ISTM 635 - 601

Cybersecurity Risk Assessment of AMC

Group Name: SCP Consultants

Submitted By: Chetan Joshi, Pallavi Tiwari, Shilpa Chanshetti, Shruthi Shetty

Aggie Honor Code

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

Group Name: SCP Consultants

Chetan Joshi

Pallavi Tiwari

Shilpa Chanshetti

Shruthi Shetty

Table of Contents

I. Executive Summary

The Aggie Medical Center is a hospital which is located in College Station, Texas. There are two labs and two remote clinics in College Station and Bryan area. The administrative organization is permanent which includes both temporary and permanent staff. The staff includes surgeons, physicians, facility staff, medical staff and maintenance. It also has a small IT department of 3 people who take care of the maintenance and upgrades of on-site networks and computers. They also handle simple help requests by the users. The AMC managers in Jan 2016 realized that they should do a complete information security review in their facility. In the following year, there would be multiple different regulations coming out. These regulations would need appropriate documentation of information security risk assessments and proper security practices. So, risk assessment process included identification of all the critical assets and their classification based on the operational, financial and legal value. Possible threats to the gaps and vulnerabilities in the system were identified and noted.

II. Asset Identification

During this phase, AMC's assets were identified and documented with a brief description and reason for cybersecurity risk assessment.

Asset Code/ID	Asset Name	Asset Description	Reason for Cybersecurity Risk Assessment
A001	ABC Systems	For maintenance and managing changes. Help desk is contacted from AMC in case any issues. Runs PDIS, creates new network user	Major application for AMC which contains sensitive information and a major security breach can occur if there is an unauthorized access
A002	AMC Help Desk	Troubleshooting team consisting of five technicians	People and machines can be compromised, and these users have access to most information for identifying/troubleshooting. Hence they pose high risk
A003	Email	A common server with important information, historical data, etc.	If compromised, unauthorized access/communication can happen within or outside the organization

A004	Emergency Care Data System (ECDS)	Tool for diagnosis, patient oversight, task management and billing	These systems are critical for patient care and contain confidential info about the health status of patients, malicious interference may impact user diagnosis which further can cascade into lethal damages
A005	External Relations	Users(use PDIS) who are responsible for controlling information being released to public	These employees/systems control critical information release and compromised systems can damage the organization by leaking and misusing information
A006	Financial Record Keeping System (FRKS)	Tool for managing Insurance, billing records, payment schedules, and other related information	Can be used for financial fraud if not secured from cyber threat
A007	Functional Servers	Systems for day to day activities	Entire IT Infrastructure can be compromised if these can attacked
A008	Internet access	Connectivity to internet	If compromised, communication can be intercepted or disrupted which can cascade into other issues where LAN/WAN connectivity is needed
A009	Medical Logistics System (MLS)	Order and Inventory management tool for supplies, real estate, tools, and pharmaceutical products.	Compromise of these systems will lead to asset theft and other illegal activities
A010	Paper Medical Records	On paper records for the patients	Contains critical information and should be stored securely
A011	Patient Data Information System (PDIS)	Patient records management system	Contains sensitive patient information and should be stored securely
A012	Personal computers	PCs for accessing tools and email	Systems which can be connected to AMC's network and if compromised can compromise the entire network
A013	Personnel Management System (PMS)	System with protected information about employees	Contains confidential employee information and can be used identity theft

A014	Pharmacy System	Drug dispensing systems	If any issue arise due to cyber-attack, incorrect medicine or dosage can be dispensed, which can harm patients
A015	Providers' Credentials	Tool for generating employee's credentials	If this system is compromised, then any secure system can be breached

III. Asset Classification

During this phase, assets were ranked according to their importance to AMC. The ranking was based on 3 criteria: Financial Value, Operational Importance and Legal Protection Requirements

Asset ID	**Financial Value**			**Mission Criticality**			**Protection Requirement**	**Total**
	Develop	**Maintain**	**Replace**	**BP1**	**BP2**	**BP3**	**Legal**	
A001	Medium	Medium	Medium	Supportive	Supportive	Supportive	High	12
A002	Medium	Medium	Medium	Important	Important	Important	Low	13
A003	Medium	Low	Medium	Important	Supportive	Supportive	Medium	11
A004	High	Medium	High	Critical	No Impact	Critical	Medium	16
A005	Medium	Medium	Medium	Critical	Supportive	Supportive	High	14
A006	High	Medium	High	Critical	Important	Critical	High	19
A007	High	High	High	Important	Important	Important	None	15
A008	Medium	Low	Medium	Critical	Critical	Critical	None	14
A009	Medium	Medium	Medium	Supportive	Critical	Supportive	High	14
A010	Low	Low	Low	Important	No Impact	Important	High	10
A011	Medium	Low	Medium	Critical	Supportive	Critical	High	15
A012	Medium	Low	Medium	Supportive	Supportive	Supportive	Low	9
A013	High	Medium	High	No Impact	No Impact	No Impact	High	11
A014	Medium	Medium	Medium	Supportive	Critical	Supportive	Low	12
A015	Low	Low	Low	Critical	Critical	Critical	Low	13

From the above ranking, the top 4 critical assets of AMC are identified as below:

1. A006 - Financial Record Keeping System (FRKS)
2. A004 - Emergency Care Data System (ECDS)
3. A011 - Patient Data Information System (PDIS)
4. A007 - Functional Servers

IV. Vulnerability and Threat Identification

During this phase, threat statements were documented for the critical assets of AMC. For each threat statement, the technical and non-technical vulnerabilities were identified along with their associated threats/threat agents and how each of these vulnerabilities can be exploited. For a better understanding of the vulnerabilities and threat, a tree analysis diagram was done (See Appendix B). Each vulnerability is explained in detail. (See Appendix B).

		Asset Failure Impact			Vulnerability			Threats and Threat Agents	
Asset	**Threat No**	**C**	**I**	**A**	**Tech**	**Non-tech**	**Exploit**	**Insider**	**Outsider**
PDIS	T01	Yes	Yes	Yes	CVE-2019-0547		When an attacker sends specially crafted DHCP response, remote code execution vulnerability exists which might corrupt the windows 10 & its servers.		Hackers
	T02	No	Yes	Yes	CVE-2017-15535	Un-updated patches	Mongo DB has a default disabled configuration setting of network message compressors. If this is enabled, attacker can exploit it to modify memory or deny service		Cyber attacker
	T03	Yes	Yes	No		Unauthorized access to sensitive data due to more privileges than required	For illegitimate reasons, staff can steal sensitive information for financial or personal gain	Any AMC employee	
	T04	No	No	Yes		Environmental and other External circumstances: Floods,	Natural disasters are unavoidable. But for issue like power outages, unavailability of backup will cause the issue		External Events (Environmental)

						Power outages, etc.			
FRKS	T05	No	No	Yes	CVE-2004-1369		Hackers can exploit this vulnerability found in oracle 10g can lead to a denial of service by using a malformed service_register_NSGR request that contains a value referring to an incorrect memory space. As evidenced in the case, there is no mention of updates or patches done on time	AMC Employee / Unpatched Server	Cyber attacker
	T06	Yes	Yes	Yes	CVE-2006-6703		Clicking on Phishing Emails and Suspicious Links	Un-Trained Employee	Cyber attacker
	T07	Yes	Yes	Yes		Manual erroneous backlog entries can be fed into FRKS system as access to the system is denied, resulting in loss of information and incorrect data.	Due to system outages, system access to staff will be denied, leading to manual entries into the FRKS system. This manual job can lead to loss of information or incorrect filing. This is also mentioned as a concern by the senior management with the system availability affecting the financial processes that can lead to incorrect insurance claims or billing to a customer.	AMC Employee	
	T08	Yes	Yes	Yes		Security of the premise is not properly implemented. Critical asset can be compromised	Any person(including staff or outsiders) can enter the room and steal confidential information because of lack of security	AMC Employee	External Attacker
ECDS	T09	Yes	Yes	No	CVE-2016-7251		Execution of malicious code	AMC employee	Cyber attacker
	T10	Yes	Yes	Yes	CVE-2016-7250		Unauthorized access	Staff with higher privileges than required or patients(if staff leaves	Cyber attacker

