MOHAMMAD ASIM

MSc Cybersecurity

Risk Assessment Report

Table of Contents

1 Case Study

1.1 Name of the organization, Business description/Mission

Organization Name: MedSecure Health Systems (MSHS)

Business Type: Healthcare Provider

Location: Doha, Qatar

Mission:

MedSecure Health Systems is committed to delivering healthcare services integrated using advanced technologies such as Electronic Health Records (EHR), IoT-based patient monitoring, and Artificial Intelligence (AI) for diagnostic support. Its mission is to ensure timely, patient-centric while maintaining the highest standards in data privacy, security, and integrity. It aims to enhance patient outcomes and operational efficiency through innovation, positioning itself as a leader in healthcare delivery in the region.

1.2 Organization structure and business analysis

MSHS has a multi-faceted organizational structure that supports its mission of delivering advanced healthcare. The central business units are:

- **Clinical:** Doctors, nurses, radiology techs, and lab staff who care for patients and do diagnostics.
- **IT and Data:** These teams manage EHR systems, IT infrastructure, and DevOps to ensure technology integration and uptime.
- **Admin:** Finance, HR, and procurement teams that oversee operational and financial sustainability.
- **Research and Innovation:** Clinical trials and AI-driven diagnostic tools to create intellectual property and competitive advantage.
- **Cybersecurity and Compliance:** A dedicated team to ensure compliance with healthcare regulations (e.g., Qatar's National Health Strategy and international standards like HIPAA) and cyber threats.

Healthcare Technology Stack:

MSHS uses a technology-driven business model to deliver healthcare services. It's healthcare technology stack includes:

- EHR System: OpenEMR with HL7 interfaces for interoperability, patient records, diagnostics, and prescriptions.
- IoT Medical Devices: Real-time monitoring of patient vital signs (e.g., heart rate, oxygen levels) with alerts for clinical staff.
- Cloud Storage: Microsoft Azure for scalable and secure storage of patient data and backups.
- Internal LAN and Wi-Fi: For staff mobility and connectivity across the hospital.
- Patient Mobile App: Web-based portal for appointment booking telemedicine and access to test results.

This setup allows MSHS to integrate technology into patient care while maintaining operational resilience.

1.3 Threat landscape and threat agents

The healthcare sector, including MSHS, is facing a changing threat landscape. According to the *HIMSS 2023 Healthcare Cybersecurity Survey* and *CISA Alert AA22-117A,* cyber-attacks target healthcare providers, especially those using advanced technologies. Key threat actors are:

- **Organized Cybercriminal Groups:** Groups like FIN12 are known to deploy ransomware (e.g., Conti, Ryuk) against hospitals to extort money by encrypting EHRs.
- **State-Sponsored Actors:** Advanced Persistent Threats (APTs) like APT29 (Cozy Bear) target healthcare organizations for espionage, especially to steal proprietary research data (e.g., AI diagnostics).
- **Malicious Insiders:** Disgruntled employees or contractors with access to PHI may leak sensitive data for personal gain or revenge.
- **Hacktivists:** Motivated by political or bioethical agendas, they may launch

DDoS attacks or deface public-facing systems like the patient portal.

Major Threat Types:

- **Ransomware:** Denies access to critical systems, patient care at risk.
- **Phishing and Credential Theft:** Exploits human weakness.
- **Data Exfiltration:** Steals PHI for sale on the dark web or competitive advantage.
- **IoT Device Compromise:** Exploits medical device vulnerabilities to manipulate data or disrupt care.
- **DDoS:** Takes down a telemedicine platform or network.

1.4 Assets Identification and Critical Systems Description

MSHS's operations depend on various assets, each with varying levels of criticality. The table below identifies these assets, their types, descriptions, and criticality ratings:

Asset	Type	Description	Criticality
EHR System	Software/Data	Stores patient data, diagnostics, medications	Critical
IoT Medical Devices	Hardware	Real-time monitoring of patient vitals	Moderate
Patient Portal	Web Application	Patient access for bookings and results	High
Staff Credentials	Digital Identity	Authentication to systems and databases	Critical
Clinical Trial Research	Intellectual Property	Proprietary AI diagnostic research data	High
Hospital Network	IT System	Backbone for connectivity and operations	Critical
Backups	Storage	Recovery data for systems and records	Moderate

1.5 Asset Prioritization with Motivation

Asset prioritization reflects their importance to MSHS's mission and the impact of compromise. Here is the list in order:

1. **EHR System (Priority 1):** The primary target for ransomware because it holds PHI and enables patient care. Disruption means life-threatening delays.
2. **Staff Credentials (Priority 2):** The gateway to all systems; attackers get broad access to sensitive assets if phished successfully.
3. **Hospital Network Infrastructure (Priority 3):** Essential for business continuity; a DDoS attack or misconfiguration would bring the hospital to a halt.
4. **Clinical Trial Research Data (Priority 4):** High-value intellectual property for state-sponsored actors for espionage, but less immediate impact on care.
5. **Patient Portal (Priority 5):** A potential entry point for phishing or cross-site scripting (XSS), patient trust, and data integrity.
6. **IoT Medical Devices (Priority 6):** Critical for real-time patient monitoring; compromise could falsify data or disable alerts.
7. **Backups (Priority 7):** Important for recovery after an attack but less targeted; loss of backups amplifies the damage rather than initiates it.

This prioritization will guide the risk analysis by focusing on the assets most critical to MSHS's operations and strategy.

2 FACTOR ANALYSIS

Executive Summary

This section does a cybersecurity risk assessment for *MedSecure Health Systems (MSHS) on* the critical assets as listed in the previous Section: Electronic Health Record (EHR) System, Staff Credentials, and Hospital Network Infrastructure. For each asset, we list the relevant threat community, threat type, and effect, then do a detailed risk evaluation using the FAIR framework. Each value is also referenced or justified. Results are presented in tables, with risk matrices per asset-threat pair, to help MSHS prioritize its cybersecurity efforts.

2.1 Scope and Methodology

This section includes four assets at MSHS: EHR System, Staff Credentials, and Hospital Network Infrastructure. For each asset, we identify the threat community, threat type, and effect based on the healthcare context and recent threat intelligence. We use the FAIR ontology tree in this assessment to calculate risk:

- **Risk** = *ƒ* (LEF, Loss Magnitude (LM))
- **LEF** = *ƒ* (TEF, Vuln)
- **TEF** = *ƒ* (CF, PoA)
- **Vuln** = *ƒ* (TCap, Diff)

For this analysis, we simplify the function *TEF = ƒ (CF, PoA)* to *TEF* = *CF* × *PoA*, assuming a direct multiplicative relationship between *CF* and *PoA* and for the rest functions. This simplification is appropriate as no additional factors (e.g., dependencies or mitigating controls) are specified that would require a more complex function.

Estimates are annualized (per year), monetary values are in USD, and confidence levels reflect data reliability. All values are backed by references or assumptions with clear motivations.

2.2 Risk Assessment for Critical Assets

2.2.1 Asset 1: EHR System (OpenEMR-based)

2.2.1.1 Identification of Threat Community, Threat type and Effect

- **Threat Community:** *Cybercriminals*. The dark web is a hotbed for illegal activity, and healthcare data, especially patient records, are big bucks. Cybercriminals know the score and are the biggest threat to healthcare organizations today. As per IBM's *Cost of a Data Breach Report 2024,* the healthcare sector is a favourite target because of the value placed on personal health information.
- **Threat Type:** *Malicious*. These cybercriminals exploit vulnerabilities in healthcare systems to get unauthorized access to sensitive data. Once they

are in, they can steal, sell or hold patient information for ransom, often for financial gain. Exploiting these vulnerabilities can lead to serious breaches of trust and security.

- **Impact:** *Confidentiality*. The impact of these attacks is the breach of patient confidentiality. When unauthorized people get access to sensitive healthcare data, patient privacy is compromised, and trust in the healthcare system is broken. Exposure to personal health information can lead to identity theft, insurance fraud, and significant emotional distress for patients.

2.2.1.2 Risk Evaluation

Contact Frequency: *Contact Frequency (CF)* refers to the estimated number of potential cyberattack attempts on the Electronic Health Record (EHR) system over a specified period (typically one year). This metric is a crucial component of the overall risk evaluation, reflecting the frequency malicious actors could target the EHR system.

- **Estimation:** A study from 2024 indicated that 92% of healthcare firms experienced at least one cyberattack in the past year, with an average of 40 attacks annually [*Source: bankinfosecurity, https://www.bankinfosecurity.com/interviews/study-92-healthcare-hit-by-cyberattacks-this-year-embarged-till-5am-i-5419*]. Since the EHR system is a prime target, we assume *50%* of those attacks are on it, so a most likely CF of *20 attempts per year (40 × 0.5)*.
- **Discussion:** The high CF is because EHR data is so valuable to cybercriminals; healthcare records are worth big money on the dark web. Confidence is Moderate because we're using industry averages, not MSHS-specific data.
- **Rating:** High (10-100).

CF (times/year)	Minimum	Most Likely	Maximum	Confidence
	15	20	30	Moderate

Probability of Action: *Probability of Action (PoA)* is the likelihood a bad guy will exploit a vulnerability in the EHR system after it's found.

Rationale

- The 2024 Verizon Data Breach Investigations Report (DBIR) shows 14% of breaches in healthcare are due to vulnerability exploitation, up from the previous year. If a vulnerability isn't addressed, it's likely to be exploited. *[Source: Help Net Security, https://www.helpnetsecurity.com/2024/05/02/verizon-2024-data-breach-investigations-report-dbir/]*
- OpenEMR has known vulnerabilities, like *CVE-2023-2948* (Cross-site Scripting, XSS), which, if not patched, increases the PoA. *[Source: VumetricCyberPortal, https://cyber.vumetric.com/vulns/open-emr/openemr/5-0-0/]*
- Patching Practices: The PoA is heavily influenced by the organization's patch management. If patched timely, the PoA is lower; if delayed or neglected, the risk of exploitation is higher.

PoA (%)	Minimum	Most Likely	Maximum	Confidence
	50	70	90	Moderate

- **Estimation**
  - Most Likely PoA: 70% (0.7)
  - Range
    - Minimum PoA: 50% (if patched regularly)
    - Maximum PoA: 90% (if not patched or neglected)
  - **Discussion:** The presence of known vulnerabilities in OpenEMR and the increasing trend of vulnerability exploitation in cyberattacks underscores the importance of robust patch management practices. Organizations should prioritize timely updates and patches to mitigate the risk of exploitation.

Threat Event Frequency: Computing the *Threat Event Frequency (TEF)*: *TEF = CF × PoA*. Using the most likely values from our findings, *TEF = 20 × 0.7 = 14 times/year.*

- Minimum TEF: 15 × 0.5 = 7.5 times/year
- Maximum TEF: 30 × 0.9 = 27 times/year

TEF (times/year)	Minimum	Most Likely	Maximum	Confidence
	7.5	14	27	Moderate

We use the following table to rate the Threat Event Frequency (TEF) in our FAIR analysis

Rating	Description
Very High (VH)	> 100 times per year
High (H)	Between 10 and 100 times per year
Moderate (M)	Between 1 and 10 times per year
Low (L)	Between 0.1 and 1 times per year
Very Low (VL)	< 0.1 times per year

- **Rating:** High (10–100). High TEF due to high frequency of attacks (CF = 20) and high probability of exploitation (*PoA = 70%*) due to OpenEMR known vulnerabilities (e.g., CVE-2023-2948) and value of healthcare data on the dark web. We consider moderate confidence due to using industry averages for CF and assumptions about our MSHS patch management affecting PoA.

Threat Capability (TCap): Cybercriminals targeting the EHR system.

