Risk Assessment Report

Understanding and mitigating cybersecurity risks is essential for protecting an organization's sensitive data, financial assets, and reputation. This report assesses the client's **risk position** using a structured **risk matrix** and the **padlock analogy**, where the absence of security measures represents an **open gate**, existing controls serve as a **basic lock**, and additional protections act as **reinforced security layers**. The goal is to **identify key risks**, assess their **likelihood and impact**, and recommend **strategic security measures** to minimize potential threats.

1. Risk Context: Assets to be Protected

The client's organization handles **sensitive customer data, financial records, and intellectual property**, making it a prime target for cyber threats. The key assets to be protected include:

- **Customer Information** – Personally Identifiable Information (PII), payment details, and credentials.
- **Financial Data** – Banking details, transactions, and payroll records.
- **Intellectual Property (IP)** – Proprietary research, software code, and confidential business strategies.
- **IT Infrastructure** – Servers, databases, cloud platforms, and network systems.

Without adequate security controls, these assets are vulnerable to cyber threats such as **data breaches, ransomware attacks, and insider threats**.

2. Risk Matrix: Likelihood, Consequence & Risk Rating

A **risk matrix** evaluates potential threats based on:

- **Likelihood (L)** – Probability of the risk occurring (Low, Medium, High).
- **Consequence (C)** – Impact severity if the risk occurs (Low, Medium, High).
- **Risk Rating (R)** – Calculated as **Likelihood × Consequence** (Low, Medium, High).

Risk Rating Scale	**Likelihood**	**Consequence**	**Risk Level**
Low (1-3)	Unlikely (1)	Minor (1)	1-3
Medium (4-6)	Possible (2)	Moderate (2)	4-6
High (7-9)	Likely (3)	Severe (3)	7-9

3. Identified Risk Scenarios

Scenario 1: Cyberattack (Data Breach via Phishing)

Description: An attacker sends a phishing email, tricking an employee into revealing credentials, leading to unauthorized access to sensitive customer data.

Scenario 2: Ransomware Attack

Description: Malware is deployed to encrypt critical systems, demanding ransom in exchange for decryption keys, leading to operational downtime and financial losses.

Scenario 3: Insider Threat (Employee Negligence)

Description: An employee accidentally exposes sensitive company information due to weak password management or misconfigured cloud settings.

4. Risk Rating Assessment

Risk Ratings Without Security Measures (No Padlock/Fence in Place)

Risk Scenario	**Likelihood (L)**	**Consequence (C)**	**Inherent Risk Rating (L × C)**
Cyberattack (Phishing)	High (3)	Severe (3)	**9 (High)**
Ransomware Attack	High (3)	Severe (3)	**9 (High)**
Insider Threat	Medium (2)	Moderate (2)	**4 (Medium)**

5. Risk Ratings With Existing Security Measures (Basic Padlock in Place)

Existing Security Measures:

1. **Firewalls & Antivirus Software** – Prevents malicious network intrusions.
2. **Email Filtering & Spam Detection** – Reduces phishing attack success rates.
3. **Data Backups & Disaster Recovery** – Limits ransomware impact.
4. **Role-Based Access Controls (RBAC)** – Restricts data access.

Risk Scenario	**Likelihood (L)**	**Consequence (C)**	**Current Risk Rating (L × C)**
Cyberattack (Phishing)	Medium (2)	Severe (3)	**6 (Medium)**
Ransomware Attack	Medium (2)	Severe (3)	**6 (Medium)**
Insider Threat	Medium (2)	Moderate (2)	**4 (Medium)**

6. Risk Ratings With Additional Security Measures (Reinforced Security in Place)

Recommended Additional Measures:

1. **Security Awareness Training** – Educates employees on phishing and insider risks.
2. **Multi-Factor Authentication (MFA)** – Prevents unauthorized access.
3. **Endpoint Detection & Response (EDR)** – Identifies threats in real time.
4. **Regular Patch Management** – Fixes vulnerabilities before they are exploited.
5. **Zero Trust Security Model** – Requires continuous authentication before granting access.

Risk Scenario	Likelihood (L)	Consequence (C)	Target Risk Rating (L × C)
Cyberattack (Phishing)	Low (1)	Moderate (2)	**2 (Low)**
Ransomware Attack	Low (1)	Severe (3)	**3 (Low)**
Insider Threat	Low (1)	Moderate (2)	**2 (Low)**

7. Summary of Findings & Risk Mitigation Strategy

Key Findings:

1. The **current risk rating** is still **medium to high** despite existing security measures.
2. A **layered defense approach** is necessary to **minimize risk exposure**.
3. **Human error remains a critical factor**, making **security awareness training essential**.

Risk Mitigation Strategy:

1. **Short-Term Actions (Immediate Implementation)**

- Enable **Multi-Factor Authentication (MFA)** across all critical systems.
- Conduct **security awareness training** for employees to recognize phishing attempts.
- Ensure **regular software updates and vulnerability patching**.

2. **Medium-Term Actions (Next 3-6 Months)**

- Deploy **Endpoint Detection & Response (EDR)** to monitor for ransomware activities.

- Improve **data encryption** and **access control measures**.
- Implement a **Zero Trust Security Model** to limit unauthorized access.

3. **Long-Term Actions (Ongoing Security Improvements)**

- Perform **regular cybersecurity audits and penetration testing**.
- Establish a **Security Operations Center (SOC)** for continuous threat monitoring.
- Foster a **culture of cybersecurity awareness** across all departments.

Conclusion

The **client's organization faces high cybersecurity risks** from **phishing, ransomware, and insider threats**. While **current security controls reduce risk**, **additional measures** are required to further mitigate potential threats. By adopting a **layered security approach**, the client can significantly **lower their risk exposure** and **enhance resilience against cyber threats**.

By implementing the recommended **short-term, medium-term, and long-term measures**, the organization can **transition from a reactive to a proactive cybersecurity stance**, ensuring **business continuity and data protection**.

Next Steps & Recommendations

1. Schedule a **comprehensive cybersecurity audit**.
2. Deploy **MFA, EDR, and security awareness training** as **high-priority** measures.
3. Conduct **annual risk assessments** to track improvements and emerging threats.
4. **By reinforcing cybersecurity defenses, the client can effectively safeguard their critical assets from evolving cyber threats.**