Disaster and Business Continuity Document

Table of Contents

Problem Statement:

Rockvale Hospital is one of the largest healthcare providers in the United States with more than 100 hospitals across the country.

Rockvale is dependent on information technology for patient care and operations. Any outage to the IT infrastructure, network, data center, or applications like the electronic health record (EHR) is a potential threat to patient care.

The hospital's operations and network can be greatly impacted or even shut down due to a natural disaster or harmful actions by bad actors.

Last year, healthcare was the most targeted industry for malware attacks, accounting for 40% of all security incidents in the third quarter. The U.S. experienced 15 natural disasters with losses exceeding $1 billion each.

Security Posture Review Statement for Rockvale Hospital

As the Senior Security Expert at Rockvale Hospital, it is my responsibility to ensure the robustness and resilience of our organization's security infrastructure. Rockvale Hospital, being one of the largest healthcare providers in the United States, is heavily reliant on information technology for patient care and operational efficiency. However, with this dependence comes the inherent risk of cyber threats, including potential disruptions from natural disasters and malicious actions by bad actors.

Considering the evolving threat landscape and the critical nature of our operations, I have undertaken a comprehensive review of Rockvale Hospital's security posture. This review aims to identify vulnerabilities, assess compliance with regulatory standards, and provide recommendations to enhance our security measures.

The current landscape underscores the urgency of our efforts. Healthcare, as evidenced by recent trends, is a prime target for cyber-attacks, with malware incidents on the rise. Moreover, the United States has experienced a significant number of natural disasters, each posing a potential risk to our operations.

Tasked with this imperative, I have divided our review into several key tasks:

Task 1: Regulatory Compliance

- Identify the laws and regulations governing the healthcare industry in the United States, particularly those pertaining to the protection of patient information. Specifically, we must ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA), which safeguards Protected Health Information (PHI) and sets stringent standards for its handling.

- **Laws and Regulations Governing Healthcare Industry:**
    - **Regulatory Act Protecting PHI:** HIPAA (Health Insurance Portability and Accountability Act).

In the healthcare sector, compliance with regulatory standards is paramount to ensuring the protection of patient data and maintaining trust with stakeholders. One of the most significant regulations in the U.S. healthcare industry is the Health Insurance Portability and Accountability Act (HIPAA). HIPAA establishes standards for the privacy and security of Protected Health Information (PHI) and imposes strict requirements on healthcare organizations, including hospitals, regarding the handling and disclosure of PHI. By identifying and understanding HIPAA and other relevant regulations, such as the Health Information Technology for Economic and Clinical Health (HITECH) Act, Rockvale Hospital can ensure that its policies and procedures align with legal requirements, thereby mitigating the risk of non-compliance and potential penalties.

Task 2: PHI Identification and Protection

- Identify and classify the various types of information considered as PHI within our organization. It is imperative that we handle these data elements securely to prevent unauthorized disclosure or misuse, thereby safeguarding patient privacy and maintaining regulatory compliance.

- **18 Types of Information Classified as PHI:**
  - Names
  - Addresses
  - Dates (birth, death, treatment)
  - Phone numbers
  - Email addresses
  - Social Security numbers
  - Medical record numbers
  - Health plan beneficiary numbers
  - Account numbers
  - Certificate/license numbers

  - Vehicle identifiers and serial numbers
  - Device identifiers and serial numbers
  - Web URLs
  - Internet protocol (IP) addresses
  - Biometric identifiers (e.g., fingerprints, voiceprints)
  - Full-face photographic images and comparable images
  - Any other unique identifying numbers, characteristics, or codes.

PHI encompasses a wide range of sensitive information contained in patients' medical records and is subject to stringent privacy and security requirements under HIPAA. Task 2 involves identifying and categorizing the specific types of information that qualify as PHI, such as names, addresses, medical record numbers, and diagnostic information. Once identified, Rockvale Hospital must implement appropriate security measures, such as access controls, encryption, and data loss prevention (DLP) solutions, to safeguard PHI from internal and external threats. By effectively protecting PHI, Rockvale Hospital can maintain patient trust, comply with regulatory requirements, and mitigate the risk of data breaches and privacy violations.