								TSPs in the treatment room, patients can get access)	
	T11	Yes	Yes	No		Employees do not follow good security practice such as resistance to social engineering	Execution of malicious code	AMC employee	Cyber attacker
	T12	Yes	Yes	Yes		Doctors leave computer screens on after they have left treatment rooms. Patients and others could have access. Passwords, logouts, timeouts, and screen savers are inconsistently used (This is inferred from the statement given: Note that the critical asset "personal computers" is a key component to PDIS and ECDS)	Unauthorized access	Staff with higher privileges than required or patients(if staff leaves TSPs in the treatment room, patients can get access)	Cyber attacker
Functional Servers	T13	Yes	Yes	No	CVE-2016-7249		Unauthorized access	Staff with higher privileges than required	Cyber attacker

	T14	Yes	Yes	Yes	CVE-2006-0271	Lack of security measures and awareness in the ABC systems	Unauthorized access and denial of service		Cyber attacker
	T15	No	No	Yes		Lack of contingency plans for access or when there is loss of connectivity	Denial of Service	Staff with higher privileges than required	Cyber attacker
	T16	Yes	Yes	Yes		Sharing of password, shoulder surfing and lack of proper security measures	Unauthorized access	Staff with higher privileges than required	Cyber attacker

V. Cybersecurity Risk Estimation

During this phase, the exploitability score and impact scores were calculated for each threat. For technical vulnerabilities, depending on the CVE ID, the scores were recorded. For non-tech vulnerabilities, we used the NVD calculator to calculate the exploitability and impact score. Details of calculations of non-tech vulnerabilities can be found in the appendix B. For each asset, threat likelihood (appendix C) and threat impact (appendix D) was given depending on the scales. Threat likelihood was calculated based on exploitability score whereas threat impact was calculated based on final impact value. Final impact value was a function of asset score and impact score.

For each threat, risk was estimated based on the risk matrix (appendix E)

Threat	Exploitability Score	Threat Likelihood	Asset score(0-27)	Scaled Asset Score(0-10)	Impact Score	FIV	Threat Impact
T01	3.9	Possible	21	7.78	5.9	13.68	Significant
T02	3.9	Possible	21	7.78	5.2	12.98	Significant
T03	0.3	Very Unlikely	21	7.78	5.2	12.98	Significant

T04	0.9	Unlikely	21	7.78	4	11.78	Moderate
T05	10	Very Likely	25	9.26	2.9	12.16	Significant
T06	8.6	Very Likely	25	9.26	6.4	15.66	Significant
T07	0.7	Unlikely	25	9.26	6	15.26	Significant
T08	0.5	Very Unlikely	25	9.26	6	15.26	Significant
T09	2.8	Possible	20	7.4	2.7	10.1	Moderate
T10	2.8	Possible	20	7.4	5.9	13.3	Significant
T11	1.3	Possible	20	7.4	5.2	12.6	Significant
T12	0.7	Unlikely	20	7.4	6	13.4	Significant
T13	2.8	Possible	18	6.67	5.9	12.57	Significant
T14	10	Very Likely	18	6.67	10	16.67	Severe
T15	1.8	Possible	18	6.67	6	12.67	Significant
T16	1.5	Possible	18	6.67	6	12.67	Significant

Note: As the impact scores are in the range of 0-10 and asset score from 0-27, scaled the asset scores from 0-10. FIV is the function of asset score and impact score.

Cybersecurity Risk Estimation for Each Threat Statement:

Threat No	Cybersecurity Risk
T01	Med High
T02	Med High
T03	Medium
T04	Low Med
T05	High
T06	High
T07	Medium
T08	Medium
T09	Medium
T10	Med High
T11	Med High
T12	Medium

T13	Med High
T14	High
T15	Med High
T16	Med High

VI. Cybersecurity Risk Management Strategy

Threat Statement	Risk Level	Strategy
T01	Mitigate risk	Patches and updates for MongoDB need to be installed on time
T02	Mitigate risk	Patches and updates for MongoDB need to be installed on time
T03	Mitigate risk	Define and Implement proper access controls to prevent unauthorized access to critical systems.
T04	Transfer risk	AMC should invest in good insurance policies which will protect them from environmental threats. This strategy can save the company from certain losses.
T05	Mitigate risk	Application updates and security patches for Oracle 10g need to be performed on time
T06	Mitigate risk	Application updates and security patches for Oracle 10g need to be performed on time
T07	Mitigate risk	Provide uninterrupted power sources such as on-site generators , UPS etc.
T08	Mitigate risk	Use biometric access in critical systems area, implement personnel security controls , background check on employees, separation of duties , rotation of duties
T09	Mitigate risk	Patches and updates for SQL Server need to be installed on time.
T10	Mitigate risk	Patches and updates for SQL Server need to be installed on time
T11	Mitigate risk	Develop and implement a security training plan for employees. Conduct periodic social engineering tests/drills to make employees aware of such practices. Ensure conformance of awareness, training and reminders periodically
T12	Mitigate risk	Proper security plans for premises, buildings and restricted areas. Have role based privileges for employees. Ensure there

		are system and network monitoring is done routinely. Administration should make sure that employees are not sharing passwords, have timeout set up for the systems
T13	Mitigate risk	Application updates and security patches for Oracle 10g need to be performed on time
T14	Mitigate risk	Application updates and security patches for SQL Server need to be performed on time
T15	Mitigate risk	Control needs to be updated for better connectivity services and back up channels for the systems and network should be set up.
T16	Mitigate risk	Develop and implement a security awareness and technical training plan for employees to make them aware of their responsibilities. Conduct periodic social engineering tests/drills to make employees aware of such practices.

VII. Appendix

Appendix A

Asset Classification is done via 3 criteria as shown below:

- *Financial value* - The factors that define the financial value of an asset are as below
    - Develop - Initial development/creation cost of the asset
    - Maintain - The cost required to maintain the asset & if any repair required.
    - Replace - If the asset requires replacement due to damage or change in process/system.

Scale for Measuring the Financial Value of an Asset			
High(3)	**Medium(2)**	**Low(1)**	**None(0)**
>10K	1K-5K	<1K	No cost required

- *Operational Importance* - 3 Business process has been identified that are critical for AMC

  - BP1 - **Patient Admission Process**: During this process, administrative staff enters and maintains patient records such as appointments, assignment to doctors and patient biography and medical history into PDIS (Patient Data Information System). This is a critical process as this information is used by the medical staff for proper diagnosis, treatment and ease of access to medical service.
  - BP2 - **Medical Order Entry**: This process deals with placing orders for hospital supplies such as medical equipment, medicines, wheelchairs, hospital assets etc. The order is placed by any physician or authorized medical staff in the MLS (Medical Logistic System) system. The order is then shared with the respective staff or a particular department which handles the supplies. The system reminds the staff about pending orders and helps to keep track of the ordered supplies.
  - BP3 - **Medical Reporting System**: This process provides physicians, administrators and other medical staff members a detailed report on a patient and related reports on the patient diagnosis and patient history and lab results. These reports are generated by the ECDS (Emergency Care Data System). This system also provides analysis services by running reports on population demographics or trending accident information which can be used for insurance and billing purpose by the hospital to improve health care services to patients.

Scale for measuring the Operational Impact of an Asset			
Critical(3)	**Important(2)**	**Supportive(1)**	**No Impact(0)**
Failure in this asset can disrupt the business and lead to critical loss of information	Failure in asset can lead to delays in information processing and transmission and can lead to loss of information	Failure in Asset will delay the information processing and transmission but will not impact the business process	Failure in asset will have very low impact on the business process

- *Legal Protection Requirements*

For legal protection requirements, the scale is made based on the Privacy Act of 1974 – which states that anyone accessing can be prosecuted for passing data to others.

