UNIT I

PROJECT EVALUATION AND PROJECT PLANNING

10. Risk Evaluation

Risk evaluation is defined by the Business Dictionary as: “Determination of risk management priorities through establishment of qualitative and/or quantitative relationships between benefits and associated risks.”

So how does that relate to managed service providers or IT administrators?

Anyone responsible for a company’s data, server, network, or software must perform a risk evaluation. A risk evaluation can help determine if those assets are at risk for a cyberattack, virus, data loss through natural disaster, or any other threat.

The benefit of a risk evaluation is simple — it provides IT professionals with knowledge of where and how their business and reputation are at risk.

Performing a Risk Evaluation:

A risk evaluation can be performed in five simple steps.

1. Identify and prioritize assets. Consider all the different types of data, software applications, servers, and other assets that are managed. Determine which of these is the most sensitive or would be the most damaging to the company if compromised.

2. Locate assets. Find and list the source of those assets. Be it desktop office computers, mobile devices, internal servers, or anything else, you’ll want to trace each asset back to its source.

3. Classify assets. Categorize each asset as either public information, sensitive internal information, non-sensitive internal information, compartmentalized internal information, or regulated information.

4. Perform a threat modeling exercise. Identify and rate all the threats faced by your top-rated assets. Microsoft's STRIDE method is a popular one.

5. Finalize data and make a plan. Once you have your evaluation, it's time to start tackling those risks, beginning with the most critical.