- **Estimation:** Cybercriminals targeting healthcare organizations are at 50th to 80th percentile, most likely at the **60th percentile**. This is because they use widely available exploit kits, which require moderate technical skills. *[Ref: https://www.isgtech.com/five-critical-cyber-stats-every-healthcare-leader-must-know/]*
- **Discussion:** Ransomware is common in healthcare, one in 42 healthcare organizations was hit in Q3 2022, according to *Check Point Software's* report *[Ref: Check Point Software, https://www.checkpoint.com/cyber-hub/cyber-security/what-is-healthcare-cyber-security/cyberattacks-on-the-healthcare-sector/]*. The cost of a data breach is over $10 million per incident *[Ref: RSM Global, https://www.rsm.global/insights/alarming-relationship-between-healthcare-and-cyber-attacks]*. Patient data in the EHR system is the primary target because it's highly valuable on the dark web. Phishing is the most common attack vector, 93% of malicious activity in healthcare, often paired with ransomware attacks *[Ref: HIPAA Times, https://hipaatimes.com/unpacking-healthcare-cybercriminal-tactics]*.

- **Confidence:** Confidence is Moderate because of the dynamic nature of cyber threats and relying on industry reports rather than MSHS-specific data.

Tcap (percentile)	Minimum	Most Likely	Maximum	Confidence
	50	60	80	Moderate

We use the following table to rate the Threat Capability (TCap) in our analysis:

Rating	Description
Very High (VH)	Top 2% when compared against the overall threat population
High (H)	Top 16% when compared against the overall threat population
Moderate (M)	Average skill and resources (between bottom 16% and top 16%)
Low (L)	Bottom 16% when compared against the overall threat population
Very Low (VL)	Bottom 2% when compared against the overall threat population

- **Rating:** High (51st–75th percentile). The 60th percentile indicates cybercriminals have above-average capabilities, using common but effective attack methods like exploit kits and phishing, which are particularly impactful in healthcare.

Difficulty (Diff): How hard to overcome (percentile).

- **Estimation:** OpenEMR's vulnerabilities (e.g., CVE-2023-2835) reduce difficulty if unpatched. MSHS has basic security (e.g., MFA), *Diff = 65 [Ref: NIST NVD, https://nvd.nist.gov/vuln/detail/CVE-2023-2835].*

- **Discussion**: 65 is moderate security for a healthcare provider of MSHS's size, based on the estimation of data.

Diff (percentile)	Minimum	Most Likely	Maximum	Confidence
	55	65	75	Moderate

We use the following table to rate the Difficulty in our analysis

Rating	Description
Very High (VH)	Protects against all but the top 2% of an average threat population
High (H)	Protects against all but the top 16% of an average threat population
Moderate (M)	Protects against the average threat agent
Low (L)	Only protects against bottom 16% of an average threat population
Very Low (VL)	Only protects against bottom 2% of an average threat population

- **Rating:** Moderate

Vulnerability (Vuln): Probability that the Target Capability (TCap) exceeds Difficulty (Diff).

- **Discussion**: The ***Vuln*** percentage is the balance between the attacker's skill (TCap) and the system's defenses (Diff).

Vulnerability

TCap \ Difficulty	VL	L	M	H	VH
VH	VH	VH	VH	H	M
H	VH	VH	H	M	L
M	VH	H	M	L	VL
L	H	M	L	VL	VL
VL	M	L	VL	VL	VL

Difficulty

We use the Risk Matrix above to calculate the Rating for Vulnerability.

- **Rating:** *High*. From the risk matrix, Cybercriminals have above-average capabilities, using standard but effective methods like exploit kits and phishing, which are particularly impactful in healthcare.

Loss Event Frequency (LEF): LEF = TEF × Vuln = 14 × 0.4 = 5.6 times/year.

LEF (times / year)	Minimum	Most Likely	Maximum	Confidence
	1.5	5.6	16.2	Moderate

- **Discussion:** High LEF means attacks will happen. This is the combination of TEF and Vuln. LEF is the frequency of loss events. 1.5 is lower attack frequency and lower vulnerability. 16.2 is a higher attack frequency and vuln. 5.6 is the most likely scenario based on current assumptions. Confidence is Moderate because TEF and Vuln can change based on attack methods, security environment, and incident response.

Loss Event Frequency

Threat Event Frequency	VL	L	M	H	VH
VH	M	H	VH	VH	VH
H	L	M	H	H	H
M	VL	L	M	M	M
L	VL	VL	L	L	L
VL	VL	VL	VL	VL	VL

Vulnerability

Loss Magnitude (LM): Cost per event (Primary Loss Magnitude, PLM)

- Estimation: *IBM 2024* reports the average healthcare breach cost as $10.1M for 1.5M records, or $6.73/record *[Ref: IBM, https://www.ibm.com/reports/data-breach].*

For the purposes of this assessment, a smaller-scale breach scenario is considered to reflect a more realistic loss event for MSHS. The cost components are broken down into:

- **Direct Costs:** Fixed at **$3,365**, covering investigation and immediate

containment.

- **Response Costs:** These include regulatory reporting, patient notification, legal consultation, and reputational recovery efforts.

Response costs are estimated as follows, with an adjustment for 2025 inflation (3% annual):

Cost Category	Original Estimate	Inflation Adjustment (3%)	Adjusted Cost (2025)
Minimum	$2,750	$2,750 × 1.03	$2,833
Most Likely	$58,250	$58,250 × 1.03	$60,000
Maximum	$222,000	$222,000 × 1.03	$228,660

These figures reflect the variability in potential incident response efforts, depending on breach scope, regulatory environment, and public exposure.

- **Discussion:** Response costs dominate due to legal and notification expenses in healthcare breaches. Confidence is Moderate due to the inflation adjustment and generalized data.

Loss Type	PLM Minimum	PLM Most Likely	PLM Maximum	Confidence
Response	$2,833	$60,000	$228,660	Moderate

We use the following table to rate the Magnitude of our analysis.

Magnitude	Range Low End	Range High End
Very High (VH)	$1M	-
High (H)	$100K	$1M
Moderate (M)	$10K	$100K
Low (L)	$1K	$10K
Very Low (VL)	$0	$1K

- **Rating:** Moderate. ($10K - $100K)

Risk: Risk = LEF × LM = 5.6 × $60,000 = $336,000/year.

Risk ($/year)	Minimum	Most Likely	Maximum	Confidence
	$4249.5	$336,000	$3,704,292	Moderate

- **Discussion**: The Moderate risk rating reflects a significant but manageable threat to the EHR system, driven by frequent attacks and moderate vulnerability.
- **Risk Matrix**

Risk

Loss Magnitude	VL	L	M	H	VH
VH	M	H	VH	VH	VH
H	L	M	H	H	H
M	VL	L	M	M	M
L	VL	VL	L	L	L
VL	VL	VL	VL	VL	VL

Loss Event Frequency

2.2.2 Staff Credentials

2.2.2.1 Identification of Threat Community, Threat Type, and Effect

- **Threat Community**: *Cybercriminals.* Cybercriminals, including organized crime and nation-state actors, are targeting healthcare organizations. They want to get staff credentials to get into sensitive systems and data. The healthcare sector has a treasure trove of personal health information, so it's a big target for these malicious activities.
- **Threat Type**: *Phishing.* Phishing is the primary method used by malicious actors. Phishing involves deceptive communications, often pretending to be a legitimate entity, to get staff to give up their login credentials. Email

spoofing, fake websites, and social engineering are used to make these phishing attempts more believable.

- **Impact**: *Confidentiality.* Compromised staff credentials are a big threat to healthcare data. Unauthorized access from stolen credentials can lead to massive data breaches, exposing patient information and disrupting critical healthcare services. Breaches violate patient privacy and have legal and financial implications for the affected organizations.

2.2.2.2 Risk Evaluation

Contact Frequency

- **Estimate**: Healthcare organizations get phished. While exact numbers vary monthly, data shows many healthcare organizations get phished yearly.
- **Discussion**: Phishing is one of healthcare's most common cyberattacks. A 2025 survey found that 63% of organizations with on-premises infrastructure got phished in the last year. *[Ref: The HIPAA Journal, https://www.hipaajournal.com/84-of-healthcare-organizations-detected-a-cyberattack-in-the-past-12-months/].* Phishing was also the most common type of cyber attack among U.S. healthcare organizations. The frequency of these attacks means you need robust security and continuous staff training to mitigate risk. *[Ref: MedCity News, https://medcitynews.com/2020/11/phishing-attacks-most-common-cybersecurity-incident-at-us-healthcare-organizations/]*

CF (times/year)	Minimum	Most Likely	Maximum	Confidence
	8	12	16	High

We use the following table to rate the Contact Frequency in our analysis

Rating	Description
Very High (VH)	> 100 times per year
High (H)	Between 10 and 100 times per year
Moderate (M)	Between 1 and 10 times per year
Low (L)	Between 0.1 and 1 times per year
Very Low (VL)	< 0.1 times per year

- **Rating:** High (10-100)

- **Confidence**: High, based on multiple industry reports and surveys supported by references.

Probability of Action

- **Estimation**: 50% of phishing attempts result in credential theft. *[Ref: Verizon, https://www.verizon.com/business/resources/reports/2024-dbir-executive-summary.pdf]*
- **Discussion:** The success rate of phishing attacks can be influenced by staff training, awareness programs, and security measures like MFA. Despite this, phishing is still a big threat. For example, a 2024 report said 94% of organizations were phished, and 96% were impacted *[Ref: GlobeNewsWire, https://www.globenewswire.com/en/news-release/2024/01/16/2809607/0/en/New-report-reveals-that-94-of-global-organizations-have-experienced-email-security-incidents-last-year.html].* The *2024 Verizon Data Breach Investigations Report (DBIR)* said the median time to click on a phishing link after opening an email was less than 60 seconds. Therefore, Phishing is very fast. *[Ref: Verus, https://veruscorp.com/stolen-credentials-and-the-60-second-phishing-trap-key-findings-from-the-2024-dbir/]*

PoA (%)	Minimum	Most Likely	Maximum	Confidence
	30	50	70	High

- **Confidence:** High, based on industry reports and studies.

Threat Event Frequency (TEF): *TEF = Contact Frequency (CF) × Probability of Action (PoA)*

- **Discussion:** The *Threat Event Frequency (TEF)* is the estimated number of times cybercriminals will target staff credentials per year in healthcare organizations. The TEF values suggest healthcare organizations may experience between 2-11 phishing incidents per year that could compromise staff credentials. This range considers the variation in phishing attempts and the effectiveness of organizational defenses and staff awareness programs.

TEF (times/year)	Minimum	Most Likely	Maximum	Confidence
	2.4	6	11.2	High

- **Confidence:** High, based on industry data on phishing attack rates and success rates in healthcare.

We use the following table to rate the Threat Event Frequency (TEF) in our FAIR analysis

Rating	Description
Very High (VH)	> 100 times per year
High (H)	Between 10 and 100 times per year
Moderate (M)	Between 1 and 10 times per year
Low (L)	Between 0.1 and 1 times per year
Very Low (VL)	< 0.1 times per year

- **Rating:** Moderate (1-10)

Threat Capability (TCap)

- **Estimation:** Phishing attacks on staff credentials through phishing campaigns are 60%.
- **Discussion:** Threat actor capability varies. *[Ref: Connor's Personal Blog, https://cmooneycollett.github.io/2023/07/23/five-dimensions-cyber-threat-actor].* Many have the skills to run effective phishing campaigns; some use advanced techniques to increase success rates. For example, a 2024 report found that threat actors are creating targeted, sophisticated phishing emails, 30.4 million of which were seen in a year. They use new social engineering techniques like AI-generated text and QR codes to bypass traditional security. CaaS (cybercrime as a service) platforms have lowered the barrier to entry so less skilled actors can run complex attacks. *[Ref: Security, https://www.securitymagazine.com/articles/101405-phishing-remains-the-preferred-technique-among-threat-actors]*

Tcap (percentile)	Minimum	Most Likely	Maximum	Confidence
	50	60	80	Moderate

- **Confidence:** Moderate as attacker skill varies and phishing techniques evolve.