Scale for Measuring the Legal Impact of an Asset

High(3)	Medium(2)	Low(1)	None(0)
Cyber-attack on assets with highly sensitive information related to health/diseases	Cyber-attack on assets which may directly or indirectly lead to loss of information causing damage to reputation or losses	Cyber-attack on assets which may create inconvenience and relative less harm(financially or physically)	Cyber-attack on assets which have no impact

Appendix B

Technical vulnerabilities:

Threat No	CVE ID	NVD link	Description	Exploitability Score	Impact Score	Vector Information
T01	CVE-2019-0547	https://nvd.nist.gov/vuln/detail/CVE-2019-0547	Windows 10 and its servers are susceptible to memory corruption because of an attack by malicious DHCP responses to a client	3.9	5.9	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
T02	CVE-2017-15535	https://nvd.nist.gov/vuln/detail/CVE-2017-15535	Denial of service or memory modification is possible because of a setting which is disabled by default in Mongo DB(3.4.x before 3.4.10, and 3.5.x-development)	3.9	5.2	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H
T05	CVE-2004-1369	https://nvd.nist.gov/vuln/detail/CVE-2004-1369	A denial of service attack is possible in Oracle 10g due to a malformed request (service_register_NSGR). This request contains an invalid pointer that is referenced to incorrect memory	10	2.9	AV:N/AC:L/Au:N/C:N/I:N/A:P
T06	CVE-2006-6703	https://nvd.nist.gov/vuln/detail/CV	Oracle Portal 9i and 10g have a vulnerability that allows attackers to cause	8.6	6.4	AV:N/AC:M/Au:N/C:P/I:P/A:P

		E-2006-6703	cross site scripting attacks(XSS) by injecting JavaScript code			
T09	CVE-2016-7251	https://nvd.nist.gov/vuln/detail/CVE-2016-7251	Microsoft SQL Server 2016 has a vulnerability to allow remote attackers to inject scripts to cause cross site scripting attacks	2.8	2.7	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
T10	CVE-2016-7250	https://nvd.nist.gov/vuln/detail/CVE-2016-7250	Attackers can gain unauthorized access to Microsoft SQL Server 2014 SP1, 2014 SP2, and 2016, leading to “Elevation of Privilege Vulnerability”. This is caused by not casting an unspecified pointer properly.	2.8	5.9	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
T13	CVE-2016-7249	https://nvd.nist.gov/vuln/detail/CVE-2016-7249	Attackers can gain unauthorized access to Microsoft SQL Server 2016, leading to “Elevation of Privilege Vulnerability”. This is caused by not casting an unspecified pointer properly.	2.8	5.9	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
T14	CVE-2006-0271	https://nvd.nist.gov/vuln/detail/CVE-2006-0271	SQL injection attack is caused in the DBMS_REGISTRY package of Oracle.(Details are not made available by Oracle)	10	10	AV:N/AC:L/Au:N/C:C/I:C/A:C

Non-technical vulnerabilities:

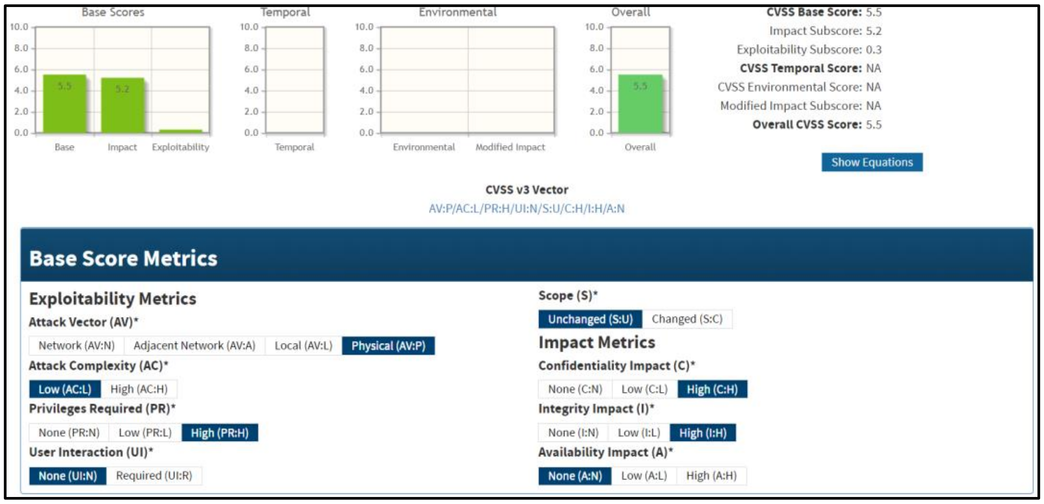
Threat No	Vulnerability Description	Evidence	Vector	Exploitability Score	Impact Score

T03	Unauthorized access to sensitive data due to more privileges than required	This can be seen in the case where the senior management has expressed concerns during the data collection part for risk assessment	(AV:P/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N)	0.3	5.2
T04	Environmental circumstances: Floods, Power outages, etc. This can cause complete loss of system. AMC requires access to PDIS 24/7.	This can be seen in the case where the senior management has expressed concerns during the data collection part for risk assessment	(AV:P/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H)	0.9	4
T07	Manual erroneous backlog entries can be fed into FRKS system as access to the system is denied, resulting in loss of information and incorrect data. Lack of UPS or other supporting system in case of a power outage can deny access to the FRKS system.	This can be seen in the case where the senior management has expressed concerns during the data collection part for risk assessment	AV:P/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H	0.7	6
T08	Security of the premise is not properly implemented.	This can be seen in the case where the senior management has expressed concerns during the data collection part for risk assessment	AV:P/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H	0.5	6
T11	Employees do not follow good security practice such as resistance to social engineering.	This is specified in the case that the employees are collocated in small spaces and often leave their systems logged in and share passwords. They have been told not to do this, but no formal training has been	AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N	2.1	5.2

		provided.			
T12	Doctors leave computer screens on after they have left treatment rooms. Patients and others could have access. Passwords, logouts, timeouts, and screen savers are inconsistently used(This is inferred from the statement given :Note that the critical asset "personal computers" is a key component to PDIS and ECDS)	As mentioned in the case, employees are collocated in small spaces and often leave their systems logged in and share passwords. They have been told not to do this, but no formal training has been provided.	AV:P/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H	0.7	6
T15	Lack of contingency plans access or connectivity is lost	This is evident from the concerns raised by the staff with internet connectivity and PDIS availability. Systems have become slower and they often crash hindering their daily activities.	AV:N/AC:H/PR:L/UI:N/S:C/C:N/I:N/A:H	1.8	6
T16	Sharing of password, shoulder surfing and lack of proper security measures	This can be identified in the case where staff share the passwords, check each other's medical records and don't log out of the devices. No proper training is being given to the employees.	AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H	1.5	6

Reasons for Calculated Base Scores:

T03: The attack could be by any AMC employee who might have extra privileges than required, so the threat agent has to be physically present there. The user need high privileges but the complexity will be low as the user will just extract the required data without changing the scope. This will impact on confidentiality as well as integrity, but the availability will not have any effect.



CVSS Base Score: 5.5
Impact Subscore: 5.2
Exploitability Subscore: 0.3
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 5.5

Show Equations

CVSS v3 Vector
AV:P/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
Network (AV:N) Adjacent Network (AV:A) Local (AV:L) [✓ Physical (AV:P)]

Attack Complexity (AC)*
[✓ Low (AC:L)] High (AC:H)

Privileges Required (PR)*
None (PR:N) Low (PR:L) [✓ High (PR:H)]

User Interaction (UI)*
[✓ None (UI:N)] Required (UI:R)

Scope (S)*
[✓ Unchanged (S:U)] Changed (S:C)

Impact Metrics

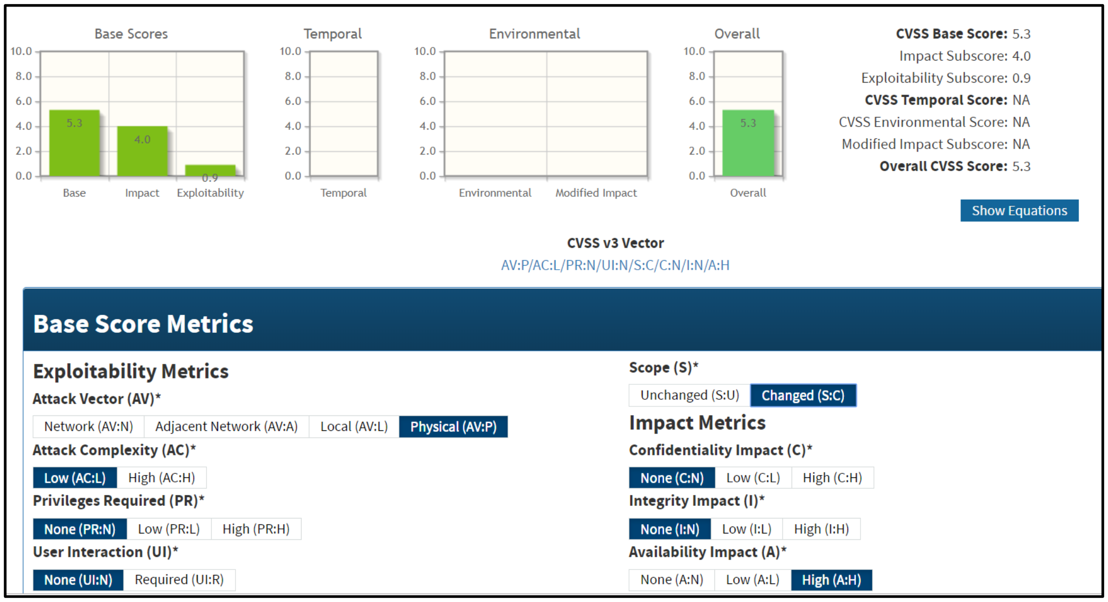
Confidentiality Impact (C)*
None (C:N) Low (C:L) [✓ High (C:H)]

