Planning for Disaster:
Assessing Risks to Your Business Data

Provided by HP

It's only a matter of time before a disaster affects your business's ability to access data. If you have a plan, you'll be halfway down the road to recovery when disaster strikes. This article reviews the basics of disaster recovery planning.

Before we get started, it's important to review some important terminology used in disaster recovery planning:

- Assets: Generally speaking, anything that's valuable to your organization. In the context of data disaster recovery planning, you're interested in tracking your organization's data assets (for example, sales data, customer records, and product designs) and data processing assets (for example, servers, workstations, and network devices).
- Vulnerabilities: Weaknesses that might allow for the failure of a control that affects the confidentiality, integrity, or availability of your data assets. For example, if your server runs an old, unpatched operating system, that's a technical vulnerability. In addition, physical vulnerabilities may pose a risk to your data (for example, the use of a water-based fire suppression system near critical electronic equipment).
- Threats: Potential events that may actually compromise your data if a corresponding vulnerability exists. For example, a skilled hacker is a threat that may be able to exploit an unpatched operating system vulnerability. Similarly, a hurricane, a tornado, or another severe storm constitutes a threat that might exploit a leaky roof vulnerability.

As you can see, assets, vulnerabilities, and threats are all closely related. A risk occurs when an asset has a vulnerability and there is the presence of a corresponding threat. This is often expressed using the following mathematical equation:

Risk = Asset x Threat x Vulnerability

You'll further explore the mathematics behind risk assessment when learning about quantitative risk assessment later in this article. For now, let's explore techniques you can use to identify assets, vulnerabilities, and threats.

Identify Assets

When identifying the assets for a full disaster recovery plan, you need to place a value on each of two types of assets: data assets and physical assets. If possible, you should use the asset's financial value. This is straightforward when you're discussing equipment but becomes more complex when dealing with the value of data. You may need to revert to a qualitative scheme that judges the value of each data element relative to each other, using a rating process, such as a 1 to 5 priority rating system where 1 means “I can’t run my business without it,” and 5 means “I wouldn’t miss it if I never saw it again.”

Before you begin to assign asset values, talk to one of your organization’s accountants. It’s possible that the accounting department conducted a similar exercise when compiling the organization’s financial statements. If you’re able to find assistance, keep in mind that accountants often talk about the “book value” of an asset, which is calculated using standardized depreciation formulas. In some cases, the book value may be significantly different from the asset’s true value to your organization. For example, a 30-year-old mainframe may be fully depreciated and have no book value but certainly has real value to your business if it plays a crucial role in transaction processing.

Identify Vulnerabilities

Vulnerability identification can be a challenging process. In fact, it’s never possible to identify all potential vulnerabilities that may affect an asset. Some vulnerabilities are undetectable or may not exist at the time of your risk assessment. You need to identify both physical and technical vulnerabilities.

The identification of physical vulnerabilities often requires the help of building/structure subject matter experts. After all, most IT professionals aren’t qualified to judge the load-bearing capacity of a floor or the soundness of a roof. It’s important that you call in appropriate people to assist you with this endeavor. Your building manager may be a good start. A number of resources are available to assist you in the identification of technical vulnerabilities. Two ways to approach the identification of technical vulnerabilities are turning to the web and using vulnerability detection software.

The Web

One way to identify your company’s vulnerabilities is to consult the website for the manufacturers of the hardware, software, and operating systems that your organization uses. Such sites often have a section dedicated to security bulletins and other announcements of potential vulnerabilities in their software. Best of all, these announcements usually come with prepared solutions, in the form of patches or configuration changes that you can use to immediately fix the vulnerabilities.

Vulnerability Detection Software

Many commercially available systems, such as the Tenable Security Center and WebInspect from SPI Dynamics, are designed to search for potential vulnerabilities in your systems and applications. If your budget is tight, you might want to consider using the free Nessus Vulnerability Scanner to search for network vulnerabilities.

Identify Threats

After you identify your assets and vulnerabilities, identifying the threats to your assets is the last piece of the puzzle. Vulnerabilities become risks only when a corresponding threat makes their exploitation possible. In terms of technical risks, there are a number of potential threats, including the following:

- Hackers
- Malicious code (for example, viruses, worms, Trojan horses)
- System component failures

- Software flaws
- Data entry errors
- Human errors

This article provides only partial lists of potential threats. Literally thousands of possible threats could pose risks to your organization.

Depending on your location, you may also be concerned with any of the following physical threats:

- Fire
- Tornado
- Hurricane
- Flood
- Theft
- Earthquake

When assessing physical risks to your organization, it's often helpful to turn to government resources for assistance. The Federal Emergency Management Agency (FEMA), the U.S. Geological Survey (USGS), and other federal, state, and local agencies spend millions of dollars each year identifying and evaluating risks from natural disasters. Similar products are available for other types of disaster, showing detailed information on the specific levels of risk in various localities throughout the country.

Now that you understand how to identify risk, learn how to conduct quantitative and qualitative risk assessments.

Conducting Quantitative and Qualitative Risk Assessments

If you're like most other IT professionals, the process of walking through the vulnerability and threat identification process described above may have made you a bit paranoid. That's okay; a healthy dose of paranoia helps keep a disaster recovery planner realistic. The next step in the process is to recognize that not every vulnerability or threat constitutes a risk. This is where risk assessment comes into play. Risk assessment is the process of evaluating the equation discussed earlier:

Risk = Asset x Threat x Vulnerability

Risk assessment can be done in two different ways. Qualitative risk assessment uses nonnumeric assessments to identify the likelihood of a particular risk materializing. Quantitative risk assessment formalizes the process through the use of mathematics. We'll begin by looking at the more formal quantitative process and then explore how you can use qualitative risk assessment when a more rigorous quantitative assessment is not possible.