We use the following table to rate the Threat Capability (TCap) in our analysis:

Rating	Description
Very High (VH)	Top 2% when compared against the overall threat population
High (H)	Top 16% when compared against the overall threat population
Moderate (M)	Average skill and resources (between bottom 16% and top 16%)
Low (L)	Bottom 16% when compared against the overall threat population
Very Low (VL)	Bottom 2% when compared against the overall threat population

- **Rating:** High

Difficulty

- **Estimation:** Assuming the implementation of Multi-Factor Authentication (MFA), the difficulty for attackers to successfully compromise staff credentials is estimated at the 70th percentile.
- **Range**

Percentile	Description
60th	Basic MFA implementation (e.g., SMS-based codes); susceptible to interception and social engineering
70th	Standard MFA deployment using authenticator apps; offers enhanced security against common phishing attacks
80th	Advanced MFA solutions incorporating biometric verification and adaptive authentication mechanisms

- **Discussion**: MFA makes it much harder for attackers to get staff credentials. According to *arXiv*, MFA is great; 99.99% of MFA-enabled accounts were secure during the test period *[Ref: arXiv, https://arxiv.org/abs/2305.00945].* However, MFA can be effective or not, depending on how it's implemented. For example, SMS MFA is more vulnerable to SIM-swapping, while authenticator apps are more secure according to New York Post *[Ref: New York Post, https://nypost.com/2024/12/19/tech/feds-issue-another-warning-about-texting-dangers-the-*

scary-reason-to-stop-using-two-factor-authentication-now]. User resistance, integration complexity, and inconsistent deployment across systems can also impact MFA solutions at Security Boulevard. *[Ref: Security Boulevard, https://securityboulevard.com/2022/04/top-8-pitfalls-of-implementing-mfa-in-2022-and-how-to-avoid-them].*

Diff (percentile)	Minimum	Most Likely	Maximum	Confidence
	60	70	80	Moderate

- **Confidence**: Moderate (assuming uniform and robust MFA deployment across our organisation).

We use the following table to rate the difficulty of our analysis

Rating	Description
Very High (VH)	Protects against all but the top 2% of an average threat population
High (H)	Protects against all but the top 16% of an average threat population
Moderate (M)	Protects against the average threat agent
Low (L)	Only protects against bottom 16% of an average threat population
Very Low (VL)	Only protects against bottom 2% of an average threat population

- **Rating:** High

Vulnerability

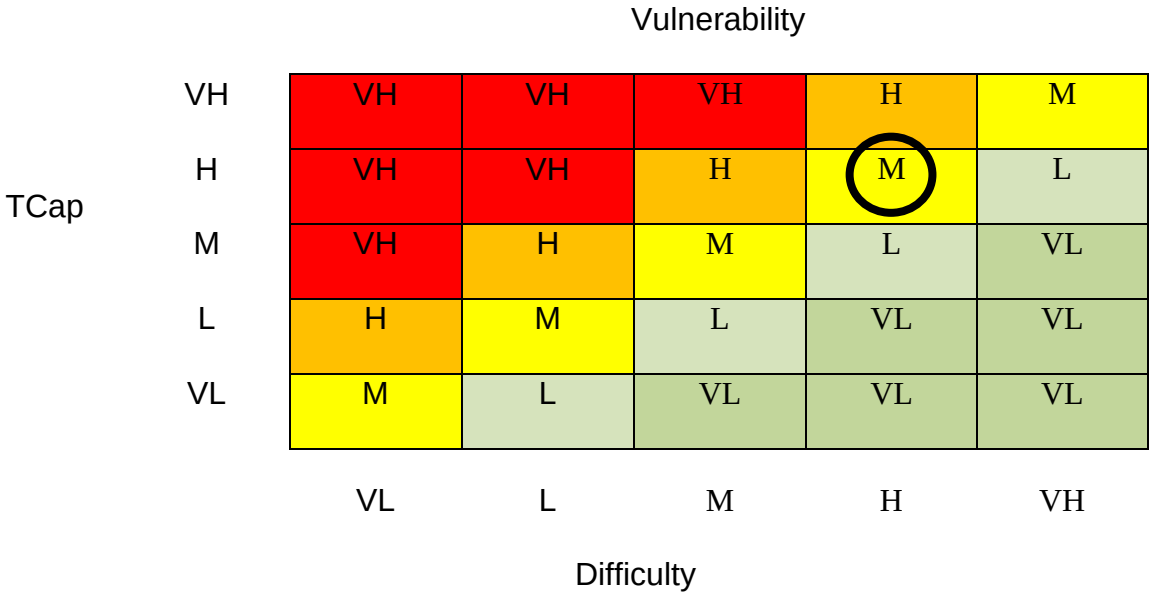
- **Calculation:** Vulnerability is calculated by comparing Threat Capability (TCap) against an attack's Difficulty (Diff).

Scenario	Threat Capability (TCap)	Difficulty (Diff)	Estimated Vulnerability (%)
Minimum	50th percentile	80th percentile	20%
Most Likely	60th percentile	70th percentile	30%
Maximum	80th percentile	60th percentile	50%

- **Discussion:** MFA makes it harder for attackers, but it's only good for implementation and user compliance. In the healthcare industry, MFA

adoption rates vary; larger organizations are more likely to have robust MFA solutions than smaller ones *JumpCloud* *[Ref: JumpCloud, https://jumpcloud.com/blog/multi-factor-authentication-statistics].* Phishing attacks have gotten more sophisticated; threat actors are using advanced techniques to bypass MFA, like phishing-resistant MFA bypass techniques Proofpoint. *[Ref: Proofpoint, https://www.proofpoint.com/us/resources/threat-reports/state-of-phish].* So, even in environments where MFA is deployed, there is still a residual vulnerability.

- **Confidence**: Moderate since MFA adoption varies across organizations and threat actors are getting more advanced.



- **Rating:** Moderate

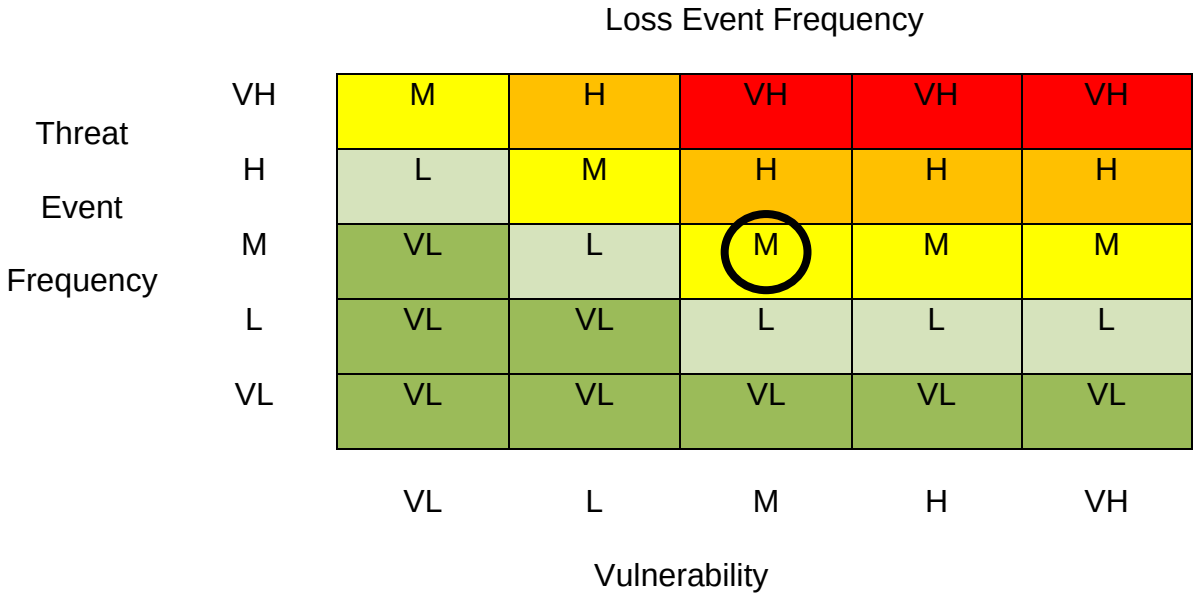
Loss Event Frequency (LEF)

- **Calculation:** Using the FAIR (Factor Analysis of Information Risk) model, Loss Event Frequency (LEF) is the expected number of times a loss event (e.g. credential compromise) will occur in a given timeframe.
    - LEF = TEF × Vuln

Scenario	TEF (Events/Year)	Vulnerability (%)	LEF (Events/Year)
Minimum	2.4	20%	0.48
Most Likely	6.0	30%	1.8

Scenario	TEF (Events/Year)	Vulnerability (%)	LEF (Events/Year)
Maximum	11.2	50%	5.6

- **Discussion**: The calculated LEF indicates a moderate frequency of loss events due to credential compromise in the healthcare industry. Phishing attacks and MFA are big factors in this. MFA reduces vulnerability but inconsistent deployment, user non-compliance and sophisticated phishing can still lead to credential theft.
- **Confidence**: Moderate, given the variability in threat actor capability and the organization's security posture.



- **Rating:** Moderate

Loss Magnitude

- **Estimation**: Credential theft in healthcare can lead to big financial losses due to the sensitive nature of the data and regulatory requirements. According to the *IBM Cost of a Data Breach Report 2024*, the average cost of a healthcare data breach is $9.77 million for the 14th year in a row. *[Ref: TechTarget, https://www.techtarget.com/healthtechsecurity/news/366599336/Average-cost-of-a-healthcare-data-breach-sits-at-977M]* While big breaches can cost millions, smaller ones like staff credential compromises can still cost a lot.

Scenario	Estimated Cost (USD)
Minimum	$2,833
Most Likely	$60,000
Maximum	$228,660

- **Discussion**: The financial impact of credential theft in healthcare is multifaceted. Direct costs are incident response, forensic investigation, legal fees, regulatory fines and patient notification. Indirect costs are reputational damage, loss of patient trust and business disruption. For example, the 2024 ransomware attack on UnitedHealth Group's Change Healthcare unit, facilitated by compromised credentials, resulted in system outages and a $22 million ransom payment. These types of incidents show how credential compromises can escalate into big breaches with big financial consequences.
- **Confidence**: Moderate, given the variability of breach outcomes and the changing threat landscape.

We use the following table to rate the Magnitude of our analysis.

Magnitude	Range Low End	Range High End
Very High (VH)	$1M	-
High (H)	$100K	$1M
Moderate (M)	$10K	$100K
Low (L)	$1K	$10K
Very Low (VL)	$0	$1K

- **Rating**: Moderate ($10K - $100K)

Risk

- **Calculation**: In accordance with the FAIR (Factor Analysis of Information Risk) model, the annualized risk is determined by multiplying the Loss Event Frequency (LEF) by the Loss Magnitude (LM):
    - Risk = LEF × LM

Scenario	LEF (Events/Year)	LM (USD)	Annualized Risk (USD)
Minimum	0.48	$2,833	$1,360
Most Likely	1.8	$60,000	$108,000
Maximum	5.6	$228,660	$1,280,496

- **Discussion**: The annualized risk is $1,360 - $1.28 million with a most likely of $108,000. This is the financial impact of credential compromise in the healthcare industry. The range is driven by phishing attacks, MFA effectiveness, and large data breaches from compromised credentials.

  The FAIR model allows for a quantitative approach to risk assessment so organizations can express risk in financial terms. This helps with prioritization and resource allocation. *[Ref: Balbix, https://www.balbix.com/insights/fair-model-for-risk-quantification-pros-and-cons]*

- **Confidence**: Moderate as the variability is high in both frequency of credential compromise and financial impact.

