

Chapter

3

Assessing Risk and Impact

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to do the following:

- Define the risks that may impact your organization.
- Investigate different risk assessments and business impact assessments.
- Set priorities for preventive measures and the recovery from any disaster situation.
- Choose a risk assessment method to be used to identify and quantify risk in an organization.
- Perform risk assessments as they might pertain to an organization.
- Use tools such as OCTAVE to assist in risk assessment.

Introduction

Risk assessment is a critical part of disaster recovery planning. Some of the questions you'll need to answer are: What is the risk? What are the chances that something will happen? What is the business impact, and what is its relevance to disaster recovery planning? What can the disaster recovery team suggest to help the organization mitigate the risk that calamity will befall the organization?

If the planner understands what can go wrong in a particular environment (business, physical, and information technology), he or she can create a plan for almost any contingency. This chapter shows you how to evaluate risk and assess the severity of impact.

To begin, we define the vocabulary that we will be working with in this chapter.

Risk: The possibility of a person or entity suffering harm or loss because of an event.

Business impact: Impact is the magnitude of the potential loss or the seriousness of the event; by extension, business impact is the magnitude of the potential loss or the seriousness of the event to the organization or the business.

Assessment: The act or result of judging the worth or value of something or someone.

Risk is connected to the event. For example, with stocks, the risk that the stock will not go up in value is assessed. In disaster recovery planning, risk is the chance that an event (hurricane, malicious disruption, hardware failure, etc.) will occur to a given organization.

Business impact is connected to the business. In other words, with a given risk that a given event will occur, what is the impact to the business of that event? The business impact (as well as the risk) may be negligible, as may be the case if the business is a sole proprietorship accounting firm and the event is data corruption caused by a disgruntled employee. The same event may have a catastrophic business impact if the business is a multinational or global organization with thousands of employees.

Defining Risk

Risk is defined as the possibility of a person or entity suffering harm or loss. Within an organization or business, risk is viewed as the possibility that the business will lose money because of a disaster occurring. The possibility of harm or loss from any given disaster is different depending on the organization, the situation, and the severity of the disaster. It is possible to assign quantitative values to the possibility that a given event will occur, and also to the amount of damage that is likely should such an event occur. In this way, it is mathematically possible to determine what might happen and the ramifications should it happen for any organization for any given event.

In order to determine the possibilities of disaster and the resulting effects, an organization needs to undertake a **risk assessment**.

Risk Assessment

Risk assessment is a careful, systematic examination of the environment and the physical, technological, or human components that could cause harm to the organization, staff, or product. Risk assessments are conducted to determine whether sufficient precautions have been taken to protect the office, factories and warehouses, and materials and personnel, and also to prevent harm to the business



and loss of revenue. Risk assessments are directed at mitigating loss of productivity: If the physical location of the business is inaccessible to the workers, they cannot continue to perform their jobs. It is important to remember, however, that loss of staff is as much a concern as loss of the physical location and materials: If no one is available to run the equipment, there will be a loss of productivity.

A risk assessment allows an organization, or a department within an organization, to determine the sensitivity of that organization or department to any given event. All potential disaster situations must be considered, even those that may at first appear to be far-fetched or inapplicable. Realistic ramifications and weights should be assigned to all events and potential outcomes.

The most important thing to remember when looking at risk assessment is to determine whether a hazard is statistically significant and whether the hazard has been sufficiently addressed with satisfactory precautions. If it is possible to determine the probability that an event will occur, then take the necessary steps to ensure that it either will not occur or that the effects will be minimal if it does occur.

For example, water can kill. Rivers flood, overflowing their banks and causing massive destruction. However, the chance of flooding in an office on the 50th floor of the USX Tower, even in downtown Pittsburgh with its three rivers, is remote. The building itself may be affected, and power to the building may be interrupted for an extended period of time (and those risks have to be addressed), but the chance of water damage attributed to a flood to that 50th floor office is remote.

