Aggieland Medical Center

Qualitative Cybersecurity Risk Assessment

Mithilesh Menakuru, Spencer Luton, Taylor Slinkard, Sabrina Tankersley
ISTM 635: Business Information Security
Dr. Ravi Sen

10 March 2024
Texas A&M Mays Business School
College Station, TX

Table of Contents

Executive Summary

Our overall objective was to determine the risk level of the threats that were identified from the Aggieland Medical Center (AMC) case study. We identified key business processes and critical IT Assets that were needed for each of the business processes of AMC. Then, we identified vulnerabilities in the software/hardware, due to gaps in policies, and due to missing physical controls for each IT asset.

We then pinpointed threats to the company due to the vulnerabilities. In order to determine the risk of each threat, we had to determine each threat's likelihood and Final Impact Value (FIV). When we determined both of those elements, we were able to determine the risk level of each threat. AMC should prioritize the threats with the highest level of risk first and then move down the list of threats from highest to lowest level of risk.

We determined that three threats had very high risk and three threats had high risk. PDIS V1 T1, PDIS V2 T2, and RxS V22 T22 had very high risk. These threat events deal with malicious code or unauthorized access to sensitive information stored in the SQL Server. Additionally, hackers would be the threat agent for these threat events. ECDS V12 T12, ECDS V19 T19, and RxS V19 T19 had high risk. ECDS V12 T12 deals with unmonitored workstations, while the other two threats consist of insufficient vulnerability management policies and procedures.

In conclusion, we identified various threats related to vulnerabilities that could be exploited within AMC's business processes. We recommend that AMC prioritize those threats with very high risk first, then those with high risk, and so on depending on whether AMC has enough resources.

Section 1: Identification of Key Business Process and Assets

Business Processes and Assets

1. **AS: Appointment Scheduling:** Patient contacts AMC online or via phone, patient's health problem documented, patient's insurance information documented or updated (optional), data and time of appointment with the relevant physician set, patient informed via email and text about the appointment, patient reminded about the appointment 24 hours in advance and required to confirm the appointment, patient informed about how to prepare for the appointment.
    a. Asset 1: Patient Data Information Server (PDIS)
    b. Asset 2: Financial Record Keeping Server (FRKS)
    c. Asset 3: Email Server (ES)
2. **PTM: Patient Treatment and Monitoring:** Patient seen by nurse for preliminary examination, patient's health measures taken, doctor examines the patient, clinical test request by the doctor (optionmalo), appointment scheduled for the recommended test, patient informed about the test results, test results analyzed by the doctor, doctor recommends the treatment.
    a. Asset 1: Emergency Care Data System (ECDS)
    b. Asset 2: Pharmacy System (RxS)
    c. Asset 3: Email Server (ES)
3. **PB: Patient Billing & Insurance Claims Handling:** AMC files insurance claims on the behalf of the patient, relevant insurance forms filled out and set to the insurance, account settled by the insurance, balance billed to the patient, payment of balance noted down in patient's records, and financial records.
    a. Asset 1: Financial Record Keeping Server (FRKS)
    b. Asset 2: Pharmacy System (RxS)
    c. Asset 3: Email Server (ES)

Section 2: Identification of Vulnerabilities

Table 1: Vulnerabilities Associated with the Assets Listed Above

Asset Name	Vulnerability ID	Vulnerability	Technical	Administrative (Policies)	Physical	Details
PDIS	V1	Remote Desktop Client Remote Code Execution Vulnerability on PDIS W10 workstations (pen-test: pg 5)	Yes			CVE-2022-21851
PDIS	V2	Remote Procedure Call Runtime Remote Code Execution Vulnerability on PDIS W10 workstations (pen-test: pg 5)	Yes			CVE-2022-21922
PDIS	V3	Training on password security is ineffective		Yes		Lack of adequate security training, only covers password management and employees still share passwords (pg 11-12)
PDIS	V4	Privilege allocation and role assignment process is faulty		Yes		Problems with new employees having inappropriate access, problems with employees switching roles (pg 8, 9, 22)
PDIS	V5	Unlocked workstations in treatment rooms (W10)			Yes	Physicians leave workstations unlocked/logged in, PDIS can only let them log into one station at a time (pg 8, pg 12)
PDIS	V6	Poor facility layout			Yes	The configuration of facilities/layout allows inappropriate viewing of systems and medical records by patients and visitors (pg. 11,12, 20)

FRKS	V7	Media Center Library Parsing RCE Vulnerability on W7 workstations (pen-test: pg 5)	Yes			CVE-2015-6131 (pen-test: pg 5)
FRKS	V8	Windows Media Center Information Disclosure Vulnerability on W7 workstations (pen-test: pg 5)	Yes			CVE-2015-6127 (pen-test: pg 5)
FRKS	V9	Could be due to ineffective *HIPAA regulation training* leading to lack of awareness among AMC employees about the importance of patient data confidentiality.		Yes		Staff could disclose patient financial information to family or friends (Table 2: pg 7)
FRKS	V10	Inadequate *security awareness* training.		Yes		Not clear that the staff understand their security roles/responsibilities and the security issues the organization faces. (pg 15-16)
FRKS	V11	Unlocked rooms			Yes	There is no physical security for the room where staff login to access FRKS (Table 2: pg 7)
FRKS	V12	Unmonitored staff workstations			Yes	Anyone in the room can see confidential FRKS information displayed on the workstations (W7). (Table 2: pg 7)
ES	V13	Vulnerability that allows local users to reboot	Yes			CVE-2000-0633

