Rick Abraham

My Company  Dallas, TX

Risk Assessment – Data Privacy Risks

Contents

[Introduction 2](#_Toc182579079)

[Purpose 2](#_Toc182579080)

[Scope 2](#_Toc182579081)

[Risk Identification 2](#_Toc182579082)

[Risk Analysis 3](#_Toc182579083)

[Mitigation Recommendations 3](#_Toc182579084)

[Customer Database 3](#_Toc182579085)

[Employee Records 4](#_Toc182579086)

[Cloud Storage 4](#_Toc182579087)

[Backup Systems 4](#_Toc182579088)

[Collaboration Tools 4](#_Toc182579089)

[Monitoring and Review 5](#_Toc182579090)

[Frequency 5](#_Toc182579091)

[Daily 5](#_Toc182579092)

[Monthly 5](#_Toc182579093)

[Quarterly 5](#_Toc182579094)

[Bi-Annually 5](#_Toc182579095)

[Annually 6](#_Toc182579096)

[Incident Response 6](#_Toc182579097)

[Documentation and Compliance 6](#_Toc182579098)

Risk Assessment – Data Privacy Risks

# Introduction

Purpose: This risk assessment evaluates threats to the confidentiality, integrity, and availability of sensitive data stored, processed, and transmitted by the organization. The assessment identifies vulnerabilities, assesses potential impacts, and provides actionable recommendations to address these risks.

Scope: Covers all systems and platforms where sensitive data resides, including on-premises servers, cloud storage, backups, employee devices, and email systems.

# Risk Identification

| **Asset** | **Threat** | **Vulnerability** | **Impact** | **Risk Rating** |
| --- | --- | --- | --- | --- |
| Customer Database | Unauthorized access by internal or external actors | Weak access control policies, shared accounts, lack of encryption | Exposure of sensitive customer information, legal penalties | High |
| Employee Records | Data exfiltration via phishing or malware | Lack of endpoint protection and monitoring | Identity theft and potential lawsuits | High |
| Cloud Storage | Accidental public exposure of private files | Misconfigured access permissions and lack of encryption | Breach of confidential data | High |
| Backup Systems | Unsecured backups targeted during ransomware attacks | Lack of encryption and physical security for backup media | Permanent data loss and operational disruption | High |
| Collaboration Tools | Unauthorized sharing of sensitive files via collaboration platforms (e.g., Teams, Slack) | Overly permissive sharing settings | Data leaks, reputational damage | Medium |

# Risk Analysis

| **Asset** | **Likelihood** | **Impact Severity** | **Overall Risk Level** |
| --- | --- | --- | --- |
| Customer Database | High | High | Critical |
| Employee Records | High | High | Critical |
| Cloud Storage | High | High | Critical |
| Backup Systems | Medium | High | High |
| Collaboration Tools | Medium | Medium | Moderate |

# Mitigation Recommendations

## Customer Database

* Enforce **fine-grained access control policies**, including segregation of duties for database administrators.
* Deploy **real-time activity monitoring tools** to track access to sensitive data fields and detect anomalies.
* Enable **transparent data encryption (TDE)** at the database level.
* Conduct **penetration testing** to identify potential SQL injection vulnerabilities.

## Employee Records

* Integrate **endpoint detection and response (EDR)** tools to monitor devices for suspicious activity.
* Restrict access to employee records using **zero-trust security** principles.
* Provide employees with training on recognizing phishing attacks and secure file sharing.
* Regularly review and purge outdated employee records that are no longer needed.

## Cloud Storage

* Utilize **cloud security posture management (CSPM)** tools to continuously monitor and enforce secure configurations.
* Apply **server-side encryption** for all files stored in the cloud.
* Restrict access to sensitive data by implementing **geo-restrictions** and **IP whitelisting**.

## Backup Systems

* Encrypt all backup data at rest and during transmission using industry-standard protocols.
* Maintain **offsite and immutable backups** to prevent tampering by ransomware.
* Conduct **regular disaster recovery drills** to ensure data can be restored within acceptable recovery time objectives (RTOs).

## Collaboration Tools

* Implement **data loss prevention (DLP)** rules to monitor and control file sharing.
* Restrict external file sharing capabilities to approved accounts only.
* Monitor collaboration tools for unauthorized file downloads or unusual activity.

# Monitoring and Review

## Frequency

### Daily

* Monitor **access logs** for sensitive data repositories (e.g., databases, file servers) to detect unauthorized or unusual access attempts.
* Review **data encryption tools** to ensure they are functioning correctly during data transfers.
* Validate alerts from **Data Loss Prevention (DLP)** tools for potential data exfiltration or unauthorized sharing.

### Monthly

* Audit permissions for sensitive data access, ensuring compliance with role-based access control (RBAC) policies.
* Review logs of employee activities involving data creation, modification, or deletion to detect patterns of negligence or misuse.
* Evaluate **encryption protocols** to ensure they meet industry standards and remain effective against new threats.

### Quarterly

* Conduct **data access audits** for all critical systems to confirm permissions are up to date and aligned with policy.
* Review reports from DLP systems for trends or recurring issues, such as frequent access violations.
* Test backup data for integrity and confirm that it is encrypted and recoverable without errors.

### Bi-Annually

* + Perform **tabletop exercises** simulating data breach scenarios to evaluate the organization’s response to data exposure incidents.
  + Evaluate the effectiveness of data privacy controls, such as encryption, DLP, and logging mechanisms.
  + Conduct **vendor compliance reviews**, focusing on data privacy agreements and secure handling of shared data.

### Annually

* Reassess data privacy risks in light of new regulations (e.g., GDPR, CCPA) and evolving organizational data usage.
* Update data privacy policies and employee training materials to reflect lessons learned from audits, simulations, and incidents.
* Conduct an organization-wide **data privacy awareness campaign** to reinforce best practices for handling sensitive information.

## Incident Response

* Maintain a dedicated **Data Privacy Response Team (DPRT)** to address and resolve data breach incidents effectively.
* Conduct **bi-annual breach simulation drills** to improve readiness and refine escalation workflows.
* Document all data privacy incidents, including affected systems, type of breach, and remediation actions taken, for compliance and improvement purposes.

## Documentation and Compliance

* Maintain detailed logs of data access, sharing, and modification activities to ensure accountability and traceability.
* Document updates to encryption, DLP, and access control systems to demonstrate continuous improvement.
* Ensure compliance with applicable data privacy regulations and standards, including:
  + **NIST SP 800-53**: AC-3 (Access Enforcement), SI-12 (Data Integrity), and SC-12 (Cryptographic Protections).
  + GDPR, CCPA, HIPAA, and ISO 27001 for privacy and data protection requirements.