Integrity Impact (I)*
None (I:N) Low (I:L) [✓ High (I:H)]

Availability Impact (A)*
[✓ None (A:N)] Low (A:L) High (A:H)

Fig: Calculated Base Score for Threat T03

T04: This is due to environmental conditions, hence the attack vector is physical, there is low attack complexity and no any privileges or user interaction is required. As there could be loss of the system, so the availability will be compromised and not confidentiality or integrity.



CVSS Base Score: 5.3
Impact Subscore: 4.0
Exploitability Subscore: 0.9
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 5.3

Show Equations

CVSS v3 Vector
AV:P/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
Network (AV:N) Adjacent Network (AV:A) Local (AV:L) [✓ Physical (AV:P)]

Attack Complexity (AC)*
[✓ Low (AC:L)] High (AC:H)

Privileges Required (PR)*
[✓ None (PR:N)] Low (PR:L) High (PR:H)

User Interaction (UI)*
[✓ None (UI:N)] Required (UI:R)

Scope (S)*
Unchanged (S:U) [✓ Changed (S:C)]

Impact Metrics

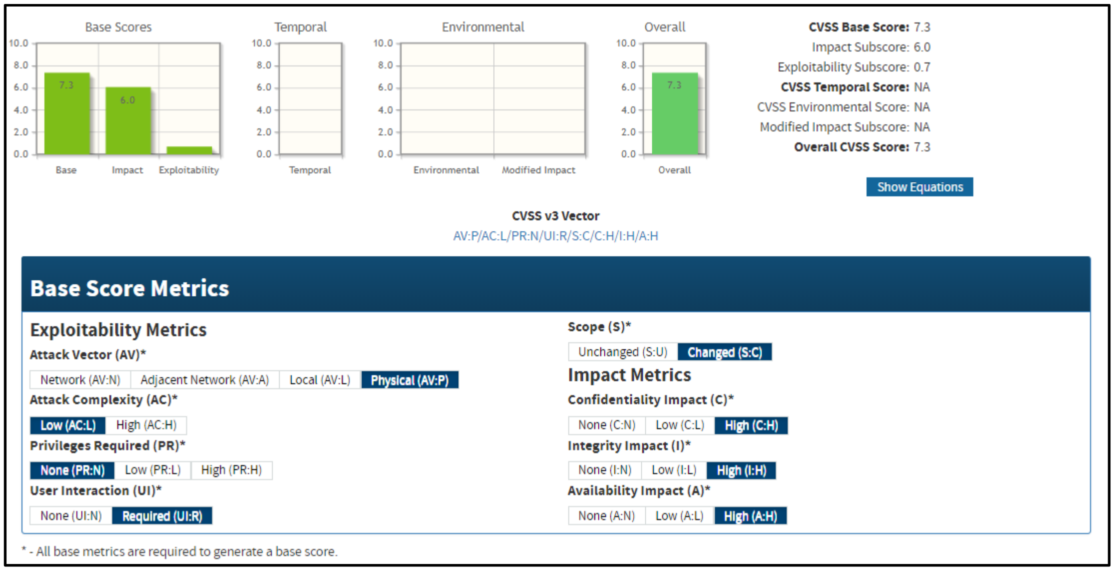
Confidentiality Impact (C)*
[✓ None (C:N)] Low (C:L) High (C:H)

Integrity Impact (I)*
[✓ None (I:N)] Low (I:L) High (I:H)

Availability Impact (A)*
None (A:N) Low (A:L) [✓ High (A:H)]

Fig: Calculated Base Score for Threat T04

T07: The vulnerability exist when a staff enter erroneous data into the system, hence it has to be a Physical Attack Vector. As the threat agent's work is not very complex as it can be done as a mistake or intentionally. The privileges are the same as what is already given to the staff. The staff has to interact with the system for it to be compromised. Hence user interaction is necessary. As the data can be changed easily on the system through manual entries, hence the scope can be changed. As data in FRKS is financial and personal data can be compromised by leaking such information, the confidentiality is high. It may not represent the same data as before, integrity is high. As the system denies access to the staff, availability is high.



CVSS Base Score: 7.3
Impact Subscore: 6.0
Exploitability Subscore: 0.7
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 7.3

CVSS v3 Vector
AV:P/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
Network (AV:N) Adjacent Network (AV:A) Local (AV:L) [✓ Physical (AV:P)]

Attack Complexity (AC)*
[✓ Low (AC:L)] High (AC:H)

Privileges Required (PR)*
[✓ None (PR:N)] Low (PR:L) High (PR:H)

User Interaction (UI)*
None (UI:N) [✓ Required (UI:R)]

Scope (S)*
Unchanged (S:U) [✓ Changed (S:C)]

Impact Metrics

Confidentiality Impact (C)*
None (C:N) Low (C:L) [✓ High (C:H)]

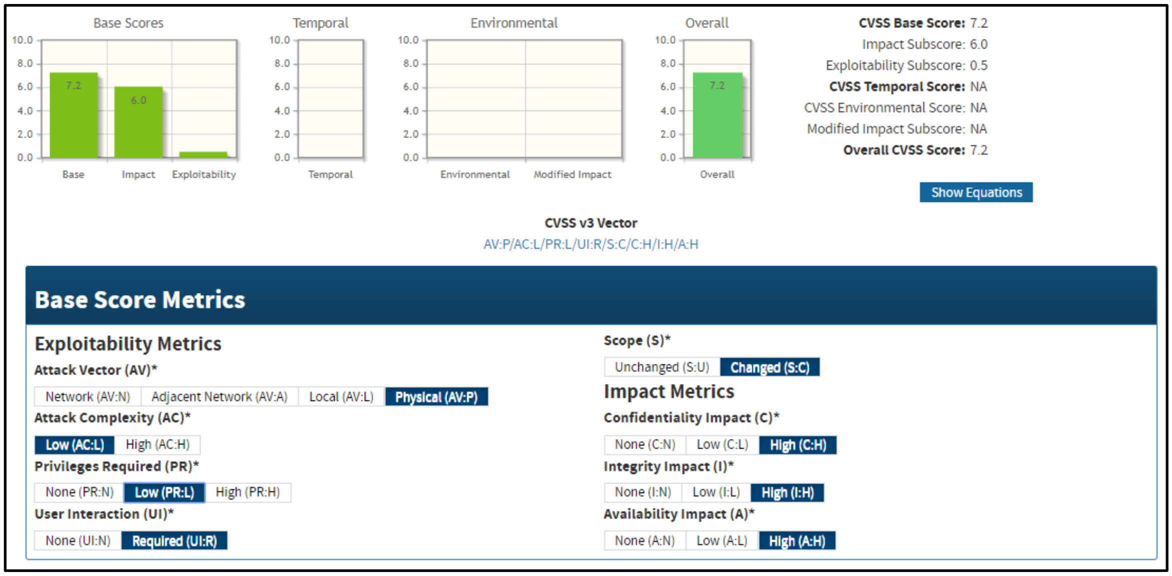
Integrity Impact (I)*
None (I:N) Low (I:L) [✓ High (I:H)]

Availability Impact (A)*
None (A:N) Low (A:L) [✓ High (A:H)]

* - All base metrics are required to generate a base score.