		or halt the system				Email uses Sendmail 8.9.3 running on Red Hat Linux 6 (pg 3, pen-test: pg 5)
ES	V14	Vulnerability that allows local users to gain root access	Yes			CVE-2000-0219 Email uses Sendmail 8.9.3 running on Red Hat Linux 6 (pg 3, pen-test: pg 5)
ES	V15	Lack of privacy standards enforcement regarding email communications		Yes		Email is used to discuss patient treatment plans (Table 9: pg 13)
ES	V16	Unencrypted email		Yes		Staff believe information cannot be viewed by unauthorized personnel, not as secure as PDIS (pg 11, Table 9: pg 13)
ES	V17	Auto lock on workstations is not required or enforced			Yes	Workstations with email messages are left logged on (pg 11)
ES	V11	Unlocked rooms			Yes	Users have easy access to rooms with workstations (W7) with email correspondence on them (Table 2: pg 7)
ECDS	V7	Media Center Library Parsing RCE Vulnerability on W7 workstations used by emergency personnel (pen-test: pg 5)	Yes			CVE-2015-6131 (pen-test: pg 5)
ECDS	V18	Insufficient data validation tools/controls	Yes			Data entered is not checked against previous entries, resulting in some individuals having multiple files (Table 5: pg 9)

ECDS	V19	Insufficient vulnerability management policies and procedures		Yes		Survey results show that it is not clear when/how vulnerability assessments are performed, staff is not up-to-date on vulnerability types/attack methods, and the IT staff is not sure what to do with vulnerability reports (pg 23)
ECDS	V20	Inadequate data entry training		Yes		Too many users are entering the data and entering it wrong. One patient may erroneously have multiple files/records when only one is needed. (Table 5: pg 9)
ECDS	V12	Unmonitored staff workstations			Yes	Hardware (W7) is not monitored and access is easy to gain (pg 4, Table 2: pg 7)
ECDS	V11	Unlocked rooms			Yes	Insufficient physical access controls, easy for individuals to access rooms with workstations (W7) with ECDS data (Table 2: pg 7)
RxS	V21	Microsoft SQL Server Remote Code Execution Vulnerability on server used by RxS system	Yes			CVE-2022-29143 (pen-test: pg 5)
RxS	V22	Microsoft SQL Elevation of Privilege Vulnerability on server used by RxS system	Yes			CVE-2021-1636 (pen-test: pg 5)
RxS	V19	Insufficient vulnerability management policies and procedures		Yes		Survey results show that it is not clear when/how vulnerability assessments are performed, staff is not up-to-date on

						vulnerability types/attack methods, and the IT staff is not sure what to do with vulnerability reports (pg 23)
RxS	V10	Possible gaps in RxS security training		Yes		The staff observed weaknesses in the training as it relates to a number of AMC systems (pg 16)
RxS	V12	Unmonitored workstations			Yes	Easy to view pharmaceutical information displayed on the workstations (W7). (Table 2: pg 7)
RxS	V11	Unlocked rooms			Yes	Easy for individuals to access rooms with workstations (W7) with pharmaceutical data (Table 2: pg 7)

Section 3: Identification of Threats

Table 2: Threats Related to the Above Vulnerabilities
Note: Asset details and vulnerability ID details (Table 1) are provided above. Threat relevance explanations are provided in Table A in the appendix.

Asset Name(s)	Vulnerability ID	Threat ID	Threat Event	Threat Agent/Source	Threat Relevance
PDIS	V1	T1	Threat agent targets remote client's drive redirection virtual channel and can execute malicious code remotely	Hacker	Anticipated
PDIS	V2	T2	Threat agents manipulate this vulnerability to execute malicious code through the RPC runtime	Hacker	Anticipated
PDIS	V3	T3	Shared passwords used to access and change PDIS information	Temporary/Rouge employee	Predicted
PDIS	V4	T4	Threat agents gain access to privileged user permissions from previous users to view and edit patient records	Temporary/Rouge employee	Predicted

PDIS	V5	T5	Exploit access to logged-on workstations to view PDIS information	Temporary/Rouge employee	Anticipated
PIDS	V6	T6	Threat agents obtain sensitive medical information	Temporary/Rouge employee	Possible
FRKS, ECDS	V7	T7	Threat agent remotely executes code via a .mcl file	Hacker	Predicted
FRKS	V8	T8	Threat agents can read files with financial data via a .mcl file	Hacker	Possible
FRKS	V9	T9	Theft of financial information	Temporary/Rogue employee	Predicted
FRKS, RxS	V10	T10	Exploit gaps in training to gain unauthorized access to workstations, systems, information, etc.	Temporary/Rouge employee	Possible
FRKS, ES, ECDS, RxS	V11	T11	Insert malicious scanning devices (e.g. wireless sniffers) inside facilities to transmit information to the adversary	Temporary/Rouge employee	Possible
FRKS, ECDS, RxS	V12	T12	Perform reconnaissance and surveillance of financial, medical, and/or pharmaceutical information displayed on workstations	Temporary/Rouge employee	Predicted
ES	V13	T13	Local threat agent can shutdown or reboot system	Temporary/Rouge employee	Possible
ES	V14	T14	Phishing attacks	Spear phisher	Anticipated
ES	V15	T15	Theft of patient treatment information	Temporary/Rouge employee	Predicted
ES	V16	T16	Unsecure email exploited to obtain patient data communicated via email.	Phisher	Possible
ES	V17	T17	Unauthorized access to email	Temporary/Rouge employee	Predicted
ECDS	V18	T18	Tampering with medical data	Temporary/Rouge employee	Predicted
ECDS, RxS	V19	T19	Threat agents can target with new, more sophisticated attack methods such as (TOAD, deep fakes) that employees are not up-to-date on.	Hacker	Possible