- **Categorization**: Based on the FAIR model risk matrix where both LEF and LM are Moderate, the overall risk is:

  Moderate × Moderate = Moderate Risk

  This means the risk is not zero but is within a manageable range if proper security controls are in place and maintained.

Risk

Loss Magnitude	VL	L	M	H	VH
VH	M	H	VH	VH	VH
H	L	M	H	H	H
M	VL	L	M	M	M
L	VL	VL	L	L	L
VL	VL	VL	VL	VL	VL

Loss Event Frequency

2.2.3 Asset 3: Hospital Network Infrastructure

2.2.3.1 Identification of Threat Community, Threat Type, and Effect

- **Threat Community**: *Nation State Actors.* Nation-state actors are increasingly targeting healthcare infrastructure, including hospital networks, for espionage, data theft, and disruption of critical services. Notably, state-sponsored groups from countries like China, North Korea, and Iran have been involved in cyberattacks against healthcare entities. For example, the Health Sector Cybersecurity Coordination Center (HC3) has identified Chinese and North Korean state-sponsored groups targeting US healthcare organizations. *[Ref: BHR, https://www.beckershospitalreview.com/healthcare-information-technology/cybersecurity/the-2-nation-state-actors-targeting-us-healthcare].* Additionally, the Cybersecurity and Infrastructure Security Agency (CISA) has issued alerts on Iranian government-sponsored advanced persistent threat (APT) groups exploiting known Microsoft Exchange and Fortinet vulnerabilities to target the healthcare sector. *[Ref: Healthcare IT News, https://www.healthcareitnews.com/news/cisa-issues-alert-iran-sponsored-hacker-group-targeting-healthcare]*
- **Threat Type**: *Malicious.* These threats are malicious and strategic. Nation-state actors use sophisticated cyber attack techniques, including APTs, to breach hospital networks. Their goals often include stealing sensitive patient data, intellectual property, and research information, and disrupting healthcare services. They may also use ransomware attacks, sometimes in conjunction with cybercriminal organizations, to cover their tracks and achieve their strategic objectives.health-isac.org. *[Ref: Health-ISAC, https://health-isac.org/health-isacs-first-annual-current-and-emerging-healthcare-cyber-threat-landscape-executive-summary]*
- **Effect**: *Availability and Confidentiality.* Breach of hospital network infrastructure by nation-state actors can have a severe impact on both availability and confidentiality.
    - **Availability**: Disruption to hospital networks can block access to critical systems, delay medical procedures, and compromise patient care. For example, the 2021 ransomware attack on Ireland's Health Service Executive (HSE) shut down all IT systems nationwide and

caused significant disruption to healthcare services. *[Ref: Wikipedia, https://en.wikipedia.org/wiki/Health_Service_Executive_ransomware_attack]*

- **Confidentiality**: Unauthorized access to hospital networks can result in exfiltration of sensitive patient data, research information and other confidential materials. The 2018 SingHealth data breach in Singapore, attributed to state-linked actors, resulted in the theft of the personal data of 1.5 million patients, including the Prime Minister. *[Ref: Wikipedia, https://en.wikipedia.org/wiki/2018_SingHealth_data_breach]*

2.2.3.2 Risk Evaluation

Contact Frequency (CF)

- **Estimation**: According to the *Sophos* report "The State of Ransomware in Healthcare 2024," 67% of healthcare organizations experienced ransomware attacks in the past year, marking a four-year high *[Ref: SOPHOS, https://www.sophos.com/en-us/press/press-releases/2024/09/two-thirds-healthcare-organizations-hit-ransomware-four-year-high]*. This translates to approximately two-thirds of healthcare entities facing at least one ransomware incident annually. While the report does not specify the exact number of attacks per month, the high percentage indicates a significant frequency of attempted breaches targeting hospital network infrastructures.
- **Range**

Scenario	Estimated CF (Attacks/Year)
Minimum	12
Most Likely	24
Maximum	36

Note: These estimates are derived from industry observations and the increasing trend of ransomware attacks in the healthcare sector.

- **Discussion:** The healthcare industry has a big attack surface with many connected systems and devices, so it's a prime target for hackers. Ransomware attacks are becoming more sophisticated, and healthcare is

critical, so the impact of a breach is huge. The frequency of attacks means you need robust security and continuous monitoring.

- **Confidence:** *High*. This is backed by recent data showing a significant increase in ransomware attacks in the healthcare industry.

We use the following table to rate the Contact Frequency in our analysis

Rating	Description
Very High (VH)	> 100 times per year
High (H)	Between 10 and 100 times per year
Moderate (M)	Between 1 and 10 times per year
Low (L)	Between 0.1 and 1 times per year
Very Low (VL)	< 0.1 times per year

- **Rating:** High (10–100). Given the number of attacks reported every year, the contact frequency is high, and the threat to the hospital network is persistent.

Probability of Action

- **Estimation:** Nation-state and APT groups are targeting healthcare organizations, exploiting network infrastructure vulnerabilities. While numbers vary, the sophistication and persistence of these actors mean there's a high likelihood of successful exploitation.
- **Range**

Scenario	Estimated PoA (%)
Minimum	40
Most Likely	50
Maximum	60

- **Discussion:** Nation-state actors want to exploit hospital network infrastructure vulnerabilities. Their goals are intel gathering, disruption of critical services and data theft. Healthcare's complex and sometimes outdated systems make it a prime target for these adversaries. The persistence of these threats means robust cybersecurity and continuous

monitoring is key.

- **Confidence:** High. This is backed up by multiple reports of ongoing and targeted attacks on healthcare organizations.

Threat Event Frequency (TEF)

- **Calculation:** *Threat Event Frequency (TEF) = Contact Frequency (CF) x Probability of Action (PoA)*

  According to recent stats, the healthcare industry has seen a lot of cyberattacks. *[Ref: SOCRadar, https://socradar.io/biggest-healthcare-industry-attacks-2023-2024].* 725 large healthcare data breaches in 2024, 3rd year in a row with over 700 breaches *[Ref: Healthcare Facilities Today, https://www.healthcarefacilitiestoday.com/posts/Report-Sheds-Light-on-Cyberattack-and-Data-Breach-Trends-from-2024--30052]*. That's a persistent threat to hospital network infrastructure.

- **Range**

Scenario	Contact Frequency (CF)	Probability of Action (PoA)	TEF (Attacks/Year)
Minimum	18	0.40	7.2
Most Likely	24	0.50	12.0
Maximum	30	0.60	18.0

- **Discussion:** The high TEF is due to the fact that hospital network infrastructures are being targeted by sophisticated threat actors. The healthcare sector has a large attack surface with many connected systems and devices, so it is a prime target for attackers. Ransomware attacks are getting more sophisticated, and healthcare services are critical, so the impact of a breach is higher. These threats are persistent, so robust security and continuous monitoring are key.

- **Confidence:** High. This is backed up by multiple reports of ongoing and

targeted attacks on healthcare organizations.

We use the following table to rate the Threat Event Frequency (TEF) in our FAIR analysis

Rating	Description
Very High (VH)	> 100 times per year
High (H)	Between 10 and 100 times per year
Moderate (M)	Between 1 and 10 times per year
Low (L)	Between 0.1 and 1 times per year
Very Low (VL)	< 0.1 times per year

- **Rating:** High (10–100). Given the number of attacks reported every year, the threat event frequency is high, and hospital network infrastructures are under persistent threat.

Threat Capability (TCap)

- **Estimation:** Nation-state actors, APT groups, are known for their advanced cyber capabilities. They have advanced tools and techniques, and zero-day exploits, and have shown that they can compromise critical infrastructure networks. Their ops are long-term network/system intrusions for espionage, data theft, and service disruption. *[Ref: CISA, https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors].*
- **Range**

Scenario	Estimated TCap (Percentile)
Minimum	80
Most Likely	90
Maximum	95

- **Discussion:** High Threat Capability means nation-state actors have advanced skills and resources. Their ability to do sophisticated cyber ops is

a big risk to hospital network infrastructures, which are part of the critical healthcare sector. The persistence of these threats means we need robust cybersecurity and continuous monitoring.

- **Confidence:** High. This is supported by sources that show advanced threat actors are ongoing and targeting critical infrastructure sectors, including healthcare.*[Ref: CISA, https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china]*

We use the following table to rate the Threat Capability (TCap) in our analysis:

Rating	Description
Very High (VH)	Top 2% when compared against the overall threat population
High (H)	Top 16% when compared against the overall threat population
Moderate (M)	Average skill and resources (between bottom 16% and top 16%)
Low (L)	Bottom 16% when compared against the overall threat population
Very Low (VL)	Bottom 2% when compared against the overall threat population

- **Rating:** Very High

Difficulty

- **Estimation:** Firewalls and network segmentation are key in healthcare cybersecurity. According to *NIST Special Publication 800-41 Revision 1*, "Guidelines on Firewalls and Firewall Policy," firewalls are for protecting network boundaries and controlling traffic flow. *[Ref:NIST, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-41r1.pdf].* NIST Cybersecurity Framework (CSF) also emphasizes network segmentation as a way to limit the impact of a cybersecurity event *[Ref: NIST CSF, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf].* Assuming these controls are in place, the difficulty for attackers is 75%.

- **Range**

Scenario	Estimated Difficulty (Percentile)
Minimum	65
Most Likely	75

Scenario	Estimated Difficulty (Percentile)
Maximum	85

- **Discussion:** Standard network defenses like firewalls and segmentation make it harder for attackers, but nation-state actors have advanced capabilities to get around these. NIST CSF says sophisticated attackers will find a way to exploit vulnerabilities despite existing controls. So, while these controls make it harder, they don't eliminate the risk from highly skilled threat actors. *[Ref: The HIPAA Journal, https://www.hipaajournal.com/hscc-hhs-guide-healthcare-nist-cybersecurity-framework]*
- **Confidence:** *Moderate*. This is based on the assumption that standard controls are in place and managed *[Ref: Qstream, https://qstream.com/content-library/nist-cybersecurity-framework-for-healthcare/].* Variations in implementation and management across healthcare organizations introduce uncertainty.

We use the following table to rate the difficulty of our analysis

Rating	Description
Very High (VH)	Protects against all but the top 2% of an average threat population
High (H)	Protects against all but the top 16% of an average threat population
Moderate (M)	Protects against the average threat agent
Low (L)	Only protects against bottom 16% of an average threat population
Very Low (VL)	Only protects against bottom 2% of an average threat population

- **Rating:** High (75% Percentile)

Vulnerability

- **Estimation:** Vuln is the likelihood a threat actor can exploit a system, considering their capabilities and the system's defenses. With nation-state actors having high TCap and standard healthcare network defenses being moderate Diff, the vuln is:

Scenario	Threat Capability (TCap)	Difficulty (Diff)	Estimated Vulnerability (%)
Minimum	80	85	50
Most Likely	90	75	70
Maximum	95	65	90

- **Discussion:** Nation-state actors have advanced capabilities, including zero-day exploits and sophisticated attack vectors. They have long-term network intrusions for espionage, data theft, and service disruption. The healthcare sector has complex and sometimes outdated systems that increase the attack surface and are prime targets for these adversaries. Standard network defenses like firewalls and segmentation increase the difficulty for attackers but may not be enough against highly skilled threat actors. The persistence of these threats means robust cybersecurity and continuous monitoring is key.
- **Confidence:** Moderate. This is based on sources that show advanced threat actors are targeting healthcare organizations. However, variations in the implementation and maintenance of security controls across healthcare organizations introduce uncertainty. *[Ref: CISA,https://www.cisa.gov/news-events/cybersecurity-advisories].*

