NIST 800-53 Framework

Security Audit

CyberTech Innovations

Risk Assessment Report

By Tanasha Bryant

**Risk Assessment Report**

**Executive Summary**

The risk assessment process aims to identify, evaluate, and prioritize cybersecurity risks affecting CyberTech Innovations. This process is essential for ensuring that all critical vulnerabilities are addressed, and that the organization’s security posture aligns with industry best practices.

**Key findings include:**

* **Phishing attacks targeting employees (CDMS):** pose a significant risk due to potential credential theft.
* **Insider threats and espionage (R&D Network):** remain a concern given the proprietary nature of research data.
* **Supply chain attacks on third-party vendors (SCMS):** could compromise the integrity of operations.
* **Payment fraud and financial breaches (PPS):** presents a high-impact threat due to regulatory and financial implications.

**Methodology**

The risk assessment employs a combination of qualitative and quantitative analysis:

* **Qualitative Analysis:** evaluates risks based on expert judgement, categorizing threats into low, moderate, and high impact.
* **Quantitative Analysis:** uses a numerical data, historical breach statistics, and industry reports to assign risk likelihood and financial impact.

This hybrid approach ensures a comprehensive assessment by considering both subjective expert evaluations and data-driven insights.

**Risk Identification and Analysis**

* **Threat Intelligence Platforms:** Use of platforms like Recorded Future to analyze potential attack vectors.
* **Risk Matrices:** application of NIST 800 53 risk matrices to prioritize and categorize risk.
* **SIEM Data Analysis:** aggregation and review of security logs via Splunk and IBM QRadar for anomaly detection.
* **Vulnerability Scanning:** examination of previous security incidents to predict emerging threats.

**Risk Prioritization**

**Risks are prioritized based on likelihood and impact using a risk matrix:**

* **High Priority:** Payment fraud (PPS), phishing attacks (CDMS)
* **Medium Priority:** Supply chain vulnerabilities (SCMS), insider threats (R&D Network)
* **Low Priority:** General system misconfigurations, minor software vulnerabilities

By leveraging these tools and techniques, CyberTech Innovations ensures that all security risks are proactively identified and mitigated.