**INFORMATION SECURITY**



**Session 2023 - 2027**

**Submitted by:**

Sumaira Hafeez 2023-CS-1

**Supervised by:**

Dr. Faiza Iqbal

**Course:**

Information Security

Department of Computer Science

**University of Engineering and Technology**

**Lahore Pakistan**

Contents

[**Step 1: Risk Identification for TechCorp** 3](#_Toc194490805)

[**1. Critical Assets at Risk (Categorized)** 3](#_Toc194490806)

[**2. Major Threats to These Assets** 3](#_Toc194490807)

[**3. Threat-Vulnerability-Asset (TVA) Worksheet** 3](#_Toc194490808)

[**Step 2: Risk Assessment (Numerical Analysis) for TechCorp** 4](#_Toc194490809)

[**1. Assumptions & Baseline Metrics** 4](#_Toc194490810)

[**2. Risk Calculations** 5](#_Toc194490811)

[**3. Ranked Threats by ALE (Highest to Lowest Impact)** 5](#_Toc194490812)

[**Step 3: Risk Control Strategy Selection for TechCorp** 5](#_Toc194490813)

[**1. Insider Threat (Source Code Repositories) ALE: $12M** 6](#_Toc194490814)

[**2. Phishing (Client Financial Data) – ALE: $10M** 6](#_Toc194490815)

[**3. SQL Injection (API/Database) – ALE: $6M** 6](#_Toc194490816)

[**4. Phishing (Employee Credentials) – ALE: $3M** 6](#_Toc194490817)

[**5. Ransomware (Internal Servers) – ALE: $1.05M** 7](#_Toc194490818)

[**Step 4: Cost-Benefit Analysis (CBA) for TechCorp** 7](#_Toc194490819)

[**1. Executive Summary** 8](#_Toc194490820)

[**2. Risk Assessment Findings** 8](#_Toc194490821)

[**A. Threat-Vulnerability-Asset (TVA) Worksheet** 8](#_Toc194490822)

[**B. Risk Matrix (Likelihood vs. Impact)** 9](#_Toc194490823)

[**3. Recommended Risk Control Strategies** 9](#_Toc194490824)

[**A. Approved Controls (CBA > 1)** 9](#_Toc194490825)

[**B. Rejected Controls (CBA ≤ 1)** 9](#_Toc194490826)

[**4. Cost-Benefit Analysis (CBA) Highlights** 9](#_Toc194490827)

[**MFA Implementation Example** 9](#_Toc194490828)

**Cyber Security Risk Assessment**

# **Step 1: Risk Identification for TechCorp**

## **1. Critical Assets at Risk (Categorized)**

TechCorp’s cybersecurity risks revolves around the following key assets:

| **Asset** | **Category** | **Description** |
| --- | --- | --- |
| Client Financial Data | Data | Sensitive bank details, transaction records, and billing information. |
| Employee Credentials | People | Weak passwords, shared logins, or stolen credentials leading to unauthorized access. |
| Source Code Repositories | Software | Proprietary software code that could be stolen or corrupted. |
| Internal Servers | Hardware | On-premise servers storing PII; vulnerable to physical or remote attacks. |
| API & Database Systems | Networking | Exposed APIs or misconfigured databases allowing unauthorized data extraction. |

## **2. Major Threats to These Assets**

The most concerning threats for TechCorp include:

1. **Phishing Attacks**: Employees tricked into revealing credentials or downloading malware.
2. **Insider Threats**: Disgruntled employees or contractors leaking or sabotaging data.
3. **Ransomware Attacks**: Encryption of critical systems (e.g., databases, servers) for extortion.

## **3. Threat-Vulnerability-Asset (TVA) Worksheet**

| **Asset** | **Threat** | **Vulnerability** |
| --- | --- | --- |
| **Client Financial Data** | Phishing / Insider Threat | Lack of multi-factor authentication (MFA); excessive employee access privileges. |
| **Employee Credentials** | Phishing / Credential Stuffing | Weak password policies; no mandatory security training. |
| **Source Code Repositories** | Insider Threat / Ransomware | No code access audits; unsecured Git repositories. |
| **Internal Servers** | Ransomware / Physical Theft | Outdated firmware; no biometric access controls. |
| **API & Database Systems** | SQL Injection / API Abuse | Unpatched vulnerabilities; no rate-limiting on API calls. |

# **Step 2: Risk Assessment (Numerical Analysis) for TechCorp**

To quantify cybersecurity risks, we’ll use **historical data** and **financial impact estimates** for each threat. Below is a structured breakdown:

## **1. Assumptions & Baseline Metrics**

* **TechCorp’s Annual Revenue:** $20M (for context on potential losses).
* **Data from Past Incidents:**
  + **Phishing Attacks:** 5 incidents/year (ARO = 5).
  + **Insider Threats:** 2 incidents/year (ARO = 2).
  + **Ransomware Attacks:** 1 incident every 2 years (ARO = 0.5).

