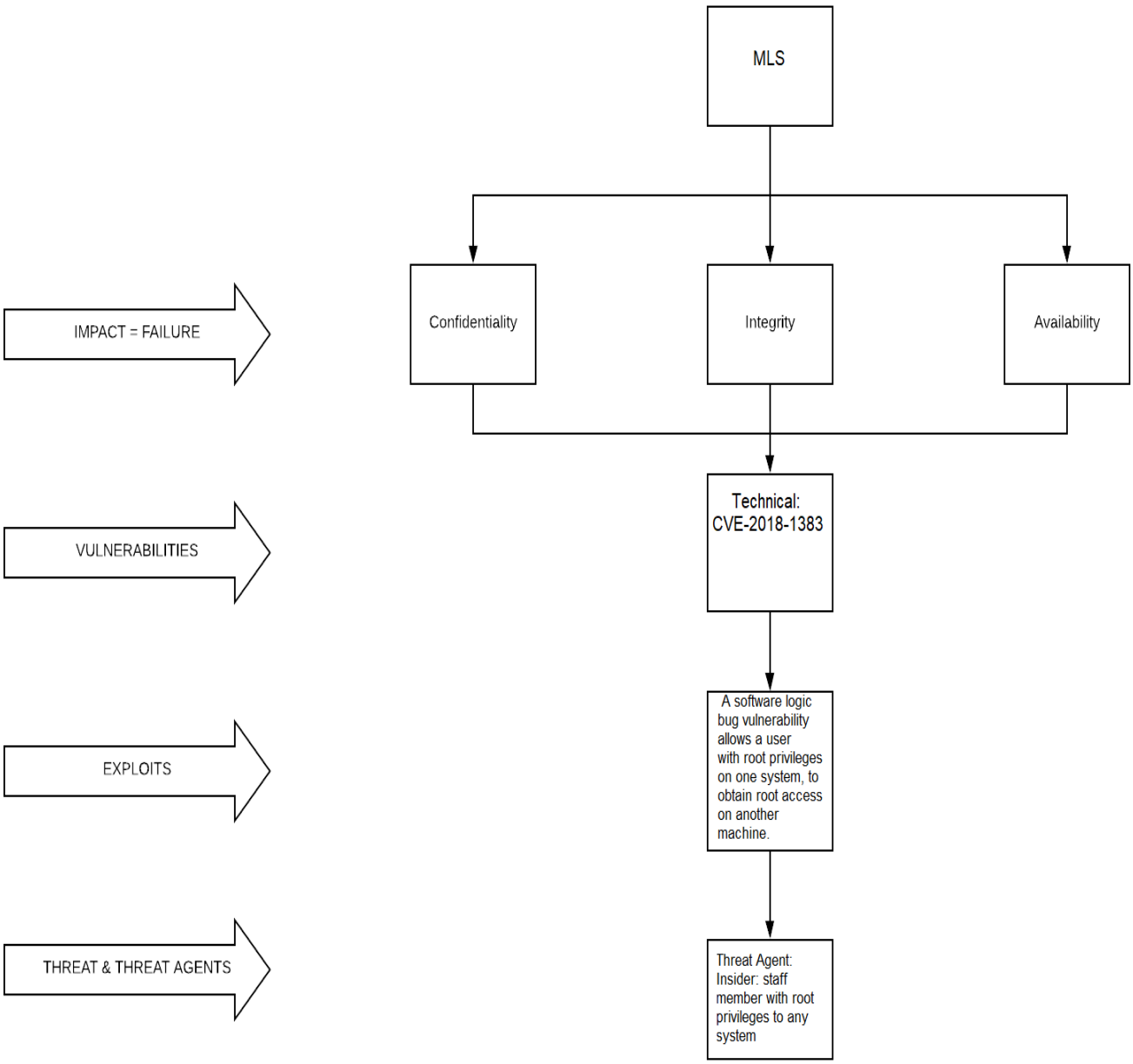
ECDS tree analysis 3



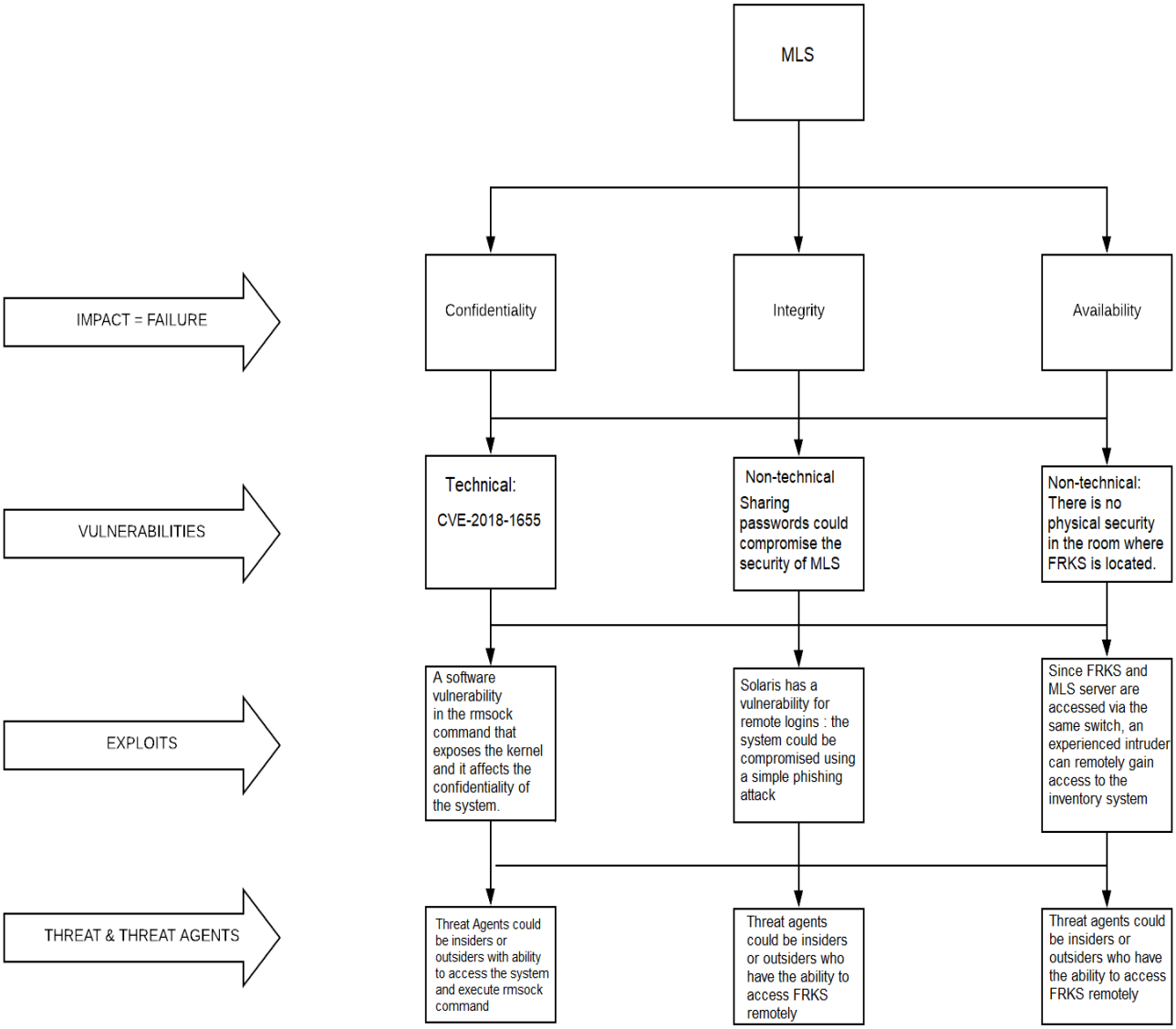
ECDS tree analysis 4



MLS tree analysis 1



MLS tree analysis 2



Appendix C – Measurement Scale for scoring Threat Likelihood

Score Value	Likelihood
7<Exploitability Score<10	Very Likely
5<Exploitability Score<7	Likely
3<Exploitability Score<5	Possible
1<Exploitability Score<3	Unlikely
Exploitability Score<1	Very Unlikely

Appendix D

Estimation of Final Impact Value

FIV = Average of Impact score and Asset Value

Asset	Threat Statement Label	Impact score	Exploitable score	Asset value score	FIV score
PDIS	A1	5.9	3.9	9.64	7.77
	A2	1.4	0.3	9.64	5.52
	A3	4	0.9	9.64	6.82
	A4	5.8	0.9	9.64	7.72
Router	B1	3.6	1.2	3.93	3.765
	B2	3.6	3.9	3.93	3.765
	B3	5.9	3.9	3.93	4.915
	B4	5.9	3.9	3.93	4.915
FRKS	C1	6.4	10	6.79	6.595
	C2	2.9	10	6.79	4.845
	C3	5.2	0.9	6.79	5.995
	C4	3.6	0.9	6.79	5.195

Asset	Threat Statement Label	Impact score	Exploitable score	Asset value score	FIV score
ECDS	D1	5.9	3.9	6.43	6.165
	D2	3.6	1.8	6.43	5.015
	D3	5.9	0.9	6.43	6.165
	D4	5.2	2.5	6.43	5.815
MLS Server	E1	3.6	1.8	7.5	5.55
	E2	6	2.3	7.5	6.75
	E3	5.2	1.2	7.5	6.35
	E4	5.9	1.2	7.5	6.7

Measurement Scale used for scoring FIV

Score Value	FIV
7<FIV<10	Severe
5<FIV<7	Significant
4<FIV<5	Moderate
3<FIV<4	Minor
FIV<3	Negligible

Appendix E - Cybersecurity Risk Matrix and Risk Management Strategy for various cybersecurity risk values

Likelihood/FIV	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

Appendix F – Assumptions

Asset ID	Asset Name	Assumption
