ISTM 635: Business Information Security

Qualitative Cybersecurity Risk Assessment

Aggieland Medical Center (AMC)

Aggie Honor Code

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

Aggie Integrity Statement

"On my honor, as an Aggie, I have neither given nor received unauthorized aid on this academic work."

Authors
Ameya Saptarshi
Bansari Paresh Kothari
Palazhy Sidharth Ravindranath
Shaheen Qadir
Yash Umeshkumar Katariya

Table of Contents

Executive Summary

The report encompasses the detailed study of Aggieland Medical Center (AMC) by gathering information and understanding the critical assets of their business model. Highly skilled cybersecurity professionals are performing the analysis of the threats and vulnerabilities that Aggieland Medical Center could face along with providing recommendations on risk management. This will ensure the improvement of existing security of the medical center and keep intruders out of the system. Based on the case study and going through detailed conversations with employees, the analysis is inferred. The possibility of various attacks have been measured at depth andir consequences have been identified. The details of which are given below.

As part of the Qualitative Risk Analysis of Aggieland Medical Center, our team has discovered a considerable number of security lapses. The remainder of this document will seek to highlight the major flaws with the current security infrastructure implemented by AMC by defining potential vulnerabilities, threats, and the likelihood of exploitation. These shall be laid out with an accurate scale of measurement for succinct yet thorough documentation of Qualitative Risks.
After a thorough analysis, the team has concluded that AMC has a wide range of potential vulnerabilities. However, there are no high-priority vulnerabilities that are an immediate threat. In light of this, the team has highlighted security control measures that need to be implemented as a top priority to ensure the safety of the assets and overall system.

The risk mitigation strategies can be planned and implemented based on the impact of threat and the exploitability of a vulnerability. The below analysis will provide details on which risk exposure areas need to be addressed to avoid failure of the system or incurring a financial loss.

Asset Identification

Asset ID	Asset Name	Asset Description	Reason for Cybersecurity Risk Assessment
A1	Patient Data Information Server - PDIS	This database is the primary repository for patient data and serves as the hub of activities. It also keeps track of appointments. It involves old database systems and is one of numerous database systems used in the system.	It is important to operate 24 hours a day, seven days a week, while maintaining confidentiality and restricting access to only authorized users. Databases are notoriously vulnerable to assaults, and if security is inadequate, critical patient data may be compromised. As a result, we must eliminate as many weaknesses as feasible.
A2	Financial Record Keeping Server - FRKS	This server maintains information about insurance, billing records, payment schedules, and other such topics. The results of daily operations are kept in this file.	To ensure that the server is secure and up to date, vulnerability checks must be performed. They store sensitive information such as financial records and payment details for customers. To avoid operational lag, it must be engaged at all times, especially during working hours.
A3	Emergency Care Data System (ECDS)	The system contains data of patient's diagnostics along with the healthcare professionals examining them, patient details, care provided, tests conducted, billing etc.	The data is critical for analyzing recent accident trends, and patient demographics. If these are unavailable, it could cause a major halt in the treatment of patients. The patients could get poor quality of care if allergies or medical history is not accounted for. The system is vulnerable to cybersecurity risks and malicious code injection.

A4	Medical Logistics System (MLS)	This is the primary system for handling orders, supply and processing of medicines, equipment, surgical supplies, and products for use by the healthcare professionals and medical support staff.	The vendor data and supplier information is critical for ensuring quality products are supplied and ordered through the system. If MLS is unavailable, the credibility and quality checks along with logistics information would be a major outage.
A5	Pharmacy System	The pharmacy system handles the medical supplies, their stock, replenishing orders and disposal for expired medicines. This also involves record of drugs and special requirements along with dosage and expiry of medicines. Supports automated drug dispensing to patients and the payment information.	Pharmacy system links payment details and medical drug history for every patient including payment information and hence is crucial to be protected.
A6	Email Server	Email servers enable email communication with various stakeholders.	It is critical in terms of cybersecurity as there is information regarding patient's personal details, treatment and financial data discussed over mails, also hospital administration information is discussed over mails.
A7	CCTV	These are the security cameras installed for vigilance and ensuring the physical safety of all other assets	CCTVs are the primary monitoring mechanism for the security team and the only way to ensure that all assets are continuously monitored. If these are unavailable, it could be a major security lapse.
A8	Computer	The computer(s) systems are the primary point of contact with HIS	Computer systems are used by all personnel to access and alter records within HIS as well as to track finances and for security purposes. If

			computer systems are unavailable, it would be a major outage as the HIS would only be accessible by smartphones - thereby restricting functionality.
A9	Router	The routers are an integral part of the AMC system framework. There are multiple routers connecting various business segments, all of them being centrally connected to a main router. The traffic coming from the internet (ISP) is run through a firewall before it gets moved across the internal network	All the internal traffic is at risk if the router gets compromised. Unauthorized access, Session hijacking, Eavesdropping, Password and Information theft are some of the issues that AMC can fall victim to if the routers are not appropriately secured.

Figure 1: Asset Identification Table

Measurement Scale for Asset Classification

Financial impact				
Very High [5]	**High [4]**	**Medium [3]**	**Low [1]**	**None [0]**
Can cause an impact of 350,000 dollars or more	Can cause impact of greater than 200,000 dollars and less than 500,000 dollars	Can cause impact of greater than 50,000 dollars and less than 200,000 dollars	Can cause impact of greater than 0 dollars and less than 50,000 dollars	No impact
Operational Impact				
Critical [5]	**Important [4]**	**Supporting[3]**	**Low [1]**	**No Impact[0]**
Complete loss of function resulting in operational failure	Partial loss of function resulting in more than 50 % and less than 100% of	Partial loss of function resulting in more than 20 % and less than 50% of	Minimal loss of function resulting in more than 0% and less than 20% of	No Impact

	operational failure	operational failure	operational failure	
Legal Protection Requirement				
Yes [5]			No [0]	

Figure 2: Measurement Scale

Asset Classification

Asset ID	**Asset name**	**Financial Impact**	**Operational Impact**			**Legal Impact**	**Total Score**
		Financial cost of asset compromise	**Availability**	**Integrity**	**Access Control Compromised**	**Compliance with Federal act of privacy, 1974**	
A1	Patient Data Information Server - PDIS	Very High [5]	Critical [5]	Critical [5]	Critical [5]	Yes [5]	25
A2	Financial Record Keeping Server - FRKS	High [4]	Important [4]	Critical [5]	Critical [5]	Yes[5]	23
A3	Emergency Care Data System (ECDS)	Very High [5]	Critical [5]	Important [4]	Important [4]	Yes [5]	23
A4	Medical Logistics System (MLS)	Very High [5]	Critical [5]	Critical [5]	Important [4]	Yes [5]	24
A5	Pharmacy	High [4]	Critical [5]	Critical	Support	Yes [5]	22

	System			[5]	ing [3]		
A6	Email Server	Medium [3]	Important [4]	Critical [5]	Critical [5]	Yes [5]	22
A7	CCTV	Medium [3]	Supporting [3]	Supporting [3]	Supporting [3]	No [0]	12
A8	Computer	Medium [3]	Important [4]	Supporting[3]	Critical [5]	Yes [5]	20
A9	Router	Very High [5]	Critical [5]	Critical [5]	Critical [5]	Yes [5]	25

