Third-Party Risk Report

Drafted by

Oyindamola Olayiwola

15th October, 2024.

Executive Summary

This Third-Party Risk Register provides a comprehensive assessment of the risks associated with the organization's reliance on third-party services, including Office 365, Salesforce, Slack, Azure, and monitoring tools. The register identifies potential vulnerabilities, evaluates their likelihood and impact, and outlines mitigation strategies.

Key Findings

- **Data Security:** Unauthorized access to sensitive data is a significant risk across all third-party services. Implementing strong access controls, encryption, and MFA are crucial mitigation strategies.
- **Phishing and Social Engineering:** Phishing attacks targeting users of Office 365, Salesforce, Slack, and Webex are a persistent threat. Anti-phishing training, MFA, and email filtering are essential countermeasures.
- **Third-Party Vulnerabilities:** Vulnerabilities in third-party services and applications can introduce risks. Regular security audits, vendor assessments, and patch management are necessary to mitigate these risks.
- **Operational Risks:** Service disruptions, configuration issues, and improper management of cloud resources can impact operations and data security. Robust monitoring, redundancy planning, and configuration management are essential.
- **Vendor Lock-in:** Reliance on certain third-party services can create vendor lock-in risks. Developing exit strategies and evaluating alternatives can mitigate this risk.

Mitigation Strategies

The register outlines various mitigation strategies, including:

- **Security Controls:** MFA, RBAC, encryption, access controls, and configuration management.
- **Training and Awareness:** Security awareness training for employees and vendors.
- **Monitoring and Auditing:** Regular security audits, vulnerability scanning, and monitoring of network traffic.
- **Third-Party Risk Management:** Vendor assessments, contract management, and incident response planning.
- **Compliance:** Adherence to data privacy regulations (e.g., GDPR, HIPAA).

Shared Responsibility Model

The register highlights the shared responsibility model between the organization and cloud service providers (CSPs) for security. Understanding these responsibilities is crucial for effective risk management.

Third-Party Risk Register

Asset Name	Risk ID	Risk Description	Category	Likelihood	Impact	Risk Score	Mitigation Strategy	Owner	Status	Residual risk	Current Controls
Office 365(O)	TPR-O-01	Unauthorized access to sensitive data	Security Risk	High	High	High	Multi-factor authentication (MFA), role-based access control (RBAC), and encryption of sensitive data.		In Progress	low	MFA
	TPR-O-02	Phishing attempts targeting Office 365 users could lead to credential theft.	Security Risk	High	High	High	Anti-phishing training, email filtering, MFA, and real-time monitoring for unusual account behavior.		In Progress	low	MFA
	TPR-O-03	Vulnerabilities in third-party services or applications integrated with Office 365 could expose users to risks.	Third-Party Risk	Medium	Medium	Medium	Vendor assessment, regular security audits, patch management, and vulnerability scanning.		In Progress	low	
	TPR-O-04	Distributed denial-of-service (DDoS) attacks or other cyber threats could disrupt Office 365 services.	Operational Risk	Medium	Medium	Medium	DDoS protection services (e.g., Azure DDoS Protection), traffic monitoring, and redundancy planning.		In Progress	low	

Salesforce CRM (SC)	TPR-SC-01	Unauthorized Access to customer sensitive Data	Security Risk	High	High	High	Encryption at rest and in transit, data access auditing, and MFA		In Progress	low	MFA
	TPR-SC-02	Integrating Salesforce with other applications can introduce additional security risks if not done securely.	Integration Risk	Medium	High	High	Secure API configurations, vulnerability scanning, and regular audits of third-party integrations.		In Progress	low	
	TPR-SC-03	Relying heavily on Salesforce can make it difficult to switch to other CRM platforms, potentially limiting flexibility and increasing costs.	Vendor Lock-in Risk	Low	Medium	Medium	Contract management, periodic vendor performance review, and business continuity planning for vendor transitions.		In Progress	low	
	TPR-SC-04	Incorrect configuration of Salesforce settings or customizations can lead to security vulnerabilities, data loss, or performance issues.	Configuration Risk	Medium	Low	Low	Configuration audits, change management policies, and automated security configuration checks.		In Progress	low	
Slack (S)	TPR-S-01	Phishing attempts can target users	Security Risk	High	High	High	Anti-phishing tools, user training,		In Progress	low	MFA