In the same way, an avalanche can kill and destroy property. However, the chance of an avalanche in downtown Houston is remote. The 2004 tsunami in Indonesia was devastating. However, the chance of a tsunami hitting Kansas City, Missouri, is remote. The point is that a disaster is relative to the location of the business and must be considered in light of the geography of the business location.

A realistic assessment requires that all participants be aware of the hazards and risks that pertain to the individual business being evaluated.

FYI

Risks vs. Hazards

This chapter discusses both risks and hazards. Before proceeding, it is important to understand the difference between the two words. A **hazard** is anything that can cause harm. A **risk** is the chance that someone or something could be harmed by the hazard. When evaluating for risk, the given risk may be either high (more likely to occur) or low (less likely to occur).

▶ CONTINUED ON NEXT PAGE

TO REMEMBER

It is important to separate the hazard from the risk that someone could be harmed by it. Although in the end the two are taken together to determine what processes need to be put in place so that the organization can withstand any event that is likely to cause significant issues, to begin the process it is important to brainstorm all the hazards that can be associated either with a location or with a line of business or particular organization.

Not every hazard needs to be considered during this process, however. Brainstorming sessions can go quickly from creative to downright silly if we do! While many events might be *conceivable*, they aren't incredibly *likely*. For example, a blizzard isn't a likely hazard that needs to be taken into account if the organization is located in central Texas or south Florida. Likewise, hurricanes should not be a concern to businesses in Montana.

Once a list of all relevant hazards is developed, the risk that each hazard will happen must be determined. For example, a shop that sells fishing bait on a riverbank in a flood-prone area that lies in the path of hurricanes has a high risk of being affected by a hurricane or a flood. However, a taconite mine in northern Minnesota with a significant investment in water relocation facilities and with a large land mass with mining operations taking place at several different levels in the mine has a low risk of being affected by a flood, partly because of the practice of mining at different levels in the mine and partly due to the investment in equipment to move water from one location to another.

Risk Management

Once the potential for loss has been determined through risk assessment, then the organization can begin to manage that risk, and develop the disaster recovery and business continuity plans to address each risk. Risk management prioritizes risks in the order of severity and potential impact on the organization. For that reason, risk management is often considered to be *reactive* rather than *proactive*. In the context of disaster recovery and risk management, a reactive company will tend to wait until situations present themselves before undertaking plans to mitigate or manage the risk of disasters occurring that would impact the organization. Proactive organizations take into consideration all the alternatives that are likely to befall the organization and attempt to plan for or around those eventualities. One reason that many organizations choose a reactive approach is that it's often difficult to assign quantitative measures to the hypothetical impact of a given situation on the organization, whether in whole or in part.



IN PRACTICE: Proactive Organization vs. Reactive Organization

Organizations choose, either actively or passively, to be proactive or reactive. We need to understand the differences and the ramifications outlined below.

Proactive Organization

Clover Warehousing is a data warehousing application service provider organization specializing in data. After spending considerable time determining what hazards were likely to be relevant to the organization, it made a list of hazards and the risks associated with them. The company then decided what measures it could take to minimize the chances that the hazards would occur and to minimize the risk to the organization if they did occur.

The company determined that, although not located in a wet climate, when floods occur they are flash floods and are typically significant. It invested in pumps to relocate water should it enter the basement of the building, elevated its generators so they were sitting above the likely water level, and built diversion ditches around the building housing the servers.

The nature of Clover's business was housing data. It had no control over what kind of data its client organizations would want to warehouse; therefore it put into place a practice of offering encryption services for sensitive information. The encryption would be specific to each client, so no two client's data would be encrypted in the same manner. This would allow for no chance that one client would accidentally see another client's data.

Electronic locks placed on the server room door were biometric, so only given personnel were granted access to the physical servers. Further, enhanced security was placed on the network to help ensure that unauthorized intrusion from either internal or external sources would be minimized or detected.

Virus scan, adware scan, spyware scan, and spam scan software was installed on all servers and desktop computers, and mandatory scans ran every day at noon so they would be minimally intrusive.