Figure 3: Asset Classification Table

Vulnerability and Threat Identification

Asset	Asset Failure Impacts			Vulnerability due to			Exploit	Threats & Threat Agents	
	C	I	A	Tech	Admin	Physical		Insider	Outsider
A1 - Patient Data Information System (PDIS)	Yes	Yes	Yes	CVE-2000-0981 (MySQL Database Authentication System Vulnerability)	Weak authentication method allowing attacker to retrieve database credentials	NA	Leak information to a potential attacker due to weak authentication method, enabling attackers to gain unauthorized access to credentials	Physicians Employees Administration Staff Appointment Scheduler	Malicious attacker having knowledge of launching attacks on database vulnerability & database version
	Yes	Yes	Yes	CVE-2012-3132	SQL injection vulnerability	NA	Attackers modify a SQL Query or inject a SQL Command to gain access to hidden data or manipulate data	Employees Administration Staff	Attacker launching SQL Injection attacks on database
	Yes	Yes	Yes	Lack of Encryption	Unsecured data transfer and data storage or using laptop in public places with open wifi & leaving the laptop unattended	NA	Unauthorized Access	Physicians Employees Administration Staff Lab Technicians	Hackers
	No	No	Yes	CVE-2020-17047	Windows File System Vulnerability (OS: Windows 7, Windows 10)	NA	Denial of Service attack on Windows Network File System leading to unavailability	Administration Staff Lab Technicians Physicians	Attackers making computer systems inaccessible to intended users for sharing patient file & reports
	Yes	Yes	Yes	CVE-2021-43267	Unpatched System (Linux OS)	NA	Issue discovered in Linux Kernel allowing attackers insufficient data validation & information disclosure	Administration Staff	Knowledge of Linux OS vulnerabilites, with low access complexity
	Yes	Yes	Yes	CVE-2017-5123 (Linux 6)	Lack of Data Validation	NA	Insufficient data validation in waitid allows to escape sandboxes on Linux.		Very little to no skill required for exploiting this vulnerability due to lack of data validation mechanism
	No	Yes	Yes	CVE-2022-21263 (Solaris Servers)	Unsecured data manipulation, access & file updates	NA	Results in unauthorized update, insert or delete access to some of Oracle Solaris accessible data and partial Denial-of-Service Attacks	Physicians Employees Administration Staff Appointment Scheduler	Malicious attacker exploiting infrastructure logon on Solaris Servers gaining access to data read/write operations
	Yes	Yes	Yes	CVE-2022-21922 (Remote Procedure Call on Windows 7 & Windows 10)	Lack of network & software communication protocol understanding while requesting service from another program on a network	NA	Results in complete system exposure with access to all system files and patient data while requesting service from another computer in a network	ABC Systems Physicians Lab Technicians Administration Staff Providers	Malicious attacker exploiting access to remote machines through remote procedure call and gaining full access to the system, compromising all patient's data
	Yes	Yes	Yes	Lack of Access Control	Improper access control mechanism implemented for PDIS System	NA	Leaving private patient data susceptible to attack and cybersecurity breach	ABC Systems Administration Staff	Lack of access management allowing hackers who have gained authorized credentials to attack and breach sensitive patient data residing in PDIS System
	Yes	Yes	Yes	CVE-2017-0528	Bypassed firewall	NA	Lack of Kernel security subsystem enabling malicious application to execute code based on a privileged access	Employees ABC Systems Physicians Lab Technicians Administration Staff	Attacker bypassing kernel level defense security to exploit code execution in context of privileged access
	Yes	Yes	Yes	Backup & Recovery mechanism not in place	Absence of data protection and recovery mechnaism	Power Outage & other Natural calamity	Lack of backup-recovery to protect the database against data loss and reconstruct the database after data loss of critical patient data	ABC Systems Administrator Staff	Possibility of data breaches, ransomware attack leading to data loss or inability of clinics to access patient data for treating the patients
A8, A9 - IT Hardware (Computer & Router)	Yes	No	No	CVE-2022-23648 (Windows 7)	Unpatched System	NA	Unauthorized access to gain access to read-only copies of arbitrary files and directories on the host	NA	Malicious External Hackers
	Yes	Yes	Yes	CVE-2022-0847 (Linux 6)	Unpatched System	NA	This issue could allow an unprivileged local user to write to pages in the page cache that are backed by read-only files, allowing them to elevate their rights on the system.	NA	Malicious External Hackers
	Yes	Yes	Yes	CVE-2021-43940 (Windows 10)	Unpatched System	NA	Allows authenticated local attackers to achieve elevated privileges through Atlassian Confluence Server.	NA	Malicious External Hackers
	Yes	Yes	Yes	CVE-2019-1652 (Cisco Firmware)	Unpatched System	NA	Allows a remote attacker to inject and execute admin commands on a remote device without a password.	NA	Malicious External Hackers
	Yes	No	No	CVE-2019-1653 (Cisco Firmware)	Unpatched System	NA	Allows a remote attacker to get sensitive device configuration details without a password.	NA	Malicious External Hackers
	Yes	Yes	Yes	Lack of Encrypted communication	Not having encryption standards	NA	Unauthorized access through communication platforms like VoIP, Social media calls hosted on the parent computers.	Administration Staff Lab Technicians Physicians	Malicious External Hackers
	Yes	Yes	Yes	Elevation of privileges (Improper authorization)	Not having proper access controls	NA	Wrong people would get elevated access.	Administration Staff Lab Technicians Physicians	NA
	Yes	Yes	Yes	Malicious code introduction into the system through CD/DVD ROMs or plugs in flash drives	Using laptop in public areas and/or leaving them unattended	Compromised ports	Remote Malicious agent can get access to the system.	Administration Staff Lab Technicians Physicians	NA
	Yes	Yes	Yes	Access through remote access sharing softwares like Teamviewer, Chrome remote dekstop etc.	Using laptop in public areas and/or leaving them unattended	Compromised ports	Remote Malicious agent can get access to the system.	Administration Staff Lab Technicians Physicians	Malicious External Hackers
	Yes	Yes	Yes	CVE-2022-25249	Unpatched System	NA	Remote malicious agent can get fully authenticated and gain access to base operating system and complete file system		Malicious agent with knowledge of launching attacks on remote systems.
	Yes	Yes	Yes	CVE-2022-25250	Unpatched System	Remotely Accessible Port	Remote malicious agent can send commands to an open port and shut down various services.		Knowledge of detecting open ports and piggybacking malicious commands over the network.
	Yes	Yes	Yes	CVE-2022-25246	Unpatched System	NA	Allows agents to decrypt credentials easily		Knowledge of remote vulnerability analysis and penetration.
	Yes	Yes	Yes	CVE-2022-25248	Unpatched System	NA	When connected to a certain port, software provides complete event log of specific service	NA	NA
	Yes	Yes	Yes	CVE-2022-25247	Unpatched System	NA	Could allow threat agent to gain access and run malicious code remotely	NA	NA

Asset	Asset Failure Impacts			Vulnerability due to			Exploit	Threats & Threat Agents	
	C	I	A	Tech	Admin	Physical		Insider	Outsider
A4 - Medical Logistics System	Yes	Yes	Yes	CVE-2022-25251	Unsecure Port	NA	Could allow threat agent to read and modify system configuration	NA	Knowledge of detecting open ports and piggybacking malicious commands over the network.
	Yes	Yes	Yes	CVE-2022-25252	Publicly Accessible Port	NA	Could allow threat agenet to crash system remotely	NA	Extensive knowledge of detecting open ports, and system penetration
	Yes	Yes	No	NA	Vendors have complete system access	NA	As vendors can recreate the MLS and orders inside, it is admin level access. Hackers can use vendors systems to penetrate MLS.	NA	Compromised system on vendor platforms, Hackers
	No	Yes	Yes	NA	Application hosting on publicly accessed server	NA	Application is hosted on a server that is accessible by vendors. This can lead to system wide penetration if this component is compromised.	NA	Hackers
A3 - Emergency Care Data System (ECDS)	Yes	Yes	Yes	NA	Ignorance to data backup on ECDS or Database on ECDS not backed up regularly.	N/A	Patient emergency data during an attack can be removed or encrypted on the system by the threat agent in demand of ransom. Having a backup of data can prevent loss losing out on important patient information on emergency care.	NA	Ransomware threat agent
	Yes	Yes	Yes	NA	Improper access control in place that could lead to unauthorized access to threat agents	N/A	Patient data can be modified by unauthorized individuals. Increased probability of gaining access to the data due to lack of access control	ABC Systems Staff, Medical Staff, Lab Technicians, Administration Staff	N/A
	Yes	No	NO	CVE-2020-11582	NA	NA	Applet in a jar file which gets executed on Solaris server. One of the jar files on the Solaris clients accepts local connections on a random port. This can be reached by threat agents via local HTTP clients.	N/A	Hackers
	Yes	Yes	Yes	CVE-2020-8635	NA	NA	ECDS runs on Solaris servers. Solaris sets insecure permissions on installation directories and configuration files as part of the vulnerability. This can be exploited by attackers as full privileges can be provided to users who do not require it.	ABC Systems Staff, Medical Staff, Lab Technicians, Administration Staff	Hackers
	Yes	Yes	Yes	CVE-2020-8634	NA	NA	Insecure permissions are set on Solaris servers which could lead to files set to full read and full write privileges to all users. This can be exploited by hackers to gain access and modify details. Can also encrypt and demand ransom	ABC Systems Staff, Medical Staff, Lab Technicians, Administration Staff	Hackers
	No	No	Yes	CVE-2018-3269	NA	NA	Successful attacks of this vulnerability can result in unauthorized access to create a partial denial of service (partial DOS) of Solaris.	NA	Hackers
	No	Yes	Yes	CVE-2022-21263	NA	NA	Can lead to unauthorized access to data on Oracle Solaris data and also could lead to partial DoS Attacks.	Administration Staff	Malicious attacker
A2 - Financial Record Keeping Server (FRKS)	Yes	Yes	Yes	CVE-2007-2118	NA	NA	Unauthorized access to data might result in data theft.	Staff of AMC	Hackers
	Yes	Yes	Yes	CVE-2007-6260	NA	NA	The use of default passwords throughout the installation process allows remote attackers to log in via the listener.	Database Administrators at AMC	Hackers
	Yes	Yes	Yes	NA	On the server, all employees have equal access.	NA	Staff may update or share confidential information.	IT Admins	Hackers
	Yes	Yes	Yes	NA	NA	There is no physical security in the room.	Anyone might walk in and look at the private information.	Internal Staff	Unautorized Visitors, Patients

