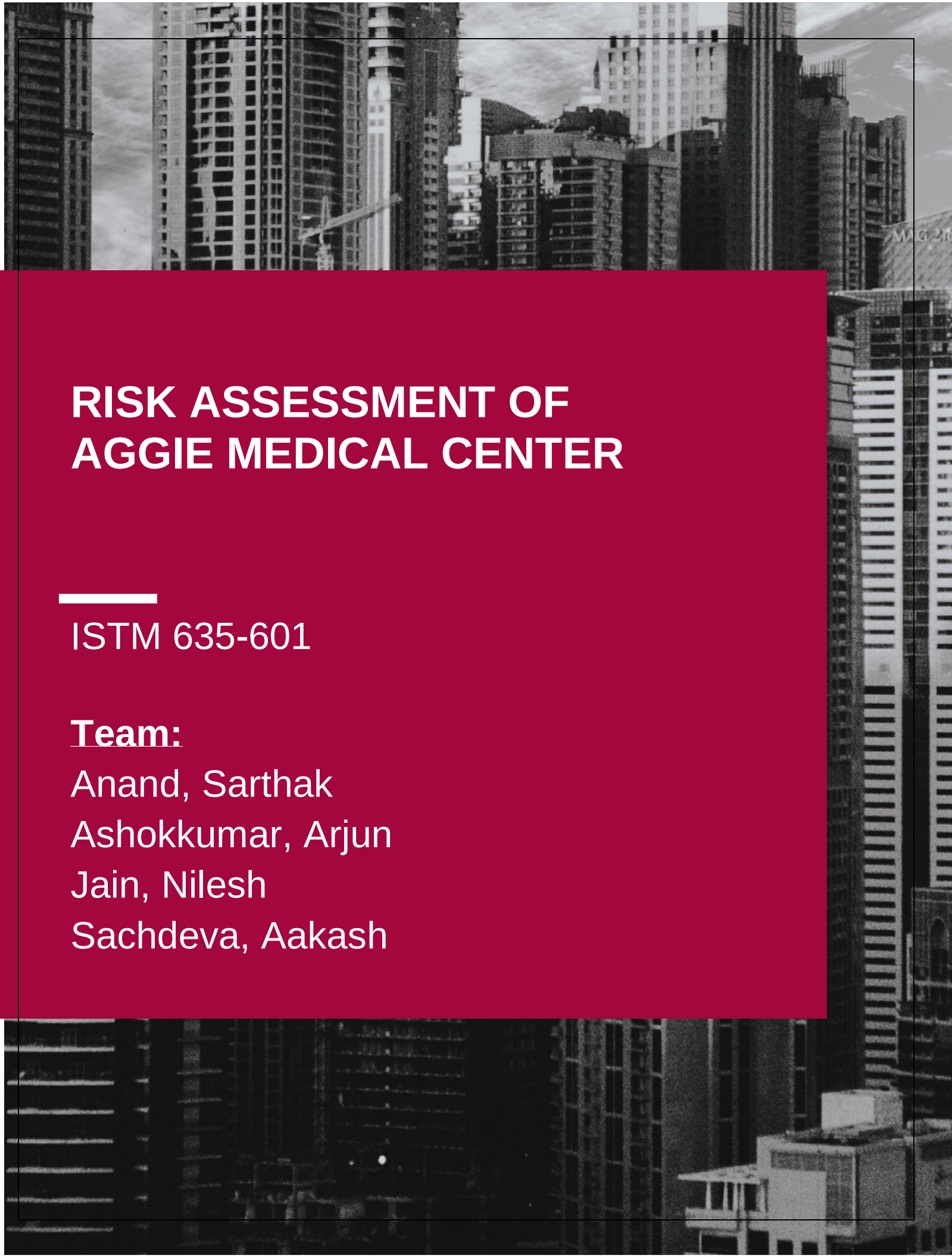


RISK ASSESSMENT OF AGGIE MEDICAL CENTER

ISTM 635-601

Team:

Anand, Sarthak

Ashokkumar, Arjun

Jain, Nilesh

Sachdeva, Aakash

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."

Table of Contents

Executive Summary

This report focusses on gathering information about the Aggie Medical Center in the Bryan/College Station area and from this information inferring the assets and vulnerabilities of their business model. This is all done in hopes to further improve the cyber security measures of the organization. Cyber Security is key in these times where cyber-attacks are often and data privacy is paramount. Several companies have realized its importance and have been setting up teams with highly skilled cyber security consultants to improve existing security measures and further introduce better and much more defensive security plans.

The project aims at assaying the existing system set in place at the AMC and try to assess the situation in terms of depth and efficiency of the protective measures. This can be done by going through the documentation of all the employee conversations regarding security and from their opinions analyze possibilities of attacks and existences of vulnerabilities. This is all done once we identify all the assets of the AMC and prioritize them on how valuable they are.

On in-depth analysis of these assets we begin to discover the existing vulnerabilities and subsequent threats that can hinder their proper functioning. The report works on unearthing the assets and the as per mentioned additional data, this information can be pivotal in the further progress of the cyber security measures. We classify the assets in terms of their impacts in areas such as finance, operational impact and also in terms of legality. We also score them in terms of their impact such as low, medium or high. The assets also have their threat statements identified and categorized under either technical issues or non-technical issues. The liabilities are recorded with their impact in the event of their failure, the exploits and the causing threat agents.

For every identified key asset, we produce two technical and non-technical vulnerability from the information analyzed on the AMC. The main assets the report discusses are the system database, network router, financial server and also the main admirative workstations. The exploits, threat agent and the possible impact to the system is documented.

Thus, the report assesses the valuable assets of the Aggie Medical Center, their vulnerabilities, risks, threats and possible repercussions. The cyber security steps that could be implemented to better protect the AMC are explained with data to back the strategy in this report. The possibilities by which hackers could compromise the system are analyzed and respective measures to combat this are discussed in the report. The report is essentially a cyber security risk document that can be used to keep a note on the current situation and further improvements to the security system at the AMC.