The company had not been faced, actively, with any of the hazards that it examined to that point, but put in place measures to make sure that it would be impacted to a far lesser degree should any of the hazards occur.

CONTINUED**Reactive Organization**

Joe's Jerky Joint is a home-based business making homemade jerky (beef, turkey, and fish). The jerky is processed using Joe's special blend of seasonings and dried in his special smoker.

Joe was making a pretty good living with his business. He kept his recipe on an index card in the file cabinet along with a paper copy of his receipts for jerky that he sold as well as supplies that he purchased. He bought a computer to computerize his files, but never got around to putting his records on disk. He kept his files—contact information for vendors he uses and vendors who contact him, as well as a record book including his accounting files—in a shoebox in the bottom drawer of his desk that he had built in the closet in his hallway. His curing shed was built under a picturesque copse of trees on the banks of a lovely river. He always meant to buy flood insurance, but had never gotten around to it. He had been in the same location for five years.

A dam up river burst in a massive rainstorm. The water raced down the river, leveling the curing shed and flooding Joe's house and his office.

When the flood waters receded, nothing was left of the shed. The records in Joe's shoebox were sodden, the ink was washed out of the record book, and the receipts were washed clean, as was the index card on which he had written his recipe. He couldn't fill the orders he had, and he couldn't even try to subcontract the orders he had as he didn't have any record of the orders. He had no tax records, no working records of supplies bought for the current year, and no way to contact his customer base to let them know what had happened.

Joe's business suffered a great loss due to his failing to plan for what was likely an inevitable emergency. He never considered the risk of a flood, even though the likelihood of a flood given his location was great. He never took into consideration what would happen to his business if an emergency situation were to present itself. He never took even the simplest precaution (insurance and secure copies of records) to help himself reestablish his business in the event of a disaster.

Emergency Situation or Event

Risk is often associated with emergency situations, situations that people often call the event or the triggering event. The word "disaster" conjures up connotations of emergency situations, natural disasters, attack by outside sources, or other catastrophes befalling the location where the organization is found. The



following situations are not the only ones that should be considered when analyzing the risks to an organization, but they are to the ones most people think of when talking about potential disasters.

Terrorist Attack In today's world, the possibility of attack by outside agencies has increased dramatically. The attacks on the World Trade Center and the Pentagon on September 11, 2001, and the attack on the Alfred P. Murrah federal building in Oklahoma City on April 19, 1995, are prime examples of how our world has changed. The possibility of terrorist attack needs to be considered, even for those organizations that never before considered it a potential threat.

This is not to say that Joe's Repair Shop or Pinky's Wireless will be the target of a terrorist attack. It is to say that anyone in business needs to be aware of the potential threat and consider it as a possibility.

Not only can a business be affected directly by an attack on its own facilities by terrorists, it can also be affected by attacks on governmental and financial institutions, suppliers upstream, and clients downstream. With the massive networks of interconnections between organizations today, attacks against any one of them, either physically or electronically, can cause a ripple effect that can affect others. It is therefore important to consider the possibility of attack either upstream or downstream in the organization's product chain as a potential risk.

Environmental Disruption Disruption of services due to a wide range of environmental problems ranging from minor fires to major earthquakes needs to be allowed for in any disaster recovery plan. People think about floods as disasters as they apply to their organization, but what about the flood that washes out the electric company's ability to provide service? What would happen if the only supplier that an organization used for raw materials couldn't ship product because of a blizzard in the area closing roads for two weeks? What would happen if your Houston, Texas small business's disaster recovery plan included driving out of Houston into Austin or Dallas and setting up business temporarily in a rented hotel suite, but you couldn't get out of Houston because all of the evacuation route roads were clogged and everyone was running out of gas? These interruptions in service are often *not* taken into account.

IN PRACTICE: Environmental Disruption

Data Divers is a data mining organization that specializes in scavenging historical tapes that have backups of emails for information that will either exonerate an organization involved in litigation or that an organization can use against ex-employees in similar situations.