Risk Mitigation Strategy:

1) Implement system segmentation: The current system architecture opens doors to a lot of potential security threats owing to the lack of segmentation. All the major components of the system should be isolated from each other so threat agents cannot penetrate all the other systems via one compromised component. [MLS]
2) The procurement application should be on an internal server that is not accessed by people outside AMC. The current application is hosted on the server which pre-certified vendors use to access the system and place/check orders. If a vendor system is compromised, it can lead to a security breach via the MLS server.
3) Prepare parameterized queries and make use of prepared statements to avoid SQL Injection Vulnerability on the PDIS Database Servers. Create database users with restricted privileges and thoroughly test the code for SQL Vulnerabilities.
4) Schedule weekly regular backups and configure data recovery mechanisms for PDIS Database Servers to achieve high availability of data in cases of flood, natural calamity, or power outages. Ensuring data duplicated on other servers will prevent important data from being lost
5) Setup access control restrictions to prevent unauthorized access. Hire talent to maintain the data and focus on employee training to prevent human errors or erroneous data from being entered into the PDIS System.
6) Implement inbound/outbound firewall rules to mitigate the risk of intrusion into the critical & sensitive PDIS Servers. Configure firewall rules to ensure data packets transferred in & out of the system have legitimate access. Block unnecessary ports opened to the public network and set up a virtual private network (VPN) to ensure the integrity and confidentiality of the data.
7) Regular data backups are scheduled to avoid loss of data. This way the data can be recovered and the ransomware attack can be nullified.(ECDS)
8) Placing access control rules can help create a more secure data access policy. Every user should be granted access permissions through appropriate access roles. (ECDS)
9) Because financial data requires approval, each access should be accompanied by a pull request. (FRKS)
10) Oracle recommends using the 12C Password format, which uses cryptography and hashing. Unauthorized access would be prevented as a result of this.(FRKS)
11) Only system administrators should have access to the data instead of the entire IT team. Any other IT personnel who require access should do so only after administrator approval. Users should be given the appropriate role-based permissions.(FRKS)
12) It is necessary to secure the room containing computers and other gadgets. To keep track of what's going on, a camera can be set up. Biometric authentication

or magnetic chip-based cards should also be used to restrict access to the room.(FRKS)

13) ISP-supplied routers should be avoided. These routers are usually less secure than the ones sold to consumers by manufacturers. They frequently have hard-coded remote support passwords that consumers are unable to modify, and fixes for their modified firmware versions lag behind patches for router manufacturers' faults.

14) Choose a good security protocol and a complex Wi-Fi password. Because older WPA and WEP are vulnerable to brute-force attacks, WPA2 (Wi-Fi Protected Access II) should be the preferred alternative. Create a guest wireless network, also protected with WPA2 and a strong password, if the router allows it. Allow visitors or friends to connect to this separate guest network rather than your regular one. Their devices may be infiltrated or infected with malware, even if they have no malevolent intent.

15) The software installed on the system by your firm is subject to cyber attacks and zero-day exploits. Updates and software patches must be installed as quickly as possible, or otherwise hackers will manufacture new N-days that will cause significant damage.

16) Password authentication services, for example, offer tiered administrator access or one-time passwords/tokens with procedural standards structured around secure resetting credentials.

17) Procedures for safely resetting passwords or other forms of credentials if they are hacked should also be in place, so that high-value assets aren't mistakenly exposed to threat adversaries who target privileged users on a regular basis.

18) Password authentication services, for example, offer tiered administrator access or one-time passwords/tokens with procedural standards structured around secure resetting credentials.

