**MODOO3264 – Digital Security**

**Comprehensive Assessment and Response Strategy for Mars University**

**Project Proposal Final Report**

**Element 010**

**─** Module Leader: Muhammad Nouman Nafees

**Prepared by:**

**SID:**

**Submission Date: 11-04-2025**

**Word Count: 2214**

Table of Contents

[1. Introduction 3](#_Toc195222543)

[2. Task 1: Risk Assessment 3](#_Toc195222544)

[A. Identification of Security Risks 3](#_Toc195222545)

[B. Risk Assessment Methodology and Analysis 4](#_Toc195222546)

[C. Threat Modeling and Justification 5](#_Toc195222547)

[3. Task 2: Cryptographic Security and Data Protection 6](#_Toc195222548)

[A. Identification of Cryptographic Security Needs 6](#_Toc195222549)

[B. Implementation of Encryption Mechanisms 6](#_Toc195222550)

[C. Cryptographic Performance Considerations 7](#_Toc195222551)

[4. Task 3: Incident Response Plan 8](#_Toc195222552)

[A. Cyber Incident Selection and Justification 8](#_Toc195222553)

[B. Structured Incident Response Plan (NIST Framework) 8](#_Toc195222554)

[C. Forensic Analysis and Threat Intelligence Integration 9](#_Toc195222555)

[5. Conclusion 10](#_Toc195222556)

[6. References 11](#_Toc195222557)

# **1.** Introduction

Mars University, a global leader in space exploration and AI, has recently been the target of a series of cyber-attacks, from malware to DDoS and unauthorized access, that have exposed profound vulnerabilities in its web presence. With a large-scale virtual presence, off-site research activities, and reliance on BYOD and cloud platforms, the university is highly susceptible to advanced, dynamic threats. This report offers a comprehensive cybersecurity strategy built on the foundation of three pillars: an environment-specific risk assessment, cryptographic shielding of sensitive data, and an incident response plan in proportion with the threats of today all built to realize the highest levels of academic and security distinction.

# **2. Task 1: Risk Assessment**

## **A. Identification of Security Risks**

A thorough risk analysis was performed to emphasize deficiencies most applicable to Mars University's operational context:

1. **Insider Threats (Negligent and Malicious):** In an information-sharing educational community, there is a high likelihood that an internal user will misuse access. Employees may inadvertently manage sensitive research, or students will misuse shared systems. A sample of a disgruntled IT administrator who reveals confidential grant proposals would result in reputational as well as financial loss. This threat has a devastating impact on Confidentiality and Integrity.
2. **Phishing and Social Engineering Campaigns:** Phishing attacks are most frequently targeted at academic institutions by attackers due to high user turnover and an open network environment. Advanced spear-phishing emails would trick employees into revealing credentials, which would jeopardize the system. Compromised credentials would then be exploited to pivot into admin portals, cloud storage, or grant databases.
3. **Distributed Denial of Service (DDoS) Attacks:** These attacks make services such as learning management systems, academic portals, and library networks unavailable. A well-coordinated DDoS attack during examination time can shut down online test systems and interfere with distance learning, contravening the Availability principle.
4. **Unsegmented and Flat Network Topology:** In the absence of network segmentation by layers (i.e., firewalls or VLANs), a compromised machine will allow an attacker to move laterally into more sensitive domains—e.g., financial or HR databases. This is a risk that is multi-dimensional along the CIA triad.
5. **Cloud Misconfigurations and Data Leaks:** As an increasing dependency upon platforms such as AWS, Google Cloud, and Microsoft 365 is growing, misconfigured S3 buckets, incorrect IAM roles, or unavailability of encryption controls may cause highly sensitive research, provide access to grant, and individual student records.
6. **Stale Software and Patch Management Failure:** Idle machines for unexplained purposes can be susceptible to exploitation of well-known attacks such as EternalBlue (CVE-2017-0144) or Log4Shell (CVE-2021-44228) and cause data leakage or remote code execution.
7. **Ineffective Authentication Mechanisms:** Without multifactor authentication (MFA), systems are susceptible to brute-force as well as credential stuffing attacks. Sharing the same password across multiple platforms or keeping passwords in plaintext raises the threats manifold.