Asset Identification

Before any cyber security measures can be employed, we ought to identify the key assets of the organization. Once they have been identified and further cyber security risks pertaining to each asset is analyzed in-depth. The key assets are further listed as follows:

Asset ID	Asset Name	Asset Description	Reason for cybersecurity assessment
A1	Patient Data Information Server - PDIS	This database is the main store for patient information and is central to operations. It also stores appointment information. One of the several database systems used in the system and it involves legacy database systems.	It is necessary to function 24/7 and remain confidential coupled with access to only authorized users. Databases are usually highly susceptible to attacks, and sensitive patient data could be compromised if security is subpar. So, we ought to eliminate as many vulnerabilities as possible,
A2	Financial Record Keeping Server - FRKS	This server stores data related to Insurance, billing records, payment schedules and other related information. Daily operations that are carried out are stored here.	Vulnerability checks must be done to test if the server is secure and updated. They contain sensitive data like financial records and customer's payment information. It must be active at all times and specifically during working hours to prevent operations lag.
A3	Personal Management System Server - PMS	This server contains personnel data including demographics, skills, assignments and other similar data. The records of patients that are on paper cannot be re-created.	This data can be easily accessed wherein it can be viewed and edited by anyone with access to the system, leading to several cases where it can be misused. The system is simple, but personnel might struggle with incident management and anomaly detection.

A4	Medical Logistics Server - MLS	All data related to supplies, organization property and equipment.	Power outages might hamper re-entry and verification. Some important financial data is stored here that is confidential, that may be mishandled.
A5	Paper Medical Records	These are records that may be used for daily operations. They cannot be re-created as they are hard copies.	It can be viewed or altered by anyone with access and therefore must be secured physically to prevent mishandling.
A6	Providers' Credentials	Medical personnel credentials. They can provide unauthorized personnel with access if leaked.	It is important for the verification of new, transferred, or temporary providers or to provide information for insurance purposes and only authorized users should access it.
A7	Emergency Care Data System - ECDS	This is the data store of data related to emergency treatment of patients including their diagnosis, reports, trends and information on accidents. It is inaccessible by home PCs and runs on SQL Server (2016).	It is ideal that the system cannot be accessed by desktop PCs, but they must be further secured as they contain sensitive data. This data must above all be protected in accordance to the Privacy Act.
A8	Email Server	It holds historic data of email correspondence. It also contains important personal patient data like treatment discussions and scheduled appointments.	Important information exchange is held here. It functions via PDIS or LAN. Server must be continuously monitored and updated to ensure protection of the patient data.
A9	Communication Lines	The various systems used by the AMC communicate with each other by means of unsecured lines.	These lines can be penetrated easily as they are unshielded. So, message transfers can be hacked easily.

A10	Routers	They help workstations access external networks, they help in accessing data and channelizing them to different parts of the system.	Most network components such as routers are prone to several vulnerabilities that can access deep parts of the system. Security measures must be placed to protect the system as they are the first barrier of entry to hackers.
A11	Administrative Workstations	The AMC's office is passable and does not possess a lot of extra space to house an administrative workstation securely. They might be shared by a number of the workers.	Workstations may be logged in and left without attention and administrative access may be misused. Also, workstations can be viewed by anybody who passes by that causes serious security impact to the system. A single ID may be used for access.

Figure 1: Asset Identification Table

Asset Classification

Assets importance is identified by its total score. Once we understand the priority to secure and avoid exploitability of the assets, we can better allocate our resources in our risk strategy. The asset score is calculated based on various parameters across financial, operational and legal domain. Appendix-A gives a detail information of the significance and quantitative value of the levels.

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	Critical	Critical	Critical	Critical	Critical	25
A2	Financial Record Keeping Server - FRKS	Medium	Medium	High	Critical	Medium	18
A3	Personal Management System Server - PMS	Medium	Medium	High	High	Medium	17
A4	Medical Logistics Server - MLS	Medium	Low	Medium	Medium	Low	17
A5	Paper Medical Records	Medium	Medium	Medium	High	Medium	16

A6	Providers' Credentials	Low	High	Critical	Critical	Low	22
A7	Emergency Care Data System - ECDS	Medium	Critical	High	High	High	20
A8	Email Server	Low	Medium	Low	Medium	None	15
A9	Communication Lines	Medium	High	Low	Medium	Medium	17
A10	Routers	Low	High	Low	Medium	Low	19
A11	Administrative Workstations	Critical	Medium	Critical	Critical	Critical	23

Figure 2: Asset Classification Table

A function is performed on each Asset Value calculated for each asset above to decrease the distribution between Asset Values and keep the range between 0-10.

Function: Sqrt (Asset Value)

Asset ID	Asset Value	Final AV = sqrt (AV)
A1	25	5
A2	18	4.24
A3	17	4.12
A4	17	4.12
A5	16	4
A6	22	4.69
A7	20	4.47
A8	15	3.87
A9	17	4.12
A10	19	4.35
A11	23	4.79

Figure 3: Asset Value Table

VULNERABILITY AND THREAT IDENTIFICATION

There are five key assets with existing technical and non-technical vulnerabilities defined below. It is important to identify these vulnerabilities and threats as they will help us realize the negative impact and mitigate them. Specific evidences and their exploits are also provided for each vulnerability. The threat agents are divided into insider and outsider to provide more insight.

