1. Framework Used – I used the NIST Framework provided by the National Institute of Standards and Technology for my security analysis of EPIC Systems Corporation. This framework is widely recognized and accepted in the cybersecurity industry, and it provides a structured approach to identifying, protecting, detecting, responding to, and recovering from security risks and incidents.



https://kybersecure.com/3-reasons-to-align-with-nist-cybersecurity-framework/

2. Initial Strategic Risk and Security Management Analysis – As a security analyst, my initial assessment of EPIC Systems Corporation’s strategic risk and security management focuses on the key components of the NIST Framework: Identify, Protect, Detect, Respond, and Recover. Each component plays a crucial role in safeguarding sensitive information and ensuring the overall security of EPIC’s software and systems.

a. Identify – This component involves understanding the organization’s assets, vulnerabilities, and potential cybersecurity risks. For EPIC Systems Corporation, this would include identifying all critical assets, such as patient records, software source code, and communication channels, and potential threats and vulnerabilities that could compromise these assets' confidentiality, integrity, and availability. Additionally, EPIC should assess its reliance on third-party vendors and the associated risks.

i. In this phase, EPIC should thoroughly assess its assets, vulnerabilities, and potential cybersecurity risks. For instance, EPIC could identify its critical patient data repositories, electronic health records (EHR) systems, and administrative networks as essential assets. Vulnerabilities include outdated software, unpatched systems, and potential entry points for cybercriminals. A more specific example of vulnerabilities and risks EPIC could face, would be outdated EHR software being susceptible to known vulnerabilities or employees unknowingly falling victim to phishing attacks due to a lack of security awareness training.

ii. Attack Example - A malicious actor targets EPIC's outdated EHR software with a known vulnerability. They exploit this vulnerability to gain unauthorized access to patient records and sensitive medical data. The attacker's activity goes unnoticed due to a lack of comprehensive vulnerability assessment and asset inventory. As a result, patient confidentiality is compromised, and EPIC faces regulatory penalties and loss of trust from patients.

b. Protect – This component focuses on implementing appropriate safeguards to ensure the security and resilience of the organization’s infrastructure and data. For EPIC, this would involve access controls, encryption, secure coding practices, network segmentation, and regular data backups. Furthermore, EPIC should have an incident response plan to handle security breaches effectively.

i. EPIC should implement various safeguards to secure its infrastructure and data. For example, access controls could be enforced through multi-factor authentication (MFA) for employees accessing patient records. Encryption should be applied to sensitive patient data both in transit and at rest to prevent unauthorized access. Secure coding practices should be incorporated into the software development lifecycle to minimize vulnerabilities in the source code.

ii. Attack Example - An insider threat, a disgruntled employee with elevated access privileges, attempts to steal patient data by bypassing access controls. Their unauthorized access is facilitated by weak password policies and inadequate monitoring. This breach leads to the theft of patient records and exposes EPIC to legal repercussions and reputational damage.

c. Detect – This component involves continuous monitoring and detection of cybersecurity events to identify potential security incidents promptly. EPIC should implement intrusion detection and prevention systems, log analysis, and anomaly detection mechanisms to quickly spot unusual or suspicious activities within its network and systems.

i. Continuous monitoring and detection mechanisms are critical in the "Detect" phase. EPIC could implement intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor network traffic for suspicious patterns or activities. Log analysis tools could be used to identify unauthorized access attempts or unusual behavior.

ii. Attack Example - An advanced persistent threat (APT) group successfully infiltrates EPIC's network and remains undetected for months. Despite their ongoing activities, EPIC's lack of robust intrusion detection mechanisms allows the APT group to exfiltrate sensitive patient data and intellectual property. The breach is only discovered when external threat intelligence reveals indicators of compromise, leading to a prolonged investigation and substantial data loss.

d. Respond – This component addresses the actions to be taken when a security incident is detected. EPIC should have a well-defined incident response plan that outlines the roles, responsibilities, and procedures to follow in the event of a breach or cybersecurity event. Timely and effective responses can minimize the impact of incidents and prevent further damage.

i. The "Respond" phase involves having a well-defined incident response plan. EPIC should outline roles, responsibilities, and procedures for different levels of security incidents.

ii. Attack Example - EPIC falls victim to a ransomware attack that encrypts patient data and demands a substantial ransom payment. The incident response team's delayed response due to an unclear incident response plan results in extended system downtime and negotiations with the attackers. This disrupts patient care and tarnishes EPIC's reputation as the incident becomes public knowledge.

e. Recover – This component focuses on restoring services and operations to normalcy after a cybersecurity incident. EPIC should have a robust business continuity plan and disaster recovery procedures to ensure that critical healthcare services are quickly restored in case of a disruption.

i. EPIC's ability to recover from a cybersecurity incident is crucial. This involves having a robust business continuity plan and disaster recovery procedures.

ii. Attack Example - Following a successful distributed denial-of-service (DDoS) attack on EPIC's critical servers, patient services are disrupted, causing widespread frustration. EPIC's lack of a well-tested disaster recovery plan and backup strategy delays the restoration of services, affecting patient care and potentially leading to legal consequences due to service level agreement violations.

