HEALTH CARE INCIDENT

EMMANUEL OWUSU OBENG

Agenda

- Executive Summary
- Incident Analysis
- Communication
- Risk Analysis and Business Analysis
- Strategy

Case Study

A large healthcare provider employs thousands of individuals and provides services for millions of customers across the country, ranging from blood tests, ultrasounds, x-rays and more. With personnel and equipment across distributed locations, cybersecurity and the management of information should be a top priority.

Case Details

Unfortunately, despite having some cybersecurity personnel and protections in place (rather limited, and under the guidance of a general IT department), this organization has experienced a breach which exposed the financial and medical data of over 4 million customers. The data included the address, phone number, social security number, name, date of birth and associated medical records of individuals. The breach was caused by an individual hacker who sent a phishing email. This email was opened by an employee on a computer which should be strictly used for tests and collecting medical test data. This computer can relay the data back to the servers for storage, and as such was not equipped with antivirus since it's not meant for regular internet use. While not being equipped with antivirus, the computer's operating system and software was up-to-date through an automated system that the security team had put in place across all computers. By opening the email, malware was unknowingly deployed , slowly making its way across systems without detection. While the breach initially took place on March 15th of last year, it was not discovered until roughly 6 months later on September 23rd. While this healthcare provider was working with a contracted security company to resolve the issue, the breach was not disclosed to the public until November 18th roughly a 2 month timeframe. The disclosure simply indicated the severity of the situation to potentially affected customers and that the company was taking steps to resolve the issues. No messages were sent to any other party beyond the public disclosure.

Upon further investigation, the contracted security company determined that there were no backups made of customer data, and the data as it has been stored is not encrypted. Beyond these discoveries, the medical equipment used to perform tests was found to operate with default credentials that can be found in manuals or online. These credentials allow the manufacturer to update the equipment remotely and transmit data. While the transfer protocols for this data are secure, this meant that a threat actor could gain access to the onboard computers in the equipment because these credentials were not changed or made unique from the manufacturer. Due to the limited security measures in place, the company is facing a lawsuit, and its reputation as a leading provider of healthcare services has been compromised. Internally, employees are also unsure how to proceed with operations and are fearful of creating a similar circumstance.

Going forward, executives are looking to expand the business by branching out further into personal health. They want to launch a new paid app that gathers an individual's health data (e.g. sleep, hydration, location, active minutes, etc.) and aggregates it with the company's existing customer health records. This service operates on a subscription basis which requires a credit card. The purpose of aggregating this data is to provide benefits such as customized nutrition and meal recommendations, exercises, and unique insights on how a user's health is trending. The app uses an algorithm to determine a proprietary "health score" which is based on the extensive data being collected

Executive Summary

- Phishing attack in the form of email
- Email was interacted with
- Malware was activated and installed
- Malware infested their systems for 6 months
- Breach was noticed but wasn‘t disclosed until after 2 months

- ***Key infomation***
- Threat was a phishing attack
- It was carried by an individual hacker .
- Data was very sensitive as it contained **Personal** , **Financial** and a **medical** data.
- The impact was also severe ; *Reputational*, *legal* and *operational*

Incident Analysis

Elements Of The CIA Triad Compromised

- Confidentiality : Personal data was exposed
- Integrity : Data may have been tampered

Factors of the Breach: People, Process and technology

People

- An employee unknowingly opened a malicious email.
- The IT team failed to implement adequate security protocols
- Executives did not disclose the breach in time

Process

- Lack of proper phishing awareness training
- Incident Response

Technology

- Data was encrypted
- No real time monitoring and alert systems for breach
- Lack of network segmentation

Risk Management

IMMEDIATE ACTIONS

- Notify customers in compliance with GDPR (Must be done within 72 hours)
- Work with law enforcements and cybersecurity agencies.
- Isolate infected systems and restrict access
- Deploy SIEM systems to detect, prevent and mitigate future incidents.
- Train employees on phishing attacks and cybersecurity threats.
- Install antivirus software and implement network segmentation for better security.
- Secure medical devices with stronger passwords or improved login details.

