Risk Assessment Report – Padlock Analogy

Client Risk Position Documentation

Prepared by: Francis Olorunfemi Jacob

Role: Cybersecurity Consultant (Simulation)

Date: 31st July, 2025

# 1. Context – Assets to Protect

|  |  |  |
| --- | --- | --- |
| Asset | Description | CIA Importance |
| Customer Data | Names, emails, phone numbers, payment info | High C, High I, Medium A |
| Intellectual Property | Source code, proprietary algorithms, product designs | High C, High I, Medium A |
| Employee Credentials | Usernames, passwords, internal authentication keys | High C, High I, Medium A |
| Financial Records | Invoices, financial transactions, vendor payment details | High C, High I, Medium A |
| Internal Communications | Emails, reports, internal memos | Medium C, Medium I, High A |

# 2. Risk Matrix Definition

Risk Rating Formula = Likelihood × Consequence

# 3. Defined Risk Scenarios

|  |  |
| --- | --- |
| Scenario | Description |
| Cyberattack | External threat actor breaches network via phishing or vulnerability |
| Insider Negligence | Employee unintentionally exposes sensitive data |
| Natural Disaster | Fire or flood damages physical servers or data centers |

# 4. Inherent Risk Rating (Without Controls)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Scenario | Likelihood | Consequence | Risk Rating | Risk Level |
| Cyberattack | 4 (Very High) | 4 (Critical) | 16 | Critical |
| Insider Negligence | 3 (High) | 3 (High) | 9 | High |
| Natural Disaster | 2 (Medium) | 4 (Critical) | 8 | High |

# 5. Risk Rating with Existing Measures (Fence and Padlock)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Scenario | Likelihood | Consequence | Risk Rating | Risk Level | Explanation |
| Cyberattack | 3 (High) | 4 (Critical) | 12 | High | Antivirus, firewall, access restrictions |
| Insider Negligence | 2 (Medium) | 3 (High) | 6 | High | Basic training, email filters |
| Natural Disaster | 2 (Medium) | 3 (High) | 6 | High | Building access control, backups |

# 6. Target Risk Rating with Additional Measures

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Scenario | Additional Measures | Likelihood | Consequence | Risk Rating | Risk Level |
| Cyberattack | EDR, MFA, SIEM, phishing simulations | 2 (Medium) | 3 (High) | 6 | High |
| Insider Negligence | Role-based access, DLP, ongoing staff training | 1 (Low) | 3 (High) | 3 | Medium |
| Natural Disaster | Off-site/cloud backups, DR plan, redundant infrastructure | 1 (Low) | 2 (Medium) | 2 | Low |

# 7. Summary & Recommendations

Summary of Findings:  
- The inherent risk (with no controls) for cyberattacks is critical, and even insider negligence poses a high risk.  
- Basic measures (like firewalls and password protection) reduce risk only moderately.  
- Advanced controls like MFA, EDR, continuous awareness, and disaster recovery planning are needed to bring risk to acceptable levels.

Recommendations:  
- Implement MFA and Endpoint Detection and Response (EDR) tools.  
- Establish a Disaster Recovery (DR) and Business Continuity Plan (BCP).  
- Create a formal cybersecurity policy, and update it quarterly.  
- Provide ongoing cybersecurity training to staff.  
- Perform quarterly risk assessments to evaluate progress.

Final Notes:  
The fence and padlock analogy represents basic controls. However, today’s cybersecurity landscape demands layered security, from physical to digital. This risk assessment enables the client to clearly understand their current exposure and provides a prioritized roadmap to reduce overall business risk.