▶ CONTINUED ON NEXT PAGE

» CONTINUED

When it was deciding where to house its servers, Data Divers looked at the locations where it wanted to lease, based on price. These locations included the first floor in a building located on the banks of a river, the basement of a building in Los Angeles, an old house built on the top of a hill in Montana, and a log cabin in the middle of the forest.

It was determined that flood was too great a risk in the first location, and there were few ways of effectively mitigating that risk. The building in Los Angeles was in an earthquake-prone location, and it would be difficult to minimize that risk. The log cabin posed too great a fire danger to be practical. But the old house on a hill in Montana was perfect. Although there is a tendency to have blizzard conditions, the addition of generators and adequate backups for the other utilities would allow the company to be self-sufficient if necessary. Because it was located on top of the hill, it would be unlikely to be in the path of an avalanche.

By doing careful research on locations that would be best for locating its new business, the company provided a careful risk analysis and was able to plan for eventualities and be able to weather the storm.

Depending on the geographic location of the organization, hurricanes, tornadoes, tsunamis, or earthquakes are often uppermost in the minds of those assisting with the disaster recovery plan. Many of these risks are geographically dependent, and contingency plans can be put into place well in advance of the event. People doing business in tornado alley or in an area prone to flooding should be aware of those tendencies and put into place plans and practices that will mean that these eventualities have the smallest impact possible and that the organization can recover as quickly as possible afterward.

Fire is a source of risk for any organization regardless of location or line of business. The risk associated with the potential of a fire and the resulting consequences of a fire will vary among lines of business. Refineries and gas stations and organizations dealing with volatile chemicals will have different risks and risk tolerances than a clothing retailer or a grocery store chain.

Proper engineering when building or renovating can diminish or prevent damage from earthquakes or hurricanes; however, the disaster recovery plan needs to provide for backup services that take these events into account. For example, even if the building is intact after an earthquake or hurricane, will there be electricity and running water? Will staff be able to get to work?

These plans can range from full real-time backups that are ready to automatically take over upon failure of the main data center, to using alternative



sites that can provide all the equipment that is necessary to allow you to use your own backup tapes as a means to bring your services back online. These sites can be geographically widely separated or can simply be in a different part of town than the primary site. The selection of the proper service will depend on the organization's tolerances for lost data and lost time. The cost of one of these services can be recouped in the savings from even a single day's lost business, if recovery procedures are properly planned.

Information Security Incidents The integrity of an organization's information has become increasingly important with the passing of time. There was a time when all an organization's information was stored on paper (and this may still be the case in many small companies today) and the recovery of that information was nearly impossible; this is not necessarily the case today. However, paper documents still have to be accounted for in every disaster recovery plan and paper still proves to be among the most difficult medium to recover. It is important to remember that many smaller organizations and businesses just starting out have a tendency to operate in a helter-skelter manner, relying on paper documents as the means to maintain records and taking chances with being able to recover these documents.

The accumulated information a business has on itself, its customers and their buying habits, and the cost of production of its products is valuable information to that organization's competitors. Therefore, the safeguarding of this information has taken on a greater importance for most organizations. Any disaster recovery plan needs to provide for the security of the information that the organization deems vital to the business functioning and thriving. This means that not only does the data have to be recoverable, but it has to be recoverable in a way that will allow for the safety of the information from being compromised.

The potential for industrial espionage is a very real threat (think of it as identity theft on a huge scale). What's more, with many of today's regulation regarding the sensitivity and security of medical information, organizations (particularly those dealing directly or tangentially with medical information of any kind) need to be aware of the potential of this information getting into the wrong hands. Medical supply houses, insurance claims processing organizations, physicians, and home healthcare organizations all need to be aware of the potential for the system to be compromised and take steps to limit the ability of anyone to compromise the system rather than to mitigate damages should compromise occur.