Appendices - Measurement Scales

Appendix A: Threat Vulnerability Identification

- **Asset 1: Patient Data Information System (PDIS)**

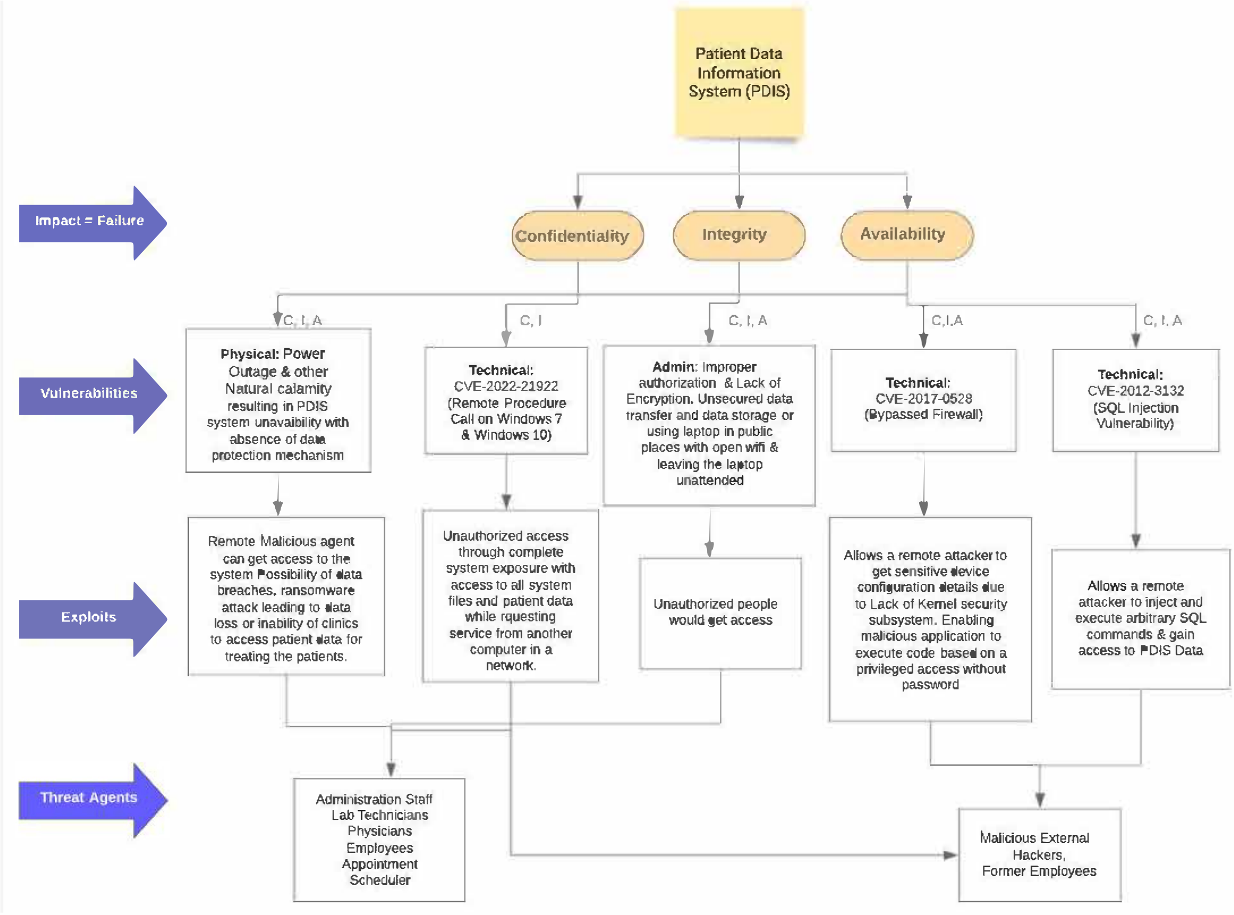

Patient Data Information System (PDIS)
Impact = Failure
Confidentiality
Integrity
Availability
Vulnerabilities
C, I, A
C, I
C, I, A
C,I,A
C, I, A
Physical: Power Outage & other Natural calamity resulting in PDIS system unavaibility with absence of data protection mechanism
Technical: CVE-2022-21922 (Remote Procedure Call on Windows 7 & Windows 10)
Admin: Improper authorization & Lack of Encryption. Unsecured data transfer and data storage or using laptop in public places with open wifi & leaving the laptop unattended
Technical: CVE-2017-0528 (Bypassed Firewall)
Technical: CVE-2012-3132 (SQL Injection Vulnerability)
Exploits
Remote Malicious agent can get access to the system Possibility of data breaches, ransomware attack leading to data loss or inability of clinics to access patient data for treating the patients.
Unauthorized access through complete system exposure with access to all system files and patient data while rquesting service from another computer in a network.
Unauthorized people would get access
Allows a remote attacker to get sensitive device configuration details due to Lack of Kernel security subsystem. Enabling malicious application to execute code based on a privileged access without password
Allows a remote attacker to inject and execute arbitrary SQL commands & gain access to PDIS Data
Threat Agents
Administration Staff
Lab Technicians
Physicians
Employees
Appointment Scheduler
Malicious External Hackers,
Former Employees

Figure 4: PDIS Asset Vulnerability-Threat Identification Tree

Technical Vulnerability

- CVE-2022-21922 (Remote Procedure Call on Windows 7 & Windows 10)

  Description: Lack of network & software communication protocol understanding while requesting service from another program on a network. This results in complete system exposure with access to all system files and patient data while requesting service from another computer in a network. A malicious attacker exploits access to remote machines through remote procedure calls and gains full access to the system, compromising all patient's data

Exploitability Score: 1.02
Impact Score: 4.9
Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

- CVE-2017-0528 (Bypassed Firewall)

  Description: Lack of Kernel security subsystem enabling the malicious application to execute code based on privileged access. Attacker bypassing kernel-level defense security to exploit code execution in context of privileged access
  Exploitability Score: 1.29
  Impact Score: 3.6
  Vector: AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

- CVE-2012-3132 (SQL Injection Vulnerability)

  Description: Attackers modify a SQL Query or inject a SQL Command to gain access to hidden data or manipulate data in the PDIS Database Server
  Exploitability Score: 1.1
  Impact Score: 2.2
  Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:H

<u>Non-Technical Vulnerability</u>

- Lack of Encryption: Unsecured data transfer and data storage or using a laptop in public places with open wifi & leaving the laptop unattended. Hackers can gain unauthorized access to the local systems of the employees
  Evidence: Areas of Concern for Important Assets (Table 2) in AMC Case Study (Page 6)
  Exploitability Score: 1.1
  Impact Score: 2.2
  Vector: AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

- Power Outages & other Natural calamities: The absence of data backup-recovery and data protection mechanism results in the PDIS system being unavailable leading to a denial of access. Data loss occurs and requires reconstruction of the database of critical patient data records
  Evidence: Areas of Concern for Important Assets (Table 2) in AMC Case Study (Page 6)
  Exploitability Score: 1.25
  Impact Score: 3.36

Vector: AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

- **Asset 2: IT Hardware (Computer & Router)**

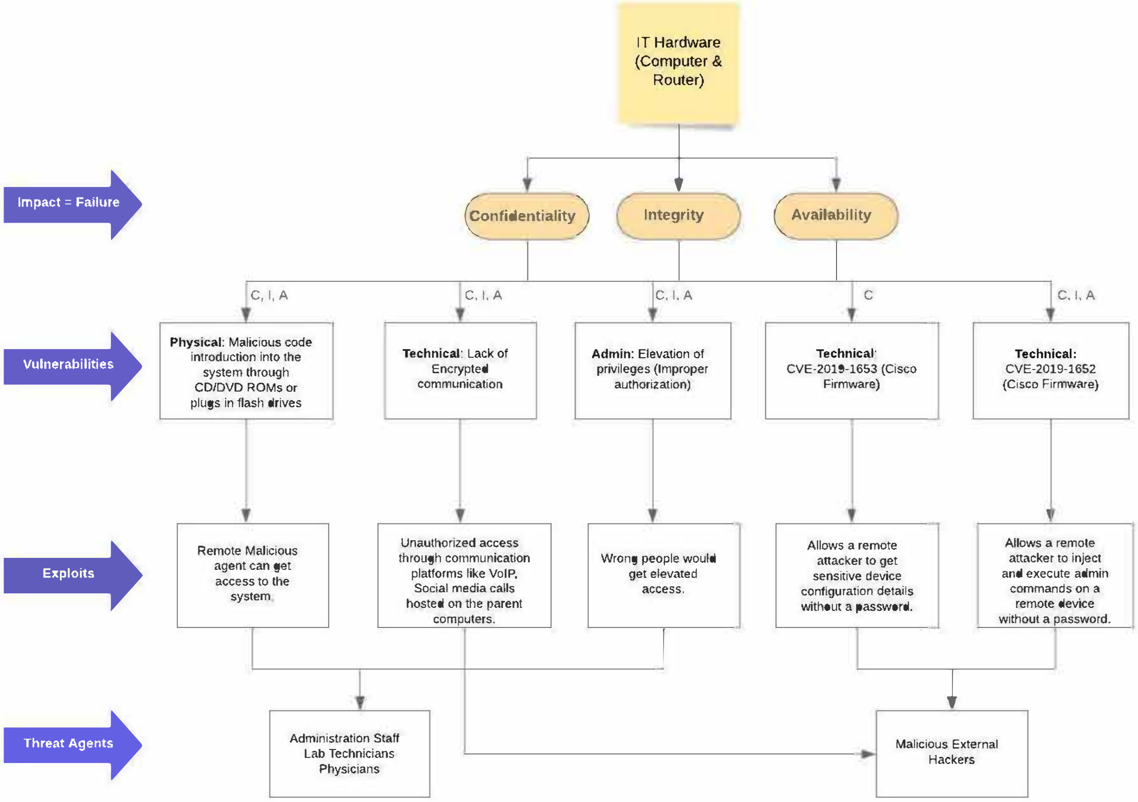

IT Hardware (Computer & Router)
Impact = Failure
Confidentiality
Integrity
Availability
C, I, A
C, I, A
C, I, A
C
C, I, A
Vulnerabilities
Physical: Malicious code introduction into the system through CD/DVD ROMs or plugs in flash drives
Technical: Lack of Encrypted communication
Admin: Elevation of privileges (Improper authorization)
Technical: CVE-2019-1653 (Cisco Firmware)
Technical: CVE-2019-1652 (Cisco Firmware)
Exploits
Remote Malicious agent can get access to the system.
Unauthorized access through communication platforms like VoIP, Social media calls hosted on the parent computers.
Wrong people would get elevated access.
Allows a remote attacker to get sensitive device configuration details without a password.
Allows a remote attacker to inject and execute admin commands on a remote device without a password.
Threat Agents
Administration Staff
Lab Technicians
Physicians
Malicious External Hackers

Figure 5: IT Hardware Asset Vulnerability-Threat Identification Tree

Technical Vulnerability:

