

Real-World Scenario 12-1: Understanding Risk and Vulnerability

Risk is the possibility of an attack or threat compromising your IT infrastructure. It is normally accomplished by exploiting vulnerabilities in computers, networks, and even people.

Scenario: You work for a medium-sized business with 200 computers and users. The company has experienced extremely fast growth, and until now has not been concerned with risk. Your task is to define risk to your company and develop plans to deal with it effectively. The board of directors is interested in finding out the annualized loss expectancy for the company's servers. The board also wishes to have some kind of management plan in place that includes analyzing network documentation and mitigating threats and potential compromise.

What type of risk assessment should you recommend?

Because you don't know exactly what will happen to your company's servers in the future, it is impossible to predict exactly what will happen to them, and when, and how much it will cost. What concept, in addition to your risk assessment method, can aid in this?

What kind of management plan should you implement? What basic steps does it entail?

(View the solution to this case study before moving on to the next case study.)

Real-World Scenario 12-1 Solution

Remember that solutions to these types of scenarios will vary. The following is one possible solution to the needs of your company.

First, you should recommend a *quantitative* risk assessment. This uses exact monetary values: $SLE \times ARO = ALE$ (the aforementioned annualized loss expectancy).

The problem with quantitative risk assessments is that they are based on the past history of your actual organization. To go beyond this, and perhaps predict the future with a bit more certainty, consider using concepts such as mean time between failures (MTBF). This information can be obtained from the manufacturer of a device. It consists of data gathered from many customers that ultimately shows the average amount of time that elapses before a failure of the device in question. Instead of relying solely on your own data and how costly failures were, you can utilize the data of other customers (anonymous, of course) to better find the median, or average, for failures and predict the future with more clarity.

Finally, you should implement a vulnerability management plan. This means documenting the network, testing the attack surface of servers, scanning systems internally and remotely, mitigating any vulnerabilities you find, and monitoring carefully.

Simulation: Complete simulations 11-1a, 11-1b, and 11-1c.