13.2.2 Risk Types and Tolerance Facts

This lesson covers the following topics:

- Asset identification
- Risk identification
- Risk analysis
- Risk response

Asset Identification

Asset identification identifies the organization's resources. Asset valuation determines the worth of that resource to the organization. This is important because it establishes the level of protection appropriate for each asset.

When identifying assets and values, be sure to include both tangible and intangible assets.

- A tangible asset is a physical item such as a computer, storage device, or document. Such items are typically purchased. The valuation of these assets can be easily determined by the cost of replacing the item.
- An intangible asset is a resource that has value and may be saleable even though it is not physical or material. Intangible assets are typically more challenging to identify and evaluate.

Assets can have both tangible and intangible components. For example, a computer that functions as a server has a tangible value associated with the replacement cost of the hardware. Intangible assets include the data on the computer, the value of the role that the computer performs within the organization, and what the computer's information is worth to a competitor or an attacker.

Risk Identification

When identifying threats, consider both external and internal threats. External threats are those events originating outside of the organization that typically focus on compromising the organization's information assets. Examples are hackers, fraud perpetrators, and viruses. Internal threats are intentional or accidental acts by employees, including:

- Malicious acts such as theft, fraud, or sabotage
- Intentional or unintentional actions that destroy or alter data
- Disclosing sensitive information through snooping or espionage
- Environmental disasters are physical events that can happen over time. These can be a result of physical components such as broken water pipes or can take the form of a natural disaster such as tornadoes, hurricanes, and floods.
- Legacy systems can create unique risks such as system incompatibility and security vulnerabilities. These risks can be amplified if current employees are not familiar with the systems.
- Intellectual property (IP) theft is a risk for most organizations and can cause extensive financial and strategic damage.

One goal of asset identification and valuation is to prioritize assets based on the seriousness of potential threats and the impact that a loss would have on normal operations. As you plan protection strategies and allocate security resources and budgeting, start with the most critical assets first.

Once assets have been identified and a valuation is established, it is important to document procedures relating to these classifications and other security procedures. This documentation should include:

- What assets need protection.
- How to store the asset.
- How to provide access to the asset.
- How to transfer and move the asset.
- How to destroy the asset.

Risk Analysis

After identifying possible sources of threats, the next step is to evaluate the possible risks and to determine if and when risk should be addressed, or if it should be tolerated.

Risk analysis is the practice of assessing which risks you identified are most relevant and pressing to the organization. This is a key part of the risk management process. The risk assessment determines quantitative or qualitative values of risk related to a particular asset and a particular threat. As a best practice, try to create risk assessments using quantitative measurements, which require us to assign a number or value to each risk identified. You can use an equation to measure risk quantitatively.

Inherent risk is the level of risk that a system has without any controls in place. Inherent risk can be determined by considering what the system is used for, who has access to the system, and how users can access the system. Once controls have been put in place, the residual risk remains. Determining residual risk would involve considering what controls were needed, and which controls had been implemented. Control risk occurs when an organization does not have the needed controls in place.

Risk Response

After you have identified the risks and their associated costs, you can determine how best to respond to the risk. Responses include:

- Taking measures to reduce the likelihood of the threat by deploying security controls or other protections. When deploying countermeasures, the annual cost of the countermeasures should not exceed the annualized loss expectancy (ALE). If it does, you are paying more to protect the asset than it is worth. Security control types can be management, operational, or technical.
- Transferring risk by purchasing insurance to protect the asset. When the incident occurs, the cost of replacing or repairing the asset is covered by insurance. When deciding to transfer the risk, be sure to compare the cost of insurance with the ALE. Purchase the insurance only if its cost is less than the ALE.
- Accepting the risk and choosing to do nothing. For example, you might decide that the cost associated with a threat is acceptable or that the cost of protecting the asset from the threat is unacceptable. In this case, you would plan for how to recover from the threat but not implement any measures to avoid it.
- Risk rejection, which is choosing not to respond to the risk even though the risk is not at an acceptable level. Risk rejection introduces the possibility of negligence and may lead to liability. Risk rejection is not an appropriate response.
- Risk deterrence, which is letting threat agents know of the consequences they face if they choose to attack the asset. This could include posting warnings on login pages to indicate prosecution policies.

Consider the following factors when implementing security controls to reduce risk:

- Compatibility with existing infrastructure
- Effectiveness
- Regulatory compliance
- Organizational policies
- Operational impact
- Feasibility
- Safety and reliability