- CVE-2019-1652 (Cisco Firmware)
  Description: Allows a remote attacker to inject and execute admin commands on a remote device without a password. An attacker could take advantage of this flaw by sending malicious HTTP POST requests to a device's web-based management interface. If the exploit is effective, the attacker will be able to run arbitrary commands as root on the underlying Linux shell.
  Exploitability Score: 0.47
  Impact Score: 3.6
  Vector: AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

- CVE-2022-23648 (Windows 7 & Linux)
  Description: Unauthorized access to gain access to read-only copies of arbitrary files and directories on the host. Containerd is a daemon-based container runtime for Linux and Windows. Containers launched with containerd's CRI

implementation on Linux with a particularly image configuration could get access to read-only copies of specific files and directories on the host due to a flaw in version 1.6.1, 1.5.10, and 1.14.12.
Exploitability Score: 2.8
Impact Score: 3.66
Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Non-Technical Vulnerability

- Lack of Encrypted communication
  Description: Unauthorized access through communication platforms like VoIP, Social media calls hosted on the parent computers. If the data is not encrypted and simply HTTPS is used, the data is readable before being sent further inside the private network, which is protected by a firewall. The data can be intercepted, changed, or manipulated by firewall operators.
  Exploitability Score: 1.52
  Impact Score: 2.07
  Vector: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:H

- Malicious code introduction into the system through CD/DVD ROMs or plugs in flash drives
  Description: Remote Malicious agents can get access to the system.
  Exploitability Score: 0.55
  Impact Score: 2.74
  Vector: AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:H

- Elevation of privileges (Improper authorization)
  Description: Wrong people would get elevated access.
  Exploitability Score: 1.09
  Impact Score: 3
  Vector: AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H

- **Asset 3: Emergency Care Data System (ECDS)**

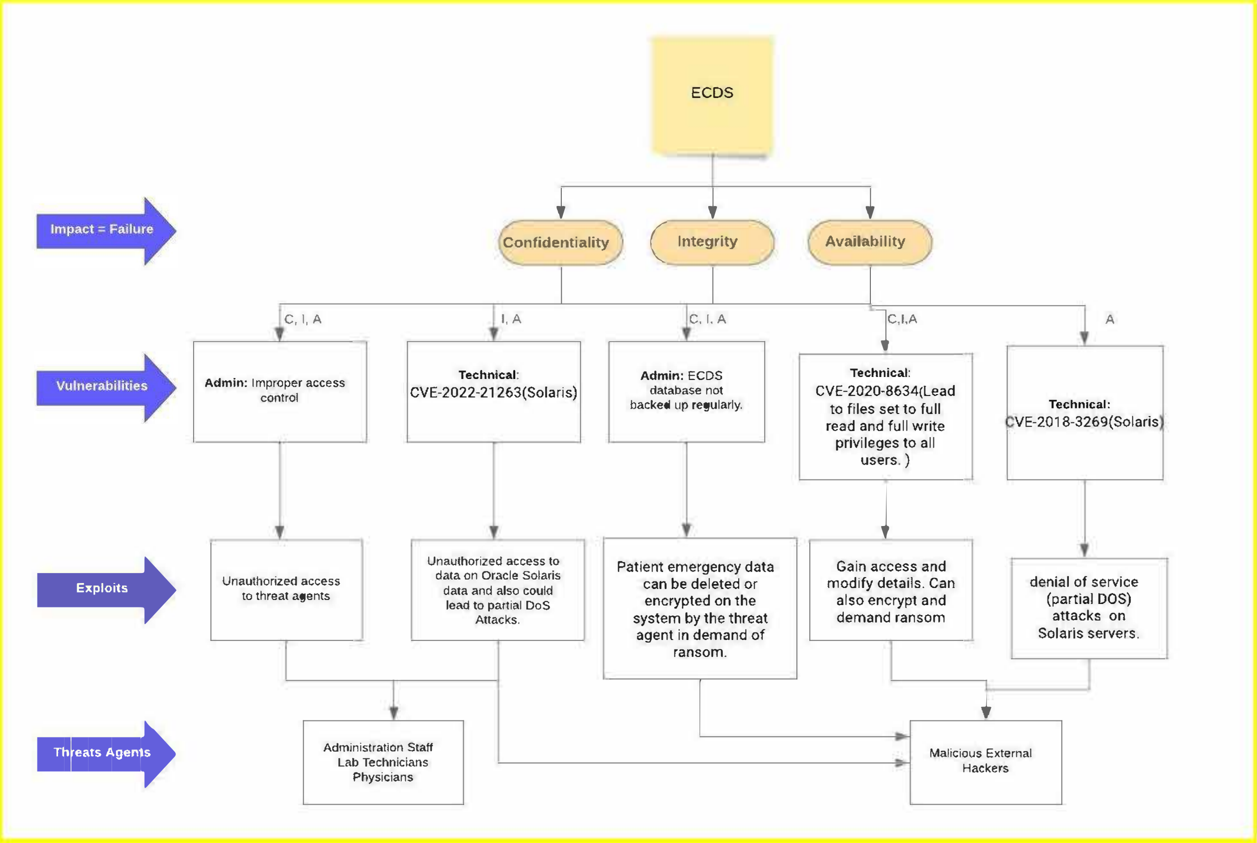

ECDS
Impact = Failure
Confidentiality
Integrity
Availability
C, I, A
I, A
C, I, A
C,I,A
A
Vulnerabilities
Admin: Improper access control
Technical: CVE-2022-21263(Solaris)
Admin: ECDS database not backed up regularly.
Technical: CVE-2020-8634(Lead to files set to full read and full write privileges to all users.)
Technical: CVE-2018-3269(Solaris)
Exploits
Unauthorized access to threat agents
Unauthorized access to data on Oracle Solaris data and also could lead to partial DoS Attacks.
Patient emergency data can be deleted or encrypted on the system by the threat agent in demand of ransom.
Gain access and modify details. Can also encrypt and demand ransom
denial of service (partial DOS) attacks on Solaris servers.
Threats Agents
Administration Staff
Lab Technicians
Physicians
Malicious External Hackers

Figure 6: ECDS Asset Vulnerability-Threat Identification Tree

Technical Vulnerability:

- CVE-2018-3269
  Description: Successful attack on this vulnerability can result in unauthorized access and also could lead to partial denial of service (partial DOS) of Solaris servers.
  Exploitability Score: 1.4
  Impact Score: 0.85
  Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L

- CVE-2020-8634
  Description: Insecure permissions are set on Solaris servers which could lead to files with full read and full write privileges to all users. This can be exploited by hackers to gain access and modify details. Threat agents can also encrypt and demand ransom.
  Exploitability Score: 0.9
  Impact Score: 3.6
  Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