Task 3: Security Controls Implementation

- Address security-related concerns raised by members of our organization by implementing appropriate security controls. These controls, categorized as managerial, operational, or technical, will help mitigate risks and enforce compliance. Specific measures, such as creating an Acceptable Use Policy (AUP) and deploying Security Information and Event Management (SIEM) systems, will be tailored to address identified issues.

Task 3: Security Controls Selection

Scenario 1: Chief Medical Officer

"Our medical staff are visiting inappropriate websites and spending too much time on social media using the hospital's internet. How can we let them know that this is unacceptable and there would be serious consequences for non-compliance?"

Control Category: Operational | Control Type: Deterrent | Control: Create AUP (Acceptable Use Policy)

Explanation:

- **Control Category:** Operational controls deal with the day-to-day procedures and practices aimed at safeguarding assets.
- **Control Type:** Deterrent controls discourage individuals from violating policies or engaging in unauthorized activities.
- **Control:** Creating an Acceptable Use Policy (AUP) establishes clear guidelines for acceptable internet usage, including restrictions on visiting inappropriate websites and spending excessive time on social media. The AUP should outline the consequences for non-compliance, such as disciplinary actions or termination. This control serves as a deterrent by making employees aware of the rules and potential repercussions for violating them.

Scenario 2: IT Admin

"We have a small information security team and lack a centralized way to collect and analyze logs and identify and respond to incidents in an effective manner. We want to find the right solution to enhance our security posture and give the team the tools to build and expand the security program as the healthcare system grows."

Control Category: Technical | Control Type: Preventative | Control: Install SIEM (Security Information and Event Management)

Explanation:

- **Control Category:** Technical controls involve the use of technology to protect assets, systems, and data.
- **Control Type:** Preventative controls aim to stop security incidents from occurring.
- **Control:** Installing a Security Information and Event Management (SIEM) solution provides a centralized platform for collecting, analyzing, and correlating logs from various sources across the network. It enables proactive monitoring for security incidents, rapid incident response, and enhanced visibility into the organization's security posture. By implementing a SIEM solution, the IT team can efficiently identify and respond to security threats, thereby enhancing the overall security posture of the healthcare system.

Task 4: Risk Analysis and Mitigation

- Conduct qualitative and quantitative risk analysis to assess the potential impact of security incidents and evaluate the Return on Security Investment (ROSI) associated with implementing a next-generation SIEM solution. By quantifying risks and analyzing the costeffectiveness of security solutions, we can make informed decisions to mitigate threats effectively.

Qualitative and Quantitative Risk Analysis:

- **Key Metrics:**
  - Security incidents per month: 1
    - Annual rate of occurrence (ARO): 12 attacks per year (one incident per month)
  - Cost per incident (Single Loss Expectancy (SLE)): $10,000
  - Total annual cost of incidents (Annual Loss Expectancy (ALE)): $10,000 * 12 = $120,000
  - ALE Modified (ALEm) mitigation ratio: 90%
  - Cost of new SIEM solution: $25,000 for license fees + $5,000 for training, installation, and maintenance = $30,000.
- **Amount Saved Per Year:**
  - 90% of incidents blocked, reducing annual cost of incidents by 90%.
  - Reduction in cost due to the SIEM solution: 90% of $120,000 = $108,000
- **Calculate Return on Security Investment (ROSI):**
  - Return on Security Investment (ROSI) in percentages:
    - (ALE * ALEm) - Cost of Solution / Cost of Solution
    - = (($120,000 * 0.90) - $30,000) / $30,000
    - = ($108,000 - $30,000) / $30,000
    - = $78,000 / $30,000
    - = 2.6 or 260%
- **Appropriate Risk Response:** Mitigate.
  - Based on the ROSI of 260%, the appropriate risk response is to mitigate the risk by implementing the SIEM solution.
- **Final Recommendations:**
  - Final recommendation to the executive leadership: Based on my findings the best option going forward would be to purchase the next-gen SIEM solution with UEBA/SOAR to enhance security posture and effectively respond to security incidents.

Task 5: Incident Diagnosis and Response

- Review recent support tickets to diagnose potential security incidents and identify adversary techniques and tactics used. This analysis will inform our incident response strategies and enhance our ability to detect and mitigate future threats.