		through Slack messages, leading to credential theft.					and integration of Slack with MFA.				
	TPR-S-02	Misconfigured settings can expose sensitive data or grant excessive permissions to unauthorized users.	Configuration Risk	Medium	High	High	Regular configuration reviews, least privilege principle, and role-based access control (RBAC). Outages or service disruptions can impact productivity and communication. Operational Risk		In Progress	low	RBAC
	TPR-S-03	Outages or service disruptions can impact productivity and communication.	Operational Risk	Medium	Medium	Medium	Service level agreements (SLAs), system redundancy, and incident response planning.		In Progress	low	
	TPR-S-04	Users may inadvertently share sensitive information or click on malicious links.	Human Erroe	High	High	High	Security awareness training, data loss prevention (DLP) tools, and URL filtering.		In Progress	low	
Webex (WX)	TPR-WX-01	Vulnerabilities in third-party services or applications integrated with Webex could	Third-Party Risk	Medium	Medium	Medium	Vendor risk assessments, regular patching, and security audits of integrated applications.		In Progress	low	

		expose users to risks.									
	TPR-WX-02	Unauthorized users could gain access to meetings or recordings.	Security Risk	Medium	Medium	Medium	Meeting password protection, encryption, and session management tools.		In Progress	low	
	TPR-WX-03	Phishing attempts targeting Webex users could lead to credential theft.	Security Risk	High	High	High	Anti-phishing measures, MFA, and phishing simulation exercises.		In Progress	low	MFA
	TPR-WX-04	Failure to comply with data privacy regulations (e.g., GDPR, HIPAA) could result in hefty fines and penalties.	Compliance Risk	High	High	High	Privacy impact assessments (PIA), GDPR/HIPAA compliance monitoring, and regular audits.		In Progress	low	
Azure Cloud Infrastructure (ACI)	TPR-ACI-01	Unauthorized access to sensitive data can lead to financial loss, reputational damage, and legal consequences.	Security Risk	High	High	High	Access controls, encryption, and regular security audits		In Progress	low	
	TPR-ACI-02	Failure to comply with data privacy regulations (e.g., GDPR, HIPAA) can result in hefty	Compliance Risk	Medium	High	High	Compliance management systems, internal audits, and staff training on regulatory requirements.		In Progress	low	

		fines and penalties.									
	TPR-ACI-03	Relying heavily on Azure can make it difficult to switch to other cloud providers in the future, potentially limiting flexibility and increasing costs.	Security Risk	Low	Low	Low	Multi-cloud strategy, vendor performance reviews, and long-term exit strategies.		In Progress	low	
	TPR-ACI-04	Improper management of cloud resources can lead to unexpected costs and budget overruns.	Compliance Risk	Low	Medium	Medium	Cloud cost management tools, budget monitoring, and capacity planning.		In Progress	low	
	TPR-ACI-05	Incorrect configurations can lead to vulnerabilities and security breaches.	Security Risk	Medium	High	High	Configuration management tools, automated security scans, and regular vulnerability assessments.		In Progress	low	
	TPR-ACI-06	Vulnerabilities in third-party services or applications used with Azure can expose organizations to risks.	Third-Party Risk	Medium	Medium	Medium	Third-party risk assessments, patch management, and secure coding practices.		In Progress	low	

Third-party cybersecurity monitoring tools and infrastructure (MI)	TPC-MI-01	Integrating monitoring tools with existing infrastructure can be challenging, leading to performance issues or disruptions.	Integration Risk	Medium	Medium	Medium	Testing in development/staging environments, system performance monitoring, and gradual integration rollouts.		In Progress	low	
	TPC-MI-02	Monitoring tools may generate false positives, leading to unnecessary investigations.	Operational Risk	Medium	Low	Low	Fine-tuned alerting rules, periodic review of alert thresholds, and AI-based alert prioritization.		In Progress	low	
	TPC-MI-03	Monitoring tools can be costly, and organizations may face unexpected expenses due to increased usage or feature upgrades.	Financial Risk	Low	Medium	Medium	Vendor contract management, usage monitoring, and regular cost-benefit analyses of features.		In Progress	low	
	TPR-S-04	Misconfigurations or vulnerabilities in monitoring tools could lead to data leaks.	Configuration Risk	Medium	High	High	Security configuration reviews, regular patching, and data encryption at rest and in transit.		In Progress	low	
Partnered ATM	TPR-PAN-04	Cyberattacks targeting the ATM network's	Security Risk	Medium	High	High	Network segmentation, encryption, and		In Progress	low	