ECDS	V20	T20	Emergency management data is corrupted or stolen	Temporary/Rouge employee	Anticipated
RxS	V21	T21	Attacker exploits vulnerability by executing a query using "$partition" function against a table with a Column Store index	Hacker	Possible
RxS	V22	T22	A threat agent can send data to an affected SQL Server when configured to run an extended event session.	Hacker	Possible

Section 4: Threat Event Likelihood Estimation

This section of the report will determine the overall likelihood of a threat event. The likelihood of threat initiation will be determined by considering the motivation (as a factor of capability, intent, and targeting) and ease of exploitability. Combining the likelihood of a threat initiation with the likelihood of adverse impact, the overall threat likelihood will be determined.

Motivation: The motivation score is calculated by ranking the capability, intent, and targeting as very low, low, moderate, high, or very high. See Table B in the appendix for the lookup table used to determine the motivation score. Table 3 below provides an explanation for the ranking of capability, intent, targeting, and overall motivation on the scale of "very low" to "very high". Table 4 lists the motivation scores for the threats identified in Table 2.

Table 3: Motivation Ranking Explanation

Ranking	Capability	Intent	Targeting	Motivation
Very High	The adversary has a very sophisticated level of expertise and has all the necessary resources and opportunities.	The adversary seeks to severely impede or destroy a core business function/mission without attack detection.	The adversary uses information obtained via reconnaissance to persistently target a specific organization, program, function, mission, positions, supporting infrastructure, and/or partnering organizations.	Adversary is almost certain to initiate the threat event.
High	The adversary has significant resources, opportunities and expertise.	The adversary seeks to impede critical assets of a business function/mission without attack detection.	The adversary uses public information and information obtained via reconnaissance to target a specific organization, program, function, or mission.	Adversary is highly likely to initiate the threat event.
Moderate	The adversary moderate resources, expertise, and opportunities.	The adversary seeks to obtain/modify specific sensitive information or usurp/disrupt the organization's cyber	The adversary uses publicly available information to target specific high-value organizations and key positions.	Adversary is likely to initiate the threat event.

		resources and is concerned about minimizing detection.		
Low	The adversary has limited resources, expertise and opportunities.	The adversary seeks to obtain/modify sensitive information or disrupt cyber resources without concern about attack detection.	The adversary uses publicly available information to target a high-value organization/class of organizations.	Adversary is unlikely to initiate the threat event.
Very Low	The adversary has very limited resources, expertise, and opportunities.	The adversary seeks to disrupt or deface the organization's cyber resources without concern about detection.	The adversary may or may not target specific organizations/class of organizations	Adversary is highly unlikely to initiate the threat event.

Table 4: Threat Motivation

Threat ID	Threat Agent/Source	Capability	Intent	Targeting	Motivation Score
T1	Hacker	High	High	High	High
T2	Hacker	High	High	High	High
T3	Temporary/Rouge Employee	Low	Moderate	High	Moderate
T4	Temporary/Rouge Employee	Moderate	Moderate	High	Moderate
T5	Temporary/Rouge Employee	Low	Low	High	Low
T6	Temporary/Rouge Employee	Moderate	Low	Moderate	Moderate
T7	Hacker	High	High	High	High
T8	Hacker	High	Moderate	High	High
T9	Temporary/Rogue employee	Moderate	Moderate	High	Moderate
T10	Temporary/Rouge employee	Moderate	Moderate	High	Moderate
T11	Temporary/Rouge employee	Low	Moderate	High	Moderate
T12	Temporary/Rouge employee	Low	Moderate	High	Moderate
T13	Temporary/Rouge employee	Moderate	Moderate	High	Moderate
T14	Spear phisher	Moderate	Moderate	High	Moderate
T15	Temporary/Rouge employee	Moderate	Moderate	Low	Moderate
T16	Phisher	Moderate	Moderate	High	Moderate

T17	Temporary/Rouge employee	Low	High	High	Moderate
T18	Temporary/Rouge employee	Moderate	Moderate	High	Moderate
T19	Hacker	Very High	High	Very High	Very High
T20	Temporary/Rouge employee	Moderate	High	Low	Moderate
T21	Hacker	Very High	High	Moderate	High
T22	Hacker	High	High	Moderate	High

Ease of Exploitability: This measure examines how easily an identified vulnerability can be exploited by a threat agent. Using version 3.1 of the Common Vulnerability Scoring Calculator, the ease of exploitability is measured by considering the impact, the attack vector, attack complexity, attack scope, privileges required, and user interaction required. Table 5 lists the criteria for the exploitability rankings while Table 6 provides the scores for each of the vulnerabilities listed in Table 1.