The theft of this information is not typically considered to be a disaster, or a triggering event for a disaster declaration, and an organization that finds itself in this kind of situation would likely not want its clients and vendors to know that their data had been compromised. This situation, however, can be classified as a disaster from the organization's perspective, and prevention, mitigation, and remediation actions need to be planned for the organization to be confident that it will continue, recover, and thrive should this disaster occur.

Equipment and System Failure Equipment failure can take on many different aspects. Individual components can fail, entire systems can crash, or key components can cause entire systems to become inaccessible, if not lost. Hard drives crash. A 240-ton production truck can take out the fiber optic network cable, disabling half of the plant. A poorly written program can be inefficient and consume massive amounts of memory, causing the Unix servers to crash. Many of these situations can be planned for and contingencies can be made for situations where these losses occur.

Data center planning, whether your data center is hosted or is wholly company owned, needs to ensure that there is no single point of failure for any system that is critical for business operations. Safeguards for immediate recovery in case of failure and notification plans for such eventualities need to be in place. Further, if high availability is critical to the organization, fault-tolerant and failover contingencies need to be provided for.

Even with modern clustering technology, disaster recovery planning needs to provide for the possibility of failure both at the single system and data center levels and have in place procedures for such losses. The rapid recovery from system loss is key to business continuation and minimizing the loss of profits.

Utility Loss The loss of utilities to a data center can be mitigated by the provision of a data center UPS or other backup system, but these measures cannot provide continuation of operations without supplementation by onsite electrical generation or onsite water purification. Consider the effects of Hurricanes Katrina and Rita in 2005 on the Louisiana and Mississippi border communities, most particularly New Orleans. These towns had more water than they could handle, but not nearly enough to use. Although the need for water purification would not be nearly as critical in most situations, there are situations where the need for access to potable water is critical. Sizing the onsite power generation properly to provide both for current needs and future growth as well as noise abatement is one key.

Another measure that can be taken to limit the single point of failure for utilities is trying to provide multiple feeds from the utility grids into the organization. This limits the chances of loss of power due to single line disruption, although it would be useless should you face grid disruption.

Malicious Disruption All businesses are vulnerable to attack both from within and outside of the organization. Both of these risks can be mitigated by the application of proper security standards to both internal and external applications. The disaster recovery plan should include provisions for dealing with security breaches ranging from denial of service attacks to the internal destruction of data by a disgruntled or terminated employee. Proper recovery operations for each type of attack need to be targeted to just the areas affected without impacting other areas of operations. Such targeting requires cooperation between functional areas to ensure minimal impact on those areas not involved in the attack.



Auditing and other detection methods can be put into place as a way to track these problems, but prevention is a much better option than detection after the fact.

IN PRACTICE Database Auditing

Many database management systems have the facility to audit what is going on within the database. This auditing can be turned on, minimally, at the user level, at the database level, or at the object level (like tables).

This auditing can add overhead (such as storage for the audit logs) to the system, but because it is possible to discover far earlier what is happening and to determine who is accessing what in the database, it is possible to determine when someone is straying outside of their authority level and to limit their access early in the process, likely before any major problems are discovered.

Enterprise level risk assessment is not a one-time task but an ongoing process. Once an assessment methodology is decided on and put into place the practice of risk assessment needs continued refinement and improvement.

Choosing the Assessment Method

A consistent method of risk assessment needs to be applied across the business enterprise. Consistency is critical because the method will go a long way toward determining the weighted outcome and coming up with a unified result set.

Regardless of the method chosen, the assessment of various levels of risks cannot be compared to each other unless the method used to assess them is the same.

You can manage the risks to your business only if you have a method of dealing with them. Each business has a unique manner of operating and therefore needs a unique method of dealing with risk management. Input from the entire disaster recovery planning team should be sought so that an overall perspective can be built up. This can then be used to both define risks and develop plans to deal with them.

