10.1 Risk Assessment

Evaluating the security of a network always starts with a risk assessment. This involves considering the assets you are trying to protect, the threats against those assets, vulnerabilities in your systems, and what measures you can take to protect them. There are formulas for calculating risk.

The most basic calculation is for a single loss expectancy (SLE), or what impact a single loss will cause. This is calculated by multiplying the asset value (AV) by the exposure factor (EF). The exposure factor is a percentage value, representing how much of the asset's value you will lose in a given incident. For example, a laptop that has depreciated by 20 percent is now only worth 80 percent of its original value, should it be lost or stolen. This formula is

SLE = AV × EF

Therefore, if a laptop is purchased for $800, and depreciates by 10 percent a year, thus yielding an exposure factor of .9 (90 percent), then the SLE for a stolen or lost laptop is

SLE = 800 (AV) × .9 (EF)
SLE = $720

The next formula is the annualized loss expectancy (ALE). This represents how much loss you can expect from a particular issue in a year. The formula is SLE multiplied by annual rate of occurrence (ARO):

ALE = SLE × ARO

So, in the previous laptop example, if you think you will lose six laptops per year, the calculation is

ALE = 720 (SLE) × 6 (ARO)
ALE = $4320

As you can see above, the mathematics involved are quite simple. Another concept to focus on is residual risk. This is basically how much risk is left over after you have taken all the steps required to deal with the risk. In addition, this topic brings us to the issue of how you deal with a risk in which you have identified. There are four categories of responses:

- **Mitigation:** This means you take steps to lessen the risk. No matter what you do, it is still likely there will be some risk left. For example, if you are concerned about malware, then running antivirus is risk mitigation. This is the most common solution.
- **Avoidance:** This is difficult to attain. It means you have zero risk. For example, if you are concerned about users downloading a virus from a website, the only way to completely avoid this from happening is by not giving them access to the web. This is not usually a viable solution.
- **Transference:** The process of transferring the risk to someone else. The clearest example is cyber breach insurance. If you have such insurance, the realized risk cost will be passed on to the insurance company.
- **Acceptance:** If the probability of the risk is very remote, or the cost of mitigation is higher than the cost of the risk being realized, you may choose to do nothing, and simply accept the risk.