Table 5: Ease of Exploitability Ranking Explanation

Ranking	CVSS 3.1 Score
Very High	When CVSS 3.1 Exploitability score range is [3.0-3.9]
High	When CVSS 3.1 Exploitability Score range is [2-3]
Moderate	When CVSS 3.1 Exploitability Score range is [1-2]
Low	When CVSS 3.1 Exploitability Score range is [.5-1]
Very Low	When CVSS 3.1 Exploitability Score range is [<.5]

Table 6: Ease of Exploitability

Threat ID	Exploitability Score	Exploitability Ranking	Attack Vector
T1	2.8	High	AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
T2	2.8	High	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
T3	.6	Low	AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:N
T4	.6	Low	AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:N
T5	.7	Low	AV:P/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N
T6	.7	Low	AV:P/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N
T7	1.0	Moderate	AV:N/AC:H/PR:H/UI:R/S:C/C:H/I:L/A:L
T8	1.0	Moderate	AV:N/AC:H/PR:H/UI:R/S:C/C:H/I:L/A:L

T9	1.5	Moderate	AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:L/A:L
T10	.8	Low	AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:L
T11	.4	Low	AV:P/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L
T12	.7	Low	AV:P/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:L
T13	3.5	Very High	AV:L/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:H
T14	1.8	Moderate	AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L
T15	1.0	Moderate	AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:L
T16	1.8	Moderate	AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N
T17	.7	Low	AV:P/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:L
T18	.3	Very Low	AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:L
T19	1.6	Moderate	AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:L
T20	.3	Very Low	AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:L
T21	1.6	Moderate	AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
T22	2.8	High	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Likelihood of Threat Initiation: The likelihood of threat initiation is determined by the motivation and the ease of exploitation using the relevant lookup table in the appendix (Table C). Table 7 lists the likelihood of threat initiation based on the information in table 4 and 6.

Table 7: Likelihood of Threat Initiation/Occurrence

Vulnerability ID	Threat ID	Motivation Score (Table 4)	Exploitability Score (Table 6)	Likelihood of Threat Initiation/Occurrence Score
V1	T1	High	High	High
V2	T2	High	High	High
V3	T3	Moderate	Low	Low
V4	T4	Moderate	Low	Low
V5	T5	Low	Low	Low
V6	T6	Moderate	Low	Low
V7	T7	High	Moderate	Moderate
V8	T8	High	Moderate	Moderate
V9	T9	Moderate	Moderate	Moderate

V10	T10	Moderate	Low	Low
V11	T11	Moderate	Low	Low
V12	T12	Moderate	Low	Low
V13	T13	Moderate	Very High	High
V14	T14	Moderate	Moderate	Moderate
V15	T15	Moderate	Moderate	Moderate
V16	T16	Moderate	Moderate	Moderate
V17	T17	Moderate	Low	Low
V18	T18	Moderate	Very Low	Low
V19	T19	Very High	Moderate	High
V20	T20	Moderate	Very Low	Low
V21	T21	High	Moderate	Moderate
V22	T22	High	High	High

Likelihood of Adverse Impact: This measures the impact caused by a successful exploitation of a vulnerability. Table 8 lists the criteria for the rankings. Table 9 lists the likelihood of adverse impact for each of the threats identified.

Table 8: Likelihood of Adverse Impact Explanation

Ranking	Explanation
Very High	Adverse impacts are almost certain
High	Adverse impacts are highly likely
Moderate	Adverse impacts are likely
Low	Adverse impacts are unlikely
Very Low	Adverse impacts are highly unlikely

Table 9: Adverse Impact

Vulnerability ID	Threat ID	Adverse Impact Score	Justification
V1	T1	High	Should an attacker insert malicious code onto a client computer, it can be used to cause a number of damages: delete files,

			compromise passwords and data, steal sensitive information, disrupt system operations, etc.
V2	T2	High	Remote running of procedures virtually allow hackers to delete files, compromise passwords and data, steal sensitive information, disrupt system operations, etc.
V3	T3	Moderate	PDIS holds the majority of the important patient information. While having a password to log into a PDIS workstation may not necessarily provide a user with the ability to bring down the system, the threat agent could still modify or steal a significant amount of patient information. The damage a threat agent can do will likely be limited by the account permissions of the account associated with the stolen password.
V4	T4	High	Considering PDIS holds a significant amount of patient information, inappropriate account permissions can result in a large number of records being fouled up.
V5	T5	Moderate	PDIS workstations are primarily in the treatment rooms and any one user can only be logged into one machine. However, the doctors consistently leave the machines unlocked and threat agents who can access the machines could view/edit/delete many patient records.
V6	T6	Low	Threat agents would only be able to view the sensitive information displayed on the workstations, not change the information.
V7	T7	High	Threat agents able to access code remotely allows them to both steal and edit sensitive data that would have a devastating impact on the organization.
V8	T8	Moderate	Threat agents reading financial data puts the users financial data at high risk and can hurt the reputation of the organization as well as break the privacy act guidelines.
V9	T9	Moderate	Similar to above, stealing financial data has reputational impacts for the organization as well as potential regulatory fines.
V10	T10	Moderate	Unauthorized access to systems can expose sensitive information and allow a disruption of certain operations.
V11	T11	Low	Wireless sniffers have a high chance of detection and still require decrypting the packet interceptions into usable information that can adversely affect the organization.
V12	T12	High	Threat agents would be able to view sensitive information about patients and may be able to access and edit information that they shouldn’t be allowed to do.
V13	T13	Very High	The threat agent would be able to stop the email server, which would slow work and communication.
V14	T14	High	The threat agent would be able to target employees that have root access and would be able to read or change sensitive patient information.