Conduct a Quantitative Risk Assessment

As long as you're able to get the data you need to plug into the calculations, performing a quantitative risk assessment is straightforward. You began this process when you assigned a value to each of the assets in your organization. However, you need a few more data elements to conduct a quantitative risk assessment.

Asset Value

Asset value (AV) is, quite simply, the value of an asset. It is usually expressed in dollars. You learned some techniques for determining the asset value earlier in this article.

Annual Rate of Occurrence

Annual rate of occurrence (ARO) is the number of times you expect a given risk to occur in a typical year. For example, if, on average, two severe thunderstorms affect your area each year, the ARO for thunderstorms in your region is 2. You may need to derive this value from other available information. Here are two examples:

- Earthquake likelihoods are often expressed as the probability that a quake will occur in a given year. You can convert this probability to an ARO by expressing the percentage as a decimal. For example, a 50-percent probability corresponds to an ARO of 0.50. Similarly, a 25-percent probability corresponds to an ARO of 0.25.
- Flood threats are described in terms of the number of years that occur between typical floods. You can convert these figures to ARO values by dividing 1 by the number of years. For example, if the area under consideration lies in a 10-year flood plain (that is, where a flood is expected every 10 years), the ARO is 1/10, or 0.10. Similarly, if the area lies in a 100-year flood plain, the ARO is 1/100, or 0.01.

Exposure Factor

Exposure factor (EF) is the percentage of an asset you expect to be damaged by each occurrence of a particular risk. If you expect a risk to completely destroy an asset, the EF is 100 percent. If you expect half of an asset to be destroyed, the EF is 50 percent.

Single Loss Expectancy

Single loss expectancy (SLE) is the value you expect to lose each time a risk occurs. You calculate SLE by using the following formula:

$$SLE = AV \times EF$$

Annual Loss Expectancy

Annual loss expectancy (ALE) is the value you expect to lose to a given risk each year. You calculate ALE by using the following formula:

$$ALE = SLE \times ARO$$

You can use the ALE for a particular risk to make decisions about measures you should take to manage particular risks. For example, if the ALE for hurricanes in your business is $10,000, you could expect to lose $100,000 (10 years x an ALE of $10,000) over the course of that 10-year period. If you're able to purchase hurricane protection that lasts for 10 years at a cost of $75,000, it's a good investment because the protection costs less than the expected loss. On the other hand, if the protection lasts only five years, it's probably not a good investment because the $75,000 cost is higher than the $50,000 expected loss.

Conduct a Qualitative Risk Assessment

Sometimes, it's simply not possible to perform a quantitative risk assessment. This is often the case when it's difficult to quantify the asset values of one or more data assets. For example, what is the asset value of a customer record? It may be difficult to identify a single numeric quantity that incorporates intangible factors, such as customer goodwill. In these cases, a qualitative risk assessment can be helpful.

To perform a qualitative risk assessment, you follow the same process used for quantitative risk assessment, but you use relative values (such as a scale of 1 to 3, where 1 represents “low,” 2 represents “medium,” and 3 represents “high”). These values produce a prioritized ordering of risks that can assist you in your risk management approach. With qualitative risk assessment, you can’t directly compare the cost of remediation options to the ALE, as you do with quantitative risk assessment, but you still get a general idea of the most significant risks facing your organization.

Once the risk assessment is done, you can focus on managing risks.

Managing Risks

After you’ve completed a risk assessment, it’s time to get to work on the “meat” of disaster recovery planning: managing your risks. For each risk you identified in the previous exercises, you need to select an appropriate risk management strategy. There are four options for managing risks: mitigation, acceptance, avoidance, and transference.

Selection of appropriate risk management strategies is an essential part of disaster recovery planning. You need to weigh the costs and benefits of each approach and select a mixture of risk mitigation, acceptance, avoidance, and transference that is uniquely suited to your organization.

Mitigate Risk

Risk mitigation is the most commonly used strategy. You can use risk mitigation to lower the risk facing your organization to an acceptable level by implementing appropriate controls. For example, you might mitigate the risk of fire by installing a fire suppression system.

Accept Risk

In some cases, the ALE for a particular risk may be low enough that you might want to just accept the risk and do nothing about it. For example, if your business is situated in a state that experiences minor earthquakes on a very infrequent basis, you might decide to accept the risk of an earthquake rather than implement earthquake protections.

Be wary when you hear people make statements such as “Management has accepted that risk.” This line is often used to shut down conversations about risk management when, in reality, management isn’t even aware of the risk. Acceptance of a significant business risk should always be a formal, conscious decision made by senior managers and communicated to appropriate stakeholders.

Avoid Risk

Another option is to change your business practices so that you’re no longer exposed to a particular risk; this is called avoidance. For example, if you have a kiosk computer located in your lobby and worry about that system being stolen, you might decide to avoid the risk of theft entirely by removing the computer.

Transfer Risk

You might decide to share some or all of a risk with others; this is called transference. Insurance is the most common form of risk transference. Consider a fire risk that you mitigate through the use of a fire suppression system. You can’t implement controls that completely eliminate the risk of fire, so you might decide to transfer the remaining risk to an insurance company by purchasing fire insurance.

Now that you understand how to plan for disaster, you should take the time to conduct a risk assessment—whether quantitative or qualitative—for your business. This hard work in advance will pay off big time.

The HP Small Business Connection brings together products, services, and solutions designed with your business in mind.