Below is the table with threat statement for key assets:

Asset	Vulnerability	Exploit	Threat Agent	
			Insider	Outsider
A1 (Patient Data Information	CVE-2017-2665	People can access information that they are not authorized,	AMC database administrators	Patients, former employees, hackers

Server-MongoDB)		because access control for the system is not present		
	CVE-2019-2386	After user deletion in MongoDB Server the improper invalidation of authorization sessions allows an authenticated user's session to persist and become conflated with new accounts, if those accounts reuse the names of deleted ones.	AMC IT Staff	ABC system employees, hackers
	Role based access is not defined and there is unauthorized access	Employees can foul some records by having access to more privileges than they are supposed to have	AMC staff, senior management	Unethical hackers/pen-testers
	Erroneous information could be entered by employees intentionally	The physicians can get incorrect reports or incorrect patient diagnosis or treatment being reported	AMC staff	Former employees, hackers
A7 (Emergency Care Data System-SQL Server)	CVE-2002-1145	The xp_runwebtask stored procedure in the Web Tasks component, which allows an attacker to gain privileges by updating a web task that is owned by the database owner	IT Staff	Hackers
	CVE-2002-0645	Arbitrary commands can be executed by users due to SQL injection	AMC IT admins	ABC support team, external contractors, hackers
	Malicious code and virus activity can enter the system due to configuration of firewall	Attackers can disrupt the system and can access the database and enter wrong data	AMC staff	Hackers
	Erroneous information entered by number of users	Data can be modified by employees resulting in unauthorized data	AMC staff	None
A2 (Financial Record Keeping Server-Oracle_10g)	CVE-2007-2118	Data access by unapproved people can lead to stealing of data	AMC staff	Financial Hackers
	CVE-2007-6260	Using of default passwords in the installation process gives remote attackers login access through the listener	AMC database administrators	ABC employees, Hackers

	Staff has equal access rights on the server	Confidential information could be changed or disclosed by staff	IT admins	Insurance sharks, hackers
	No physical security for the room	Anyone could wander in and see the confidential information	Internal Staff	Unauthorized visitors, patients
A11 (Administrative Workstations-Windows10)	CVE-2019-1358	Windows Jet Database Engine improperly handles objects in memory which can cause remote code issues	AMC staff	Attackers
	CVE-2019-0733	Security feature of the machine could be bypassed by an attacker	AMC IT admins	Hackers
	Workstations are shared amongst employees	Data can be accessed and misused by those who do not have authorization	AMC staff	Hackers
	Lot of workstations are out in the open without any security	Theft of data by staff through the open workstations	AMC staff	Unauthorized trespassers
A8 (Email Server-SMTP Server)	CVE-2010-0024	Attackers can send a denial of service attack with a crafted response	AMC staff	Hackers
	CVE-2010-0025	Email commands can be sent by attackers to read fragments of e-mail messages	IT staff	Hackers, former employees
	Information seen by unauthorized personnel	Employees can see information of patients and share with others	AMC staff	Former employees
	Medical personnel use email to discuss treatment plans for patients	Information can be leaked to attackers or employees	AMC staff	Hackers

Figure 4. Vulnerability and Threat Identification Table

CYBERSECURITY RISK ESTIMATION

The Cybersecurity Risk Estimation estimates the risk of each threat statement using the Final Impact Value (FIV) and the Likelihood of the threat by mapping the FIV and the Likelihood to the Risk Matrix. The FIV is calculated by adding the Asset Score and Impact value which can be found in Appendix-D.

The threats and their corresponding risk values are given in the following table:-

Asset	Vulnerability	Likelihood	FIV	Risk
A1	CVE-2017-2665	Very Unlikely	Moderate	Low Medium

(Patient Data Information Server-MongoDB)	CVE-2019-2386	Very Unlikely	Moderate	Low Medium
	Role based access is not defined and there is unauthorized access	Very Unlikely	Moderate	Low Medium
	Erroneous information could be entered by employees intentionally	Very Unlikely	Moderate	Low Medium
A7 (Emergency Care Data System-SQL Server)	CVE-2002-1145	Very Likely	Significant	High
	CVE-2002-0645	Very Likely	Significant	High
	Malicious code and virus activity can enter the system due to configuration of firewall	Very Unlikely	Moderate	Low Medium
	Erroneous information entered by number of users	Very Unlikely	Moderate	Low Medium
A2 (Financial Record Keeping Server-Oracle_10g)	CVE-2007-2118	Very Likely	Moderate	Medium High
	CVE-2007-6260	Very Likely	Minor	Medium
	Staff has equal access rights on the server	Unlikely	Moderate	Low Medium
	No physical security for the room	Very Unlikely	Moderate	Low Medium
A11 (Administrator Workstation)	CVE-2019-1358	Very Unlikely	Moderate	Low Medium
	CVE-2019-0733	Very Unlikely	Moderate	Low Medium
	Workstations are shared amongst employees	Very Unlikely	Moderate	Low Medium
	Lot of workstations are out in the open without any security	Very Unlikely	Moderate	Low Medium
A8 (Email Server- SMTP Server)	CVE-2010-0024	Very Likely	Minor	Medium
	CVE-2010-0025	Very Likely	Minor	Medium
	Information seen by unauthorized personnel	Unlikely	Moderate	Low Medium
	Medical personnel use email to discuss treatment plans for patients	Unlikely	Moderate	Low Medium

Figure 5. Cybersecurity Risk Estimation Table

CYBER SECURITY RISK MANAGEMENT STRATEGY

Asset	Vulnerabilities	Threat	Risk Mitigation Strategy
A1 (MongoDB)	CVE-2017-2665	There is no access control for MongoDB by default, hence anyone can access the database.	Risk can be executed is to execute the following command: ~]# chmod 600 /etc/skyring/skyring.conf. This gives back the complete read/write permission to the owner. 6 provides read/write access to the owner. The following 0 removes existing permissions of other users.
	CVE-2019-2386	This allows remote authenticated users to cause a denial of service (crash) or read system memory via a crafted BSON object in the column name in an insert command, which triggers a buffer over-read	This issue has been corrected in version 2.3.2 of MongDb and an update should be carried out if it hasn't. A link to the Github repository has also been provided by us [6]. This shows the code changes performed on the BSON object to prevent this issue from happening.
	Unauthorized access. Roles aren't defined amongst users	This leads to difficult in management of access and supervising changes in privileges. Employees could obtain more than adequate information from the database	Roles and permissions must be defined and set by the administrator to prevent unauthorized access.
	Erroneous information could be entered by employees intentionally	Employees or outsiders with unauthorized access can intentionally enter erroneous data and damage system integrity	High integrity and cross reference data must be enforced to make sure erroneous data is not submitted to the system.
A7 (ECDS)	CVE-2002-1145	This would allow an attacker to gain privileges to the server by updating a webtask that is owned by the database owner through the msdb.dbo.mswebtasks table, which does not have strong permissions.	To mitigate this, Microsoft has released an updated cumulative patch which includes an installer. Patch ID is Q327068. The AMC ECDS server would need to be updated with this patch to mitigate the risk.
	CVE-2002-0645	Hackers and attackers can exploit the database system by using attacks like SQL Injection	Firstly, all the procs and query execution must be locked and table must be granted access with different level of permission to read/write data from different server/system/user
	Malicious code and virus activity can enter the system due to configuration of firewall	Attackers can disrupt the system and can access the database and enter wrong data	We can implement firewall at various levels and filter packages based on rule as well as roles. A logger should be in place to keep track of events and fishy trends should be monitored.
	Erroneous information	Employees or outsiders with unauthorized access can intentionally enter erroneous	High integrity and cross reference data must be enforced to make sure