V15	T15	High	The threat agent would be able to have access to any sensitive information that is shared through email due to the lack of controls dealing with the policy of sharing information.
V16	T16	High	The threat agent who is partaking in social engineering could be able to gain sensitive patient information through email since there are no stricter policies in place dealing with sharing patient treatment information over email.
V17	T17	High	Threat agents would be able to view sensitive information about patients from the email messages since the auto-lock feature is not on.
V18	T18	High	Threat agents would be able to view sensitive information regarding the patient's diagnosis, the healthcare professional who examined the patient which include the procedures, tests, billing etc.
V19	T19	Very High	This threat could potentially cost a lot because it holds the information of patients drug dosage, dispensing to patients and handling the relevant billing details too.
V20	T20	Low	This threat could happen due to incorrect data entry or multiple entries of data create confusion and acts as a duplicate data of a particular patients
V21	T21	High	By gaining elevated privileges, an attacker can gain control over systems that use the SQL server.
V22	T22	Very High	This is a high severity vulnerability that can allow an attacker to gain access and control over systems that use the SQL Server.

Overall Likelihood of a Threat Event: The *overall* likelihood of a threat event is determined by (1) the likelihood of threat event initiation or occurrence (Table 7) and (2) the likelihood of adverse impact (Table 9). See Table D in the appendix for more details on how scores in Table 11 were determined. Table 10 provides the explanation for score rankings.

Table 10: Overall Likelihood of a Threat Event

Ranking	Explanation
Very High	Threat will happen
High	Threat event will most likely happen
Moderate	Threat is likely to happen
Low	Threat is unlikely to happen
Very Low	Threat will likely not happen

Table 11: Overall Likelihood of a Threat Event				
Vulnerability ID	**Threat ID**	**Likelihood of Threat Event Initiation/Occurrence Score**	**Likelihood of Threat Event Resulting in Adverse Impacts Score**	**Overall Likelihood of a Threat Event Score**
V1	T1	High	High	High
V2	T2	High	High	High
V3	T3	Low	Moderate	Low
V4	T4	Low	High	Moderate
V5	T5	Low	Moderate	Low
V6	T6	Low	Low	Low
V7	T7	Moderate	High	Moderate
V8	T8	Moderate	High	Moderate
V9	T9	Moderate	Moderate	Moderate
V10	T10	Low	Moderate	Low
V11	T11	Low	Low	Low
V12	T12	Low	High	Moderate
V13	T13	High	Very High	Very High
V14	T14	Moderate	High	Moderate
V15	T15	Moderate	High	Moderate
V16	T16	Moderate	High	Moderate
V17	T17	Low	High	Moderate
V18	T18	Low	High	Moderate
V19	T19	High	Very High	Very High
V20	T20	Low	Low	Low
V21	T21	Moderate	High	Moderate
V22	T22	High	Very High	Very High

Section 5: Estimation Impact on IT Assets, Business Processes, and Organization

This section estimates the impact a threat event can have on an organization's business processes. Tables 11-14 provide explanations for the scores/rankings of the impact on confidentiality, integrity, and availability, business processes, financial and legal considerations. Specifically, the legal implications for the HIPAA (Health Insurance Portability and Accountability Act) are considered. Table 15 uses these values to identify the business process impact should PDIS, FRKS, ES, ECDS, or RxS fail.

Table 11: Scale for Impact on Confidentiality, Integrity, and Availability of IT Asset

Ranking	Explanation
High [10]	Confidentiality/Integrity/Availability is fully compromised
Moderate [5]	Confidentiality/Integrity/Availability is partially compromised
Low [1]	Confidentiality/Integrity/Availability is not compromised

Table 12: Impact on Business Process

Ranking	Explanation
Critical[10]	Asset failure will result in a total disruption of the business process for at least 2 hours
Important[5]	Asset failure will result in slowing down of the business process
Supportive[1]	Asset failure will have minimal impact on the business process
No Impact [0]	Asset failure will have no impact on the business process

Table 13: Assessment Scale for Financial Impact on the Organization

Ranking	Explanation
High [10]	Threat event will result in the cost of detection & escalation, incident notification, incident response, and lost business over 10% of gross annual revenues
Medium [5]	Threat event will result in the cost of detection & escalation, incident notification, incident response, and lost business between 5-10% of gross annual revenues
Low [1]	Threat event will result in the cost of detection & escalation, incident notification, incident response, and lost business up to 5% of gross annual revenues

Table 14: Assessment Scale for Legal Impact on the Organization - HIPAA	
Ranking	**Explanation**
High[10]	Asset failure will result in legal action that could include imprisonment for up to 10 years and fines up to $250,000
Medium[5]	Asset failure will result in only a fine
Low[1]	Asset failure results in a warning
None[0]	Asset failure will have no legal impact

Table 15: Business Process Impact due to Failure of an IT Asset					
IT Asset	**Financial Impact**	**Operational Impact**			**Legal Impact**
		Patient Billing (PB)	**Appointment Scheduling (AS)**	**Patient Treatment and Monitoring (PTM)**	**Health Insurance Portability and Accountability Act (HIPAA)**
Patient Data Information System (PDIS)	**High[10]**	**Important[5]**	**Critical[10]**	**Important[5]**	**High[10]**
Financial Record Keeping Server (FRKS)	**High[10]**	**Critical[10]**	**Important[5]**	**No Impact**	**None[0]**
Email Server (ES)	**Low[1]**	**Important[5]**	**Critical[10]**	**Supportive[1]**	**Low[1]**
Pharmacy System (RxS)	**Low[1]**	**Important[5]**	**No Impact**	**Important[5]**	**Important[5]**
Emergency Care Data System (ECDS)	**Moderate[5]**	**Important[5]**	**Supportive[1]**	**Critical[10]**	**High[10]**

Lastly, Tables 16 and 17 provide an analysis of the final impact value due to a threat event tied to a specific vulnerability on a specific asset.