1) **Diagnosis of Tickets: 3**
2) Ticket #1
    a) **Ticket # 1002 |Date: 2/2/2022 | Submitted By: Bob Wood (Accountant)**
        i. *I received an email from my manager, Kieth James asking me to make an emergency payment to his friend. He mentioned that this was a personal payment and that he would repay the money the next day. He shared his friend's bank account details. What should I do?*
            1. Tier 1 support notes | Looked at email message - received from Keith James <cfoonline@cox.net>. This domain does not belong to the hospital.
                a. Diagnosis: Spear Phishing
                    i. Explanation: The attacker targeted Bob by impersonating his manager, a technique often used in spear phishing attacks where the attacker customizes the phishing attempt to a specific individual or organization.
                b. Adversary Technique: Spoofing
                    ii. Explanation: The attacker spoofed the email address of Bob's manager to appear legitimate, aiming to deceive Bob into believing the request is genuine.
                c. Adversary Tactic: Urgency
                    iii. Explanation: By creating a sense of urgency (claiming it's an emergency payment), the attacker tries to pressure Bob into acting quickly without questioning the legitimacy of the request.
3) Ticket #2:
    b) Ticket # 1207 |Date: 2/8/2022 | Submitted By: James Clay (Admin Assistant)

i. *I received a call from one of our senior doctors. Well, he said he was the head neurosurgeon. He was angry that the printer was not working and threatened to fire me. He emailed me a file that needed to be printed. I opened it but there was no document. It's weird, every hour my application closes, and my computer restarts.*

1. Tier 1 support notes | Found a script running in scheduled tasks to force a computer restart.

a. Diagnosis: Hoax

i. Explanation: The caller falsely claimed to be a senior doctor and used intimidation tactics to coerce James into complying with their demands.

b. Adversary Technique: Logic Bomb

ii. Explanation: The file sent to James contained a script that triggered periodic computer restarts, disrupting normal operations.

c. Adversary Tactic: Intimidation

iii. Explanation: The caller threatened James with job termination to intimidate him into complying with their instructions.

4) Ticket #3:

c) Ticket # 1345 |Date: 2/9/2022 | Submitted By: Shiela Shaz (Nurse)

i. *I received an email from IT to install an application to update my security settings. I was asked to install the application ASAP as the hospital was under a major cyber threat. Now, when I try to open the hospital website, I am unable to log in even if I provide the correct credentials. Similarly, I am unable to log in to my bank website. Several websites that are opening look fake. What did they make me install?*

1. Tier 1 support notes | Found router DNS settings to be misconfigured with malicious entries.

a. Diagnosis: Phishing

i. Explanation: Shiela was tricked into installing malicious software by a fake email claiming to be from IT, a common tactic used in phishing attacks.

b. Adversary Technique: Spoofing

ii. Explanation: The attacker spoofed the email to make it appear as if it came from the hospital's, IT department, aiming to deceive Shiela into trusting the instructions.

c. Adversary Tactic: Urgency

    iii. Explanation: The urgency conveyed in the email pressured Shiela to act quickly, bypassing her usual caution when installing software.

Task 6: Prevention Strategies

- Develop comprehensive prevention strategies against social engineering attacks, emphasizing security awareness training for all employees. By educating our workforce on recognizing and responding to phishing attempts, spoofing, and other manipulation tactics, we can fortify our defenses against cyber threats.

Best Prevention Against Social Engineering Attacks:

The **BEST** prevention against social engineering attacks is comprehensive security awareness training for all employees, teaching them to recognize and respond appropriately to suspicious emails, phone calls, and other attempts to manipulate them into divulging sensitive information or performing unauthorized actions. To implement a means to bring more comprehensive security awareness would be introducing forms of training/exposure/rules by way of Phishing simulations, Multi-factor Authentication, systematic email filtering and content scanning, as well as a Policy Enforcement and Incident Response Protocol.

By implementing these prevention strategies, Rockvale Hospital can substantially bolster its defenses against social engineering attacks, reduce the risk of data breaches and other security incidents. They can promote a culture of cybersecurity awareness and resilience among its employees. Investing in proactive means to mitigate social engineering risks are essential for safeguarding patient data, preserving organizational integrity, and maintaining trust with stakeholders.

The security posture review of Rockvale Hospital is a critical undertaking aimed at fortifying our defenses, ensuring regulatory compliance, and safeguarding the continuity of our operations. By addressing vulnerabilities, implementing robust security controls, and developing a culture of security awareness, we will strengthen our resilience against cyber threats and uphold our commitment to patient care and organizational integrity.