All such threats were evaluated according to Mars University's cyber priorities and framework, maintaining their essential role in academic continuity, research integrity, and data confidentiality.

## **B. Risk Assessment Methodology and Analysis**

In order to give a structured and data-based evaluation, a combination of NIST Risk Management Framework (RMF), ISO/IEC 27005:2018, and FAIR (Factor Analysis of Information Risk) methodology was used.

* **Step 1: Asset Identification** – Determining the core assets of the university: student databases and research databases, transactional financial systems, collaboration tools in the cloud, endpoint devices, and network infrastructure.
* **Step 2: Identification of Threats** – Threats were classified as external (e.g., nation-state attackers, ransomware attackers), internal (malcontent or careless users), and environmental (e.g., power outages impacting availability).
* **Step 3: Vulnerability Analysis** – Mars University's setup contains vulnerabilities in the form of legacy systems, disparate access controls, novice employees, and divided visibility between departments.
* **Step 4: Impact and Likelihood Assessment**:
  + **Qualitative**: Utilized heat maps to determine likelihood and business impact scores for risks.
  + **Quantitative**: For instance, revelation of AI research data worth £1.2 million with threat probability 0.6 and vulnerability impact 0.75 gives an expected risk impact of £540,000.

Internal logs, penetration testing reports, and benchmarks like IBM's Cost of a Data Breach report were used to validate assumptions. Risk levels were then prioritized for mitigation, incident response planning, and governance control.

## **C. Threat Modeling and Justification**

Mars University culture requires a scalable and holistic response to threat modeling. Microsoft STRIDE was chosen because it was flexible and simple. All of the six categories of STRIDE were employed:

* **Spoofing:** Spoofed university email addresses can be used by the attackers to phish the staff. SSO systems are particularly susceptible to identity-based attacks.
* **Tampering:** Manipulating research data or gradebooks kept in shared folders can violate academic integrity.
* **Repudiation:** Without audit logs, attackers can deny their actions, particularly in multi-access environments.
* **Information Disclosure:** An insecurely stored unencrypted database backup on a misconfigured server may reveal confidential research or student information.
* **Denial of Service:** A cyberattacker might use open ports or amplify traffic to crash important servers.
* **Privilege Elevation:** An attacker who leverages a misconfigured application in order to attain administrator privileges on the Active Directory of the university.

STRIDE's control mapping allowed the university to predict threat vectors in application, user, network, and infrastructure layers. The framework made control mapping to OWASP ASVS and ISO/IEC 27001 Annex A possible.

# **3. Task 2: Cryptographic Security and Data Protection**

## **A. Identification of Cryptographic Security Needs**

Cryptographic security has to be implemented throughout Mars University's computer system, especially the very sensitive and controlled nature of its data. Some areas have to be encrypted with cryptography

1. **User Verification:** Authentication mechanisms must be public-key infrastructure (PKI) based, with certificate-based login supported by passwords. Multi-factor authentication (MFA), employing time-based one-time passwords (TOTP) or biometric authentication, provides strong identity verification.
2. **Safe Storage of Data:** Cryptography-at-rest with AES-256 must be employed in order to protect intellectual property or government-funded research. Confidential information such as exam records, transcripts, or financial aid information must also employ cryptography as per GDPR and UK data protection law.
3. **Encrypted Communications:** Remote work, university-to-university collaboration, and cloud access require end-to-end encryption of all communications. These include emails, chat software, and file transfers via TLS 1.3 and secure VPN protocols like OpenVPN or WireGuard.
4. **Financial Transactions:** Payment systems for tuition and grants online should be protected by secure payment gateways and SSL certificates. Tokenization and strong encryption secure payment fraud and ensure PCI-DSS compliance.
5. **Cloud Storage:** Student study material and university files are generally stored in OneDrive, Google Drive, or AWS S3. All these should have encryption in transit and at rest on the basis of KMS (Key Management Services) with role-based key access controls.

These articles touch upon significant aspects of the CIA triad — confidentiality of research and individual information, integrity of financial and examination data, and availability of assets without tampering or unauthorized entry.