Table 16: Final Impact Value (FIV) Ranking Explanation

Ranking	Explanation
Very High	FIV Semi-Quantitative Value is greater than or equal to 65
High	FIV Semi-Quantitative Value is greater than or equal to 50 and less than 65
Moderate	FIV Semi-Quantitative Value is greater or equal to 35 and less than 50
Low	FIV Semi-Quantitative Value is greater than or equal to 20 and less than 35
Very Low	FIV Semi-Quantitative Value is less than 20

Table 17: Final Impact Value (FIV) due to a Threat Event

Asset ID	Vulner-ability ID	Threat ID	Impact								FIV Semi-Quantitative Value	FIV Qualitative Value
			IT Asset			Business Process			Organization			
			C	I	A	PB	AS	PTM	Financial	Legal		
PDIS	V1	T1	10	10	10	5	10	10	10	10	75	Very High
PDIS	V2	T2	10	10	10	5	10	10	10	10	75	Very High
PDIS	V3	T3	10	10	1	5	5	5	5	1	42	Moderate
PDIS	V4	T4	10	10	1	5	10	5	10	5	47	Moderate
PDIS	V5	T5	10	10	1	1	1	5	5	10	43	Moderate
PDIS	V6	T6	10	10	1	1	1	1	1	5	30	Low
FRKS	V7	T7	10	10	1	10	1	1	10	5	48	Moderate
ECDS	V7	T7	10	10	1	5	5	10	10	10	61	High
FRKS	V8	T8	10	5	5	10	5	1	10	10	56	High
FRKS	V9	T9	10	5	5	10	5	1	10	10	56	High
FRKS	V10	T10	10	10	5	5	1	1	5	5	42	Moderate
RxS	V10	T10	10	10	5	1	1	1	1	1	10	Very Low
FRKS	V11	T11	10	10	5	10	5	1	10	10	61	High

ES	V11	T11	10	10	5	5	5	5	10	10	60	High
ECDS	V11	T11	10	10	5	1	5	5	5	10	51	High
RxS	V11	T11	10	10	5	5	1	5	1	1	38	Moderate
FRKS	V12	T12	10	10	5	10	10	1	10	1	57	High
ECDS	V12	T12	10	10	5	1	10	10	10	10	66	Very High
RxS	V12	T12	10	10	5	5	1	5	5	1	42	Moderate
ES	V13	T13	5	5	10	1	10	1	1	1	34	Low
ES	V14	T14	5	5	5	5	10	5	5	5	45	Moderate
ES	V15	T15	10	10	5	1	5	5	5	5	46	Moderate
ES	V16	T16	5	5	1	1	5	5	5	5	32	Low
ES	V17	T17	10	10	5	5	10	5	5	5	55	High
ECDS	V18	T18	10	10	5	5	1	10	1	10	52	High
ECDS	V19	T19	10	10	5	5	1	10	5	10	46	Moderate
RxS	V19	T19	10	10	5	5	1	10	5	5	51	High
ECDS	V20	T20	10	10	5	5	1	10	10	10	61	High
RxS	V21	T21	10	10	10	5	1	10	1	10	57	High
RxS	V22	T22	10	10	10	10	1	10	5	10	66	Very High

Section 6: Cybersecurity Risk Estimation

This final table details the cybersecurity risk level. Table E in the appendix lists the matrix used to lookup risk level as a function of the overall threat event likelihood (Table 11) and the final impact value (FIV – Table 17).

Table 18: Cybersecurity Risk to IT Assets

Asset ID	Vulnerability ID	Threat ID	Overall Threat Event Likelihood	Final Impact Value (FIV)	Risk Level
PDIS	V1	T1	High	Very High	Very High
PDIS	V2	T2	High	Very High	Very High
PDIS	V3	T3	Low	Moderate	Low
PDIS	V4	T4	Moderate	Moderate	Moderate

PDIS	V5	T5	Low	Moderate	Low
PDIS	V6	T6	Low	Low	Low
FRKS	V7	T7	Moderate	Moderate	Moderate
ECDS	V7	T7	Moderate	Moderate	Moderate
FRKS	V8	T8	Moderate	High	Moderate
FRKS	V9	T9	Moderate	High	Moderate
FRKS	V10	T10	Low	Moderate	Low
RxS	V10	T10	Low	Very Low	Very Low
FRKS	V11	T11	Low	High	Low
ES	V11	T11	Low	High	Low
ECDS	V11	T11	Low	High	Low
RxS	V11	T11	Low	Moderate	Low
FRKS	V12	T12	Moderate	High	Moderate
ECDS	V12	T12	Moderate	Very High	High
RxS	V12	T12	Moderate	Moderate	Moderate
ES	V13	T13	Very High	Low	Moderate
ES	V14	T14	Moderate	Moderate	Moderate
ES	V15	T15	Moderate	Moderate	Moderate
ES	V16	T16	Moderate	Low	Low
ES	V17	T17	Moderate	High	Moderate
ECDS	V18	T18	Moderate	High	Moderate
ECDS	V19	T19	Very High	Moderate	High
RxS	V19	T19	Very High	High	High
ECDS	V20	T20	Low	High	Low
RxS	V21	T21	Moderate	High	Moderate
RxS	V22	T22	Very High	Very High	Very High

References

CSRC NIST GOV . “SP 800-30 Rev. 1, Guide for Conducting Risk Assessments | CSRC.” n.d. Accessed March 7, 2024. https://csrc.nist.gov/pubs/sp/800/30/r1/final.

HIPAA JOURNAL. “What Are the Penalties for HIPAA Violations? 2024 Update.” n.d. Accessed March 7, 2024. https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/.