Fig: Calculated Base Score for Threat T07

T08: The vulnerability exist when a person enters the premise enter erroneous data into the system, hence it has to be a Physical Attack Vector. As outsiders are able to get in as easily as the staff can, hence the attack complexity is low. The privileges for outsiders may not be as per the staff, hence external attackers might require certain privileges. For a theft to occur, the threat agent need to interact. As the system is compromised, the scope may be changed and information can be leaked. Hence the confidentiality and integrity is high. As the complete system can stole, availability of that system is high.



CVSS Base Score: 7.2
Impact Subscore: 6.0
Exploitability Subscore: 0.5
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 7.2

CVSS v3 Vector
AV:P/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | [✓ Physical (AV:P)]

Attack Complexity (AC)*
[✓ Low (AC:L)] | High (AC:H)

Privileges Required (PR)*
None (PR:N) | [✓ Low (PR:L)] | High (PR:H)

User Interaction (UI)*
None (UI:N) | [✓ Required (UI:R)]

Scope (S)*
Unchanged (S:U) | [✓ Changed (S:C)]

Impact Metrics

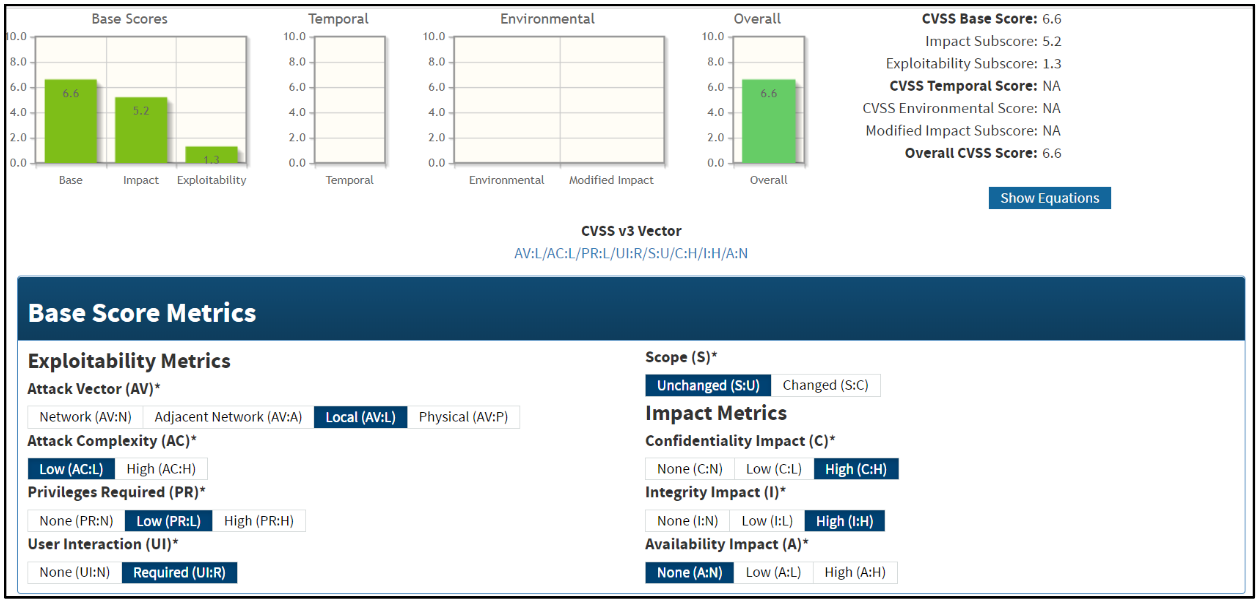
Confidentiality Impact (C)*
None (C:N) | Low (C:L) | [✓ High (C:H)]

Integrity Impact (I)*
None (I:N) | Low (I:L) | [✓ High (I:H)]

Availability Impact (A)*
None (A:N) | Low (A:L) | [✓ High (A:H)]

Fig: Calculated Base Score for Threat T08

T11: This vulnerability exists when a person takes control of the personal computers or systems to execute malware or malicious code locally. Since there is lack of awareness about the social engineering attacks and computers are left unlocked, the attack complexity is low. Privileges required are also low due to the reason mentioned above. When the attack is through spam/phishing mails, user interaction is required in that case. The scope remains unchanged as the malware infects the system. When the system is compromised, the patient data can be changed and leaked. Hence, the confidentiality and integrity is high. The availability may not be impacted and hence it is taken as none.



CVSS Base Score: 6.6
Impact Subscore: 5.2
Exploitability Subscore: 1.3
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 6.6

CVSS v3 Vector
AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
Network (AV:N) | Adjacent Network (AV:A) | [✓ Local (AV:L)] | Physical (AV:P)

Attack Complexity (AC)*
[✓ Low (AC:L)] | High (AC:H)

Privileges Required (PR)*
None (PR:N) | [✓ Low (PR:L)] | High (PR:H)

User Interaction (UI)*
None (UI:N) | [✓ Required (UI:R)]

Scope (S)*
[✓ Unchanged (S:U)] | Changed (S:C)

Impact Metrics

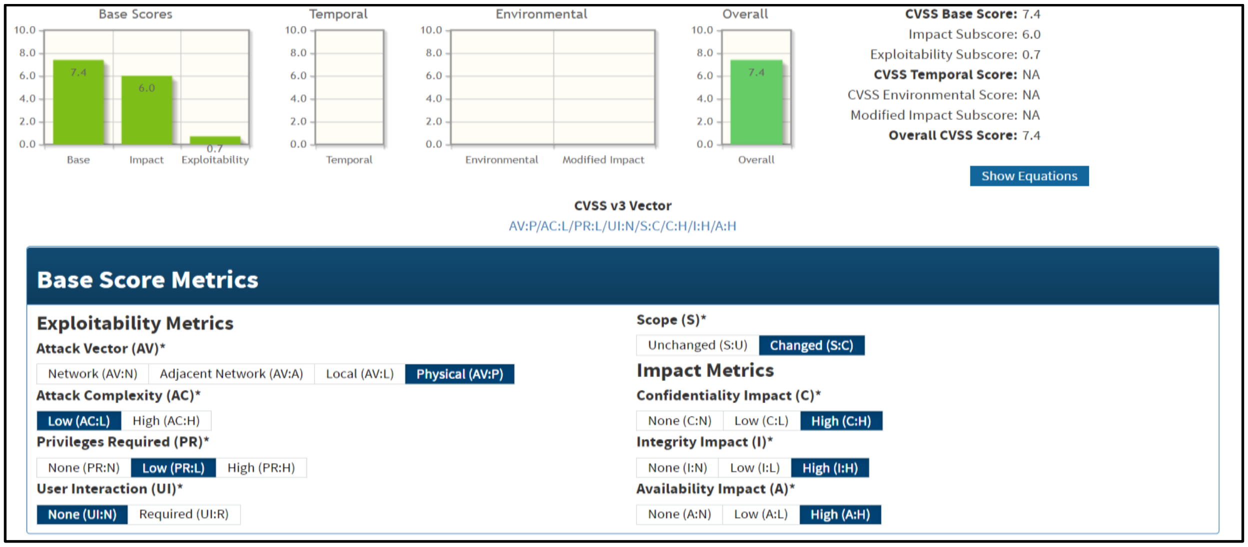
Confidentiality Impact (C)*
None (C:N) | Low (C:L) | [✓ High (C:H)]

Integrity Impact (I)*
None (I:N) | Low (I:L) | [✓ High (I:H)]

Availability Impact (A)*
[✓ None (A:N)] | Low (A:L) | High (A:H)

Fig: Calculated Base Score for Threat T11

T12: This vulnerability occurs when a person accesses the system physically and tries to change the system. Hence the scope is changed for this. Since the doctors often leave the system screens unlocked often, the attack complexity is low and no user interaction is required. The information can be modified and unauthorized access of privileged information can be gained. On gaining access, the person can execute code or destroy the system. Hence, all three i.e. confidentiality, integrity and availability are rated high.



