Third-Party Risk Report for MAISON

Rohan Shah

9/18/2024

1. Executive Summary

This report provides an analysis of third-party risks related to MAISON's digital-first hotel operations. MAISON relies on third-party vendors, including cloud service providers and external companies like a car rental service. To mitigate risks, this report outlines the shared responsibility model between MAISON and these vendors, focusing on risk management strategies that cover data security, regulatory compliance, and access control.

2. Third-Party Risk Register

MAISON collaborates with several third-party vendors to enhance the customer experience and support its cloud infrastructure. However, this reliance introduces several risks that must be identified and mitigated.

Vendor/Service	Risk	Impact	Likelihood	Mitigation
Cloud Provider (AWS/Azure)	Misconfiguration leading to data breach	Severe	Medium	Regular audits, security configurations, access control
Car Rental API Integration	API vulnerabilities exposing customer data	High	Medium	API security best practices (OAuth2.0, rate limiting)
Payment Processor	Non-compliance with PCI-DSS, leading to fines	Critical	Low	Ensure PCI-DSS compliance, tokenization of payment data
CRM Provider	Unauthorized access to guest information	Severe	Low	Role-based access control, regular security updates
Third-Party Maintenance	IoT devices (smart locks) being compromised	High	Medium	Firmware updates, secure communication protocols

Key Risks Identified:

1. **Cloud Misconfigurations**: Misconfigured cloud infrastructure could lead to data breaches, exposing sensitive customer information (e.g., booking and payment details).
2. **API Vulnerabilities**: Third-party integrations like the car rental company's API could expose MAISON's systems to attacks, leading to data leaks.
3. **Non-Compliance with PCI-DSS**: Payment processors may not meet PCI-DSS requirements, which could lead to financial penalties and a loss of trust.

4. **Unauthorized Access to CRM**: The CRM system could be accessed by unauthorized personnel, leading to guest data leaks.
5. **IoT Device Maintenance**: Compromised third-party-maintained IoT devices (e.g., smart locks) could result in unauthorized room access.

3. Shared Responsibility Model

A shared responsibility model defines the security obligations of MAISON and its third-party vendors. By clearly delineating these responsibilities, MAISON can ensure that all parties understand their roles in protecting customer data and maintaining system integrity.

Cloud Infrastructure (AWS/Azure):

- **Cloud Provider's Responsibilities**:
  - Physical security of data centers
  - Infrastructure resilience and availability
  - Compliance with regulatory standards (e.g., SOC 2, ISO 27001)
- **MAISON's Responsibilities**:
  - Configuring and managing access control policies
  - Encrypting sensitive data at rest and in transit
  - Managing user identities and roles (e.g., MFA, least privilege)
  - Monitoring and logging activities for potential security breaches

Car Rental Integration (API):

- **Car Rental Company's Responsibilities**:
  - Secure handling of customer data (e.g., driver's license, insurance)
  - Ensuring API security (e.g., OAuth2.0 authentication)
  - Compliance with data protection regulations (e.g., GDPR, CCPA)
- **MAISON's Responsibilities**:
  - Secure API integration (rate limiting, input validation)
  - Monitoring API interactions for suspicious activities
  - Handling data deletion requests and ensuring customer data privacy

Payment Processors:

- **Payment Processor's Responsibilities**:
  - PCI-DSS compliance for handling customer payment data
  - Tokenization of payment information to prevent data exposure
  - Real-time fraud detection and prevention
- **MAISON's Responsibilities**:

- Ensuring secure integration with payment gateways
- Regular audits to verify compliance with PCI-DSS
- Immediate response to detected fraud attempts or payment anomalies

CRM Provider:

- **CRM Provider's Responsibilities**:
  - Secure storage of guest data
  - Regular security patches and updates to prevent vulnerabilities
  - Role-based access control within the CRM system
- **MAISON's Responsibilities**:
  - Defining user roles and permissions for accessing guest data
  - Ensuring proper security training for staff using the CRM
  - Monitoring access logs for any unauthorized activities

IoT Device Maintenance:

- **IoT Provider's Responsibilities**:
  - Secure firmware updates and patching for IoT devices (e.g., smart locks)
  - Regular audits of device communication protocols (e.g., NFC, Bluetooth)
  - Ensuring data privacy for any IoT-stored information
- **MAISON's Responsibilities**:
  - Configuring secure communication between IoT devices and the cloud
  - Regular monitoring for vulnerabilities in connected IoT devices
  - Conducting penetration tests on smart devices to assess security

4. Risk Management Strategies

To mitigate the risks posed by third-party vendors, the following strategies are recommended:

6. **Vendor Security Assessments**:
   - Conduct security assessments for all third-party vendors, including cloud providers, payment processors, and API providers. Ensure they meet security standards (SOC 2, PCI-DSS, GDPR).
7. **Third-Party Audits and Compliance**:
   - Regularly audit third-party vendors for compliance with security regulations (e.g., PCI-DSS, GDPR) and ensure they follow secure coding practices.
8. **API Security**:
   - Implement secure API practices for third-party integrations, such as using **OAuth2.0**, **rate limiting**, and **input validation**. Ensure that data transfers between MAISON and vendors are encrypted.

9. **Data Encryption**:
    - Encrypt all data shared between MAISON and third-party vendors. This includes customer data passed to the car rental API, payment information, and CRM data.
10. **Contractual Agreements**:
    - Ensure that contracts with third-party vendors include security clauses that specify data protection responsibilities, incident response procedures, and compliance with legal frameworks.
11. **Incident Response Coordination**:
    - Establish coordinated incident response procedures between MAISON and third-party vendors, ensuring swift communication and action in case of a breach.

5. Conclusion

MAISON's reliance on third-party vendors to provide a seamless digital experience comes with inherent risks. Through a well-defined shared responsibility model, clear contractual agreements, and continuous vendor assessments, MAISON can mitigate third-party risks and ensure secure integrations with cloud services, APIs, payment processors, and IoT devices. Strengthening these relationships will help MAISON maintain its position as a secure, digital-first hotel company.