3.9.2 Third-Party Integration Security Facts

In the modern business world, it's very common for one organization to work directly with another in either a vendor or partner relationship. These relationships frequently require the information systems used by each party to connect and integrate with each other. However, doing so potentially exposes each network to risks.

Before entering into a relationship, take steps to ensure that the integration process maintains the security of each party's network. Careful attention should be paid to both the *onboarding* phase, when the relationship is initiated, and the *off-boarding* phase, when the relationship is terminated. Consider the following issues for each phase:

Relationship Phase	**Considerations**
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 in one or more parties? - What are the risks associated with entering into this relationship? - Identify how data ownership will be determined. Will ownership be based simply 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? - If the data involved in the relationship contains personally-identifying information (PII), identify how privacy will be protected. 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 will need 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? Prior to entering into a third-party agreement, it is critical that all aspects of the relationship be agreed upon in writing. To accomplish this, most organizations will utilize an Interoperability Agreement (IA). There are several key documents that may be included within an IA that you should be familiar with: - A Service Level Agreement (SLA) specifies exactly which services will be performed by the third party and what level of performance they guarantee. An SLA may also define how disputes will be managed, provide warranties, specify disaster recovery procedures, and specify when the agreement will be terminated. - A Blanket Purchase Order (BPO) 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. - A Memorandum of Understanding (MOU) is a very important document that provides a brief summary of which party in the relationship is responsible for performing specific tasks. In essence, the MOU specifies who is going to do what, and when they will do it. - An Interconnection Security Agreement (ISA) documents how the information systems of each party in the relationship will be connected and how they will share data.
Ongoing 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.
Off-Boarding	When the relationship with the third party ends, you need to ensure that all of the doors that were opened between organizations during the onboarding phase are closed. Consider the following: - 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 third parties to access your organization's data. - Reset any passwords used by the third party to access data or applications on your network.