## **B. Implementation of Encryption Mechanisms**

Mars University must have a tailor-made layered encryption framework for particular targeted use cases at endpoints, servers, and in the cloud:

* **Symmetric Encryption (AES-256):** Suitable for encrypting large data sets at high speeds, like university assignments or teacher directories. Use Galois/Counter Mode (GCM) to include both encryption and integrity checks.
* **Asymmetric Encryption (RSA-2048/ECC): Used** for encrypting e-mails (using S/MIME or PGP) and SSL certificates. ECC (Elliptic Curve Cryptography) can be used by mobile and embedded devices because it is cost-effective.
* **Hashing (SHA-256 and bcrypt):** Employed to store passwords securely in databases and check for software or document integrity. Bcrypt provides salting and stretching of the key to better resist brute-force attacks.
* **TLS 1.3 with Forward Secrecy:** All online processes, including the university portal and payment plans, must have TLS 1.3 configuration to provide HTTPS connections secured through ephemeral key exchanges for Perfect Forward Secrecy (PFS).
* **Key Management Systems (KMS):** Employ centrally managed KMS, ideally hardware-based (HSMs), to provision, rotate, and retire keys. Use Active Directory or Azure AD for access and logging.
* **Backup Encryption:** Backup information must be encrypted by full-disk or file-level encryption and must be kept in secure containers offsite.

The encryption design needs to be checked annually and updated as part of the security maintenance cycle of the university.

## **C. Cryptographic Performance Considerations**

Cryptographic protocols have to be chosen on the basis of a compromise between computational efficiency, scalability, and long-term security:

* **AES-256 versus ChaCha20:**
  + AES-256 is Intel processor hardware-accelerated (AES-NI) and hence optimized on university workstations and servers.
  + ChaCha20 is optimized for performance on mobile clients and browser clients, perfect for BYOD environments or student portals.
* **Post-Quantum Cryptography (PQC):**
  + With the extended retention periods of student and research data, PQC is necessary. Mars University can start testing NIST PQC finalist algorithms like CRYSTALS-Kyber (key exchange) and Dilithium (digital signatures).
  + Increased key sizes, higher CPU utilization, and backward compatibility are some of the issues. These issues can be solved by hybrid key exchange (classical + quantum-safe) and phased-deployment in non-critical systems.

Performance statistics must be monitored constantly, and encryption thresholds must be invoked on system upgrades to achieve maximum throughput with minimum overhead.

# **4. Task 3: Incident Response Plan**

## **A. Cyber Incident Selection and Justification**

The attack selected is a successful ransomware attack via spear-phishing email, against academic staff during exam marking. It is a real, successful, and well-documented ransomware attack against UK organizations:

* **Technique:** Phishing email that appears to be from internal IT support asks users to download an "urgent patch" as a Word document with malicious macros.
* **Execution:** The malware encrypts network-shared and local files, demands Bitcoin payment, and threatens to leak data.
* **Impact:**
* Denial of access to educational resources, suspension of graduation and grading activities.
* Possible exposure of students' personal information, triggering GDPR reporting.
* Downtime, reputation loss, and recovery cost.

It is characteristic of current trends where ransomware gangs take advantage of busy institutions. It emphasizes preparedness, resilience, and swift recovery actions.

## **B. Structured Incident Response Plan (NIST Framework)**

The response plan is founded on the NIST SP 800-61r2 Computer Security Incident Handling Guide, which is structured into four major stages:

1. **Preparation:**
   * Establish a Cyber Incident Response Team (CIRT) with defined roles (e.g., incident commander, forensic analyst, communications lead).
   * Offer training and simulation exercises (e.g., phishing exercises).
   * Develop phishing, ransomware, and insider threat playbooks and checklists.
2. **Detection and Analysis:**
   * Monitor logs using SIEM products (e.g., Splunk, Microsoft Sentinel).
   * Detect ransomware activity through EDR tool monitoring (e.g., mass file encryption, registry modifications).
   * Indicators of Compromise (IoCs), file hashes, and malicious IPs.
   * Log discovery time, infected systems, and scope of infection.
3. **Containment, Eradication, and Recovery:**
   * Segment infects endpoints from the network.
   * Disable impacted accounts and remove access tokens.
   * Forensically delete malware and reimaged systems.
   * Restore de backups limpos and validate file integrity with hash checks.
   * Inform stakeholders like employees, students, and police officials as and when necessary.
4. **Post-Incident Activities**

* Root cause analysis.
* Effectiveness of detection, response, and containment.
* Policies, procedures, and incident runbooks update.
* Share threat intelligence with UK's NCSC and education-sector threat sharing groups.