Vulnerability

TCap	VL	L	M	H	VH
VH	VH	VH	VH	H	M
H	VH	VH	H	M	L
M	VH	H	M	L	VL
L	H	M	L	VL	VL
VL	M	L	VL	VL	VL

Difficulty

Loss Event Frequency

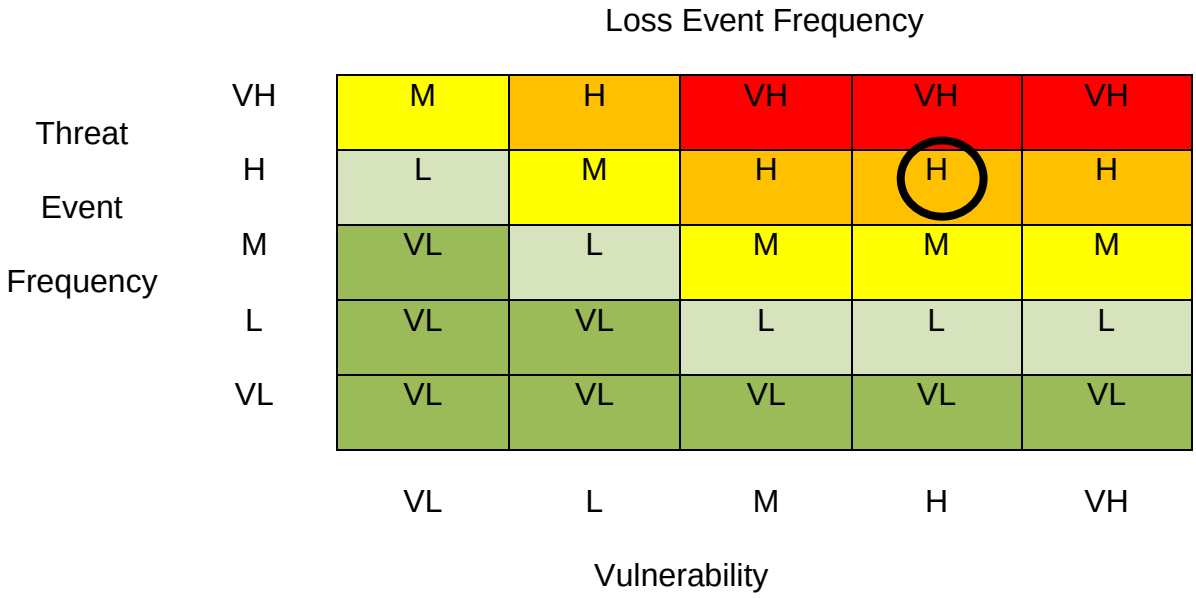
- **Calculation:** *Loss Event Frequency (LEF) = Threat Event Frequency (TEF) x Vulnerability (Vuln)*

  According to recent data, the healthcare industry has seen a lot of cyber attacks. For example, in 2024, *Health-ISAC* reported 458 ransomware attacks in the healthcare industry, so the threat landscape for hospital networks is ongoing. *[Ref: TechTarget, https://www.techtarget.com/healthtechsecurity/news/366619250/Healthcare-cyberattacks-continue-to-escalate-in-2025]*

- Range

Scenario	TEF (Attacks/Year)	Vulnerability (%)	LEF (Successful Attacks/Year)
Minimum	7.2	50	3.6
Most Likely	12.0	70	8.4
Maximum	18.0	90	16.2

- **Discussion:** The healthcare industry has a large attack surface with many connected systems and devices, so it's a prime target for attackers. Ransomware is getting more sophisticated, and healthcare is critical, so the impact of a breach is high. The ongoing nature of these threats means that strong cybersecurity and continuous monitoring are required.
- **Confidence:** Moderate. This is based on credible sources of advanced threat actors targeting healthcare organizations. However, variations in security controls across healthcare organizations introduce uncertainty.
- **Rating:** High. With so many attacks reported annually, the loss event frequency is High, and the threat to hospital networks is ongoing.



Loss Magnitude

- **Estimation:** Cyber-attacks on hospital network infrastructure can be costly in terms of operational disruption and data breach.
  - **Operational Disruption**: Data center outages, which are critical to hospital operations, are getting more expensive. A 2016 *Ponemon Institute* and *Emerson Network Power* study found the average cost of a data center outage was $740,357, with the cost per minute of downtime at $9,000.
  - **Data Breach**: The healthcare industry still has the highest cost of data breach. According to the *2024 IBM* and *Ponemon Institute report*, the average cost of a healthcare data breach was $9.8 million.
- **Range**

Scenario	Estimated Loss Magnitude (USD)
Minimum	$20,000
Most Likely	$100,000
Maximum	$500,000

- **Discussion**: The high Loss Magnitude reflects the significant financial repercussions of cyberattacks on hospital networks. Operational disruptions can halt critical healthcare services, while data breaches can lead to substantial costs related to data recovery, legal liabilities, and reputational damage. The reliance on interconnected digital systems in healthcare amplifies the potential impact of such cyber incidents.
- **Confidence**: Moderate. While the estimates provided are based on authoritative sources, actual costs can vary widely depending on the specific circumstances of each incident.

We use the following table to rate the Magnitude of our analysis.

Magnitude	Range Low End	Range High End
Very High (VH)	$1M	-
High (H)	$100K	$1M
Moderate (M)	$10K	$100K
Low (L)	$1K	$10K
Very Low (VL)	$0	$1K

- **Rating**: High. Given the potential for significant financial and operational impact, the Loss Magnitude is rated as high.

Risk

- **Calculation**: Risk is calculated by multiplying the Loss Event Frequency (LEF) by the Loss Magnitude (LM):

Risk = LEF × LM

- **Risk ($/year)**

Scenario	Estimated Annual Risk (USD)
Minimum	$72,000

Scenario	Estimated Annual Risk (USD)
Most Likely	$840,000
Maximum	$8,100,000

- **Categorization**: Given the High LEF and High LM, the overall risk is categorized as **High**.
- **Discussion**: The healthcare sector continues to face significant financial repercussions from cyberattacks. According to *IBM's 2024 Cost of a Data Breach Report*, the average cost of a data breach in healthcare was $9.77 million, maintaining its position as the most expensive industry for data breaches for the 14th consecutive year. *[Ref: TechTarget, https://www.techtarget.com/healthtechsecurity/news/366599336/Average-cost-of-a-healthcare-data-breach-sits-at-977M?utm_source=chatgpt.com].* These costs encompass various factors, including operational disruptions, data recovery, legal liabilities, and reputational damage. The reliance on interconnected digital systems in healthcare amplifies the potential impact of such cyber incidents.
- **Confidence**: Moderate. The provided estimates are based on authoritative sources.

Risk

Loss Magnitude	VL	L	M	H	VH
VH	M	H	VH	VH	VH
H	L	M	H	H	H
M	VL	L	M	M	M
L	VL	VL	L	L	L
VL	VL	VL	VL	VL	VL

Loss Event Frequency

2.3 Discussion and Recommendations

The Hospital Network is at the highest risk due to nation-state actors and downtime/data breach. EHR, Staff Credentials are moderate risk due to cybercriminals exploiting for financial gain.

Recommendations:

1 Hospital Network Infrastructure (High Risk)

Threat: Nation-state actors targeting hospital infrastructure.

Recommendations

- **IDPS**: Deploy IDPS to monitor for malicious activity and respond to threats.
- **Segmentation**: Segment the network to contain breaches and stop lateral movement.
- **Regular Assessments**: Do vulnerability assessments and penetration testing to find and fix security holes.
- **Employee Training**: Train staff on cybersecurity to prevent social engineering attacks.

2 Electronic Health Record (EHR) System (Moderate Risk)

Threat: Exploitation of known vulnerabilities in EHR systems like OpenEMR.

Recommendations

- **Patch Now**: Update EHR systems to fix known vulnerabilities, like OpenEMR versions before 7.0.0, which allow unauthorized access and system compromise, SC Media.
- **Access Controls**: Lock down access and monitor user activity to detect unauthorized access.
- **Data Encryption**: Encrypt patient data at rest and in transit to prevent data breaches.

3. Staff Credentials (Moderate Risk)

Threat: Phishing attacks to steal credentials.

Recommendations:

- **Multi-Factor Authentication (MFA)**: Add an extra layer of security beyond just passwords TIL Security.
- **Phishing Awareness Training**: Run regular training sessions to educate staff on how to spot and respond to phishing.
- **Email Filtering**: Use advanced email filtering to detect and block phishing emails before they get to staff inboxes.

By doing these, cybersecurity risks can be reduced, and patient data can be protected.

3 Threat Intelligence

3.1 Identification of Relevant MITRE ATT&CK Groups Targeting MSHS

3.1.1 APT29 (Cozy Bear – Nation-State Actor)

APT29 (Cozy Bear) is a Russian state-sponsored cyber espionage group tied to the Russian Foreign Intelligence Service (SVR). They have a history of targeting healthcare organizations to steal IP and sensitive data. Given MSHS's involvement in clinical trial research and development of proprietary AI-driven diagnostic tools, they are a high-value target for nation-state actors looking for strategic advantage. The Health Sector Cybersecurity Coordination Center (HC3) has warned about the threat to healthcare from Russian state-sponsored groups during global health crises.

Evidence of Healthcare Targeting:
In 2020, APT29 was implicated in cyberattacks targeting healthcare organizations involved in COVID-19 vaccine research across the United States, United Kingdom, and Canada *[Ref: HealthcareITNews, https://www.healthcareitnews.com/news/russian-hackers-targeting-healthcare-orgs-coronavirus-vaccine-info]*. The group employed custom malware, including WellMess and WellMail, to extract information related to vaccine development. These activities were confirmed by joint advisories from the UK's National Cyber Security Centre (NCSC), the US Cybersecurity and Infrastructure Security Agency (CISA), and Canada's Communications Security Establishment (CSE). [Ref: RollCall, https://rollcall.com/2020/07/16/russian-cyber-hacking-group-said-to-target-covid-19-vaccine-development]

Given MSHS's focus on AI diagnostics and its strategic location in Qatar—a hub for innovation—the organization is a plausible target for APT29's espionage operations.

3.1.2 (Winnti Group – Nation-State Actor with Cybercrime Elements)

APT41, also known as the Winnti Group or Double Dragon, is a Chinese state-sponsored cyber threat actor that conducts both cyber espionage and financially motivated cybercrime. They have a history of targeting healthcare organizations to steal patient data and intellectual property. Given MSHS's advanced hospital network infrastructure (Priority 3) and Electronic Health Record (EHR) systems (Priority 1), they are a likely target for APT41's multi-faceted cyber attacks. The Health Sector Cybersecurity Coordination Center (HC3) has highlighted the healthcare sector's vulnerability to these types of threats and the importance of protecting protected health information (PHI) and the sector's unprepared IT infrastructures.*[Ref: TechTarget, https://www.techtarget.com/healthtechsecurity/news/366593990/HC3-Details-APT41-Cyberattack-Tactics-Risks-to-Healthcare-Cybersecurity].*

Evidence of Healthcare Targeting:

APT41 has been involved in multiple healthcare sector cyber attacks. *[Ref: Scmedia, https://www.scworld.com/analysis/apt41-spear-phishing-supply-chain-campaigns-target-pharma-healthcare].* In 2020, they exploited Citrix and Zoho vulnerabilities to get into healthcare networks. *[Ref: TechTarget, https://www.techtarget.com/healthtechsecurity/news/366593990/HC3-Details-APT41-Cyberattack-Tactics-Risks-to-Healthcare-Cybersecurity].* These attacks were to get access to patient data and medical research. APT41 has also used spear-phishing, supply chain attacks and custom malware to compromise healthcare organizations. *[Ref: Scmedia, https://www.scworld.com/analysis/apt41-spear-phishing-supply-chain-campaigns-target-pharma-healthcare].*

In 2021, APT41 added SQL injections and zero-day exploits to their attack vectors, showing their continued threat to the healthcare sector.