	entered by number of users	data and damage system integrity	erroneous data is not submitted to the system.
A2 (Financial Record Keeping Server-Oracle_10g)	CVE-2007-2118	Data access by unapproved people can lead to stealing of data	Financial data would need approval, hence and access should have a pull request associated with it.
	CVE-2007-6260	It allows remote attackers to obtain login access by connecting to the listener	Oracle suggests to use a 12C Password format which incorporates cryptography and hashing. This would prevent unauthorized access
	All the internal IT staff have equal privileges on the server	Financial claims for any patients can be changed which could lead to false insurance claims	Instead of all the IT staff, only system administrators should have necessary access. If any other IT staff needs to access, it should be done after administrator verification. Proper role-based permissions should be assigned to the users
	No physical security for the room	Anyone could wander in and see the confidential information	The room with computers and other devices should be secured. A camera can also be installed to monitor the activities. Access to the room should also be prevented based on bio-metric authentication or magnetic chip-based cards
A11 (Administrator Workstation)	CVE-2019-1358	Windows Jet Database Engine improperly handles objects in memory which can cause remote code issues	Windows cumulative update should be installed frequently
	CVE-2019-0733	Security feature of the machine could be bypassed by an attacker	Both the in-built firewall and anti-virus software should be frequently updated on the administrator workstation
	Workstations are shared amongst employees	Employees would have access to their colleague's confidential data	Only those who enter data in the system should be given access to the workstations. Employees must be trained and instructed to avoid using their colleagues' workstations. They should only sign into devices using their respective IDs.
	Lot of workstations are out in the open without any security	If there is no security, there is a possibility of theft of data or even the workstations.	Workstations should be secured in isolated rooms. Each device's service tag should also be preserved in order to track later in case of misplacement. Data replication can also be carried out, preventing the impact that loss of data (their most valuable asset) can have on the system

A8 (Email Server-SMTP Server)	CVE-2010-0024	Attackers can send a denial of service attack with a crafted response	Make sure package filter are implemented based on rule so that mails coming from unauthorized servers are routed there first to check authenticity
	CVE-2010-0025	Email commands can be sent by attackers to read fragments of e-mail messages	Make sure email filters mark spam for mails and also give notification along with mails having suspicious links, contents and commands. Guide employees to be more careful while accessing links via emails
	Information seen by unauthorized personnel	Employees can see information of patients and share with others	Train employee regarding the privacy laws. Ensure limited information access is provided and means of duplicating the records are only after approval.
	Medical personnel use email to discuss treatment plans for patients	Information can be leaked to attackers or employees	Make sure emails are archived and cannot be used to share information regarding the patient without encryption or via unauthorized methods

Figure 6. Cybersecurity Management Strategy

APPENDICES – Measurement SCALES

Appendix-A: Measurement Scales for Asset Classification

Factors:

1. FINANCIAL

A) Financial cost of asset compromise

Critical	Asset failure resulting in large fines imposed on the organization up to $1 million, mass exodus of clients from service, several forms of loss due to operational halts and subsequent supplier gripes in regards to lesser demand (lesser clients lead to lesser supplies needed by the organization and leads to suppliers taking loses), costs incurred due to incident discovery, recovery, response; thus lost businesses cause losses exceeding $1million. Finally, the public perception and brand image is tainted.
High	Asset failure resulting in a fair number of fines imposed on the organization up to $0.5 million, A far from ideal situation arises when some clients withdraw from service leading to situations where the organizations must negotiate with suppliers to scale down supply. Losses due to operational delay and costs of incident discovery, recovery and response lead to losses exceeding $0.5 million but less than $1 million.

Medium	Asset failure resulting in a far from ideal situation arises when some clients withdraw from service temporarily and will require administration corrective actions. Losses due to operational delay and costs of incident discovery, recovery and response lead to losses less than $0.5 million.
Low	Losses due to operational delay and costs of incident discovery, recovery and response lead to minor losses.

Critical	High	Medium	Low
>$1M	$0.5M-1M	$20,000-$50000	$10,000-$20,000

Figure 7: Financial Impact Table

2. Operational Impact

A) Availability

Critical	System availability is compromised for more than a day. Connectivity issues leading to no access to needed systems and services. Availability cannot be recovered by inhouse IT staff.
High	System availability is compromised for up to a couple of hours. Connectivity issues leading to no access to needed systems and services. Availability can be recovered by inhouse IT staff
Medium	Intermediate downtime for less than an hour. Availability issues are addressable by inhouse IT team.
Low	Availability issues are addressable by inhouse IT team by remote access and within minutes of observation/reporting

B) Integrity

Critical	System data veracity is threatened when unauthorized users are able to access the resources. Modification of data by system faults and sensitive data is compromised, can lead to business processes being compromised and lead to loss of business. Cost of incident discovery and recovery is high.
High	System data is modified or altered on accident by employees and no malicious intent is discerned. The data is recovered but leads to momentary loss of data and business issues. Cost of incident discovery and recovery is substantial.
Medium	System data is compromised by some system fault and no data is lost per se. The issue is able to be fixed easily and no threat from third parties. Issue is fixed by the technology team and no cost is incurred.
Low	Issue is addressable by the technology team and no cost is incurred.