CVSS Base Score: 7.4
Impact Subscore: 6.0
Exploitability Subscore: 0.7
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 7.4

Show Equations

CVSS v3 Vector
AV:P/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
Network (AV:N) Adjacent Network (AV:A) Local (AV:L) [✓ Physical (AV:P)]

Attack Complexity (AC)*
[✓ Low (AC:L)] High (AC:H)

Privileges Required (PR)*
None (PR:N) [✓ Low (PR:L)] High (PR:H)

User Interaction (UI)*
[✓ None (UI:N)] Required (UI:R)

Scope (S)*
Unchanged (S:U) [✓ Changed (S:C)]

Impact Metrics

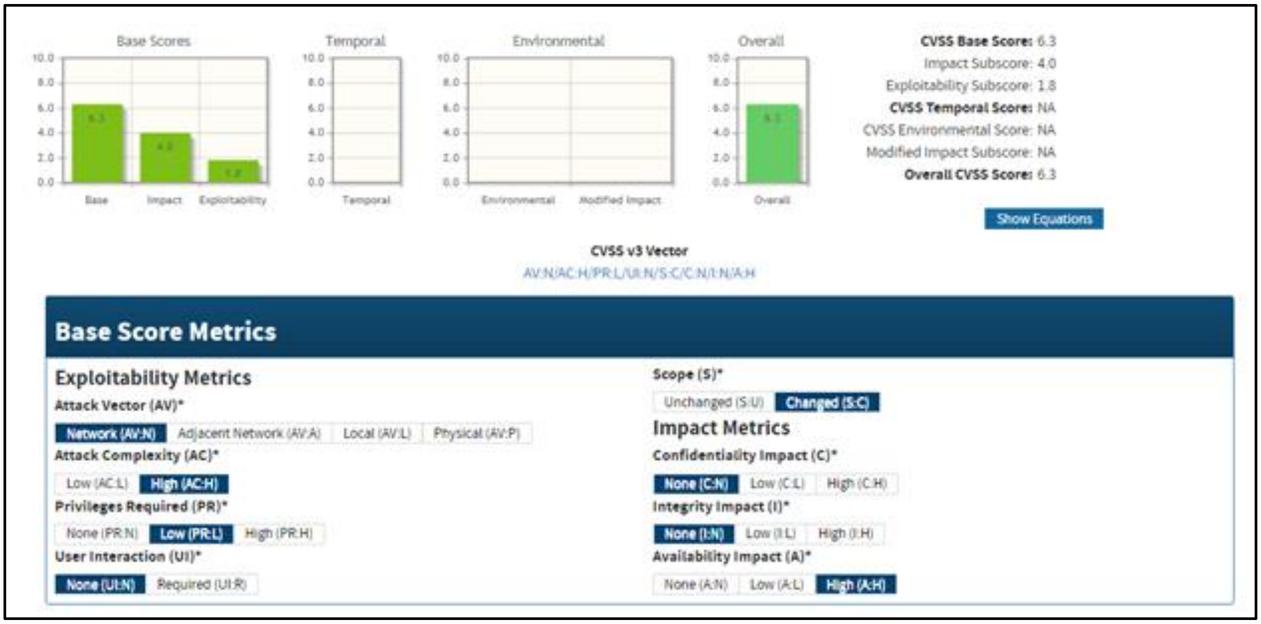
Confidentiality Impact (C)*
None (C:N) Low (C:L) [✓ High (C:H)]

Integrity Impact (I)*
None (I:N) Low (I:L) [✓ High (I:H)]

Availability Impact (A)*
None (A:N) Low (A:L) [✓ High (A:H)]

Fig: Calculated Base Score for Threat T12

T15: This vulnerability can expose network denial and attacks from remote systems using complex attacking methodologies such as DDOS, without having any privilege to the system and user interaction. This can have a cascading effect to other systems and evidently availability of systems will be compromised. Integrity and confidentiality will not be impacted with DDOS.



CVSS Base Score: 6.3
Impact Subscore: 4.0
Exploitability Subscore: 1.8
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 6.3

Show Equations

CVSS v3 Vector
AV:N/AC:H/PR:L/UI:N/S:C/C:N/I:N/A:H

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
[✓ Network (AV:N)] Adjacent Network (AV:A) Local (AV:L) Physical (AV:P)

Attack Complexity (AC)*
Low (AC:L) [✓ High (AC:H)]

Privileges Required (PR)*
None (PR:N) [✓ Low (PR:L)] High (PR:H)

User Interaction (UI)*
[✓ None (UI:N)] Required (UI:R)

Scope (S)*
Unchanged (S:U) [✓ Changed (S:C)]

Impact Metrics

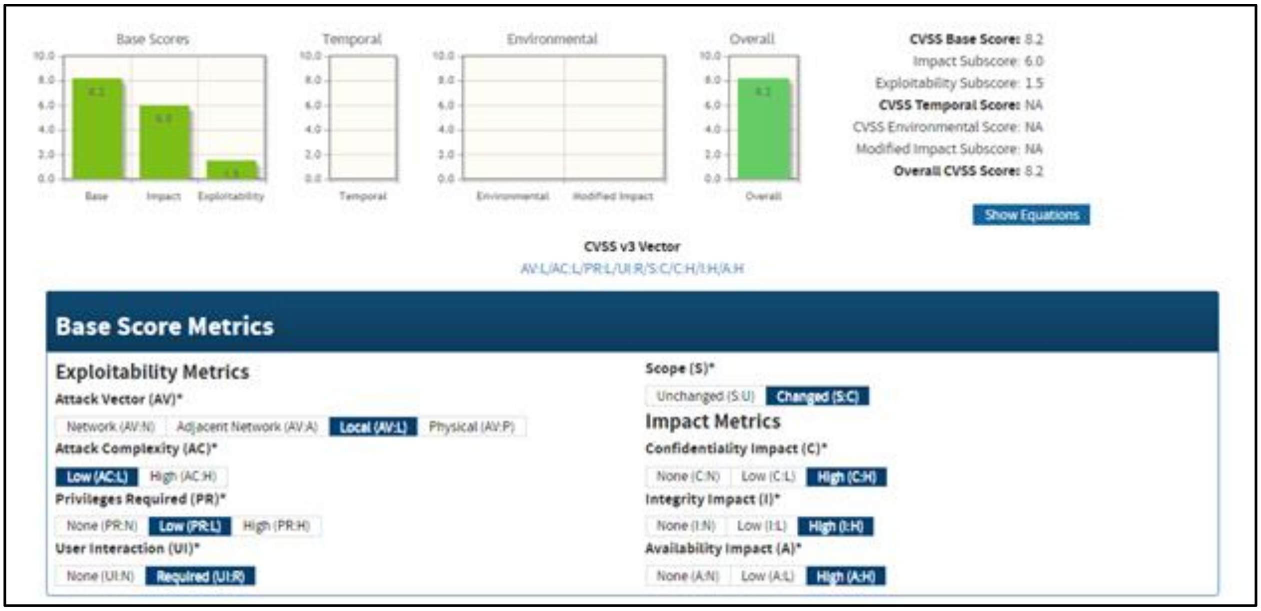
Confidentiality Impact (C)*
[✓ None (C:N)] Low (C:L) High (C:H)

Integrity Impact (I)*
[✓ None (I:N)] Low (I:L) High (I:H)

Availability Impact (A)*
None (A:N) Low (A:L) [✓ High (A:H)]

Fig: Calculated Base Score for Threat T15

T16: There is wrong sense of trust between the employees and even after being told not to share the passwords, people often share the information. People check each other's medical records and people don't log out of the devices. No proper training is being given to the employees and there is lack of proper controls for the systems.



