

Auditing Third Party Vendors ...An overview

Adetokunbo Omotosho
Managing Consultant
Infoprive Services Limited

Facts about 3rd Party Vendors



65% of companies that reported sharing customer data with a partner also reported a subsequent breach through that partner.



Facts about 3rd Party Vendors



32% of companies don't evaluate their Third Party Vendors

[NAVEX Global survey](#)

11% of respondents don't even know how many service providers they have .

Security Impact of 3rd Party Vendors

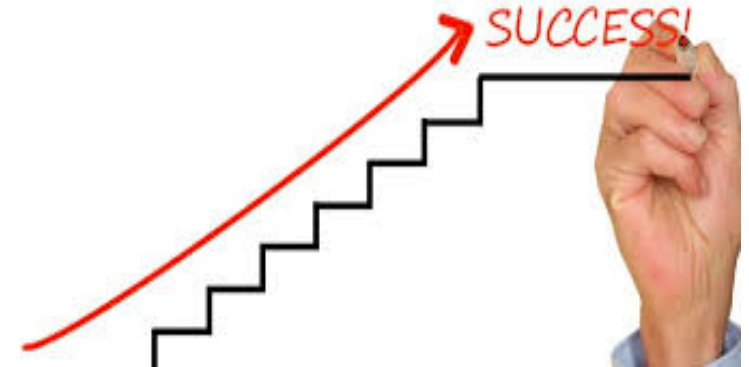


They could increase your risk profile by increasing you to new threats

- Loss of revenue
- Loss of Reputation and goodwill
- Hamper business operations

Effective third party vendor management

- Identify Your Third Party Vendors
- Review Your Current Third Party Vendors
 - Develop a list of high impact vendors
- Conduct a Risk Assessment on the Third Party Vendors
 - Identify your assets exposed to vendors and vendors that store your data.
- Develop a due diligence program that suits each Third Party category.
 - Manage the relationship and monitor cyber hygiene
 - Carry out ongoing monitoring.



Auditing Internet Service Providers

- Are there security standards to Audit against?
 - ISO 27001
 - ISO 22301
 - NIST Framework for improving critical infrastructure
- What is important to you ?
 - Confidentiality
 - Privacy
 - Availability



Auditing Mobile Network Operators

- Are there any standards to audit against ?
 - GSMA Security Group Standards
 - ISO 27001
 - ISO 22301
 - NIST Framework for improving critical infrastructure
- Considerations could be
 - Authenticity Strength (Resilience to Impersonation)
 - Privacy Protection (Resilience to Interception)
 - Usage Anonymity (Resilience to Tracking)



Auditing Payment Application Developers

- Are there any standards to audit against ?
 - PA-DSS
 - ISO/IEC 27034
 - OWASP
 - NIBSS requirement for application developers.
- What is important to you ?
 - Confidentiality
 - Privacy
 - Availability



Ultimately

Focus should be on what is important to you and how your third party vendor affects /impacts that .



Ultimately

- Does the third party's philosophies, align with your organization's?
- Does the third party operate in a legal and compliant manner?
- What is the financial stability of the third party?
- What is the third party's business history and reputation?
- Has the third party's senior management completed and passed thorough background checks?
- Does the third party have effective policies and processes?
- What sort of information will the third party need access to?
- Does the third party have proper information security procedures?
- What is the third party's management of information systems?
- Does the third party have a complete disaster recovery plan?
- Does the third party maintain incident reporting and management programs?
- Does the third party maintain security of its facilities, technology systems and employees?
- Does the third party ensure human resource management policies and programs?
- Does the third party properly evaluate risk of subcontractors and contractual arrangements?
- Does the third party have complete insurance coverage against losses?