C) Access control compromised

Critical	Access control to the system data is threatened when unauthorized users are able to access it. Modification of system data and other system configurations can lead to several issues entailed by business operations halted. Access method is publicized leading to subsequent attacks. Cost incurred due to incident discovery, recovery and future solutions.
High	System access is compromised but is able to be fixed by updating existing security measures. If left unnoticed can lead to high levels of risk. Cost incurred due to incident discovery, recovery and future solutions. The access control is also considered for complete rediscovery.
Medium	System access is compromised to a small extent, the password, key or some other data is lost. Some business processes are stopped by malicious intent, However, in this case the entire system is not compromised and ways to combat issues exist. Cost incurred due to incident discovery, recovery and future solutions.
Low	Access control is not compromised and the security system in place is trustworthy.

3. LEGAL IMPACT

A) Compliance with Federal act of privacy, 1974

Critical	System data is highly confidential as it involves patients' sensitive information, breach in this data and access to third parties with malicious intent can lead to several lawsuits and litigations. The sensitive data is broadcasted by hackers, the data is sold on the black market and the security systems' access control as a result is also compromised. Cost incurred due to incident discovery, recovery and legal solutions.
High	System data is compromised but is able to be fixed by data is not accessed by third parties. If left unnoticed can lead to high levels of risk. Cost incurred due to incident discovery, recovery and legal solutions. The access control is also considered for complete rediscovery.
Medium	System data is compromised to a small extent, the breach is internal or inconsequential. Some business processes are stopped by malicious intent. However, in this case the entire system is not compromised and ways to combat issues exist as complete data recovery or segmentation of encrypted data. Cost incurred due to incident discovery, recovery.
Low	Confidential data is not compromised and the security system in place is trustworthy.

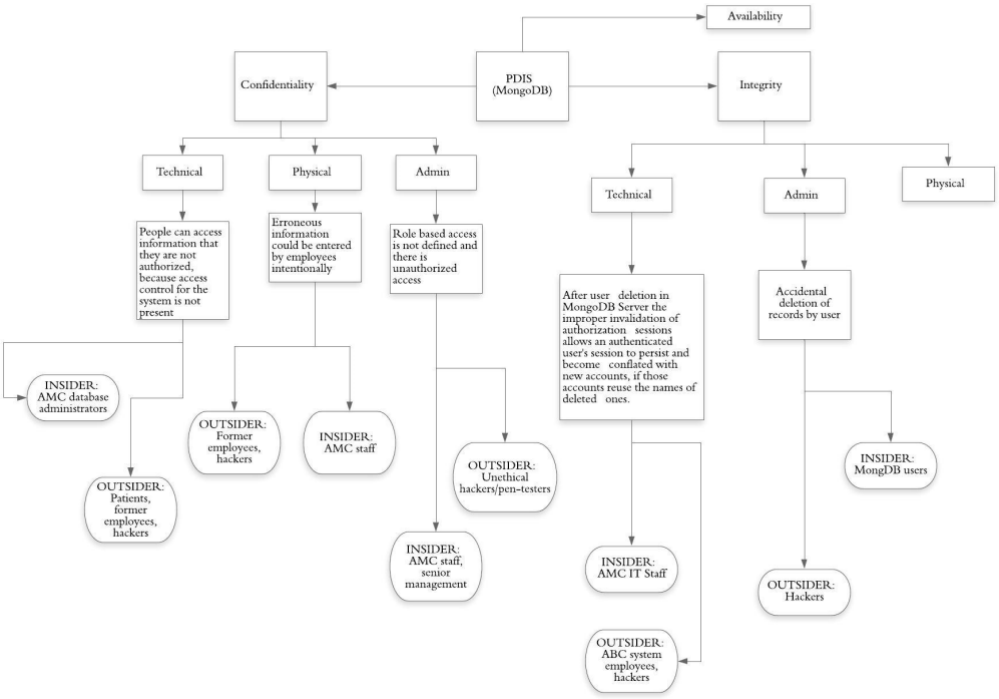
4. PARAMETRIC SCALE

Scale	Critical	High	Medium	Low	None
Value	5	4	3	2	1

Figure 8. Parametric Scale Table

APPENDIX B: Vulnerability-Threat identification

1. Asset-1: MongoDB



Technical Vulnerability

- **CVE-2017-2665:** https://nvd.nist.gov/vuln/detail/CVE-2017-2665

Any local user who has access to system running skyring service will be able to get password stored in plain text form in /etc/skyring/skyring.conf file.
Exploitability Score: 1
Impact Score: 5.9
Vector: AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

- **CVE-2019-2386:** https://nvd.nist.gov/vuln/detail/CVE-2019-2386

An authenticated user's session can become conflated with new accounts, if the names of deleted ones are used by those accounts.
Exploitability Score: 1.2
Impact Score: 5.9
Vector: AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H

Non-technical Vulnerability

- Unauthorized access

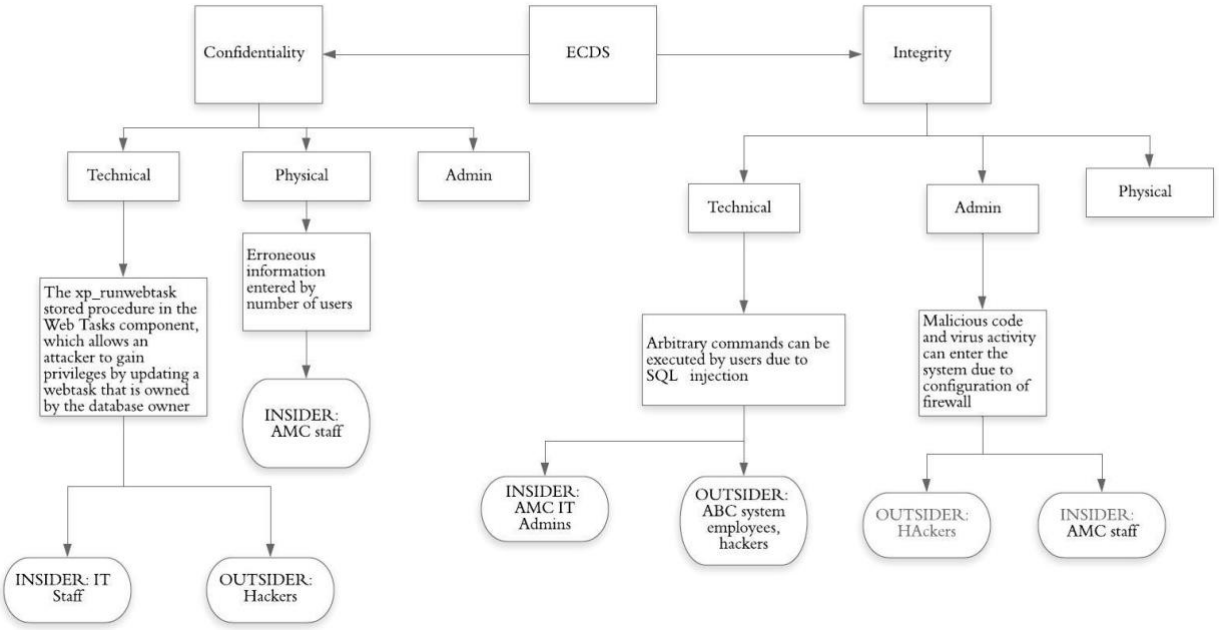
Evidence: Areas of Concern for Important Assets (Page 6, AMC case)