NVD NIST CALCULATOR. “CVSS V3 Calculator - NVD.” n.d. Accessed March 7, 2024.https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator.

Microsoft Security Response Center (MSRC). “SANS Internet Stormcenter Daily Cyber Security Podcast (Stormcast ..” n.d. Accessed March 7, 2024.

VULNERABILITIES. “Vulnerabilities - NVD.” n.d. Accessed March 7, 2024. https://nvd.nist.gov/vuln.

Appendix

Table A: Assessment Scale to Measure the Relevance of Threat Events

Value	Description
Confirmed	The threat event has been seen by AMC.
Expected	The threat event has been seen by the AMC’s peers or partners.
Anticipated	The threat event has been reported by AMC staff.
Predicted	The threat event has been predicted by a trusted source (i.e. AMC staff)..
Possible	The threat event has been described by a credible source (i.e. AMC staff)..
N/A	The threat event is not currently applicable.

Table B: Motivation Score Lookup Table

TABLE 7B: Look-Up table to estimate the qualitative value of Threat Agent/Source's Motivation				
Capability	**Intent**	**Targeting**	**Motivation Score**	**Motivation Score Explaination**
Very High	Very High	Very High	Very High	Adversary is almost certain to initiate the threat event
Very High	Very High	High	Very High	Adversary is almost certain to initiate the threat event
Very High	Very High	Moderate	High	Adversary is highly likely to initiate the threat event
Very High	Very High	Low	Moderate	Adversary is likely to initiate the treat event
Very High	Very High	Very Low	Moderate	Adversary is likely to initiate the treat event
Very High	High	Very High	Very High	Adversary is almost certain to initiate the threat event
Very High	High	High	Very High	Adversary is almost certain to initiate the threat event
Very High	High	Moderate	High	Adversary is highly likely to initiate the threat event
Very High	High	Low	Moderate	Adversary is likely to initiate the treat event
Very High	High	Very Low	Moderate	Adversary is likely to initiate the treat event
Very High	Moderate	Very High	High	Adversary is highly likely to initiate the threat event
Very High	Moderate	High	High	Adversary is highly likely to initiate the threat event
Very High	Moderate	Moderate	Moderate	Adversary is likely to initiate the treat event
Very High	Moderate	Low	Moderate	Adversary is likely to initiate the treat event
Very High	Moderate	Very Low	Moderate	Adversary is likely to initiate the treat event
Very High	Low	Very High	Moderate	Adversary is likely to initiate the treat event
Very High	Low	High	Moderate	Adversary is likely to initiate the treat event
Very High	Low	Moderate	Moderate	Adversary is likely to initiate the treat event
Very High	Low	Low	Low	Adversary is unlikely to initiate the threat event
Very High	Low	Very Low	Low	Adversary is unlikely to initiate the threat event
Very High	Very Low	Very High	Moderate	Adversary is likely to initiate the treat event
Very High	Very Low	High	Moderate	Adversary is likely to initiate the treat event
Very High	Very Low	Moderate	Low	Adversary is unlikely to initiate the threat event
Very High	Very Low	Low	Low	Adversary is unlikely to initiate the threat event
Very High	Very Low	Very Low	Low	Adversary is unlikely to initiate the threat event
High	Very High	Very High	Very High	Adversary is almost certain to initiate the threat event
High	Very High	High	Very High	Adversary is almost certain to initiate the threat event
High	Very High	Moderate	High	Adversary is highly likely to initiate the threat event
High	Very High	Low	Moderate	Adversary is likely to initiate the treat event
High	Very High	Very Low	Moderate	Adversary is likely to initiate the treat event
Moderate	Very High	Very Low	Moderate	Adversary is likely to initiate the treat event
Moderate	High	Very High	High	Adversary is highly likely to initiate the threat event
Moderate	High	High	High	Adversary is highly likely to initiate the threat event
Moderate	High	Moderate	Moderate	Adversary is likely to initiate the treat event
Moderate	High	Low	Moderate	Adversary is likely to initiate the treat event
Moderate	High	Very Low	Moderate	Adversary is likely to initiate the treat event
Moderate	Moderate	Very High	High	Adversary is highly likely to initiate the threat event
Moderate	Moderate	High	Moderate	Adversary is likely to initiate the treat event
Moderate	Moderate	Moderate	Moderate	Adversary is likely to initiate the treat event
Moderate	Moderate	Low	Moderate	Adversary is likely to initiate the treat event
Moderate	Moderate	Very Low	Moderate	Adversary is likely to initiate the treat event
Moderate	Low	Very High	Moderate	Adversary is likely to initiate the treat event
Moderate	Low	High	Moderate	Adversary is likely to initiate the treat event
Moderate	Low	Moderate	Moderate	Adversary is likely to initiate the treat event
Moderate	Low	Low	Low	Adversary is unlikely to initiate the threat event
Moderate	Low	Very Low	Low	Adversary is unlikely to initiate the threat event
Moderate	Very Low	Very High	Moderate	Adversary is likely to initiate the treat event
Moderate	Very Low	High	Moderate	Adversary is likely to initiate the treat event
Moderate	Very Low	Moderate	Moderate	Adversary is likely to initiate the treat event
Moderate	Very Low	Low	Low	Adversary is unlikely to initiate the threat event
Moderate	Very Low	Very Low	Low	Adversary is unlikely to initiate the threat event
Low	Very High	Very High	Moderate	Adversary is likely to initiate the treat event
Low	Very High	High	Moderate	Adversary is likely to initiate the treat event
Low	Very High	Moderate	Moderate	Adversary is likely to initiate the treat event
Low	Very High	Low	Low	Adversary is unlikely to initiate the threat event
Low	Very High	Very Low	Low	Adversary is unlikely to initiate the threat event
Low	High	Very High	Moderate	Adversary is likely to initiate the treat event
Low	High	High	Moderate	Adversary is likely to initiate the treat event
Low	High	Moderate	Moderate	Adversary is likely to initiate the treat event
Low	High	Low	Low	Adversary is unlikely to initiate the threat event
Low	High	Very Low	Low	Adversary is unlikely to initiate the threat event