| **Asset** | **Threat** | **EF (Exposure Factor)** | **Asset Value (AV)** | **Annual Rate of Occurrence (ARO)** |
| --- | --- | --- | --- | --- |
| Client Financial Data | Phishing | 40% | $5M | 5 |
| Employee Credentials | Phishing | 30% | $2M | 5 |
| Source Code Repositories | Insider Threat | 60% | $10M | 2 |
| Internal Servers | Ransomware | 70% | $3M | 0.5 |
| API & Database Systems | SQL Injection | 50% | $4M | 3 |

## **2. Risk Calculations**

**Formulas:**

* **Single Loss Expectancy (SLE)** = AV × EF
* **Annualized Loss Expectancy (ALE)** = SLE × ARO

| **Asset** | **Threat** | **SLE (AV × EF)** | **ALE (SLE × ARO)** |
| --- | --- | --- | --- |
| Client Financial Data | Phishing | $2M | **$10M** |
| Employee Credentials | Phishing | $600K | **$3M** |
| Source Code Repositories | Insider Threat | $6M | **$12M** |
| Internal Servers | Ransomware | $2.1M | **$1.05M** |
| API & Database Systems | SQL Injection | $2M | **$6M** |

## **3. Ranked Threats by ALE (Highest to Lowest Impact)**

1. **Insider Threat (Source Code)** → **$12M ALE**
   * Why? Theft of proprietary code can cripple TechCorp’s market position and competitive advantage.
2. **Phishing (Client Financial Data)** → **$10M ALE**
   * Why? Regulatory fines and customer distrust can cause severe financial and reputational damage.
3. **SQL Injection (APIs/Databases)** → **$6M ALE**
   * Why? Exposing customer data can lead to lawsuits and loss of business credibility.
4. **Phishing (Employee Credentials)** → **$3M ALE**
   * Why? Stolen credentials enable further exploits like privilege escalation and data breaches.
5. **Ransomware (Servers)** → **$1.05M ALE**
   * Why? While less frequent, a successful attack can cause severe operational downtime.

# **Step 3: Risk Control Strategy Selection for TechCorp**

Based on the **ALE rankings**, here’s how TechCorp should prioritize risk response by balancing cost, feasibility, and impact.

### **1. Insider Threat (Source Code Repositories) ALE: $12M**

* **Strategy:** **Defend + Mitigate**
  + **Defend:**
    - Implement **role-based access control (RBAC)** and **code signing.**
    - Use **GitGuardian** or **GitHub Advanced Security** to detect leaks.
  + **Mitigate:**
    - Create a **DLP (Data Loss Prevention) policy** with automated alerts for code exfiltration.

### **2. Phishing (Client Financial Data) – ALE: $10M**

* **Strategy:** **Defend + Transfer**
  + **Defend:**
    - Enforce **MFA and Zero Trust Architecture** for financial systems.
    - Deploy **AI-powered email filters**.
  + **Transfer:**
    - Purchase **cybersecurity insurance** to cover breach-related fines.

### **3. SQL Injection (API/Database) – ALE: $6M**

* **Strategy:** **Defend + Terminate**
  + **Defend:**
    - OWASP guidelines recommend using parameterized queries to prevent SQL injection by ensuring user inputs are treated as data, not code. Additionally, Web Application Firewalls (WAFs) like Cloudflare filter and block malicious requests before they reach the database. Use these
  + **Terminate:**
    - Deprecating unpatched legacy APIs removes security liabilities, reducing attack surfaces. Migrating to GraphQL with rate-limiting enhances security by enforcing strict query constraints and preventing excessive data exposure.

### **4. Phishing (Employee Credentials) – ALE: $3M**

* **Strategy:** **Defend + Mitigate**
  + **Defend:**
    - Mandatory phishing simulations train employees to recognize and avoid phishing attacks, reducing credential theft risks. FIDO2 security keys provide phishing-resistant authentication by requiring hardware-based verification.
  + **Mitigate:**
    - "24/7 Security Operations Center (SOC) monitoring continuously analyzes login patterns for unusual activity. Solutions like CrowdStrike detect and respond to credential misuse in real time."

### **5. Ransomware (Internal Servers) – ALE: $1.05M**

* **Strategy:** **Mitigate + Accept**
  + **Mitigate:**
    - **Air-gapped backups** ensure data recovery by storing copies on isolated systems, preventing ransomware encryption. **CIS Hardening Guidelines** enhance server security through best practices like disabling unnecessary services and enforcing strict access controls
  + **Accept:**
    - Given low ALE, focus on **response readiness** over costly prevention. ResponseReadiness refers to an organization's ability to quickly detect, respond to, and recover from security incidents. Instead of investing heavily in costly prevention measures, TechCorp will focus on having incident response plans, backups, and rapid containmentstrategies to minimize the impact of ransomware attacks.