3.1.3 Lapsus$ (Cybercriminal Group – Data Extortion and Insider Threats)

Lapsus$ is a cybercriminal group known for data extortion and leveraging insider threats. The group often targets organizations with valuable data or weak insider threat programs. MSHS's staff credentials (Priority 2) and Electronic Health Record (EHR) system (Priority 1) are vulnerable to Lapsus$'s tactics, which include recruiting insiders

or exploiting stolen credentials to access sensitive systems. The Health Sector Cybersecurity Coordination Center (HC3) has highlighted the healthcare sector's susceptibility to such threats, emphasizing safeguarding protected health information (PHI) and the sector's relatively unprepared IT infrastructures.

Evidence of Healthcare Targeting:

While Lapsus$ has not directly targeted healthcare organizations, their breach of Okta, an identity management service provider with healthcare clients, had implications for the sector. *[Ref: TechTargetNetwork, https://www.techtarget.com/healthtechsecurity/news/366594850/HC3-Warns-of-Lapsus-Cyber-Threat-Group].* The Department of Health and Human Services (HHS) issued a threat brief detailing the tactics used by Lapsus$, urging healthcare entities to prioritize the use of multi-factor authentication and to bolster defenses against social engineering attacks. *[Ref: ScMedia. https://www.scworld.com/analysis/lapsus-breach-of-okta-prompts-hhs-alert-for-healthcare-organizations].*

3.1.4 Anonymous (Hacktivists – Ideological Motivation)

Anonymous is a loose collective of hacktivists who target organizations they deem to be unethical, particularly when it comes to privacy and data. MSHS's patient portal (Priority 5) and hospital network (Priority 3) could be vulnerable to DDoS or defacement. Anonymous may see MSHS's use of AI diagnostics or data sharing (e.g. with Microsoft Azure for cloud storage) as a privacy risk and will attack to expose or disrupt.

Evidence of Healthcare Targeting:

In 2014, Anonymous-affiliated hacker Martin Gottesfeld launched DDoS attacks against Boston Children's Hospital and the Wayside Youth and Family Support Network as part of #OpJustina, protesting the hospital's treatment of a patient. These attacks disrupted hospital operations and fundraising efforts, leading to significant financial losses. *[Ref: Sopohos News, https://news.sophos.com/en-us/2016/10/24/anonymous-hacker-charged-with-opjustina-ddos-attacks-on-hospitals]*

While not directly linked to Anonymous, in 2023, a group identifying as Anonymous Sudan conducted DDoS attacks on nine Danish hospitals, temporarily taking their websites offline. The group claimed the attacks were in response to Quran burnings,

highlighting how ideological motivations can lead to cyberattacks on healthcare institutions. *[Ref: The Record Media, https://therecord.media/danish-hospitals-hit-by-cyberattack-from-anonymous-sudan]*

3.1.5 APT38 (Lazarus Group – Nation-State Actor)

APT38, a subset of the North Korean Lazarus Group, is financially motivated and has been known to conduct large-scale thefts from financial institutions. While they have primarily focused on the financial sector, their tactics could be applied to MSHS and other healthcare organizations, given the value of healthcare data and the potential to make money from ransomware attacks.

Evidence of Healthcare Targeting:

The 2017 WannaCry ransomware attack, which severely impacted the UK's National Health Service (NHS), has been widely attributed to the Lazarus Group. The attack led to the cancellation of thousands of appointments and operations, with at least 81 of the 236 NHS trusts in England affected. *[Ref: digitalHealth, https://www.digitalhealth.net/2017/10/wannacry-impact-on-nhs-considerably-larger-than-previously-suggested]*. Notably, the attack exploited unpatched vulnerabilities in outdated Windows systems, highlighting the importance of regular system updates and patches.

3.1.6 Wizard Spider (Cybercriminals – Ransomware and Malware)

Wizard Spider is a Russian based cybercriminal group that operates TrickBot and deploys Ryuk and Conti ransomware. They target healthcare organisations because of the value of patient data and the critical nature of healthcare services, which increases the likelihood of paying the ransom. MSHS's Electronic Health Record (EHR) system (Priority 1) and Internet of Things (IoT) medical devices (Priority 6) are vulnerable to Wizard Spider's malware and ransomware attacks which can disrupt patient care and steal sensitive data. The 2024 Sophos report showed high ransomware in healthcare which aligns with Wizard Spider's activity. *[Ref: Sophos, https://www.sophos.com/en-us/press/press-releases/2024/09/two-thirds-healthcare-organizations-hit-ransomware-four-year-high].*

Evidence of Healthcare Targeting:

Wizard Spider was behind the 2021 ransomware attack on Ireland's Health Service

Executive (HSE) where Conti ransomware, delivered via TrickBot, took down all IT systems across the country and caused massive disruption to healthcare services. With a focus on healthcare and the ability to exploit vulnerabilities in connected systems, MSHS is a prime target, especially with its reliance on IoT devices and EHR systems for patient care.

3.2 Identification of Possible Techniques

This section describes the techniques that the identified MITRE ATT&CK groups—APT29 (Cozy Bear), APT41 (Winnti Group), Lapsus$, Anonymous, APT38 (Lazarus Group), and Wizard Spider—might use to target *MedSecure Health Systems (MSHS).* Each technique is listed with its MITRE ATT&CK code and name, and its relevance to MSHS's assets (EHR system, IoT medical devices, staff credentials, hospital network, clinical trial research, patient portal) is explained. Techniques are from the groups known TTPs as documented in the MITRE ATT&CK framework and recent threat intelligence. More common techniques that appear across multiple groups or are used in healthcare attacks are bolded to highlight their importance in MSHS's threat landscape.

3.2.1 Techniques Used by Identified Groups

Below is a comprehensive list of techniques, grouped by the MITRE ATT&CK tactic categories, that the identified groups might employ against MSHS:

Initial Access

- **T1190 – Exploit Public-Facing Application** (Used by APT29, APT41, APT38, Wizard Spider)
    - **Description:** Attackers exploit vulnerabilities in public-facing applications to get in. For MSHS, this could be exploiting known vulnerabilities in the OpenEMR-based EHR system (Priority 1), like CVE-2023-2948 (Cross-site Scripting, XSS), or the patient portal (Priority 5), which is a web application *[Ref: MITRE ATT&CK, https://attack.mitre.org/techniques/T1190/].*
    - **Relevance to MSHS:** APT29 and APT41 target healthcare systems for espionage, APT38 and Wizard Spider for malware or ransomware.

MSHS uses OpenEMR which has documented vulnerabilities so this is likely an entry point.

- **T1566 – Phishing** (Used by APT29, APT41, Lapsus$, APT38, Wizard Spider)
    - **Description:** Attackers send phishing emails to trick users into giving up credentials or executing malicious payloads. At MSHS, this targets staff credentials (Priority 2) to get into sensitive systems like the EHR or hospital network *[Ref: MITRE ATT&CK, https://attack.mitre.org/techniques/T1566/].*
    - **Relevance to MSHS:** Phishing is the most common initial access method for all groups except Anonymous. Wizard Spider uses phishing to deliver TrickBot malware, APT29, APT41 and APT38 use spear-phishing for espionage or financial gain. Lapsus$ uses phishing to steal credentials for extortion. The 2024 Verizon DBIR says phishing accounts for 93% of malicious activity in healthcare so this is a frequent tactic *[Ref: HIPAA Times, https://hipaatimes.com/unpacking-healthcare-cybercriminal-tactics].*
- **T1655 – Insider Threat** (Used by Lapsus$)
    - **Description:** Attackers recruit or coerce insiders to get into systems or data. For MSHS, this could be a disgruntled employee leaking staff credentials (Priority 2) or EHR data (Priority 1) *[Ref: MITRE ATT&CK, https://attack.mitre.org/techniques/T1655/].*
    - **Relevance to MSHS:** Lapsus$ is known to exploit insiders, as seen in the 2022 Impresa health group attack. MSHS has no specific insider threat data so this is a higher risk.

Execution

- **T1059 – Command and Scripting Interpreter** (Used by APT29, APT41, APT38, Wizard Spider)
    - **Description:** Attackers execute malicious scripts or commands to do actions on compromised systems, like deploy malware or ransomware. At MSHS, this could be used to execute payloads on the hospital network (Priority 3) or IoT devices (Priority 6) *[Ref: MITRE ATT&CK,*

https://attack.mitre.org/techniques/T1059/].

- **Relevance to MSHS:** APT29 and APT41 use this for espionage, APT38 and Wizard Spider for ransomware or data-wiping malware. MSHS's connected systems are vulnerable to script-based attacks that spread across the network.

Persistence

- **T1098 – Account Manipulation** (Used by APT41, Lapsus$, APT38)
  - **Description:** Attackers manipulate accounts to stay in, like changing staff credentials (Priority 2) so they can get into MSHS's systems *[Ref: MITRE ATT&CK, https://attack.mitre.org/techniques/T1098/].*
  - **Relevance to MSHS:** APT41 and APT38 use this for long term espionage, Lapsus$ uses stolen credentials for extortion. MSHS uses staff credentials to get into systems so this is a big persistence vector.

Credential Access

- **T1555 – Credentials from Password Stores** (Used by APT29, APT41, Lapsus$, APT38)
  - **Description:** Attackers steal credentials from password stores or browsers, targeting staff credentials (Priority 2) to get into MSHS's EHR system or hospital network *[Ref: MITRE ATT&CK, https://attack.mitre.org/techniques/T1555/].*
  - **Relevance to MSHS:** This is used by APT29, APT41 and APT38 for espionage, Lapsus$ for extortion. The 2024 Verizon DBIR says credential theft is a common outcome of phishing in healthcare, so this is a frequent technique *[Ref: Verizon, https://www.verizon.com/business/resources/reports/2024-dbir-executive-summary.pdf].*

Collection

- **T1005 – Data from Local System** (Used by Lapsus$, APT38, Wizard Spider)
  - **Description:** Attackers collect data from compromised systems, like patient records from the EHR system (Priority 1) or clinical trial research

data (Priority 4) at MSHS *[Ref: MITRE ATT&CK, https://attack.mitre.org/techniques/T1005/]*.

- **Relevance to MSHS:** Lapsus$ collects for extortion, APT38 and Wizard Spider steal patient data for financial gain. MSHS's EHR and research data is valuable.

Command and Control

- **T1219 – Remote Access Software** (Used by Anonymous)
  - **Description:** Attackers use remote access tools to command-and-control attacks, like DDoS'ing MSHS's patient portal (Priority 5) or hospital network (Priority 3) *[Ref: MITRE ATT&CK, https://attack.mitre.org/techniques/T1219/]*.
  - **Relevance to MSHS:** Anonymous uses this to manage distributed attacks, often for ideological reasons. MSHS's public facing systems are vulnerable to this.

Exfiltration

- T1041 – Exfiltration Over C2 Channel (Used by APT29, APT41, APT38)
  - **Description:** Attackers exfiltrate stolen data over command-and-control channels, targeting MSHS's clinical trial research data (Priority 4) or EHR data (Priority 1) *[Ref: MITRE ATT&CK, https://attack.mitre.org/techniques/T1041/]*.
  - **Relevance to MSHS:** APT29, APT41 and APT38 use this for espionage, stealing sensitive data for strategic or financial gain. Healthcare data's high value on the dark web, as noted in Section 2.2.1.2, makes this a frequent technique for nation-state actors targeting MSHS.

Impact

- T1486 – Data Encrypted for Impact (Used by APT38, Wizard Spider)
  - **Description:** Attackers encrypt data to disrupt operations and demand ransom, targeting MSHS's EHR system (Priority 1) or IoT devices (Priority 6) [Ref: MITRE ATT&CK, https://attack.mitre.org/techniques/T1486/].