Exploitability Score: 1.8
Impact Score: 5.9
Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L

- Erroneous information could be entered by employees

Evidence: Areas of Concern for Important Assets (Page 6, AMC case)
Exploitability Score: 1.8
Impact Score: 5.5
Vector: CVSS:3.0/ AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L

2. Asset-2: ECDS



Technical Vulnerability

- **CVE-2002-1145:** https://nvd.nist.gov/vuln/detail/CVE-2002-1145

The xp_runwebtask stored procedure in the Web Tasks component of Microsoft SQL Server 7.0 and 2000, Microsoft Data Engine (MSDE) 1.0, and Microsoft Desktop Engine (MSDE) 2000 can be executed by PUBLIC, which allows an attacker to gain privileges by updating a webtask that is owned by the database owner through the msdb.dbo.mswebtasks table, which does not have strong permissions.

Exploitability Score: 10
Impact Score: 10
Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

- **CVE-2002-0645:** https://nvd.nist.gov/vuln/detail/CVE-2002-0645

SQL injection vulnerability in stored procedures for Microsoft SQL Server 2000 and Microsoft Desktop Engine (MSDE) 2000 may allow authenticated users to execute arbitrary commands

Exploitability Score: 10
Impact Score: 6.4
Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Non-technical Vulnerability

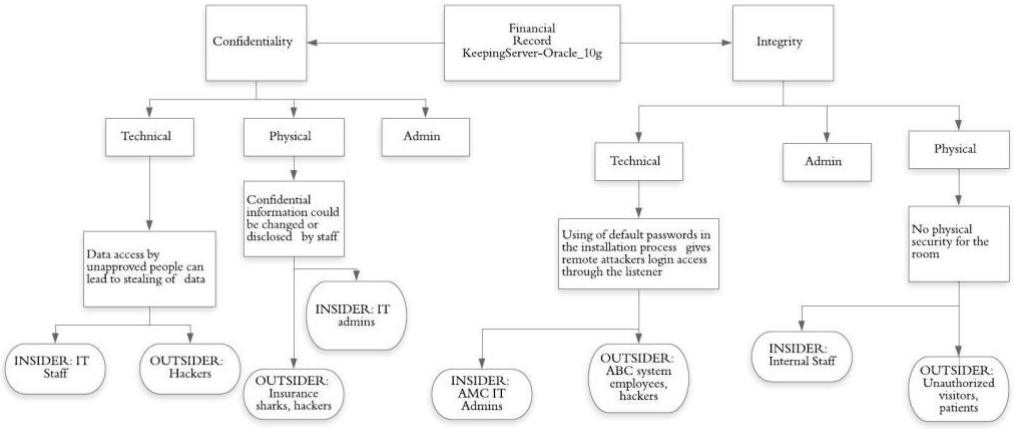
- Malicious code and virus activity can enter the system due to configuration of firewall

Evidence: Areas of Concern for Important Assets (Page 9, AMC case)
Exploitability Score: 1.6
Impact Score: 5.9
Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

- Erroneous information entered by number of users

Evidence: Security Requirements for Important Assets (Page 9, AMC case)
Exploitability Score: 0.4
Impact Score: 5.9
Vector: CVSS:3.0/AV:P/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

3. Asset-3: Financial Server



Technical Vulnerability

- **CVE-2007-2118:** https://nvd.nist.gov/vuln/detail/CVE-2007-2118

Unspecified vulnerability in the Upgrade/Downgrade component of Oracle Database 9.0.1.5 and 9.2.0.7 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: 10

Impact Score: 6.4
Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

- **CVE-2007-6260:** https://nvd.nist.gov/vuln/detail/CVE-2007-6260

The installation process for Oracle 10g and llg uses accounts with default passwords, which allows remote attackers to obtain login access by connecting to the Listener.
Exploitability Score: 8.6
Impact Score: 2.9
Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