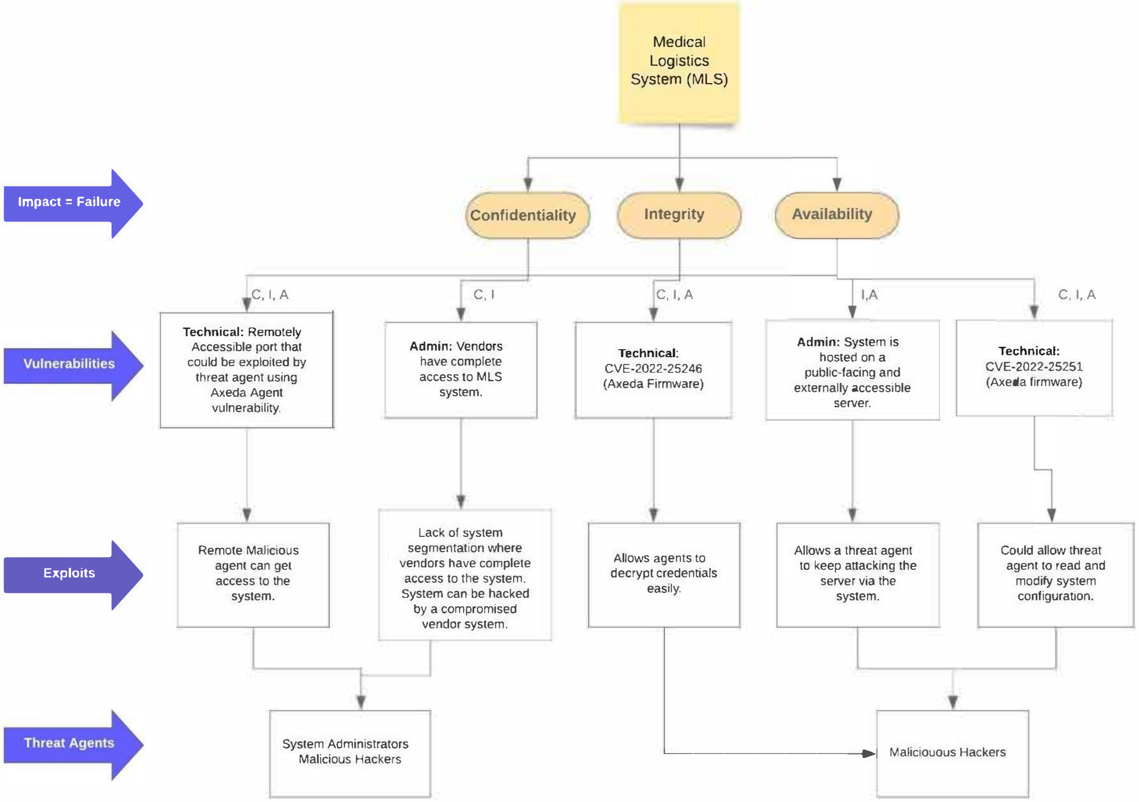
- CVE-2022-21263
  Description: Can lead to unauthorized access to data on Oracle Solaris data and also could lead to partial DoS Attacks.
  Exploitability Score: 0.57
  Impact Score: 2.07
  Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L

Non-Technical Vulnerability:

- Database on ECDS not backed up regularly.
  Description: Ignorance to data backup on ECDS could lead to exploitation by threat agents. Patient emergency data during an attack can be removed or encrypted on the system by the threat agent in demand of ransom. Having a backup of data can prevent losing out on important patient information on emergency care.
  Exploitability Score: 1.65
  Impact Score: 3.36
  Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H

- Improper access controls
  Description: Lack of proper access controls lead to unauthorized access. This can be leveraged by the threat agents. Patient data can be modified by unauthorized individuals. Increased probability of gaining access to the data due to lack of access control
  Exploitability Score: 1.521
  Impact Score: 3.66
  Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

- **Asset 4: Medical Logistics System (MLS)**



Medical Logistics System (MLS)
Impact = Failure
Confidentiality
Integrity
Availability
C, I, A
C, I
C, I, A
I,A
C, I, A
Vulnerabilities
Technical: Remotely Accessible port that could be exploited by threat agent using Axeda Agent vulnerability.
Admin: Vendors have complete access to MLS system.
Technical: CVE-2022-25246 (Axeda Firmware)
Admin: System is hosted on a public-facing and externally accessible server.
Technical: CVE-2022-25251 (Axeda firmware)
Exploits
Remote Malicious agent can get access to the system.
Lack of system segmentation where vendors have complete access to the system. System can be hacked by a compromised vendor system.
Allows agents to decrypt credentials easily.
Allows a threat agent to keep attacking the server via the system.
Could allow threat agent to read and modify system configuration.
Threat Agents
System Administrators
Malicious Hackers
Maliciouous Hackers

Figure 7: MLS Asset Vulnerability-Threat Identification Tree

Technical Vulnerability:

- CVE-2022-25246 (Axeda Firmware)
  Description: Allows a remote attacker to gain administrative and system-wide control of the targeted system
  Exploitability Score: 1.52
  Impact Score: 1.95
  Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

- CVE-2022-25251 (Axeda Firmware)
  Description: Allows remote attackers to send code to certain ports. If successful, the attacker could read and modify system configurations.
  Exploitability Score: 1.52
  Impact Score: 1.95
  Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Non-Technical Vulnerability:

- System hosted on external-facing and remotely accessible server.
  Description: Could allow remote hackers to keep attacking the system and exploit the underlying server - if successful.
  Exploitability Score: 1.09
  Impact Score: 1.35
  Vector: AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:H

- Vendors have admin level access to MLS system.
  Description: Allowing vendors to have the level of access as that of an Administrator could endanger the system. A compromised vendor computer could lead threat agents straight into MLS system.
  Exploitability Score: 1.2
  Impact Score: 3.0
  Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

- **Asset 5: Financial Record Keeping Server (FRKS)**

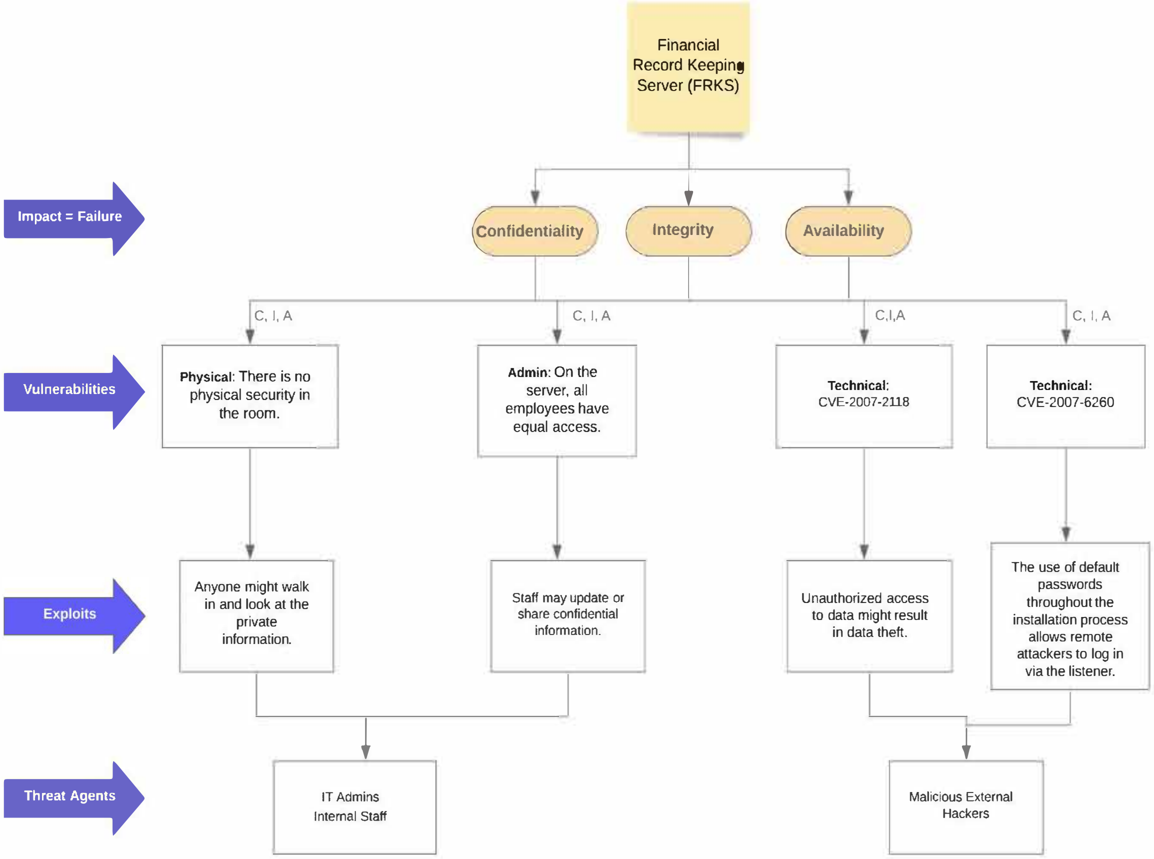

Financial Record Keeping Server (FRKS)
Impact = Failure
Confidentiality
Integrity
Availability
C, I, A
C, I, A
C,I,A
C, I, A
Vulnerabilities
Physical: There is no physical security in the room.
Admin: On the server, all employees have equal access.
Technical: CVE-2007-2118
Technical: CVE-2007-6260
Exploits
Anyone might walk in and look at the private information.
Staff may update or share confidential information.
Unauthorized access to data might result in data theft.
The use of default passwords throughout the installation process allows remote attackers to log in via the listener.
Threat Agents
IT Admins Internal Staff
Malicious External Hackers

