NIST 800-53 Framework

Security Audit

CyberTech Innovations

By Tanasha Bryant

**Risk Mitigation Strategies**

**Introduction**

Risk mitigation is essential to safeguarding CybetTech Innovations’ systems, protecting sensitive data, and ensuring business continuity. This section outlines the strategies for mitigating identified risks to minimize their impact.

**Key high priority risks include:**

* **Phishing attacks targeting employees (CDMS):** leading to credential theft.
* **Insider threats and espionage (R&D Network):** compromising proprietary research data.
* **Supply chain attacks on third-party vendors (SCMS):** affecting operational integrity.
* **Payment fraud and financial breaches ():** posing a risk to regulatory compliance and financial stability.

**Risk Mitigation Approaches**

The mitigation strategies will follow four primary approaches:

* **Avoidance**: eliminating the risk my removing vulnerabilities or discontinuing risk processes.
* **Reduction**: implementing controls to minimize the likelihood or impact of risks.
* **Sharing**: distributing the risk through third-party partnerships or cybersecurity insurance.
* **Acceptance**: acknowledging and managing risks within defined thresholds.

**Detailed Mitigation Strategies**

For each high-priority risks, specific mitigation strategies are proposed:

1. **Phishing Attacks (CDMS)**

* **Strategy**: implement advanced email filtered and multi-factor authentication (MFA).
  + 1. **Justification**: reducing the success rate of phishing attempts protects employee credentials and sensitive data.
    2. **Steps for implementation:** 
       1. Deploy email security tools.
       2. Conduct periodic phishing simulations and awareness training.
       3. Enforce MFA for all critical system logins.
  + **Assigned Responsibilities**: IT security team and HR training department.

1. **Insider Threats (R&D Network)**
   * **Strategy:** implement Zero Trust architecture and role-based access controls (RBAC).
     1. **Justification:** restricting data access limits the potential damage from insider threats.
     2. **Steps for implementation:** 
        + Define and enforce least privilege access policies.
        + Monitor and log privileged account activities using SIEM tools.
        + Conduct regular employee background checks and behavior analysis.
   * **Assigned Responsibilities:** Cybersecurity team and compliance officers.
2. **Supply Chain Attacks (SCMS)**
   * **Strategy:** Conduct third-party assessments and implement blockchain-based tracking.
     1. **Justification:** strengthening vendor security reduces vulnerabilities in the suppl chain.
     2. **Steps for Implementation**

* Require third-party vendors to comply with cybersecurity standards (e.g., ISO 27001).
* Deploy blockchain technology to verify supply chain transactions.
* Establish a vendor risk management framework.
* **Assigned Responsibilities:** Vendor management team and IT security.

1. **Payment Fraud (PPS)**
   * **Strategy:** implement AI-based fraud detection and end-to-end encryption**.** 
     1. **Justification:** enhancing fraud detection ensures compliance with PCI DSS and reduces financial risks.
     2. **Steps for Implementation**
        + Integrate fraud detection tools into payment systems.
        + Encrypt all payment transactions in transit and at rest.
        + Implement transactions monitoring for anomalies.
   * **Assigned Responsibilities:** Payment security team and compliance officers.

**Monitoring and Review Plan**

To ensure effectiveness, mitigation strategies will be continuously monitored and reviewed:

* **Security Audits**: quarterly cybersecurity audits to assess control effectiveness.
* **Incident Reporting**: continuous monitoring through SIEM tools (Splunk, IBM QRadar) real-time threat detection.
* **Policy Updates**: regular updates to security policies in response to emerging threats.
* **Employee Training**: annual security awareness training and refresher courses.
* **Vendor Compliance Checks**: bi-annual third-party vendor security assessments.

By implementing these mitigation strategies and monitoring measures, CyberTech Innovations will enhance its cybersecurity resilience, protect sensitive data, and ensure compliance with industry regulations.

Audit Completion Sign-Off Sheet

The following personnel acknowledge that the cybersecurity audit and risk mitigation assessment have been completed and reviewed:

IT Leadership [Date]

Governance Auditor [Date]