Non-technical Vulnerability

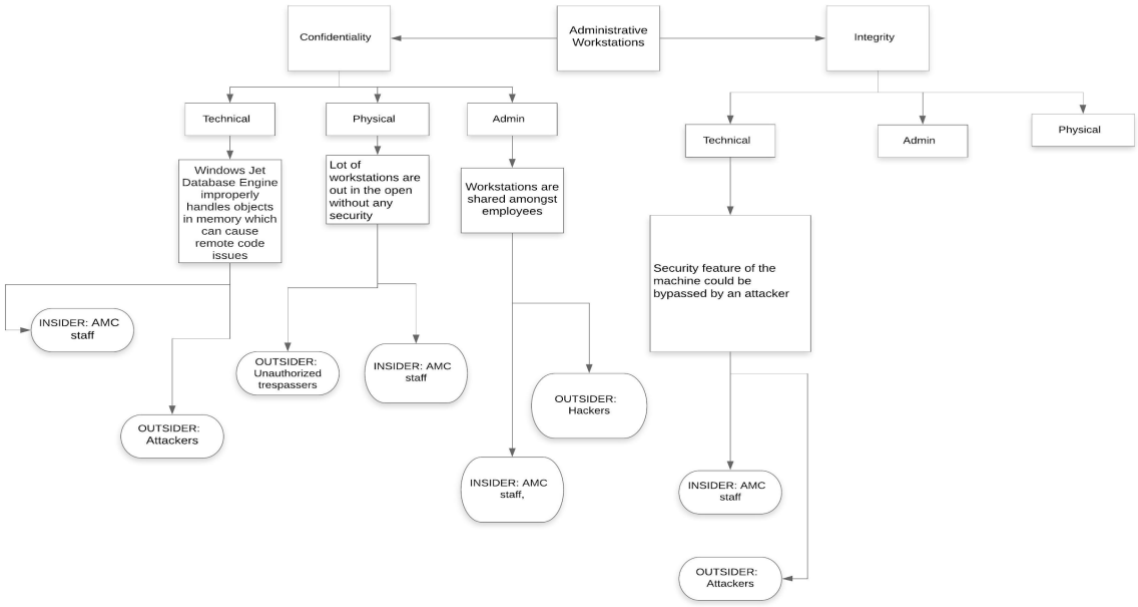
- Staff has equal access rights on the server.

Evidence: Areas of Concern for Important Assets (Page 6, AMC case)
Exploitability Score: 2.8
Impact Score: 5.9
Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

- No physical security for the room

Evidence: Areas of Concern for Important Assets (Page 6, AMC case)
Exploitability Score: 0.7
Impact Score: 5.9
Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

4. Asset-4: Administrator Workstation



Technical Vulnerability

- **CVE-2019-1358:** https://nvd.nist.gov/vuln/detail/CVE-2019-1358

A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability.

Exploitability Score: 1.8
Impact Score: 5.9
Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

- **CVE-2019-0733:** https://nvd.nist.gov/vuln/detail/CVE-2019-0733

A security feature bypass vulnerability exists in Windows Defender Application Control (WDAC) which could allow an attacker to bypass WDAC enforcement, aka 'Windows Defender Application Control Security Feature Bypass Vulnerability'.

Exploitability Score: 1.8
Impact Score: 3.4
Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L

Non-technical Vulnerability

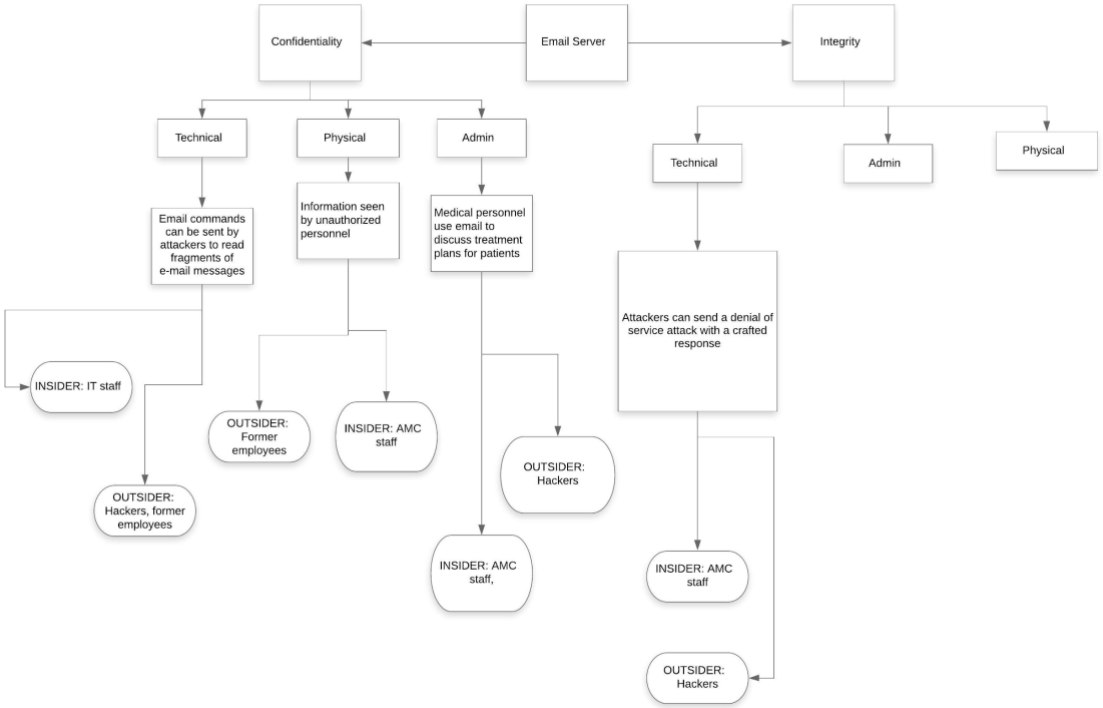
- Workstations are shared amongst employees

Evidence: General Staff Conversation about PDIS (Page 12, AMC case)
Exploitability Score: 0.7
Impact Score: 5.9
Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

- Lot of workstations are out in the open without any security

Evidence: Areas of concern (Page 8, AMC case)
Exploitability Score: 0.7
Impact Score: 5.9
Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

5. Asset-5: Email Server



Technical Vulnerability

- **CVE-2010-0024:** https://nvd.nist.gov/vuln/detail/CVE-2010-0024

The SMTP component does not properly parse MX records, which allows remote DNS servers to cause a denial of service (service outage) via a crafted response to a DNS MX record query, aka "SMTP Server MX Record Vulnerability."

Exploitability Score: 10
Impact Score: 2.9
Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

- **CVE-2010-0025:** https://nvd.nist.gov/vuln/detail/CVE-2010-0025

The SMTP component does not properly allocate memory for SMTP command replies, which allows remote attackers to read fragments of e-mail messages by sending a series of invalid commands and then sending a STARTTLS command, aka "SMTP Memory Allocation Vulnerability."