In conclusion, EPIC Systems Corporation’s strategic risk and security management should align with the NIST Framework to address the unique challenges of securing sensitive patient information in the healthcare industry. By diligently implementing the key components of the framework – Identify, Protect, Detect, Respond, and Recover – EPIC can strengthen its cybersecurity posture, mitigate potential risks, and maintain the trust and confidence of its customers and stakeholders. Continuous improvement and adaptation to the evolving threat landscape are crucial to ensuring the long-term security and success of EPIC’s software and healthcare solutions.

**Current Threat Examples**

As the threat landscape evolves, it is important to know some of the common cyberattack types:

|  |  |  |
| --- | --- | --- |
| Cyberattack Incident | Potential Effects on EPIC | Recommended Response |
| Phishing Attack | Unauthorized access to patient records  Data breaches and loss of sensitive information  Compromised employee credentials | Educate Employees about phishing risks  Regularly update email filtering and security awareness training |
| Ransomware Attack | Encryption of patient data  Disruption of healthcare services  Financial losses due to ransom payment or recovery efforts | Maintain offline backups for data recovery  Isolate infected systems  Engage law enforcement for further advice and action  Follow incident response plan for recovery |
| Insider Data Theft | Unauthorized access to patient records  Intellectual property theft  Legal and reputational consequences | Monitor and detect abnormal employee behavior  Restrict access based on the principle of least privilege  Conduct periodic security audits and access reviews |

**A graph of different colored bars

Description automatically generated**https://www.kroll.com/en/insights/publications/cyber/threat-intelligence-reports/q2-2022-threat-landscape-ransomware-healthcare-hit

The healthcare industry is becoming increasingly more targeted, thus making EPIC a feasible target. A timeline for implementation of the NIST Framework is crucial to reaching digital resilience in the industry.

**Timeline for Analysis and Implementation**

|  |  |
| --- | --- |
| Timeline | Activities |
| Month 1-2 | * Assemble cross-functional team * Conduct initial security assessment |
| Month 3-4 | * Create asset inventory and risk profile * Develop a plan to address vulnerabilities and threats |
| Month 5-6 | * Test and ensure multi-factor authentication is functional and secure (MFA) * Roll out encryption protocols * Establish secure coding practices * Develop and communicate incident response plan |
| Month 7-8 | * Deploy intrusion detection and prevention systems (IDS/IPS) * Implement log analysis tools |
| Month 9-10 | * Conduct tabletop exercises * Establish communication protocols |
| Month 11-12 | * Develop and test business continuity and disaster recovery plan * Regularly review and update incident response and recovery plans |
| Ongoing | * Monthly vulnerability assessments and penetration tests * Quarterly updates to access controls, encryption protocols * Annual cybersecurity training and awareness programs |

**Company Goals**

1. Strengthen Comprehensive Cybersecurity Resilience

Objective: Implement a holistic approach to cybersecurity that integrates the NIST Framework across all levels of the organization to safeguard patient data, intellectual property, and operational continuity.

Key Initiatives:

* Complete the implementation of the NIST Framework by the end of Year 1.
* Regularly assess and update the risk profile and asset inventory to stay ahead of emerging threats.
* Establish a continuous monitoring system to detect and respond to emerging cyber threats promptly.

2. Cultivate a Culture of Proactive Cybersecurity Awareness

Objective: Foster a company-wide commitment to cybersecurity awareness and best practices among employees, ensuring their active involvement in maintaining a secure digital environment.

Key Initiatives:

* Develop and deliver an ongoing cybersecurity training program for all employees, recognizing and mitigating common cyber threats.
* Implement a rewards and recognition system to acknowledge employees contributing to the organization’s cybersecurity goals.
* Conduct simulated phishing exercises to assess and improve employees’ responses to phishing attempts.

3. Enhance Incidence Response and Business Continuity Preparedness

Objective: Establish a robust incident response and business continuity framework to minimize the impact of cyber incidents, ensuring a swift recovery and continuity of critical healthcare services.

* Develop and maintain a comprehensive disaster recovery plan prioritizing the timely restoration of patient care services.
* Conduct annual assessments of incident response capabilities and adjust plans based on lessons learned and evolving threat landscapes.

**References**

Brittain, T. (n.d.). *Q2 2022 threat landscape: Ransomware returns, healthcare hit*. Kroll. https://www.kroll.com/en/insights/publications/cyber/threat-intelligence-reports/q2-2022-threat-landscape-ransomware-healthcare-hit

Cohen, J. (2019, December 30). *3 reasons to align with the NIST Cybersecurity Framework*. Kyber Security. https://kybersecure.com/3-reasons-to-align-with-nist-cybersecurity-framework/

Kaplan, J. M., Rezek, C., Marcus, A., O’Halloran, D., & Bailey, T. (2015). *Beyond Cybersecurity: Protecting your Digital Business*. Wiley.

*Privacy policies*. Epic. (n.d.). https://www.epic.com/about/privacypolicies