Figure 8: FRKS Asset Vulnerability-Threat Identification Tree

Technical Vulnerability:

- CVE-2007-2118
  Description: Unspecified vulnerability in the Upgrade/Downgrade component of Oracle Database has unknown impact and attack vectors, aka DB13. NOTE: as of 20070424, Oracle has not disputed reliable claims that this is a buffer overflow involving the "mig utility."
  Exploitability Score: 1.09
  Impact Score: 3.66
  Vector: AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

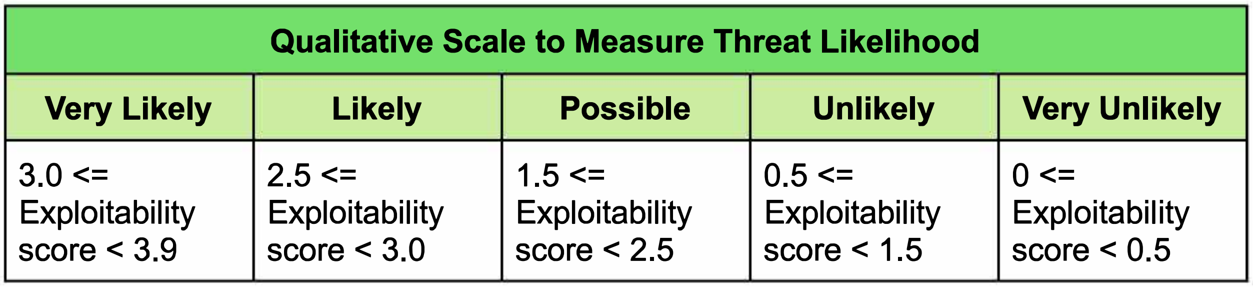
- CVE-2007-6260
  Description: The installation process for Oracle 10g and 11g uses accounts with default passwords, which allows remote attackers to obtain login access by connecting to the Listener.
  Exploitability Score: 1.09
  Impact Score: 3.23
  Vector: AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:L

Non-Technical Vulnerability:

- On the server, all employees have equal access.
  Description: Staff may update or share confidential information.
  Exploitability Score: 1.7
  Impact Score: 3.59
  Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

- There is no physical security in the room.
  Description: Unauthorized Visitors can gain access to data.
  Exploitability Score: 0.42
  Impact Score: 3.59
  Vector: AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

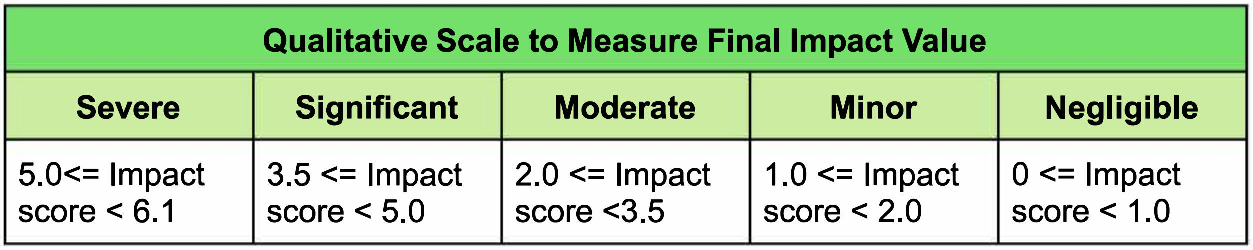
Appendix B - Measurement Scale for Scoring Threat Likelihood



Qualitative Scale to Measure Threat Likelihood				
Very Likely	**Likely**	**Possible**	**Unlikely**	**Very Unlikely**
3.0 <= Exploitability score < 3.9	2.5 <= Exploitability score < 3.0	1.5 <= Exploitability score < 2.5	0.5 <= Exploitability score < 1.5	0 <= Exploitability score < 0.5

Figure: Threat Likelihood Scale

Appendix C - Estimation of Risk Impact



Qualitative Scale to Measure Final Impact Value				
Severe	**Significant**	**Moderate**	**Minor**	**Negligible**
5.0<= Impact score < 6.1	3.5 <= Impact score < 5.0	2.0 <= Impact score <3.5	1.0 <= Impact score < 2.0	0 <= Impact score < 1.0

Figure: Final Impact Value Scale

CVSS version 3.1 is used for exploitability scores on a scale of 0 to 3.9 and impact scores on a scale of 0 to 6.1 Scores are calculated from the following website: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Asset	Asset Failure Impacts			Vulnerability due to			Impact (Scale of 6.1)	Impact Interpretation	Exploitability (Scale of 3.9)	Likelihood Interpretation	Risk Score	CVSS v3.1 Vector
	C	I	A	Tech	Admin	Physical						
A1 - Patient Data Information System (PDIS)	Yes	Yes	Yes	CVE-2000-0981 (MySQL Database Authentication System Vulnerability)	Weak authentication method allowing attacker to retrieve database credentials	NA	3.60	Moderate	0.62	Possible		AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H
	Yes	Yes	Yes	CVE-2012-3132	SQL injection vulnerability	NA	2.87	Moderate	1.09	Unlikely	Low Medium	AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:H
	Yes	Yes	Yes	Lack of Encryption	Unsecured data transfer and data storage or using laptop in public places with open wifi & leaving the laptop unattended	NA	3.66	Moderate	1.09	Likely	Med	AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H
	No	No	Yes	CVE-2020-17047	Windows File System Vulnerability (OS: Windows 7, Windows 10)	NA	2.44	Moderate	0.66	Possible	Low Medium	AV:N/AC:L/PR:H/UI:R/S:C/C:N/I:N/A:H
	Yes	Yes	Yes	CVE-2021-43267	Unpatched System (Linux OS)	NA	3.66	Minor	1.09	Likely	Medium High	AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H
	Yes	Yes	Yes	CVE-2017-5123 (Linux 6)	Lack of Data Validation	NA	2.26	Moderate	0.82	Possible	Low Medium	AV:A/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L
	No	Yes	Yes	CVE-2022-21263 (Solaris Servers)	Unsecured data manipulation, access & file updates	NA	2.07	Moderate	0.51	Possible	Low Medium	AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L
	Yes	Yes	Yes	CVE-2022-21922 (Remote Procedure Call on Windows 7 & Windows 10)	Lack of network & software communication protocol understanding while requesting service from another program on a network	NA	3.60	Moderate	1.09	Likely	High	AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
	Yes	Yes	Yes	Lack of Access Control	Improper access control mechanism implemented for PDIS System	NA	4.03	Minor	0.9	Very Likely	High	AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H
	Yes	Yes	Yes	CVE-2017-0528	Bypassed firewall	NA	3.66	Significant	1.21	Very Likely	High	AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
	Yes	Yes	Yes	Backup & Recovery mechanism not in place	Absence of data protection and recovery mechnaism	Power Outage & other Natural calamity	3.90	Moderate	0.98	Very Likely	High	AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
A8, A9 - IT Hardware (Computer & Router)	Yes	No	No	CVE-2022-23648 (Windows 7)	Unpatched System	NA	2.20	Significant	1.09	Unlikely	Medium	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
	Yes	Yes	Yes	CVE-2022-0847 (Linux 6)	Unpatched System	NA	3.60	Moderate	0.82	Possible	Medium	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
	Yes	Yes	Yes	CVE-2021-43940 (Windows 10)	Unpatched System	NA	3.60	Significant	0.7	Unlikely	Medium	AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
	Yes	Yes	Yes	CVE-2019-1652 (Cisco Firmware)	Unpatched System	NA	3.60	Significant	0.47	Unlikely	Medium	AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
	Yes	No	No	CVE-2019-1653 (Cisco Firmware)	Unpatched System	NA	2.20	Negligible	1.52	Possible	High	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
	Yes	Yes	Yes	Lack of Encrypted communication	Not having encryption standards	NA	3.66	Moderate	1.52	Possible	High	AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:H
	Yes	Yes	Yes	Elevation of privileges (Improper authorization)	Not having proper access controls	NA	3.66	Moderate	1.09	Possible	Medium High	AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H
	Yes	Yes	Yes	Malicious code introduction into the system through CD/DVD ROMs or plugs in flash drives	Using laptop in public areas and/or leaving them unattended	Compromised ports	3.34	Moderate	0.55	Unlikely	Medium High	AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:H
	Yes	Yes	Yes	Access through remote access sharing softwares like Teamviewer, Chrome remote dekstop etc.	Using laptop in public areas and/or leaving them unattended	Compromised ports	2.87	Moderate	0.47	Unlikely	Medium High	AV:A/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:H
A4 - Medical Logistics System	Yes	Yes	Yes	CVE-2022-25249	Unpatched System	NA	2.20	Moderate	1.52	Possible	Medium	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
	Yes	Yes	Yes	CVE-2022-25250	Unpatched System	Remotely Accessible Port	2.20	Moderate	1.52	Possible	Medium	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
	Yes	Yes	Yes	CVE-2022-25246	Unpatched System	NA	2.38	Moderate	1.52	Possible	Medium	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
	Yes	Yes	Yes	CVE-2022-25248	Unpatched System	NA	1.71	Minor	1.52	Possible	Low Med	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
	Yes	Yes	Yes	CVE-2022-25247	Unpatched System	NA	2.38	Moderate	1.52	Possible	Medium	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
	Yes	Yes	Yes	CVE-2022-25251	Unsecure Port	NA	2.38	Moderate	1.52	Possible	Medium	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
	Yes	Yes	Yes	CVE-2022-25252	Publicly Accessible Port	NA	2.20	Moderate	1.52	Possible	Medium	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
	Yes	Yes	No	NA	Vendors have complete system access	NA	1.65	Minor	1.09	Unlikely	Low Med	AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L
	No	Yes	Yes	NA	Application hosting on publicly accessed server	NA	3.66	Significant	1.2	Unlikely	Medium	AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:H
A3 - Emergency Care Data System (ECDS)	Yes	Yes	Yes	NA	Ignorance to data backup on ECDS or Database on ECDS not backed up regularly.	N/A	3.36	Moderate	1.092	Unlikely	Low Med	AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H
	Yes	Yes	Yes	NA	Improper access control in place that could lead to unauthorized access to threat agents	N/A	3.66	Moderate	1.521	Possible	Medium	AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
	Yes	No	NO	CVE-2020-11582	NA	NA	3.22	Moderate	1.321	Unlikely	Low Med	AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
	Yes	Yes	Yes	CVE-2020-8635	NA	NA	3.60	Moderate	0.9	Unlikely	Low Med	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
	Yes	Yes	Yes	CVE-2020-8634	NA	NA	3.60	Moderate	0.9	Unlikely	Low Med	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
	No	No	Yes	CVE-2018-3269	NA	NA	0.85	Negligible	1.4	Possible	Low	AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L
	No	Yes	Yes	CVE-2022-21263	NA	NA	2.07	Minor	0.57	Possible	Low Med	AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L
A2 - Financial Record Keeping Server (FRKS)	Yes	Yes	Yes	CVE-2007-2118	NA	NA	3.66	Moderate	1.09	Very Likely	Medium High	AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H
	Yes	Yes	Yes	CVE-2007-6260	NA	NA	3.23	Moderate	1.09	Very Likely	Medium	AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:L
	Yes	Yes	Yes	On the server, all employees have equal access.	NA	NA	3.59	Moderate	1.7	Very Likely	Low Medium	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
	Yes	Yes	Yes	There is no physical security in the room.	NA	NA	3.59	Moderate	0.42	Unlikely	Low Medium	AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Appendix D - Cybersecurity Risk Matrix & Risk Management Strategy

