

Incident Scenario : MedData Solution Breach

Task 1: CNSS Model (McCumber Cude) Analysis

Map The breach across the three dimensions of the CNSS Model

- **Identify which Information Characteristics were compromised and at which stage**
 - Confidentiality
 - Confidentiality was compromised when attackers exfiltrated sensitive patient health records.
 - Unauthorised individuals gained access to medical information.
 - The use of unencrypted internal communication channels increased the risk of data exposure.
 - Integrity
 - Integrity was compromised because ransomware altered and encrypted database contents.
 - Authorised users could no longer trust the accuracy and completeness of the stored data.
 - Availability
 - Availability was severely impacted when ransomware encrypted local databases.
 - Employees and customer could not access health records and analytics services during the attack.
- **Identify the Information Stated involved.**
 - Storage
 - Patient records stored on the legacy server were encrypted by ransomware.
 - Stored data became inaccessible to authorized users.
 - Transmission
 - Patient data transmitted across internal unencrypted channels was intercepted and stolen.
 - Data moving between systems lacked appropriate protection.
 - Processing
 - Processing functions were disrupted because encrypted databases prevented applications from accessing and processing health records normally.
- **Identify which Security Countermeasures failed or were missing explaining how their absence enabled the breach.**
 - Policy
 - No formal Enterprise Information Security Policy (EISP) existed.
 - There were also no clearly defined security standards for patch management, encryption, risk management, or system upgrades.
 - Executive management did not prioritize cybersecurity governance.

- Education
 - No Security Education, Training, and Awareness (SETA) program was implemented.
 - Employee and managers lacked awareness about cybersecurity risks.
- Technology
 - An Outdated legacy server remained unpatched and vulnerable.
 - Insufficient security controls allowed attackers to exploit a zero-day vulnerability and deploy ransomware.

Its cost them \$7m to settle everything. An estimated 100,000 – 1M records were affected.

Task 2 : Governance vs Management & Communities of interest

- **Analyze the breakdown between Governance and Management .**
 - Governance
 - Governance is responsible for providing strategic direction, ensuring risks are managed appropriately, and making cybersecurity an organizational priority.
 - They rejected funding requests to replace the vulnerable legacy server and failed to establish an effective cybersecurity strategy. This created conditions that allowed the attack to occur.
 - Management
 - Management is responsible for implementing security controls, policies, and operational processes.
 - The InfoSec manager failed to establish a formal Enterprise Information Security Policy (EISP) and did not implement a Security Education, Training, and Awareness (SETA) program.
- **Discuss how misaligned priorities among the three Communities of Interest contributed to this failure.**
 - InfoSec
 - No formal EISP was established.
 - No Employee security awareness training was provided.
 - Security risks were not effectively communicated to senior leadership.
 - IT
 - IT correctly recognized the vulnerability.
 - Management ignored IT's recommendation to modernize the infrastructure.
 - Non-Technical Management
 - Non-technical management is responsible for balancing business objectives with organizational risk.
 - Cybersecurity risks were not integrated into strategic business planning.

Task 3 : Strategic Remediation via the “Six Ps”

- **Planning**
 - MedData Solution should develop a comprehensive information security strategy that aligns with business objectives and addresses identified risks.
 - The organization should conduct regular risk assessments, create incident response plans, disaster recovery plans, and business continuity plans to ensure preparedness for future cyberattacks.
- **Policy**
 - The company should establish a formal Enterprise Information Security Policy (EISP) that defines security responsibility, risk management requirement, access controls, data protection standards, and patch management procedures.
 - Additional Issue-Specific Security policies (ISSPs) should be implemented for areas such as encryption, acceptable use, data handling, and incident reporting .
- **Programs**
 - MedData Solutions should introduce a Security Education, Training and Awareness (SETA) program to educate employees about cyber threat, phishing attacks, ransomware risks and security best practices.
 - Regular awareness campaigns, simulations and compliance training should be conducted to strengthen the organization’s overall security culture.
- **Protection**
 - The organization should implement stronger technical security controls, including Replacing outdated legacy servers, Applying regular security patches and updates, Encrypting sensitive data both at rest and in transit, and implementing multi-factor authentication(MFA).
- **People**
 - Employees, Managers and executives must be actively involved in cybersecurity efforts.
 - Security responsibilities should be clearly defined, and management should prompt a culture where cybersecurity is viewed as a shared responsibility rather than solely an IT function.
- **Project Management**
 - The remediation program should be managed as a formal security project with defined objectives, timelines, budgets, and performance metrics.
 - Progress should be continuously monitored to ensure that security improvements are implemented effectively and within agreed deadlines.