CVSS Base Score: 8.2
Impact Subscore: 6.0
Exploitability Subscore: 1.5
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 8.2

CVSS v3 Vector
AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
Network (AV:N) | Adjacent Network (AV:A) | [✓ Local (AV:L)] | Physical (AV:P)

Attack Complexity (AC)*
[✓ Low (AC:L)] | High (AC:H)

Privileges Required (PR)*
None (PR:N) | [✓ Low (PR:L)] | High (PR:H)

User Interaction (UI)*
None (UI:N) | [✓ Required (UI:R)]

Scope (S)*
Unchanged (S:U) | [✓ Changed (S:C)]

Impact Metrics

Confidentiality Impact (C)*
None (C:N) | Low (C:L) | [✓ High (C:H)]

Integrity Impact (I)*
None (I:N) | Low (I:L) | [✓ High (I:H)]

Availability Impact (A)*
None (A:N) | Low (A:L) | [✓ High (A:H)]

Fig: Calculated Base Score for Threat T16

Tree Diagrams:

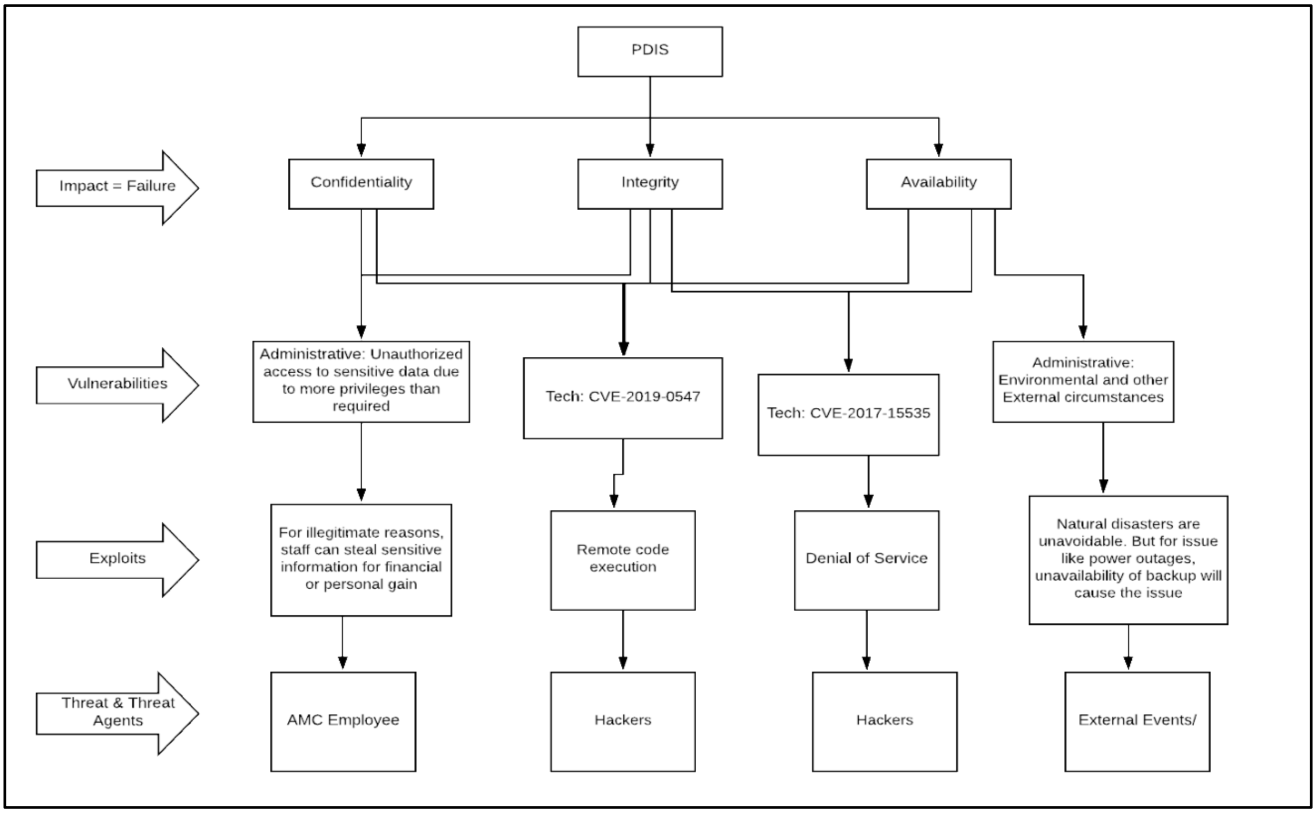

PDIS
Impact = Failure
Confidentiality
Integrity
Availability
Vulnerabilities
Administrative: Unauthorized access to sensitive data due to more privileges than required
Tech: CVE-2019-0547
Tech: CVE-2017-15535
Administrative: Environmental and other External circumstances
Exploits
For illegitimate reasons, staff can steal sensitive information for financial or personal gain
Remote code execution
Denial of Service
Natural disasters are unavoidable. But for issue like power outages, unavailability of backup will cause the issue
Threat & Threat Agents
AMC Employee
Hackers
Hackers
External Events/

Fig: Tree Analysis for PDIS

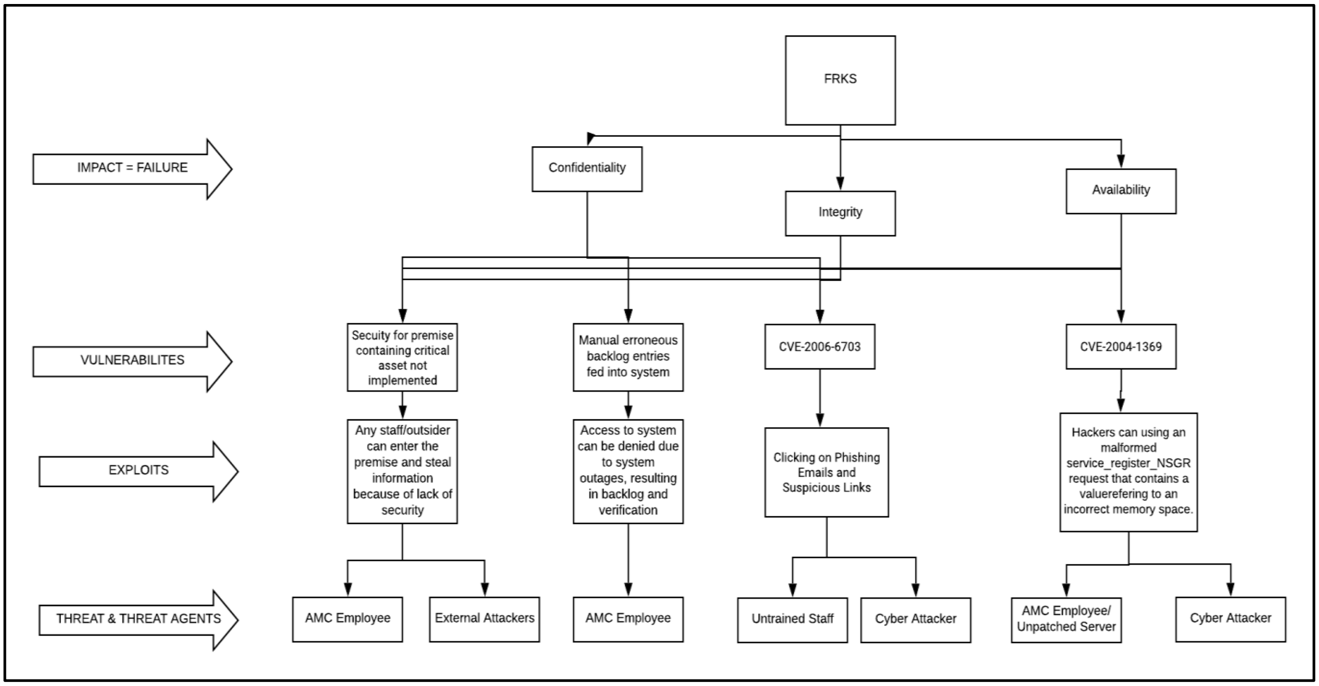

FRKS
IMPACT = FAILURE
Confidentiality
Integrity
Availability
VULNERABILITES
Secuity for premise containing critical asset not implemented
Manual erroneous backlog entries fed into system
CVE-2006-6703
CVE-2004-1369
EXPLOITS
Any staff/outsider can enter the premise and steal information because of lack of security
Access to system can be denied due to system outages, resulting in backlog and verification
Clicking on Phishing Emails and Suspicious Links
Hackers can using an malformed service_register_NSGR request that contains a valuerefering to an incorrect memory space.
THREAT & THREAT AGENTS
AMC Employee
External Attackers
AMC Employee
Untrained Staff
Cyber Attacker
AMC Employee/ Unpatched Server
Cyber Attacker

