Rick Abraham

My Company  Dallas, TX

Risk Assessment – Insider Threats

Contents

[Introduction 2](#_Toc182579029)

[Purpose 2](#_Toc182579030)

[Scope 2](#_Toc182579031)

[Risk Identification 2](#_Toc182579032)

[Risk Analysis 3](#_Toc182579033)

[Mitigation Recommendations 3](#_Toc182579034)

[Financial Records 3](#_Toc182579035)

[Intellectual Property (IP) 3](#_Toc182579036)

[IT Systems 3](#_Toc182579037)

[Employee Data 4](#_Toc182579038)

[Vendor Access 4](#_Toc182579039)

[Monitoring and Review 4](#_Toc182579040)

[Frequency 4](#_Toc182579041)

[Daily 4](#_Toc182579042)

[Monthly 4](#_Toc182579043)

[Quarterly 5](#_Toc182579044)

[Bi-Annually 5](#_Toc182579045)

[Annually 5](#_Toc182579046)

[Incident Response 5](#_Toc182579047)

[Documentation and Compliance 5](#_Toc182579048)

Risk Assessment – Insider Threats

# Introduction

Purpose: This risk assessment evaluates the potential for insider threats to compromise organizational security. Insider threats include malicious actions, negligent behaviors, and accidental disclosures by employees, contractors, or third-party partners. The assessment identifies vulnerabilities, their impacts, and strategies for mitigation.

Scope: Covers all employees, contractors, and third-party vendors with access to organizational systems, data, and physical facilities.

# Risk Identification

| **Asset** | **Threat** | **Vulnerability** | **Impact** | **Risk Rating** |
| --- | --- | --- | --- | --- |
| Financial Records | Malicious access by employees for personal gain | Overly permissive access rights | Financial fraud, reputational damage | High |
| Intellectual Property (IP) | Unauthorized copying or sharing by contractors | Lack of activity monitoring and DLP tools | Loss of competitive advantage, legal issues | High |
| IT Systems | Disruption caused by a disgruntled employee | Lack of account activity monitoring and delayed termination processes | Operational downtime, security breaches | High |
| Employee Data | Accidental disclosure by HR staff | Lack of encryption and secure email policies | Identity theft, compliance violations | Medium |
| Vendor Access | Exploitation of vendor privileges to access sensitive systems | Lack of vendor access reviews and audits | Data breaches, supply chain disruptions | Medium |

# Risk Analysis

| **Asset** | **Likelihood** | **Impact Severity** | **Overall Risk Level** |
| --- | --- | --- | --- |
| Financial Records | Medium | High | High |
| Intellectual Property (IP) | Medium | High | High |
| IT Systems | Medium | High | High |
| Employee Data | High | Medium | High |
| Vendor Access | Medium | Medium | Moderate |

# Mitigation Recommendations

## Financial Records

* Enforce **role-based access control (RBAC)** to restrict access to financial systems to authorized personnel only.
* Monitor account activity for suspicious behavior, such as unauthorized transfers or data exports.
* Implement **audit trails** and periodic access reviews to ensure compliance with financial security policies.

## Intellectual Property (IP)

* Deploy **Data Loss Prevention (DLP)** tools to prevent unauthorized copying, sharing, or downloading of sensitive documents.
* Encrypt all sensitive IP assets stored on shared drives or transmitted via email.
* Provide contractors with minimal access required for their roles and monitor their activity.

## IT Systems

* Implement **automated account deactivation** immediately after employee termination.
* Monitor for unusual login times or access patterns using **behavioral analytics** tools.
* Limit access to administrative systems to a small group of vetted employees with enhanced monitoring.

## Employee Data

* Enforce secure email practices, including encryption for emails containing sensitive employee information.
* Conduct periodic training for HR staff on safe handling of personal data.
* Maintain centralized, encrypted storage for employee records, with access restricted to HR personnel.

## Vendor Access

* Conduct regular **vendor risk assessments** to evaluate third-party security practices.
* Apply **least privilege principles** to vendor accounts and enforce access expiration dates.
* Require vendors to sign agreements outlining acceptable use and data protection standards.

# Monitoring and Review

Frequency

### Daily

* Monitor email filtering systems for blocked phishing attempts and review logs for failed login attempts.
* Track flagged messages in collaboration tools (e.g., Teams, Slack) for suspicious content or links.

### Monthly

* Review phishing simulation reports to measure employee susceptibility and identify at-risk departments.
* Audit logs from email servers and authentication systems to detect abnormal login patterns.

### Quarterly

* Audit permissions and shared access across email accounts and collaboration tools, removing unused or unnecessary access.
* Review metrics from advanced threat protection tools to detect new trends in phishing attempts.

### Bi-Annually

* Conduct a **comprehensive phishing simulation drill** across all departments, targeting various attack vectors (e.g., email, phone, and collaboration platforms).
* Evaluate the effectiveness of current anti-phishing tools, such as email filtering and link scanning systems, and compare against the latest industry benchmarks.
* Perform **tabletop exercises** with the Phishing Response Team (PRT) to simulate phishing incidents and evaluate response protocols. Update playbooks based on lessons learned.
* Assess vendor security protocols and conduct a **third-party phishing risk audit**, focusing on communication channels and access policies.

### Annually

* Reassess the overall phishing risk landscape, incorporating the latest trends, such as deepfake audio for vishing or AI-driven phishing emails.
* Update organization-wide phishing awareness training materials to reflect emerging attack techniques.
* Evaluate organizational compliance with regulatory requirements, including GDPR and NIST guidelines.

Incident Response

* Establish a **Phishing Response Team (PRT)** and conduct bi-annual tabletop exercises to improve readiness.
* Develop a bi-annual **Incident Response Summary Report**, which includes:
  + The number of phishing incidents reported.
  + Response times and remediation outcomes.
  + Identified gaps in current response protocols.
* Test phishing-related breach escalation processes every six months, ensuring alignment with regulatory notification timelines.

Documentation and Compliance

* Maintain detailed logs of phishing incidents, including type, source, affected systems, and remediation actions taken.
* Document all updates to email filtering configurations, link scanning tools, and endpoint protection measures.
* Record phishing simulation results, including employee susceptibility rates and training outcomes, to track progress and improve defenses.
* Ensure compliance with applicable cybersecurity regulations and standards, including:
  + **NIST SP 800-53**: AC-2 (Access Control), SI-4 (System Monitoring), AT-2 (Training), and IR-4 (Incident Response).
  + GDPR, CCPA, and other data protection frameworks.
* Maintain audit trails for email filtering systems, collaboration tools, and anti-phishing software configurations.
* Regularly review and update phishing awareness training materials to reflect emerging social engineering techniques.