Exploitability Score: 10
Impact Score: 2.9
Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

Non-technical Vulnerability

- Information seen by unauthorized personnel

Evidence: Areas of Concern for Important Assets (Page 13, AMC case)
Exploitability Score: 2.8
Impact Score: 5.5
Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L

- Medical personnel use email to discuss treatment plans for patients

Evidence: Areas of concern for Important Assets (Page 13, AMC case)
Exploitability Score: 2.8
Impact Score: 5.5
Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L

APPENDIX C: Scale for Threat Likelihood estimation

Qualitative Scale to Measure Threat Likelihood				
Very Likely	Likely	Possible	Unlikely	Very Unlikely
8<Exploitability Score<10	6<Exploitability Score<8	4<Exploitability Score<6	2<Exploitability Score<4	Exploitability Score<2
The Exploitability Scores are calculated from the website https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator				

Figure 8. Threat Likelihood Scale

Appendix D: Final Impact Value Calculation and Risk Matrix

Function used to calculate Final Impact Value:
Asset Value Score + Impact Score= FIV

Final Impact Value associated with each Threat statement			
Asset	Asset Value Score	Impact Score	FIV
A	5	5.9	10.9
	5	5.9	10.9
	5	5.9	10.59
	5	5.5	10.55
B	4.47	10	14.47
	4.47	10	14.47
	4.47	5.9	10.37
	4.47	5.9	10.37
C	4.24	6.4	10.64
	4.24	2.9	7.14
	4.24	5.9	10.14
	4.24	5.9	10.14
D	4.79	5.9	10.69
	4.79	3.4	8.19
	4.79	5.9	10.69
	4.79	5.9	10.69
E	3.87	2.9	6.77
	3.87	2.9	6.77

	3.87	5.5	9.37
	3.87	5.5	9.37
Asset Value Scores were calculated in the Asset Classification phase CVSS Impact scores are obtained from NVD.(Range: 0-10) Final Impact Value (FIV) is found by adding the Asset Value Score to the Impact Score			

Figure 9. Final Impact Value Calculation Table

Qualitative Scale to Measure the Impact of a Cybersecurity Threat				
Severe	Significant	Moderate	Minor	Negligible
FIV>16	12<=FIV<16	8<=FIV<12	5<=FIV<8	FIV<4

Figure 10. Final Impact Value Qualitative Scale

Appendix E: Risk Matrix

Threat Likelihood	Final Impact Value (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

Figure 11: Cybersecurity Risk Matrix

Appendix F: Assumptions

Following are the assumptions that we have made:

1) Aggie Medical Center stores all the patient information in Patient Data Information Server (PDIS) using the database server MongoDB.
2) Aggie Medical Center stores all the data related to patients, diagnosis, their reports, trends, etc. using the Microsoft SQL Server.
3) Aggie Medical Center stores all the financial information such as insurance, billing records, payment schedules, and other related information Oracle 10g.
4) Aggie Medical Center uses Microsoft SMTP email server to exchange all the information over e-mails.

Appendix G: Baseline for hardening Windows 10 workstations

Baseline for hardening Windows 10 workstations used by AMC employees-

1) No workstations should be out in the open and be should be protected by passwords.
2) The workstations should not be shared among employees.
3) Set up passwords on all workstations with screensaver.
4) Firewall should be turned on.
5) Auto-updates for the operating system should be enabled.
6) Important files should be backed up periodically.
7) Only authorized users should have physical access to the workstations.
8) Anti-virus should be installed and regularly updated on all the workstations.

Appendix H: Network Access Policy and corresponding ACL

Number	Action	Protocol	Source Address	Source Port	Destination Address	Destination Port
1	Deny	TCP	ANY	ANY	172.16.11	666
2	PERMIT	IP	ANY	80	172.16.12	ANY
3	PERMIT	TCP	ANY	ANY	172.16.13	443
4	PERMIT	TCP	ANY	80	172.16.14	80
5	PERMIT	TCP	66.11.10	ALL	172.16.15	25

6	Deny	UDP	ANY	ANY	172.16.16	110
7	Permit	TCP	ANY	ALL	172.16.17	110

Figure 12. ACL for Firewall

Network Access Policy for Firewalls:

Default To Denial – All the connection path and service requests that are not specifically permitted by the ACL policy and outside listed domains are defaulted to denial in access. An inventory of all access paths into and out of the AMC internal networks must be maintained by the Information Technology department.

Connections between Machines– The real time connection set up among servers and machines via hypervisors or other remote access mechanism must be approved by the IT department and the access logs shall be maintained. Every access must be reported to the IT department.

Intrusion Detection – AMC systems have deployed intrusion detection systems as per the guidelines and approval of IT department considering the policies of data privacy and integrity. These intrusion detection systems should cover the following key areas and detect unauthorized modifications to firewall system files, and detect denial of service attacks in progress.

External Connections - All in-bound real-time Internet connections to AMC internal networks or multi-user computer systems must pass through a firewall before users can reach access any AMC system resource. Aside from personal computers that access the Internet on an outbound singleuser session-by-session dial-up basis, for which special VPN provision are required.

Extended User Authentication - Inbound traffic previously approved by the Information Technology department, that accesses the AMC network through a firewall must in all instances involve extended user authentication measures approved by the Information Technology department.

Virtual Private Networks - To reduce and stop unauthorized access to sensitive and valuable information, all inbound traffic, with the exception of Internet mail, approved news services, and push broadcasts, that accesses the AMC network must be encrypted with the products approved by the Information Technology department and maintained by the ABC systems.

References:

1) https://www.cvedetails.com/vulnerability-list/
2) https://nvd.nist.gov/
3) https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator
4) https://txwes.edu/media/twu/content-assets/documents/it/policyprocedures/firewall-policy.pdf
5) AMC Case Study

Task Allocation Matrix

Task	Team Member
Title Page	Arjun
Table of Contents	Arjun
Executive Summary	Arjun
Asset Identification	Arjun
Asset Classification	Nilesh
Vulnerability and Threat Identification	Aakash
Cybersecurity Risk Estimation	Sarthak
Cybersecurity Risk Management Strategy	Nilesh
Appendices	Arjun, Nilesh, Aakash, Sarthak
References	Nilesh, Aakash