Third-Party Risk Report

Prepared by: Isabelle Jaber
Date: September 18th, 2024

Table of Contents:

EXECUTIVE SUMMARY

This report provides a comprehensive third-party risk analysis for VISION, focusing on the security implications of incorporating AI technologies in collaboration with external vendors. VISION, specializing in computer vision, relies on various third-party vendors for its operational needs, including data management, cloud services, and cybersecurity. Given the sensitive nature of the data involved, particularly with the recent engagement with a large healthcare provider, it is crucial to assess the risks associated with these third-party relationships and ensure effective management strategies are in place. This analysis aims to identify potential risks, outline responsibilities within cloud service models, and recommend strategies for mitigating third-party risks, especially in the context of AI security.

THIRD-PARTY RISK REGISTER

Asset	Description	Potential Impact	Likelihood	Migations
Cloud Service Providers (eg. AWS)	Risks related to data breaches, inadequate data encryption, and service outages.	High	High	Implement encryption standards, monitor service level agreements (SLAs), and conduct regular security assessments.
Cybersecurity Monitoring Team (eg. contracted team in India)	Risks of insufficient monitoring coverage during off-hours, potential lack of alignment with VISION's security policies.	High	Medium	Enhance coordination with the team, establish clear security protocols, and ensure continuous coverage and regular audits.
Data Annotation and Labeling Tools	Risks related to data privacy, potential exposure of sensitive medical data, and tool vulnerabilities.	High	Medium	Use tools with strong security certifications, implement access controls, and conduct regular security reviews.
IT Vendors (eg. cleaning, office supplies/snacks)	Risks of data leakage or system access through less secure vendor interactions.	Low	Low	Implement strict access controls and regular vendor security assessments.

Consultants and Contractors	Risks of unauthorized access to VISION's systems, inconsistent security practices, and data handling procedures.	Medium	Medium	Ensure contracts include stringent security requirements and conduct regular audits and compliance checks.

SHARED RESPONSIBILITY MODEL

In cloud infrastructure models, the shared responsibility model delineates the division of security responsibilities between the cloud service provider and the customer. This model varies based on the type of cloud service utilized:

SOFTWARE AS A SERVICE (SaaS)

- **Provider's Responsibility:** Securing the application, including data encryption, patch management, and overall application security.
- **Customer's Responsibility:** Managing access controls, ensuring proper user authentication, and securing data shared with the SaaS application.

PLATFORM AS A SERVICE (PaaS)

- **Provider's Responsibility:** Protecting the underlying infrastructure, including servers, networking, and storage, as well as the platform itself.
- **Customer's Responsibility:** Securing applications and data developed on the platform, including application configuration and data protection measures.

INFRASTRUCTURE AS A SERVICE (IaaS)

- **Provider's Responsibility:** Ensuring the security of the infrastructure components such as physical hardware, network, and virtualization.
- **Customer's Responsibility:** Managing and securing the operating systems, applications, and data on the infrastructure, including configuring firewalls and managing access controls.

Given VISION's reliance on cloud services for data storage, processing, and AI model management, understanding and managing these responsibilities is critical to ensuring comprehensive security.

RISK MANAGEMENT STRATEGIES

VENDOR DUE DILIGENCE

- **Assessment and Selection:** Evaluate third-party vendors based on their security practices, compliance with relevant regulations, and their ability to protect sensitive data.
- **Regular Reviews:** Conduct periodic security assessments and audits of third-party vendors to ensure continued adherence to security standards.

CONTRACTUAL AGREEMENTS

- **Security Clauses:** Include robust security and compliance clauses in vendor contracts, specifying data protection requirements and incident response protocols.
- **SLAs and Performance Metrics:** Define clear service level agreements and performance metrics related to security and data protection.

DATA PROTECTION MEASURES

- **Encryption:** Implement strong encryption for data at rest and in transit, ensuring that sensitive data is protected from unauthorized access.
- **Access Controls:** Establish stringent access controls to limit data access to authorized personnel only.

MONITORING AND INCIDENT RESPONSE

- **Continuous Monitoring:** Use advanced monitoring tools to track and analyze data traffic and detect potential security threats in real-time.
- **Incident Response Plans:** Develop and maintain a comprehensive incident response plan to address any security breaches or data leaks promptly.

TRAINING AND AWARENESS

- **Security Training:** Provide regular security training to employees and contractors to ensure they are aware of best practices and potential threats.
- **Vendor Training:** Work with third-party vendors to ensure they understand and adhere to VISION's security policies and procedures.

CONCLUSION

Effective management of third-party risks is crucial for VISION, particularly with its focus on AI technologies and the sensitive nature of its healthcare client engagements. By understanding and applying the shared responsibility model, implementing robust risk management strategies, and maintaining vigilance in vendor assessments and contract management, VISION can mitigate potential risks associated with third-party vendors. Ensuring comprehensive security across all third-party interactions is essential for protecting sensitive data, maintaining client trust, and safeguarding the integrity of AI solutions.