There are several different types of assessments that can provide the organization with the information needed. Each assessment comes at the situation a little differently, some from the perspective of the disaster, some from the perspective of the assets of the company that is involved, and some from the impact that a disruption could have on the organization. Combinations of these assessments are often used (for example, a disaster-based risk assessment alongside an asset-based risk or business impact assessment).

There are many methods that you can use. This chapter covers the following methods:

- Disaster-based risk assessment
- Asset-based risk assessment
- Business impact assessment
- OCTAVE risk assessment

There are likely myriad other methods—whether different methods or combinations—that you could find if you did some research on risk assessment.

Matching the Response to the Threat

Although a fire that destroys large parts of a building may require invoking the full disaster recovery plan, a denial of service attack on a Web site does not. Each threat needs a plan and a measured response spelled out in the disaster recovery (DR) plan. Each response should detail the use of resources, and assign only those resources needed to fix the problem.

Identifying Mission-Critical Processes and Systems

Each system and each process contributes to the operation of the enterprise, but there are some without which the enterprise cannot carry out the others. Identifying each of these processes and systems and then providing for their rapid recovery within the DR plan is one of the keys to successful business continuation.

Evaluating Critical Functions

Functions need to be assessed by problems that their loss will cause to the everyday operations of the business. Will the loss of a function affect the continued manufacture of the product? Will it affect the receiving of goods or their shipment? Will it affect the tracking of goods through the enterprise? Although a decision support system (DSS) such as a management dashboard may provide information to management, it may not be critical to the operation of the business. The decisions as to which functions are critical and which are not need to be made in an objective and independent manner.

Setting Priorities Based on Time Horizons

It's important to remember that everything can't be done at once. Although this may not be the solution that will please all stakeholders and upper management, it's important to maintain a realistic outlook on what can be accomplished and



when it can be completed. To this end it is important to set priorities for preventive measures and the recovery from any disaster situation.

One of the first things that must be accomplished when determining both the risk analysis and the resulting disaster recovery plan is a prioritized list of those processes and applications that are critical to the organization. It is often possible to divide this list into two sections, planning for recovery in phases. Typically, these chunks are based on time horizons defined in service level agreements (SLAs) with external or internal clients.

For example, many processes must be recovered within 36 to 48 hours. This time may be stretched to 72 hours based on organizational requirements. These preliminary systems may include order processing, payment processing, or other customer-related processes so that the organization can restore relations with customers and vendors as quickly as possible.

A second tier of processes may include the ability of the organization to write checks, process payroll, and provide important although less critical systems to the organization and its vendors, partners, and customers. These processes may need to be brought online within the first 2 weeks or months after a disaster. Depending on the time horizons identified, the ability for accounting to close the books and provide financial information to interested parties may fall within this time frame.

A third tier may include those processes that provide functionality to the organization but which are not critical or highly important to the day-to-day processing or week-to-week functioning of the organization. These processes may include time tracking, operational reporting, and printing and mailing reports to external organizations.

Implementing Disaster Avoidance

The best disaster is the one you don't have to recover from. The time and money invested in planning and implementing programs to avoid threats and risks will pay for themselves in continued operations.

One of the primary outcomes of the risk assessment exercise will be a list of things that can be done, preliminarily, within your organization to help you to avoid disaster rather than having to recover from it. Although not all disasters, hazards, or vulnerabilities will be avoidable, avoiding the ones that you can will be key to limiting the impact that all disasters have on your organization and limiting the scope of what you have to recover from.

Avoiding Disasters through Effective Preventive Planning

Identifying risks to the enterprise's operations allows you to effectively plan the ways that you can avoid the possibility of exploitation of the risks. Finding and nullifying risks to critical processes by doing things like providing multiple suppliers for critical parts or providing security for critical computer applications is

part of any good DR plan. If you can prevent something from failing, you nullify the need for recovery.

Although there are many types of disaster and hazard threats that cannot be avoided, the risk assessment process will point out those areas where new or altered processes or security measures can help to avoid the potential loss of data or unscheduled downtime. If the risk assessment is successful, you will easily be able to see those areas where you can put into place measures that will allow you to avoid as many of the threats as possible.