    - **Relevance to MSHS:** APT38 (e.g., WannaCry) and Wizard Spider (e.g., Conti) use ransomware to disrupt healthcare operations. The 2024 Sophos report notes 67% of healthcare organizations faced ransomware attacks, so this is a big one *[Ref: Sophos, https://www.sophos.com/en-us/press/press-releases/2024/09/two-thirds-healthcare-organizations-hit-ransomware-four-year-high].*

- T1490 – Inhibit System Recovery (Used by APT41, APT38)
    - **Description:** Attackers disable system recovery mechanisms, like MSHS's backups (Priority 7), to maximize the impact of ransomware or destructive attacks *[Ref: MITRE ATT&CK, https://attack.mitre.org/techniques/T1490/].*
    - **Relevance to MSHS:** APT41 and APT38 do this to ensure maximum disruption, often as part of ransomware campaigns or espionage operations. MSHS's backups are key to recovery, so this is a big deal.
- T1499 – Endpoint Denial of Service (Used by Anonymous)
    - **Description:** Attackers launch DDoS attacks to disrupt services, targeting MSHS's patient portal (Priority 5) or hospital network (Priority 3) *[Ref: MITRE ATT&CK, https://attack.mitre.org/techniques/T1499/].*
    - **Relevance to MSHS:** Anonymous uses DDoS for ideological reasons, as seen in the 2021 Canadian healthcare attack. MSHS's public-facing systems are vulnerable to this.
- T1531 – Account Access Removal (Used by Anonymous)
    - **Description:** Attackers deface or disable accounts on public-facing systems, like MSHS's patient portal (Priority 5), to send a message *[Ref: MITRE ATT&CK, https://attack.mitre.org/techniques/T1531/].*
    - **Relevance to MSHS:** Anonymous does this to impact patient trust and draw attention to perceived privacy issues, which aligns with their hacktivist motives.
- **T1657 – Financial Theft** (Used by Lapsus$, APT38, Wizard Spider)
    - **Description:** Attackers extort organizations by threatening to leak stolen data or demand ransom, targeting MSHS's EHR system (Priority 1) for financial gain *[Ref: MITRE ATT&CK, https://attack.mitre.org/techniques/T1657/].*

- **Relevance to MSHS:** Lapsus$ does this for extortion, while APT38 and Wizard Spider do it with ransomware campaigns. Healthcare data is valuable, so this is a big one.

Lateral Movement

- **T1021 – Remote Services** (Used by Wizard Spider)
  - **Description:** Attackers move laterally within the network using remote services, targeting MSHS's hospital network (Priority 3) to infect IoT devices (Priority 6) or EHR systems (Priority 1) *[Ref: MITRE ATT&CK, https://attack.mitre.org/techniques/T1021/].*
  - **Relevance to MSHS:** Wizard Spider uses this to spread TrickBot and ransomware across healthcare networks, as seen in the 2020 HSE attack. MSHS's connected systems increase this risk.

3.3 Mapping of Techniques/Tactics to MSHS Assets

This section maps the MITRE ATT&CK techniques from Section 3.2 to the MedSecure Health Systems (MSHS) assets in Section 1.5: EHR System, IoT Medical Devices, Patient Portal, Staff Credentials, Clinical Trial Research, Hospital Network, and Backups. Each technique is associated with one or more assets based on its applicability, the groups that use it (APT29, APT41, Lapsus$, Anonymous, APT38, Wizard Spider), and MSHS's operational environment as a healthcare provider. The mapping is in a table, so we can see how each technique targets specific assets critical to MSHS's mission of patient-centric care while maintaining data privacy and operational efficiency.

3.3.1 Mapping Table

The table below maps each technique (with its MITRE ATT&CK code and name) to the relevant MSHS asset(s), with a brief explanation. Techniques that don't target a specific asset are noted with their broader impact on MSHS's operations.

Technique Code	Technique Name	Targeted MSHS Asset(s)	Justification
T1190	Exploit Public-Facing Application	EHR System, Patient Portal	Exploits vulnerabilities in public-facing systems like OpenEMR (EHR) and the patient portal (web application), as seen with groups like APT29, APT41, APT38, and Wizard Spider targeting healthcare systems for initial access [Ref: Section 3.2.1].
T1566	Phishing	Staff Credentials	Phishing targets staff to steal credentials, enabling access to systems like the EHR or hospital network. Used by APT29, APT41, Lapsus$, APT38, and Wizard Spider, with 93% of healthcare malicious activity linked to phishing [Ref: Section 3.2.1].
T1655	Insider Threat	Staff Credentials, EHR System	Lapsus$ recruits insiders to leak credentials or directly access EHR data, compromising patient confidentiality [Ref: Section 3.2.1].
T1059	Command and Scripting Interpreter	Hospital Network, IoT Devices	Executes scripts to deploy malware or ransomware on the hospital network or IoT devices, impacting availability. Used by APT29, APT41, APT38, and Wizard Spider [Ref: Section 3.2.1].
T1098	Account Manipulation	Staff Credentials	Modifies staff credentials to maintain persistent access to systems, a tactic used by APT41, Lapsus$, and APT38 for espionage or extortion [Ref: Section 3.2.1].
T1555	Credentials from Password Stores	Staff Credentials	Steals credentials from password stores, directly targeting staff credentials to access critical systems. Used by APT29, APT41, Lapsus$, and APT38 [Ref: Section 3.2.1].
T1005	Data from Local System	EHR System, Clinical Trial Research	Collects sensitive data like patient records (EHR) or AI diagnostic research, a goal of Lapsus$, APT38, and Wizard Spider for extortion or financial gain [Ref: Section 3.2.1].
T1219	Remote Access	Patient Portal,	Used by Anonymous to coordinate DDoS attacks,

Technique Code	Technique Name	Targeted MSHS Asset(s)	Justification
	Software	Hospital Network	targeting the patient portal or hospital network to disrupt availability [Ref: Section 3.2.1].
T1041	Exfiltration Over C2 Channel	EHR System, Clinical Trial Research	Exfiltrates patient data (EHR) or research data for espionage, a frequent technique by APT29, APT41, and APT38 due to healthcare data's dark web value [Ref: Section 3.2.1].
T1486	Data Encrypted for Impact	EHR System, IoT Devices	Encrypts EHR systems or IoT devices to disrupt operations, a ransomware tactic by APT38 and Wizard Spider, impacting patient care [Ref: Section 3.2.1].
T1490	Inhibit System Recovery	Backups	Disables backups to amplify ransomware impact, used by APT41 and APT38, directly targeting MSHS's recovery capabilities [Ref: Section 3.2.1].
T1499	Endpoint Denial of Service	Patient Portal, Hospital Network	Anonymous launches DDoS attacks to disrupt the patient portal or hospital network, affecting availability and patient access [Ref: Section 3.2.1].
T1531	Account Access Removal	Patient Portal	Anonymous defaces or disables accounts on the patient portal to send ideological messages, impacting patient trust [Ref: Section 3.2.1].
T1657	Financial Theft	EHR System	Extorts MSHS by threatening to leak EHR data, a tactic by Lapsus$, APT38, and Wizard Spider, leveraging the high value of patient data [Ref: Section 3.2.1].
T1021	Remote Services	Hospital Network, IoT Devices	Wizard Spider moves laterally within the hospital network to infect IoT devices or EHR systems, escalating the attack's impact [Ref: Section 3.2.1].

3.3.2 Discussion

The map shows how the identified techniques target MSHS's critical assets, matching the groups' motivations and the healthcare sector's threat landscape. The EHR

System (Priority 1) is a prime target for techniques like T1190 (Exploit Public-Facing Application), T1005 (Data from Local System), T1041 (Exfiltration Over C2 Channel), T1486 (Data Encrypted for Impact), and T1657 (Financial Theft) as it's valuable for both espionage (APT29, APT41, APT38) and financial gain (Lapsus$, APT38, Wizard Spider). Staff Credentials (Priority 3) are heavily targeted by T1566 (Phishing), T1655 (Insider Threat), T1098 (Account Manipulation), and T1555 (Credentials from Password Stores) as they're the gateway to other systems. The Hospital Network (Priority 3) and IoT Medical Devices (Priority 6) are at risk from T1059 (Command and Scripting Interpreter), T1499 (Endpoint Denial of Service), and T1021 (Remote Services) which can disrupt operations and patient care. Clinical Trial Research (Priority 4) is targeted by espionage-focused techniques like T1005 and T1041 and the Patient Portal (Priority 5) is vulnerable to disruptive attacks (T1499, T1531) by Anonymous. Finally, Backups (Priority 7) are at risk from T1490 (Inhibit System Recovery) which amplifies the impact of ransomware attacks. This map shows we need asset specific defenses like patch management for EHR system, MFA for staff credentials and network segmentation for hospital network and IoT devices.

3.4 Actionable Information to Protect MSHS

This section provides guidance to protect *MedSecure Health Systems (MSHS)* from the cyber threats posed by the MITRE ATT&CK techniques in Section 3.2 used by APT29 (Cozy Bear), APT41 (Winnti Group), Lapsus$, Anonymous, APT38 (Lazarus Group) and Wizard Spider. Each recommendation is linked to a specific technique, based on the scenario of MSHS as a healthcare provider in Doha, Qatar, delivering patient centric care through advanced technologies like Electronic Health Records (EHR) via OpenEMR, IoT medical devices, AI driven diagnostics, patient portal and hospital network infrastructure. The recommendations aim to mitigate risks to MSHS's critical assets (EHR System, IoT Medical Devices, Patient Portal, Staff Credentials, Clinical Trial Research, Hospital Network, Backups) while ensuring business continuity, patient safety and compliance to healthcare regulations like Qatar's National Health Strategy and international standards like HIPAA.

3.4.1 Actionable Recommendations

Below is the actionable information for each MITRE ATT&CK technique in Section 3.2, with the motivations based on MSHS's operational scenario:

1. Technique: T1190 – Exploit Public-Facing Application (Targets: EHR System, Patient Portal)

    - **Actionable Information:** Implement a patch management program to keep the OpenEMR-based EHR system and patient portal up to date with the latest patches for known vulnerabilities like CVE-2023-2948 (XSS). Deploy a Web Application Firewall (WAF) to monitor and block exploit attempts on public-facing applications.

    - **Motivation:** MSHS's EHR system (Priority 1) and patient portal (Priority 5) are critical for patient care and access but are vulnerable to APT29, APT41, APT38 and Wizard Spider who target public-facing applications to get initial access. The 2024 Verizon DBIR notes that 14% of healthcare breaches are due to vulnerability exploitation and most of the time it's because of delayed patching [Ref: Section 2.2.1.2]. Timely patching and WAF will prevent unauthorized access and ensure patient data confidentiality and business continuity.

2. Technique: T1566 – Phishing (Target: Staff Credentials)

    - **Actionable Information:** Implement advanced email filtering to detect and block phishing emails and do regular phishing training for staff to identify and report suspicious emails. Also, enable Multi-Factor Authentication (MFA) on all systems that require staff credentials.

    - **Motivation:** Phishing, used by APT29, APT41, Lapsus$, APT38 and Wizard Spider, is the most common technique used to target MSHS's staff credentials (Priority 2), 93% of malicious activity in healthcare is linked to phishing [Ref: Section 3.2.2]. As a healthcare provider, MSHS staff are busy and may fall for phishing attempts especially under pressure. Email filtering and training reduces the chances of successful attacks and MFA adds an extra layer of security to prevent unauthorized access to systems like EHR or hospital network and protect patient data and care delivery.

3. T1655 – Insider Threat (Targets: Staff Credentials, EHR System)

- **Actionable:** Establish an insider threat program, monitor user activity for unusual behavior (e.g. EHR access patterns) and implement least privilege access to limit staff to only what they need for their role.
- **Motivation:** Lapsus$ exploits insiders to steal staff credentials or EHR data, as seen in the 2022 Impresa health group attack [Ref: 3.1.4]. MSHS in a high stakes healthcare environment may face risks from disgruntled employees or contractors, especially with no insider threat data (assuming typical for a healthcare provider). Monitoring and least privilege access can detect and limit insider threats, protect patient confidentiality and trust.