Fig: Tree Analysis for FRKS

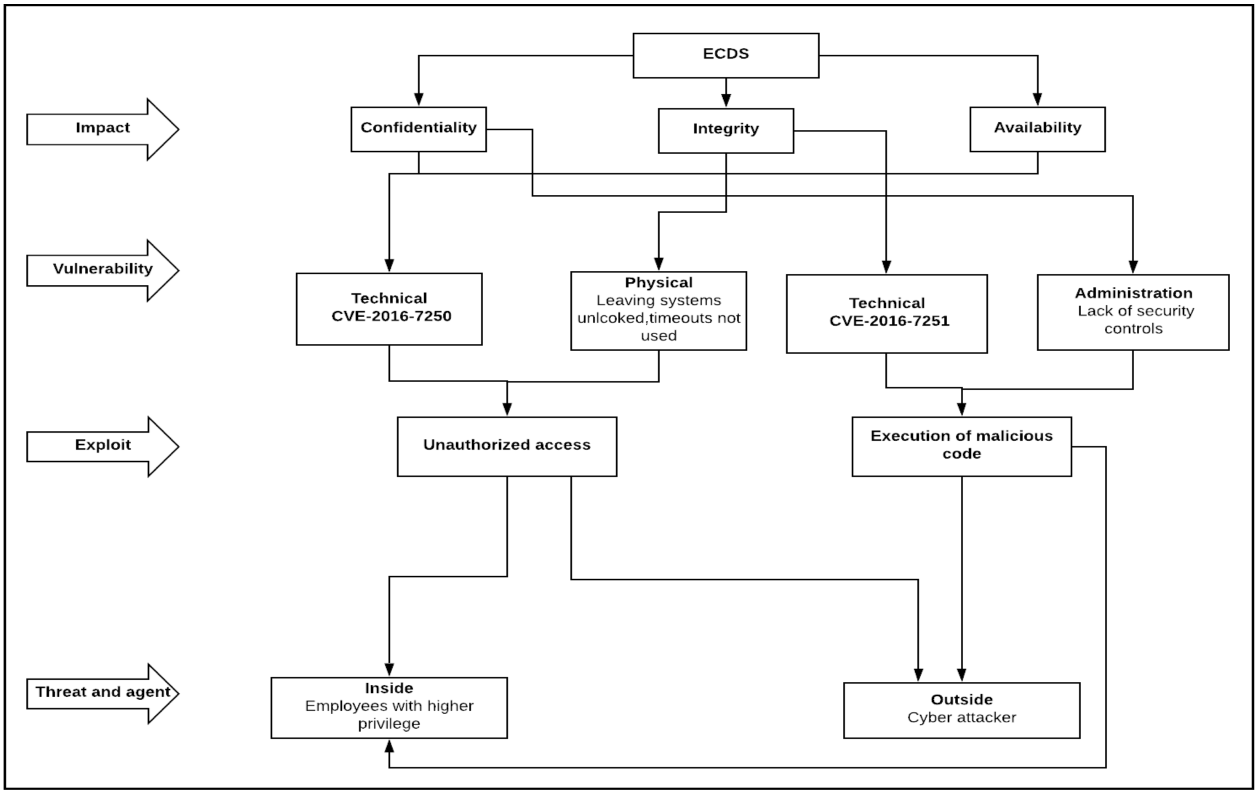


Fig: Tree Analysis for ECDS

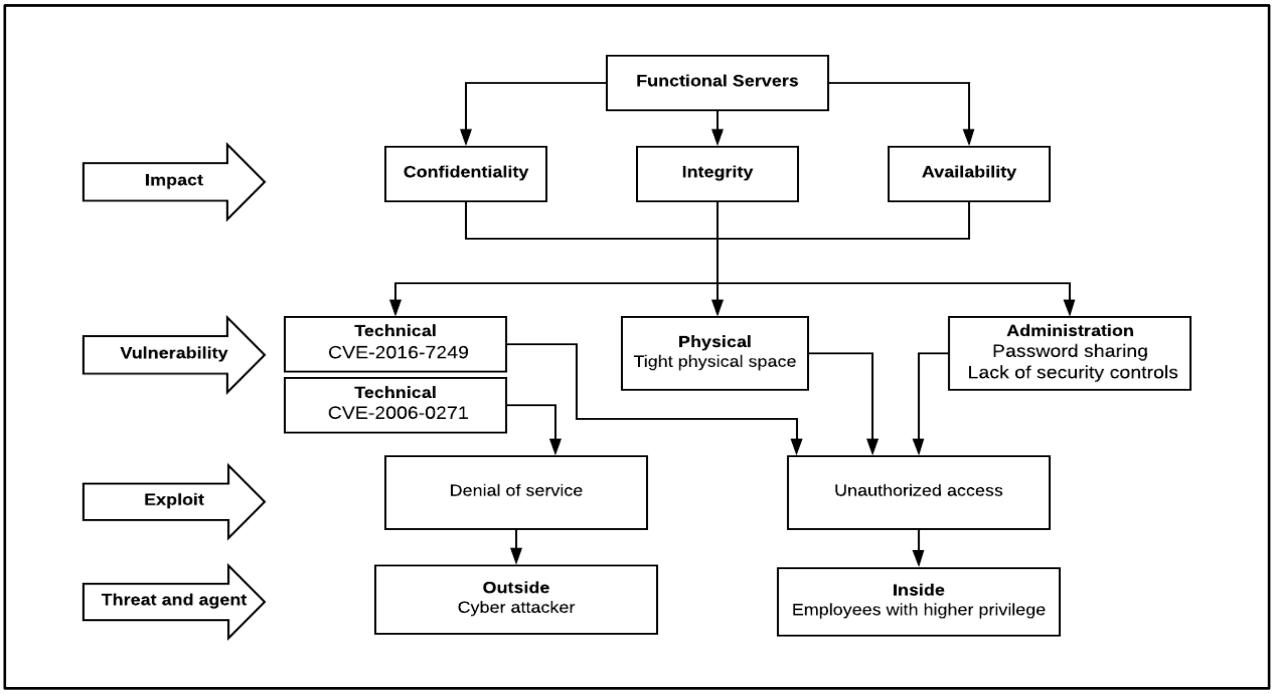


Fig: Tree Analysis for Functional Server

Appendix C

Measurement Scale for Threat Likelihood				
Very Likely	**Likely**	**Possible**	**Unlikely**	**Very Unlikely**
7 < Exploitability Score <=10	4 < Exploitability Score <=7	1 <Exploitability Score <=4	0.5 <Exploitability Score <=1	Exploitability Score <=0.5

Appendix D

As the impact scores are in the range of 0-10 and asset score from 0-27, scaled the asset scores from 0-10. FIV is the function of asset score and impact score.

Asset score(0-27)	Scaled Asset Score(0-10)
21	7.78
25	9.26
20	7.4
18	6.67

Final Impact Value = Impact score (0-10) + Asset Score (1-10)
Therefore, the FIV is out of 20. Below is the scale to calculate the threat impact

Measurement Scale for Threat Impact				
Severe	**Significant**	**Moderate**	**Minor**	**Negligible**
FIV >= 16	12 =< FIV < 16	8 <= FIV < 12	4 <= FIV < 8	FIV < 4

Appendix E

	IMPACT					
THREAT LIKELIHOOD		Negligible	Minor	Moderate	Significant	Severe
	Very Likely	Low Med	Medium	Med High	High	High
	Likely	Low	Low Med	Medium	Med High	High
	Possible	Low	Low Med	Medium	Med High	Med High
	Unlikely	Low	Low Med	Low Med	Medium	Med High
	Very Unlikely	Low	Low	Low Med	Medium	Medium

Fig: Risk Matrix

Risk Management Strategy for Risk Values:

Cybersecurity Risk	Strategy
Low	It is better to ignore such risks as investing on mitigation is more expensive than the cost of control.
Low Medium	These can be transferred by investment in good insurance policies to save the company in case of any natural or manmade disasters.
Medium	These risk can be eradicated by implementing physical security, data backup, UPS and biometric access to critical systems. Security guidelines should be established for avoiding cyber-attacks.

Medium High	These can be mitigated by updating patches for vulnerable servers frequently and establishing network security controls.
High	Risks of this order are critical to the company and should be mitigated by frequently updating and installing patches for critical servers and having excellent cyber security measures in place. Constant monitoring and alerts should be setup to avoid any incoming attacks.

VIII. References

1. ***https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf***
2. ***https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator***

IX. Glossary

Acronym or term	**Description**
AMC	Aggie Medical Center
DDOS	Distribute Denial of Service
C	Confidentiality
I	Integrity
A	Availability
FRKS	Financial Record Keeping System
ECDS	Emergency Care Data System
PDIS	Patient Data Information System
CVE	Common Vulnerabilities and Exposures
NVD	National Vulnerability Database
FIV	Final Impact Value