Some measures may be as simple as changing passwords from the defaults and on a regularly scheduled basis, or enforcing organizational statutes. It may mean rearranging seating within your organization so that only those who require access to the servers have that privilege. It may mean adding security hardware to the infrastructure to limit access to the assets should inappropriate individuals attempt to physically access the hardware.

Creating Contingency Plans for Unavoidable Threats

Even if you can prevent most of the risks from being exploited, there will be some risks that are unavoidable. Planning to mitigate the effects of these risks is both necessary and prudent. However, the amount of time and resources invested in that planning should be dependant on the probability of the event occurring. You would not spend much time planning for an earthquake in upstate Vermont, but a lot of time looking at the possibility of snow causing a roof collapse.

People in the World Trade Center and in the Pentagon likely never foresaw the eventuality of September 11, 2001. Even if they had foreseen the potential for terrorist attacks via airline crash, the ability to put into place any means to nullify the threats would have been futile and likely would have fostered a false sense of security in those involved.

The remainder of this chapter covers each risk assessment method previously described in greater detail. Some are less complicated than others, some deeper and broader. As with everything, the tools that you choose (in this case the assessment methods) are often are the ones that fit the situation. They may be the ones that you are told you have to use. Whatever the tools, however, the methodologies are similar.

Disaster-based Risk Assessment

The premise of this type of assessment is that the decisions relating to risk management and disaster recovery should be made based on awareness of existing risk factors rather than out of habit or based on what may prove to be unfounded fears. Leaders, particularly those who are in charge of the disaster

recovery team, should act with keen appreciation for the essential factors that make each risk situation unique. They should understand it as it relates to the organization and undertake it in that manner, rather than simply on conditioned responses and as a means to get to the next step. Management needs to be able to rely on support personnel internally, or find those individuals on a contractual basis to fill the gaps should these people be required and are unavailable. They should be able to rely upon those contracts to be carried out in the best interest of the organization and to a degree that will allow the organization to continue in the event of an emergency situation.

Hazards exist. It's a fact of life. However, hazards (or the reactions to hazards) do not have to be so great that the organization is stifled or smothered. The purpose of the risk assessment and resultant risk management and disaster recovery process is to ensure that not only are the risks identified but also that any of those risks that may exist can have proven means of remediation or recovery. Hazards and the associated risks cannot be avoided, but they can be mitigated and planned for. In many cases, this is the best we can do.

One of the most common structured approaches to risk assessment is the disaster-based risk assessment process. This process breaks down the overall process of risk assessment into small, discrete chunks, or more delineated tasks that provide the user with an overall understanding of how those tasks relate to each other. This section will discuss the disaster-based process in more detail and provide information on its use.

Table 3.1 shows an example of a broad tracking document to determine exactly where the organization is in its disaster recovery process. Each department is listed, and progress on the goals is tracked in the columns. Remember, this is often an interactive process, with corrections being made

TABLE 3.1 Departmental risk assessment steps.

Disaster Recovery Planning Process	Risk Assessment Steps				
	Step 1 Identify hazards	Step 2 Assess hazards	Step 3 Develop controls and make risk decisions	Step 4 Implement controls	Step 5 Test and evaluate
Accounting	X	X			
Systems Administration	X	X	X	X	
Human Resources	X				
Marketing					
Sales	X	X	X	X	X

to the process and to the plans based on both the implementation process and the results of testing. For more detail, various components of each step also can be listed, and each of those tasks checked off the list as they are completed. This document should be reviewed frequently at update meetings, and managers can offer encouragement and incentives to get the various tasks completed.

This process is broken down into five steps:

1. Identify hazards.
2. Assess hazards.
3. Develop controls and make risk decisions.
4. Implement controls.
5. Test and evaluate.

The following sections explain each step in greater detail.