4. T1059 – Command and Scripting Interpreter (Targets: Hospital Network, IoT Devices)

    - **Actionable:** Deploy Endpoint Detection and Response (EDR) on the hospital network and IoT devices to detect and block malicious script execution. Segment the network to isolate IoT devices from critical systems like EHR, limit the spread of malware.
    - **Motivation:** APT29, APT41, APT38 and Wizard Spider use this technique to execute malware or ransomware on MSHS's hospital network (Priority 3) and IoT devices (Priority 6) which are critical for real-time patient monitoring. A malware outbreak could impact patient care, as seen in the 2020 HSE attack by Wizard Spider [Ref: 3.1.7]. EDR and network segmentation can prevent script-based attacks from spreading, ensure availability of critical systems and patient safety.

5. T1098 – Account Manipulation (Target: Staff Credentials)

    - **Actionable:** Monitor account changes (e.g. password resets, privilege escalations) and enforce strict access controls, such as time based access restrictions for staff credentials to prevent unauthorized modifications.
    - **Motivation:** APT41, Lapsus$ and APT38 use account manipulation to maintain access to MSHS's systems via staff credentials (Priority 2). In a healthcare environment where staff access multiple systems under

time pressure, unauthorized account changes could go unnoticed, allowing long term espionage or extortion. Monitoring and access controls can detect and prevent such manipulations, protect system integrity and patient data.

6. T1555 – Credentials from Password Stores (Target: Staff Credentials)

    - **Actionable:** Use a password manager for staff to store credentials securely and implement policies to disable credential storage in browsers. Audit systems regularly for exposed credentials and enforce strong, unique passwords.
    - **Motivation:** APT29, APT41, Lapsus$ and APT38 target staff credentials stored in password stores or browsers, a common technique in healthcare breaches [Ref: 3.2.2]. MSHS staff use browsers to access systems quickly, increasing the risk of credential theft. Secure storage and audits can prevent attackers from getting access to critical systems like EHR or hospital network, protect patient data.

7. Technique: T1005 – Data from Local System (Targets: EHR System, Clinical Trial Research)

    - **Actionable Information:** Encrypt sensitive data at rest on the EHR system and clinical trial research servers, and use Data Loss Prevention (DLP) to monitor and block unauthorized data access or exfiltration.
    - **Motivation:** Lapsus$, APT38, and Wizard Spider steal data from local systems like MSHS's EHR (Priority 1) and clinical trial research (Priority 4) for extortion or financial gain. MSHS's AI-driven diagnostics research is a high-value target, and a breach could compromise patient confidentiality and competitive advantage. Encryption and DLP can prevent unauthorized access and data theft, as per HIPAA and Qatar's data privacy regulations.

8. Technique: T1219 – Remote Access Software (Targets: Patient Portal, Hospital Network)

    - **Actionable Information:** Deploy an Intrusion Detection and Prevention

System (IDPS) to monitor for unauthorized remote access attempts on the patient portal and hospital network. Restrict remote access software usage to approved tools only.

- **Motivation:** Anonymous uses remote access software to coordinate DDoS attacks against MSHS's patient portal (Priority 5) and hospital network (Priority 3), to disrupt services for ideological reasons. As a healthcare provider, MSHS relies on these systems for patient access and operational continuity, and a disruption could delay care and erode trust. IDPS and access restrictions can detect and block such activities, to maintain service availability.

9. Technique: T1041 – Exfiltration Over C2 Channel (Targets: EHR System, Clinical Trial Research)

    - **Actionable Information:** Monitor for anomalous outbound traffic and use a firewall to block unapproved command-and-control (C2) communications. Encrypt data in transit to prevent interception during exfiltration.
    - **Motivation:** APT29, APT41, and APT38 use this technique to exfiltrate MSHS's EHR and clinical trial research data for espionage, as healthcare data has high value on the dark web [Ref: Section 3.2.2]. MSHS's focus on AI diagnostics makes its research a strategic target, and a breach could result in intellectual property loss and patient privacy violations. Network monitoring and encryption can prevent data exfiltration, to protect MSHS's reputation and compliance.

10. Technique: T1486 – Data Encrypted for Impact (Targets: EHR System, IoT Devices)

    - **Actionable Information:** Keep offline, encrypted backups of the EHR system and IoT device configurations and conduct regular disaster recovery drills to ensure quick recovery after a ransomware attack. Deploy anti-ransomware solutions to detect and block encryption.
    - **Motivation:** APT38 and Wizard Spider use ransomware to encrypt MSHS's EHR system (Priority 1) and IoT devices (Priority 6), to disrupt

patient care, as seen in the 2017 WannaCry attack by APT38 [Ref: Section 3.1.6]. MSHS's dependence on these systems for patient monitoring and care delivery makes ransomware a high-risk threat. Offline backups and anti-ransomware tools can mitigate the impact, to ensure continuity of care and patient safety.

11. T1490 – Inhibit System Recovery (Target: Backups)

    - **Actionable Information:** Store backups in a secure, air-gapped environment and test backup integrity and recovery processes regularly to ensure they are not compromised. Limit backup system modifications to authorized personnel only.
    - **Motivation:** APT41 and APT38 disable backups (Priority 7) to amplify ransomware impact, making recovery difficult for MSHS after an attack. As a healthcare provider, MSHS relies on backups to restore critical systems like EHR and a failure to recover could shut down operations and put patients at risk. Air-gapped backups and access controls can protect recovery capabilities, ensuring business continuity.

12. T1499 – Endpoint Denial of Service (Targets: Patient Portal, Hospital Network)

    - **Actionable Information:** Deploy a Content Delivery Network (CDN) with DDoS protection for the patient portal and rate-limiting and traffic filtering on the hospital network to mitigate DDoS attacks. Have an incident response plan in place to manage service disruptions.
    - **Motivation:** Anonymous uses DDoS attacks to disrupt MSHS's patient portal (Priority 5) and hospital network (Priority 3) for ideological reasons, as seen in the 2021 Canadian healthcare attack [Ref: Section 3.1.5]. MSHS's patients rely on the portal for appointments and results and network downtime could delay care. DDoS protection and incident response can keep services available, preserving patient trust and access.

13. T1531 – Account Access Removal (Target: Patient Portal)

- **Actionable Information:** Log and monitor patient portal accounts for unauthorized access or defacement attempts. Use CAPTCHA and strong authentication to prevent automated attacks on user accounts.
- **Motivation:** Anonymous targets patient portal to deface or disable accounts to send ideological messages about privacy concerns. MSHS's public-facing portal is a visible target and such an attack could damage patient trust and disrupt access to services. Logging, monitoring and authentication can prevent and detect such incidents, protecting MSHS's reputation and patient experience.

14. T1657 – Financial Theft (Target: EHR System)

- **Actionable Information:** Do security awareness training to educate staff on extortion threats and have a ransomware response plan that includes legal and negotiation protocols. Encrypt EHR data to reduce the value of stolen data if exfiltrated.
- **Motivation:** Lapsus$, APT38 and Wizard Spider extort MSHS by threatening to leak EHR data (Priority 1) as patient data is highly valuable. As a healthcare provider MSHS is a prime target for financial gain and a data leak could result in regulatory fines and reputational damage. Training, a response plan and encryption can mitigate the risk and impact of extortion, ensuring compliance and patient trust.

15. T1021 – Remote Services (Targets: Hospital Network, IoT Devices)

- **Actionable Information:** Disable unnecessary remote services (e.g. RDP) on the hospital network and IoT devices and use a VPN with strong authentication for any required remote access. Audit network configurations regularly for unauthorized remote access points.
- **Motivation:** Wizard Spider uses remote services to move laterally within MSHS's hospital network (Priority 3) and infect IoT devices (Priority 6), amplifying the impact of malware or ransomware, as seen in the 2020 HSE attack [Ref: Section 3.1.7]. MSHS's connected systems increase the risk of lateral movement which could impact patient monitoring and care. Disabling unnecessary services and securing

remote access can limit the attacker's ability to move, protect critical infrastructure and patient safety.

3.4.2 Discussion

The information provided addresses each identified MITRE ATT&CK technique, with practical mitigations for MSHS as a healthcare provider. The recommendations focus on protecting MSHS's critical assets while ensuring patient care continuity, data privacy and compliance. For example, patch management (T1190) and email filtering with MFA (T1566) counter the most common techniques targeting the EHR system and staff credentials which are high priority assets (Priorities 1 and 2). Network segmentation (T1059, T1021) and DDoS protection (T1499) protect the hospital network and patient portal, ensuring business continuity. Encryption (T1005, T1041, T1657) and offline backups (T1486, T1490) protect against data theft and ransomware, critical for patient trust and regulatory compliance. These measures reduce MSHS's attack surface, limit the impact of an incident and align with healthcare cybersecurity best practices such as NIST and HIPAA guidelines.

4 Conclusion

This *MedSecure Health Systems (MSHS)* cybersecurity risk assessment has given a full analysis of the threats, vulnerabilities and risks facing the organisation as a leading healthcare provider in Doha, Qatar. MSHS's mission to deliver patient-centric care through advanced technologies – OpenEMR-based Electronic Health Record (EHR) system, IoT medical devices, AI-driven diagnostics, patient portal, and hospital network infrastructure makes it a prime target for various cyber threat actors. The assessment has identified critical assets, evaluated their risk exposure using the FAIR framework, mapped relevant MITRE ATT&CK groups and techniques and provided actionable recommendations to mitigate these risks so MSHS can continue to deliver high quality care while protecting patient data and operational integrity.

Asset prioritisation (Section 1.6) showed the EHR system, IoT medical devices, staff credentials and hospital network infrastructure as the top assets, with the EHR system (Priority 1) being the primary target as it's involved in patient care and is vulnerable to ransomware attacks. The FAIR based risk analysis (Sections 1.7-1.9) showed the hospital network infrastructure has the highest risk, High risk, driven by nation state

actors like APT29, APT41 and APT38 who pose threat to both availability and confidentiality through sophisticated attacks. The EHR system and staff credentials were assessed as Moderate risk, primarily due to cybercriminals like Lapsus$ and Wizard Spider exploiting vulnerabilities for financial gain, such as phishing and ransomware. These findings highlight the need for targeted defences to protect MSHS's most valuable assets from disruption and data breaches.The threat intelligence analysis (Section 3) broke down the threat landscape into six MITRE ATT&CK groups that are likely to target MSHS: APT29 (Cozy Bear), APT41 (Winnti Group), Lapsus$, Anonymous, APT38 (Lazarus Group) and Wizard Spider. These groups are a mix of nation state actors, cybercriminals and hacktivists with different motivations from espionage and financial gain to ideological disruption. 15 techniques were mapped to MSHS's assets (Section 3.3), with common techniques like **Phishing (T1566)**, **Credentials from Password Stores (T1555)** and **Exfiltration Over C2 Channel (T1041)** showing the prevalence of credential theft and data exfiltration in healthcare attacks. The actionable recommendations (Section 3.4) provide practical mitigations such as patch management for the EHR system (T1190), email filtering and MFA to counter phishing (T1566), network segmentation to protect IoT devices and hospital network (T1059, T1021). These will reduce MSHS's attack surface, mitigate the impact of potential incidents and comply with Qatar's National Health Strategy and international standards like HIPAA.

MSHS is facing a dynamic and complex cyber threat landscape and needs a proactive and layered approach to cybersecurity. The risk to the hospital network infrastructure and the moderate risk to the EHR system and staff credentials requires immediate action to implement the recommended controls such as encryption, robust access controls and DDoS protection to protect patient care and data privacy. By addressing the identified vulnerabilities and implementing the proposed mitigations MSHS can harden itself against cyber threats, maintain patient trust and continue to deliver innovative technology driven healthcare in the region. Ongoing monitoring, regular security assessments and staff training will be key to staying ahead of the threat landscape and long term security in a digital healthcare world.