13.2.4 Analyzing Risks Facts

This lesson covers the following topics:

- Risk analysis methods
- Quantitative analysis

Risk Analysis Methods

Risk analysis is the practice of determining which identified threats are relevant and pressing to the organization. Once identified, each relevant and pressing threat is given a potential cost that may be incurred if the threat occurs. There are two general risk assessment methods:

- The *quantitative analysis* method assigns real numbers to the costs of damages and countermeasures. It also assigns concrete probability percentages to risk occurrence.
- The *qualitative analysis* method uses scenarios to identify risks and responses. Qualitative risk analysis is more speculative (based on opinion) and results in relative costs or rankings.

The strict quantitative value of the loss is typically not possible. The determination of value must also include qualitative components.

Quantitative Analysis

Measuring risks quantitatively requires identifying the following components:

- *Single loss expectancy* (SLE) is the amount of loss expected for any single successful threat attack on any given asset. This is a monetary value that describes how much an incident will cost in terms of lost asset value.
- *Exposure factor* is the percentage of the asset lost because of a successful threat attack.
- *Annualized rate of occurrence* (ARO) identifies how often in a single year the successful threat attack will occur. ARO information is frequently obtained from insurance companies, law enforcement agencies, and computer incident-monitoring organizations. For example, an ARO of 2 indicates that the incident is expected to occur twice a year, while an ARO of .25 means the incident is expected once every four years.
- *Annual loss expectancy* (ALE) estimates the annual loss resulting from an incident. For example, if you expect a successful attack every four years. The ALE for the incident would be 1/4 of the SLE.

The quantitative value of risk can be determined with the following calculation: SLE x ARO = ALE. This tells you how much a potential threat costs each year. For example, if the asset loses $1,000 for each incident and you expect an incident every four years, the annual cost for that asset would be $250.

As you attempt to quantify and assess risks, consider creating a risk register early in the risk management process. A risk register provides details of each known risk, including a risk category, description, unique identification number, projected impact, likelihood of occurrence, and risk response plan. This information can be used to create a scatter plot that represents the possible impact of each risk in relation to its overall probability. Having a visual representation of risks can help stakeholders better assess the risks.