17	Administration's workstations	Not all workstations are affected at the same time and that MLS is accessible from other unaffected workstations too - this may slow down processes (BP3) tremendously and impair them, but won't result in process stoppage
3	Physician's workstations	Assuming that not all physician's workstation fail and physicians cuold access few workstations, it would impact and delay the business process of managing medicine supplies but not failure of the process

References

- https://study.com/academy/lesson/it-threat-mitigation-definition-strategies.html
- https://nvd.nist.gov/
- https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Glossary

Abbreviations used:

AMC	Aggie Medical Center
FIV	Final Impact Value
NVD	National Vulnerability Database

Team Work

Team Member	Tasks completed
Sandheep Sridar	Asset description - Inroduction, vulnerability classification, tree analysis, FIV calc, risk estimation introduction, risk estimation calculation, Appendix attachements, Compilation of report, review
Harmit Jasani	Executive summary, acknowledgements, tree analysis, risk management strategies, asset identification and asset classification, document review
Mihir Bhende	Asset identification and classification - Introduction, Asset identification and classification, tree analysis, risk management strategies, document review
Pratik Toshniwal	Vulnerability identification, tree analysis, FIV calculation, risk estimation and risk matrix and threat likelihood identification, risk estimation calculations document review
Sai Subhasree Pakina	Vulnerability identification, Asset identification and classification, tree analysis, risk management strategies, asset identification and asset classification, document review