Network (PAN)		infrastructure can compromise security and lead to data breaches.					real-time monitoring of ATM traffic.				
	TPR-PAN-05	Unauthorized individuals may use stolen or compromised cards to withdraw funds from ATMs.	Financial Risk	Medium	Medium	Medium	wo-factor authentication (e.g., chip + PIN), fraud detection systems, and transaction monitoring.		In Progress	low	
	TPR-PAN-06	Technical failures, maintenance issues, or network outages can lead to ATM downtime, causing inconvenience to customers.	Operational Risk	Medium	Medium	Medium	Redundancy and failover systems, regular maintenance schedules, and real-time monitoring.		In Progress	low	
	TPR-PAN-07	Malicious individuals can install skimming devices on ATMs to capture card data and PINs.	Security Risk	Medium	High	High	Anti-skimming devices, physical inspections, and monitoring systems to detect tampering.		In Progress	low	

Shared Responsibility Model

Application & Services	Cloud Model	CSP Responsibility	Customer Responsibility
Microsoft Azure (Data Hosting)	Infrastructure as a Service (IaaS)	CSP manages the physical infrastructure (servers, storage, networking) and security of the data center.	Customer is responsible for managing virtual machines, operating systems, applications, and data.
OneDrive (File Storage)	Software as a Service (SaaS)	CSP manages the entire software stack, including application security, infrastructure, and platform.	Customer is responsible for data security, access management, file sharing policies, and compliance.
Salesforce (CRM)	Software as a Service (SaaS)	CSP manages the application, infrastructure, and security of the platform.	Customer manages user access, data input, and ensuring compliance with internal policies.
Office 365 (Collaboration)	Software as a Service (SaaS)	CSP is responsible for managing the software, infrastructure, and updates.	Customer manages user accounts, data security, and usage policies.
Slack (Messaging/Collaboration)	Software as a Service (SaaS)	CSP manages the software stack, data storage, and infrastructure security.	Customer is responsible for managing user permissions, securing shared data, and compliance.
Webex (Video Conferencing)	Software as a Service (SaaS)	CSP handles the infrastructure, software, and data security at the application level.	Customer manages user access, content shared during meetings, and compliance with internal policies.

Monitoring Tools	Platform as a Service (PaaS)	CSP manages the infrastructure and platform required to run the monitoring tools.	Customer is responsible for configuration, monitoring setup, data analysis, and responding to alerts.
Azure Virtual Machines	Infrastructure as a Service (IaaS)	CSP manages the physical infrastructure, networking, and data center security.	Customer is responsible for managing the operating system, installed software, and data.

Risk Management Strategies

To effectively manage third-party risks, the following strategies are recommended:

Vendor Risk Assessment: Conduct thorough due diligence and risk assessments before engaging with vendors. This should include evaluations of security practices and compliance history.

Contractual Risk Management: Ensure contracts specify security responsibilities, data protection measures, and right-to-audit clauses. Clearly outline the roles of both parties in maintaining security.

Continuous Monitoring: Implement ongoing monitoring processes to assess vendor performance, compliance, and security posture. Regular assessments will help identify emerging risks.

Incident Response Planning: Develop joint incident response plans with third-party vendors to ensure coordinated actions during security incidents. Include breach notification protocols.

Training and Awareness: Provide training to employees and vendors regarding security practices, data protection, and incident response. Regular workshops can enhance awareness and preparedness.

Cyber Insurance: Ensure that third-party vendors maintain adequate cyber insurance to cover potential losses due to data breaches or other incidents.

Exit Strategy: Define clear offboarding procedures and data retrieval processes when terminating vendor relationships to ensure data is handled securely.

Conclusion

The evaluation of third-party risks associated with key services such as Office 365, Salesforce, Slack, and Azure underscores the critical importance of robust security practices and vigilant monitoring. With the increasing integration of third-party services into daily operations, organizations must remain proactive in assessing and managing potential vulnerabilities.

The **Third-Party Risk Register** highlights various risks, their likelihood, and potential impacts, providing a clear framework for prioritizing mitigation strategies. Implementing multifactor authentication (MFA), regular security audits, and continuous monitoring are essential steps to protect sensitive data and maintain operational integrity.

Additionally, understanding the **Shared Responsibility Model** clarifies the division of security responsibilities between Cloud Service Providers (CSP) and customers, reinforcing the need for customer diligence in managing their data and configurations.

To effectively mitigate third-party risks, organizations should adopt comprehensive risk management strategies, including vendor risk assessments, continuous monitoring, and well-defined incident response plans.

By fostering a culture of security awareness and maintaining strong vendor relationships, organizations can navigate the complexities of third-party integrations while safeguarding their assets and ensuring compliance with regulatory standards. As cyber threats continue to evolve, an adaptive approach to risk management will be crucial for sustaining business resilience.