Low	Moderate	Very High	Moderate	Adversary is likely to initiate the treat event
Low	Moderate	High	Moderate	Adversary is likely to initiate the treat event
Low	Moderate	Moderate	Moderate	Adversary is likely to initiate the treat event
Low	Moderate	Low	Low	Adversary is unlikely to initiate the threat event
Low	Moderate	Very Low	Low	Adversary is unlikely to initiate the threat event
Low	Low	Very High	Low	Adversary is unlikely to initiate the threat event
Low	Low	High	Low	Adversary is unlikely to initiate the threat event
Low	Low	Moderate	Low	Adversary is unlikely to initiate the threat event
Low	Low	Low	Low	Adversary is unlikely to initiate the threat event
Low	Low	Very Low	Very Low	Adversary is highly unlikely to initiate the threat event
Low	Very Low	Very High	Very Low	Adversary is highly unlikely to initiate the threat event
Low	Very Low	High	Very Low	Adversary is highly unlikely to initiate the threat event
Low	Very Low	Moderate	Very Low	Adversary is highly unlikely to initiate the threat event
Low	Very Low	Low	Very Low	Adversary is highly unlikely to initiate the threat event
Low	Very Low	Very Low	Very Low	Adversary is highly unlikely to initiate the threat event
Very Low	Very High	Very High	Moderate	Adversary is likely to initiate the treat event
Very Low	Very High	High	Moderate	Adversary is likely to initiate the treat event
Very Low	Very High	Moderate	Moderate	Adversary is likely to initiate the treat event
Very Low	Very High	Low	Moderate	Adversary is likely to initiate the treat event
Very Low	Very High	Very Low	Moderate	Adversary is likely to initiate the treat event
Very Low	High	Very High	Moderate	Adversary is likely to initiate the treat event
Very Low	High	High	Moderate	Adversary is likely to initiate the treat event
Very Low	High	Moderate	Moderate	Adversary is likely to initiate the treat event
Very Low	High	Low	Moderate	Adversary is likely to initiate the treat event
Very Low	High	Very Low	Moderate	Adversary is likely to initiate the treat event
Very Low	Moderate	Very High	Moderate	Adversary is likely to initiate the treat event
Very Low	Moderate	High	Low	Adversary is unlikely to initiate the threat event
Very Low	Moderate	Moderate	Low	Adversary is unlikely to initiate the threat event
Very Low	Moderate	Low	Low	Adversary is unlikely to initiate the threat event
Very Low	Moderate	Very Low	Low	Adversary is unlikely to initiate the threat event
Very Low	Low	Very High	Low	Adversary is unlikely to initiate the threat event
Very Low	Low	High	Low	Adversary is unlikely to initiate the threat event
Very Low	Low	Moderate	Low	Adversary is unlikely to initiate the threat event
Very Low	Low	Low	Low	Adversary is unlikely to initiate the threat event
Very Low	Low	Very Low	Very Low	Adversary is highly unlikely to initiate the threat event
Very Low	Very Low	Very High	Moderate	Adversary is likely to initiate the treat event
Very Low	Very Low	High	Low	Adversary is unlikely to initiate the threat event
Very Low	Very Low	Moderate	Very Low	Adversary is highly unlikely to initiate the threat event
Very Low	Very Low	Low	Very Low	Adversary is highly unlikely to initiate the threat event
Very Low	Very Low	Very Low	Very Low	Adversary is highly unlikely to initiate the threat event

Table C: Likelihood of Threat Initiation Look-Up Table

Ease of Exploitability	**Motivation of the Threat Agent/Source**				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Very Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

Likelihood of Threat Initiation Measures Explanation	
Very High	Threat is almost certain to be initiated
High	Threat will very likely be initiated

Moderate	Threat will likely be initiated
Low	Threat may be initiated
Very Low	Threat will likely not be initiated

Table D: Overall Likelihood of a Threat Event Look-Up Table					
Likelihood of Threat Event Initiation/Occurrence	**Likelihood Threat Events Result in Adverse Impacts**				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

Likelihood of Threat Event Measurement Explanation	
Very High	Threat event will happen
High	Threat event will most likely happen
Moderate	Threat event is likely to happen
Low	Threat event may happen
Very Low	Threat event is unlikely to happen

Table E: Risk Matrix					
Likelihood that Threat Events Occurs and Results in Adverse Impact	**FIV**				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Very Low	Moderate	High	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High

Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Very Low	Very Low

Level of Risk Measure Explanation	
Very High	A threat event could be expected to have multiple severe adverse effects on operations, assets, other organizations, and/or individuals.
High	A threat event can be expected to have a severe adverse effect on operations, assets, other organizations, and/or individuals.
Moderate	A threat event can be expected to have a serious effect on operations, assets, other organizations, or individuals.
Low	A threat event can be expected to have limited adverse effects on operations, assets, other organizations, or individuals.
Very Low	A threat event can be expected to have negligible adverse effect on operations, assets, other organizations, or individuals.