

13.1.4 Managing Third Parties Facts

This lesson covers the following topics:

- Third-party relationships
- Onboarding
- Daily operations
- Offboarding

Third-Party Relationships

In the modern business world, it's very common for one organization to work directly with a third party in one of the following ways:

Relationship	Description
Vendor	A vendor is a company that sells a organization's goods or provides supplies an organization needs.
Supply chain	Supply chain relationships are collaborative relationships in which companies work together to achieve their operational objectives.
Business partner	A business partnership is an agreement between parties to operate a business together and to share its profits.

These relationships frequently require the information systems used by each party to connect and integrate. Doing so exposes each network to risks. Before entering into a relationship, take the steps needed to ensure the security of each party's network. Similar to an employment agreement, pay careful attention to the onboarding phase, the ongoing operations phase, and the offboarding phase.

Onboarding

During the onboarding phase of a relationship, consider the following issues and formulate a plan to address them:

- Compare your organization's security policies and infrastructure against each partner organization's policies and infrastructure, then answer the following questions:
 - Are the security policies for each organization similar, or are there significant differences between them?
 - Do both organizations have similar incident response procedures or are there differences in how incidents will be handled by each party?
 - Are the security controls used by each party similar, or are there differences?
 - Are both organizations' audit policies similar, or are there significant differences between them?
 - Is the security posture of each party compatible enough to work together, or will the integration expose vulnerabilities?
 - Identify the risks associated with entering into this relationship.
- Identify how data ownership will be determined. Will ownership be based on the storage location, or will it be determined by patent, trademark, copyright, or contract law?
- Identify who will be responsible for protecting data. Who will be responsible for performing data backups? Will redundancy be used to ensure high availability?

- Identify how privacy will be protected. If the data involved in the relationship contains personally-identifying information (PII). Can information classification labels be used to protect this type of data?
- Identify how data will be shared. In most relationships, only a limited subset of data needs to be shared between parties. The rest of each organization's data must remain protected. How will unauthorized data sharing be prevented? If unauthorized data sharing occurs, how will it be detected?

Before entering into a third-party agreement, all aspects of the relationship must be agreed upon in writing. To accomplish this, most organizations use an Interoperability Agreement (IA). Several key documents may be included within an IA:

Document	Description
Service Level Agreement (SLA)	A Service Level Agreement specifies the services performed by the third party and what level of performance is guaranteed. An SLA may also define how disputes will be managed, the warranties provided, specific disaster recovery procedures, and when the agreement will be terminated.
Blanket Purchase Order (BPO)	A Blanket Purchase Order or Blanket Purchase Agreement (BPA) is an agreement with a third-party vendor to provide services on an ongoing basis. BPOs are typically negotiated to take advantage of a preset discounted pricing structure.
Memorandum of Understanding (MOU)	A Memorandum of Understanding is a document that provides a summary of which party in the relationship is responsible for performing specific tasks. In other words, the MOU specifies who is going to do what, and when they will do it.
Interconnection Security Agreement (ISA)	An Interconnection Security Agreement documents how the information systems of each party in the relationship will be connected and how they will share data.
Non-disclosure Agreement (NDA)	A Non-disclosure Agreement is a contract in which the third party agrees not to share any of the information gathered during the completion of the work.
Measurement System Analysis (MSA)	A Measurement System Analysis states the measurements to be used for determining the quality and effectiveness of provided services.

Daily Operations

During the ongoing operations phase of the relationship, observe the following:

- Regularly verify compliance with the IA documents.
- Conduct periodic vulnerability assessments to verify that the network interconnections created by the relationship have not exposed or created security weaknesses.
- Conduct regular security audits to ensure that each party in the relationship is following the security-related aspects of the IA documents.
- Communicate vulnerability assessment and security audit findings with all of the parties in the relationship to maintain risk awareness.

Offboarding

When the relationship with the third party ends, ensure that doors that were opened between organizations during the onboarding phase are closed. Consider the following:

- Create an End of Life (EOL) document at the end of a business relationship. It reviews the purpose of the original contract, the date of the contract start and end, and any obligations related to the end of the relationship.
- Create an End of Service (EOS) letter when things do not work out with the third party. The letter reviews the purpose for the original contract, the date the contract started, the date the contract is being terminated, the reason for terminating the document, and any obligations related to the termination.
- Reset or disable any VPN, firewall, router, or switch configurations that allowed access to your network from the third-party network.
- Disable any domain trust relationships that were established between the organizations.
- Disable any user and group accounts used by a third party to access your organization's data.
- Reset any passwords used by the third party to access data or applications on your network.

Copyright © 2022 TestOut Corporation All rights reserved.