# **Step 4: Cost-Benefit Analysis (CBA) for TechCorp**

**Proposed Control:** **Multi-Factor Authentication (MFA) for Client Financial Data Access**  
(Mitigates Phishing → 2nd Highest ALE: $10M)

#### **1. Input Data**

* **Annualized Loss Expectancy (ALE) without MFA:** **$10M** (as determined in Step 2).
* **Estimated ALE with MFA:** Reduced by **70%** (standard industry reduction rate for MFA effectiveness).
  + **New ALE = $10M × (1 – 0.7) = $3M**.
* **Annualized Cost of Safeguard (ACS):**
  + **Duo Security MFA License (500 users):** **$15,000/year**.
  + **IT Labor (Setup + Maintenance):** **$10,000/year**.
  + **Total ACS = $25,000/year**.

#### **2. Cost-Benefit Analysis (CBA) Calculation**

The formula for CBA is:

CBA=(ALEwithout−ALEwithACS)/ACS

=$10M−$3M$25K

=$7M/$25K=280

**Interpretation:**

* **CBA = 280** means **every $1 spent on MFA saves $280 in potential losses**.
* Since a CBA greater than **1** is considered cost-effective, the implementation of MFA is highly justified from a financial perspective.

#### **3. Non-Financial Benefits**

* **Regulatory Compliance:** MFA ensures TechCorp complies with data protection laws like GDPR and CCPA, minimizing the risk of penalties for data breaches. This helps maintain legal and ethical standards for handling sensitive information.
* **Reputation:** By preventing breaches, MFA safeguards TechCorp’s brand reputation, avoiding headlines related to security failures. A strong security posture increases customer trust and loyalty.
* **Productivity:** MFA streamlines access management, reducing the time spent on password resets and security-related IT support. This leads to improved operational efficiency and reduced administrative overhead.

#### **4. Conclusion: Should TechCorp Implement MFA?**

**Yes, immediately.**

* **Payback Period:** The implementation will pay for itself in under **2 days**, considering the $7M savings vs. the $25K cost.
* **Risk Tolerance:** Even if MFA only reduces ALE by **50%** (CBA = 140), it still provides significant value.

## **1. Executive Summary**

TechCorp’s recent data breach exposed critical gaps in authentication and access controls. This report documents:

* **Top cybersecurity risks** (ALE-driven prioritization).
* **Cost-effective mitigation strategies** (CBA-backed recommendations).
* **Actionable roadmap** to reduce risk exposure by **50%+ within 12 months**.

## **2. Risk Assessment Findings**

### **A. Threat-Vulnerability-Asset (TVA) Worksheet**

| **Asset** | **Threat** | **Vulnerability** | **ALE** |
| --- | --- | --- | --- |
| Source Code | Insider Threat | No RBAC, unmonitored Git repos | $12M |
| Client Financial Data | Phishing | Lack of MFA | $10M |
| API/Database Systems | SQL Injection | Unpatched CVEs | $6M |
| Employee Credentials | Phishing | Weak passwords | $3M |
| Internal Servers | Ransomware | No air-gapped backups | $1.05M |

### **B. Risk Matrix (Likelihood vs. Impact)**

| **Threat** | **Likelihood** | **Impact** | **Risk Level** |
| --- | --- | --- | --- |
| Insider Threat | Medium | Critical | **High** |
| Phishing | High | High | **High** |
| SQL Injection | Medium | High | **Medium** |
| Ransomware | Low | Critical | **Medium** |

## **3. Recommended Risk Control Strategies**

### **A. Approved Controls (CBA > 1)**

| **Control** | **CBA** | **Justification** |
| --- | --- | --- |
| **MFA for Client Data** | 280 | Prevents 70% of phishing-related breaches. |
| **DLP for Source Code** | 150 | Reduces insider theft risk by 60%. |
| **SOC Monitoring** | 20 | Cuts credential misuse response time by 80%. |

### **B. Rejected Controls (CBA ≤ 1)**

| **Control** | **CBA** | **Reason for Rejection** |
| --- | --- | --- |
| Biometric Server Access | 0.8 | High cost ($100K) for minimal ALE reduction. |
| Cyber Insurance (Standalone) | N/A | Only viable as **supplement** to MFA/DLP. |

## **4. Cost-Benefit Analysis (CBA) Highlights**

### **MFA Implementation Example**

* **ALE Reduction:** $10M → $3M (70% improvement).
* **ACS:** $25K/year (Duo Security + labor).
* **CBA:** **280** – Every $1 spent saves $280.