Long term Action

- Implement a Zero trust policy.
- Conduct regular audits and simulated cyberattack drills.
- Establish an internal cybersecurity team.

New App integration

- Conduct thorough security assessments before collecting additional customer data.
- Use a secure payment gateway and comply with PCI-DSS standards.
- Provide customers with options to opt out of providing certain data.
- Implement tokenization for credit card transactions to avoid storing raw card details.

Likelihood of reoccurrence is high

- Phishing attacks are increasing and may recur if adequate training is not provided.
- Lake of network segregation means that any infection could spread rapidly.
- Medical devices still use generic login credentials, making them highly vulnerable to breaches.

- Given this high likelihood of recurrence, this issue should be included in the future risk register.

Risk Register

Risk	Priority (Likelihood x Impact)	Risk Management Approach	Solution
Phishing	High	Employee training , email filtering	Conduct cyber threat training for staffs and implement strong email filtering policies .
Unsecured medical devices	High	Change default credentials	Change the default credentials to one which is secure and difficult to hack
Lack of Data encryption	Medium	Implement and enforce secure encryption on stored and transferred data	All data must be encrypted both at rest and in transit
Regulatory non-compliance	Medium	Regular Audit	Comply to all legal and regulatory standards
Insider threat	Medium	Network segregation , Backups and monitoring systems real-	Implement role based privileges and conduct real-time monitoring on users activities .

Risk Management Approaches

- ***Risk Avoidance***: Remove default credentials and prevent unnecessary internet access for sensitive devices.
- ***Risk Reduction***: Implement security awareness training, AI-based threat detention,and apply Multi-factor -Authentication (MFA).
- ***Risk Sharing***: Partner with cyber insurance providers to mitigate potential financial losses.
- ***Risk Acceptance***: Maintain a risk register and define acceptable risk management thresholds.

Cybersecurity Strategy

The company currently operates at a low-to-moderate level of cybersecurity maturity, with several critical gaps that need to be addressed

- Insufficient Security Personnel.
- Lack of Proactive Monitoring.
- Network Vulnerabilities.
- Inadequate Endpoint Security..
- Data Protection Failures.
- Risky Medical Equipment.

NIST Framework

The company should enhance its Cybersecurity posture by improving the following functions as outlined in the NIST Cybersecurity Framework (CSF)

Identify (ID)
• Perform a comprehensive risk assessment on systems that manage sensitive medical and financial data.
• Establish a vendor risk management specifically for medical equipment manufacturers.

Protect (PR)
• Implement network segmentation to limit the spread of malware within the network.
• Enforce multi-factor authentication (MFA) for access to all critical systems.

Detect (DE)
• Deploy a Security Information and Event Management (SIEM) system to monitor logs and identify suspicious activities.
• Set up automated mechanisms for threat detection and alerting.

Respond (RS)
• Develop an Incident Response (IR) Plan that clearly defines roles and actions in the event of a security breache.
• Provide regular cybersecurity training to reduce phishing risks.

Recover (RC)
• Create and regularly test disaster recovery plans, ensuring offline encrypted backups are available.
• Conduct post-incident reviews to refine and improve response strategies.

What to do to address risk identified

1. Implement a strict endpoint security
2. Enforce strict access controls
3. Encrypt sensitive data
4. Develop a security awareness program
5. Monitor system logs with SIEM

People

• Hire a dedicated cybersecurity team (SOC analysts, IR specialists).
• Train existing IT staff on security fundamentals.

Technical

• SIEM & log management tools (e.g., Splunk, Microsoft Sentinel).
• Endpoint security solutions (EDR, anti-malware software).
• Network segmentation solutions (firewalls, VLANs).
• Encryption tools for customer data protection.

Capabilities

• Incident response & forensics expertise.
• Regulatory compliance knowledge (HIPAA, GDPR).
• Threat intelligence & proactive monitoring.

KEY TAKEAWAYS

To prevent future incidents, the company should

1. Dedicated Cybersecurity Team..
2. Cybersecurity Governance Framework.
3. AI-Driven Threat Detection..
4. Compliance with Healthcare Regulations.
5. Employee Awareness programs.