Final Impact Value (FIV)

	Impact					
		Negligible	**Minor**	**Moderate**	**Significant**	**Severe**
Threat Likelihood	**Very Likely**	Low Med	Medium	Medium Hi	High	High
	Likely	Low	Low Med	Medium	Medium Hi	High
	Possible	Low	Low Med	Medium	Medium Hi	Medium Hi
	Unlikely	Low	Low Med	Low Med	Medium	Medium Hi
	Very Unlikely	Low	Low	Low Med	Medium	Medium

Figure: Cybersecurity Risk Matrix

Risk	Risk Mitigation Strategy	Description
Low	Ignore	Accept the risk & do nothing
Low Med	Avoid	Try to avoid risk by replacing the asset
Medium	Transfer	Transferring the risk to an Insurance Company
Medium Hi	Mitigate	Implement control measures
High	Mitigate	Implement tools and technology to control & prevent the risk

Figure: Risk Management Strategy for Risk Values

Appendix E: Assumptions

Following are the assumptions made for the Aggieland Medical Center (AMC) Case:

1. Aggieland Medical Center stores all important patient information in the Patient Data Information System on MySQL Database Server
2. Aggieland Medical Center uses remote procedure calls to access and share data from another program or computer in the network
3. All financial information, including insurance, billing records, payment schedules, and other associated data, is stored in Oracle 10g at Aggie Medical Center.
4. MLS System allows connections for vendors and other entities using Axeda Agent and Axeda Desktop Server.

References:

1. Worldwide systems affected as part of the attack (MLS): https://www.cybermdx.com/access7-affected-devices/
2. https://healthitsecurity.com/news/7-new-vulnerabilities-threaten-supply-chain-medical-device-security
3. https://www.forescout.com/blog/access-7-vulnerabilities-impact-supply-chain-component-in-medical-and-iot-device-models/
4. https://www.techdee.com/protect-your-data-from-power-outage/ (3 Ways to protect your data from Power Outage)
5. https://www.nist.gov (The National Institute of Standards and Technology (NIST))
6. https://www.cvedetails.com (The ultimate security vulnerability data source)
7. https://mailtrap.io/blog/smtp-security/ (Everything you need to know about SMTP Security)
8. https://www.cdc.gov/phlp/publications/topic/hipaa.html (HIPAA Privacy Rule)
9. https://www.first.org/cvss/ (Common Vulnerability Scoring System SIG)

Glossary:

1.SMTP : An SMTP server is a program that sends, receives, and/or relays email between senders and receivers. The address (or addresses) of an SMTP server can be set by the mail client or application you're using, and it's usually formatted as smtp.server address.com. [7]

2.HIPPA : The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that mandated the development of national standards to secure sensitive patient health information from disclosure without the patient's agreement or knowledge. The HIPAA Privacy Rule was developed by the US Department of Health and Human Services (HHS) to implement the HIPAA obligations. The HIPAA Security Rule safeguards a portion of the information that is protected under the Privacy Rule. [8]

3.CVE : A list of publicly revealed computer security weaknesses is known as Common Vulnerabilities and Exposures (CVE). When someone mentions a CVE, they're referring to a security problem with a CVE ID number. [6]

4. CVSS : The Common Vulnerability Scoring System (CVSS) is a method for capturing a vulnerability's key characteristics and generating a numerical score that reflects its severity. The numerical score can then be converted into a qualitative representation (low, medium, high, or critical) to assist companies in correctly assessing and prioritizing their vulnerability management activities. [9]

Team Work Allocation:

Task	Team Member/s
Executive Summary	Bansari
Asset Identification	Ameya & Shaheen
Asset Classification	Yash
Vulnerability and Threat Identification	Bansari & Siddharth
Cybersecurity Risk Estimation	Yash & Siddharth
Cybersecurity Risk Likelihood Measurement Scale	Shaheen & Bansari
Cybersecurity Risk Impact Value Measurement Scale	Yash & Ameya
Cybersecurity Risk Management Strategy	Ameya & Sidharth
Appendices - Measurement Scales	Yash
Appendix A - Threat & Vulnerability Identification Tree	Shaheen & Sidharth
Appendix B - Measurement Scale for	Bansari

Scoring Threat Likelihood	
Appendix C - Estimation of Risk Impact	Sidharth
Appendix D - Cybersecurity Risk Matrix	Ameya
Appendix E - Assumptions	Sidharth & Ameya
References	Shaheen & Yash
Glossary	Bansari