This managed methodology minimizes reaction time, preserves evidence for forensic examination, and enables security posture to evolve continuously.

## **C. Forensic Analysis and Threat Intelligence Integration**

Post-breach forensic analysis would be needed to determine how the breach happened and how to prevent breach occurrences in the future:

* **Forensic Steps:**
  + Review access logs, firewall events, and endpoint event logs to recreate the attack timeline.
  + Use memory analysis (e.g., Volatility Framework) to examine ransomware activity.
  + Conduct static analysis and dynamic malware analysis in a sandbox.
* **Threat Intelligence Integration:**
  + Exchange IoCs with databases like VirusTotal, MISP, and MITRE ATT&CK for correlation of patterns.
  + Subscribe to industry-specific threat feeds (e.g., Jisc, UK NCSC) to receive alerts and signature updates.
  + Replay detection rule based on reverse-engineered malware indicators.
* **Lessons Learned:** 
  + Recognize technical control weaknesses (e.g., lack of MFA, unmonitored devices). Measure the effect of incidents in terms of downtime, data loss, and user confidence.
  + Define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). This cross-forensic and intelligence loop converts every incident into an avenue for hardened defenses and institution building resilience.

# **5. Conclusion**

Mars University is based in an active, high-risk cyber world. The report has identified several interrelated security issues and recommended a layered reaction. Utilizing thoroughly tested frameworks such as STRIDE, ISO 27005, and NIST SP 800-61r2, we have suggested measurable measures to prevent threats, enhance cryptographic capacity, and establish an adaptive incident response process. Through dedication of its leadership, implementation of technical controls, and ongoing adaptation, the university can create a secure cyber world for its academic and research constituents.

# **6. References**

1. **National Institute of Standards and Technology (NIST),** 2012. *Guide for Conducting Risk Assessments (SP 800-30 Rev. 1).* Gaithersburg, MD: NIST. Available at: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>
2. **National Institute of Standards and Technology (NIST),** 2020. *Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5).* Gaithersburg, MD: NIST.
3. **National Institute of Standards and Technology (NIST),** 2018. *Computer Security Incident Handling Guide (SP 800-61r2).* Gaithersburg, MD: NIST.
4. **ISO/IEC,** 2018. *ISO/IEC 27005:2018 Information Security Risk Management.* Geneva: International Organization for Standardization.
5. **Microsoft,** 2023. *STRIDE Threat Modeling.* Microsoft Docs. Available at: <https://docs.microsoft.com/en-us/security/compass/stride-threat-modeling>
6. **OWASP,** 2023. *OWASP Top Ten 2023.* Available at: <https://owasp.org/www-project-top-ten/>
7. **ENISA,** 2021. *ENISA Threat Landscape Report 2021.* European Union Agency for Cybersecurity.
8. **MITRE Corporation,** 2023. *MITRE ATT&CK Framework.* Available at: <https://attack.mitre.org/>
9. **Ali, M., Khan, S. and Vasilakos, A.V.,** 2015. Security in cloud computing: Opportunities and challenges. *Information Sciences,* 305, pp.357–383.
10. **Zetter, K.,** 2015. Inside the cunning, unprecedented hack of Ukraine’s power grid. *Wired.* Available at: https://www.wired.com/story/ukraine-power-grid-hack/
11. **ACM Digital Library,** 2023. *Cybersecurity research papers.* Available at: <https://dl.acm.org/>
12. **IEEE Xplore,** 2023. *Cybersecurity Conference Proceedings.* Available at: <https://ieeexplore.ieee.org/>
13. **Bisson, D.,** 2020. Ransomware attack brings university to a standstill. *Tripwire.* Available at: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/ransomware-attack-university/
14. **UK Government National Cyber Security Centre (NCSC),** 2023. *Ransomware guidance for education providers.* Available at: <https://www.ncsc.gov.uk/>
15. **IBM Security,** 2023. *Cost of a Data Breach Report.* Available at: <https://www.ibm.com/reports/data-breach>