Task ‘Cybersecurity Threat Assessment and Mitigation Plan’ Unit 8

The MedCoreTelePac Threat from Ransomware groups

Introduction

Businesses today are under constant threat from different threat actors, each with different motivations. This Cybersecurity Threat Assessment and Mitigation Plan addresses the recent cyber threats and vulnerabilities affecting MedCoreTelePac. It provides a detailed overview of the identified threats and vulnerabilities, along with the proposed mitigation strategies. The ethical and legal considerations of these scenarios are also covered.

Identified Threats and Vulnerabilities

A security assessment of MedCoreTelePac's IT and operational systems was initiated and critical vulnerabilities were exposed, including the lack of encryption. Outdated access controls, firewalls lack modern functionality and excessive rules. MFA is not enforced in many areas. Assets management and security event monitoring are lacking. The organization is subject to US and EU medical device regulations. Some events have been identified and classified as attempted intrusion attacks and investigations have revealed potential attacks. The company is being targeted by various ransomware groups. One of the company's branch offices is located at FEMA flooding area.

(McKey, 2024).

Detailed Mitigation Strategies with Justifications

Establish effective control measures, policies, guidelines and procedures

Justification: Instructions like patch and change management processes can reduce the probability and impact of negative events.

Move the data center to higher ground

Justification: Reduces the probability of negative events from occurring and the impact when these do occur, for instance, in this case, flooding.

Implement detective and preventive measures

Justification: Effective firewall and SOC/EDR with active malware protection are very effective in reducing risk to an acceptable level.

Set an effective organization wide asset management

Justification: include structured visibility and accountability for assets. While it is an ITSM tool, it supports security and could integrate with vulnerability scanners.

Apply compensating measures such as MFA

Justification: Combined with "Type 1 authentication" and one-time password (OTP), it reduces the risk of unauthorized access.

Develop controls such as an emergency incident response lifecycle (IR) and disaster recovery planning (DRP)

Justification: Helps ensure the ability to restore the business back to operational state after a disaster.

Conduct threat modelling

Justification: Helps to identify and protect new solutions before being introduced.

Encrypt data at rest, in transit, and in use

Justification: Includes data routes, communication tools, databases, and network connections — this is crucial for maintaining confidentiality.

Encrypt backups and maintain off-site backups

Justification: Ensures backups can be retrieved in the event of a natural disaster or any other scenario.

Ensure most up-to-date hashing algorithm

Justification: Use a SHA-256, SHA-384, SHA-512 or SHA-3-256 hashing algorithm for all software to ensure data integrity.

Protect all HTTPS-based connections, browsers, and APIs

Use TLS 1.2 or 1.3, along with a certificate management solution and PKI, to maintain integrity and confidentiality.

Adopt ISO/IEC standards

Justification: ISO/IEC 27001 provides a high-level standard strategy, and ISO/IEC 27002 offers more in-depth practical guidelines for implementing mitigation strategies.

Discussion of Ethical and Legal Considerations Related to the Scenario

It is essential to establish data classification and data handling policies that clearly and strictly define how data is to be managed, collected, and retained. This will help reduce the risk of a breach and, therefore, liability in the event of a violation. Furthermore, this improves the alignment with compliance with regulatory requirements, for instance the FDA, EU-MDR and GDPR regulations, thereby reducing potential risks. Failing to notify the relevant parties within the required timeframe (for instance, Article 33 of the GDPR) could lead to penalties and additional unplanned costs.

(Malka, 2025)

References

McKey, M., (2024). Coastal Resilience: Environmental Hazards, Development, and Insurance in Southern Mississippi Available at: https://egrove.olemiss.edu/hon_thesis/3065/ [Accessed 10 September. 2025]

Malka, A, (2025). Security Risk Assessment Report: Security Measures to Mitigate Risks Unit 7 Available at: https://www.my-course.co.uk/mod/assign/view.php?id=1218399 [Accessed 10 September. 2025]

This document has been written solely for educational purposes. All references, names, and trademarks mentioned here remain the property of their respective owners and are used here strictly for the educational context. Grammarly was used exclusively for proofreading and enhancing the clarity and language of the text. All academic writing, analysis, argumentation, and conclusions are entirely the original work of the author.