Identify Hazards or Risks

Creating a list of all possible risks may seem like a daunting task. There are many events and conditions that can be considered a risk to the organization, from a fire to a meteor hitting the building. However, only a portion of the list will apply with any significance to a particular business, and the chances of some (like the meteor) are so remote as to be negligible. The DR team needs to examine each business unit and each department and determine which risks apply to that group.

Each department or business unit should work on its own list independently. This will allow the tasks to be done in parallel and will allow each business unit or department to get a better feel for what events will actually affect it and, by extension, the organization as a whole.

There will emerge, from this exercise, a list of the most common risks to the organization as well as a better idea of the interdependencies between the various business units. These risks and interdependencies will then allow not only the disaster recovery team but also the organization as a whole to come up with a complete picture of the risks affecting the business as a whole. It will also be the basis from which the overall disaster recovery plan will be derived.

Hazards are actual or potential conditions that can occur:

- Injury, illness, or death of key personnel due to bio-terrorism
- Damage to or loss of plant equipment due to hurricane
- Damage to or loss of plant equipment due to tornado
- Damage to or loss of plant equipment due to fire



- Damage to or loss of plant equipment due to flood
- Damage to or loss of property due to hurricane
- Damage to or loss of property due to tornado
- Damage to or loss of property due to fire
- Damage to or loss of property due to flood
- Losing or having compromised intellectual property due to network hacking
- System degradation due to extensive adware and spyware
- System inaccessibility due to denial of service attack
- Inability for users to communicate with the system due to network failure
- Loss of system, in part or all, due to disk or other hardware failure

The hazards, risks, or sources of danger can be attributed to enemy, adversary, environmental, or any condition that causes undo loss or strife upon an organization. In this case, the hazards are the hardware failure, tornado, denial of service attack, or other events. Hazards are found in every area, in every region of the country and of the world, and are capable of wreaking havoc to one degree or another upon an organization. Some hazards are unique to an area and others can be categorically ruled out for another area. Hurricanes don't hit Denver, Colorado; blizzards rarely hit Bangalore, India. Adding the information on what can transpire should the event occur will give you a better idea as to the organizational ramifications connected with the hazard. More information that you can use will be presented later, but this information is not necessary at this point in the process.

Accurately identifying hazards to the organization is key to the organization's ability to recover from these disasters. Also, hazards often change rapidly. Things that you consider to be of little risk at one point in time can quickly become major threats based on a given set of circumstances. That is why vigilance and risk assessment are typically ongoing activities. Complacency, ignoring the fact that existing controls may or may not continue to provide the hazard control that they have in the past, and ignorance of rapidly changing situations can together be considered to be a hazard in themselves.

The leaders of the team first have to analyze the current goals of the disaster recovery team and the goals of the organization, both stated and implied. This has to be done with the understanding about what needs to be accomplished and with an eye on setting intermediate milestones along the way for the team.

Risk assessment is often a difficult and complicated undertaking. This is particularly true if it is being undertaken as a whole rather than in stages. It is often easier for the team or for individuals connected to the risk assessment to complete the undertaking in bite-sized pieces. This may be an hour at a time, twice a week, or until a good understanding of the risks can be accomplished.

Goals that are too complicated or goals that are too lofty allow (and encourage) inaccuracies in the process. Actual risks can be missed in the process of trying to meet impossible deadlines, and perceptions of risk where risk does not exist can lead to misplaced effort.

Remember that hazard identification and the whole risk assessment process will end up being a different scale, a different scope, depending on the size of the organization that is performing the assessment. Many of the events that are hazards for a multinational organization are also hazards for small businesses, but many are unique to the location, the size, and the complexity of the organization.

Team members should constantly consider their enemies, which may be human, technological, or environmental. Also, they should remain conscious of the capabilities that the enemies have to disrupt your organization. Table 3.2 is an example of a small business' hazard identification list. This business is a family-owned specialty grocery store located on a hill in western Pennsylvania. In this list the organization in question has determined the hazards that are most likely to affect the organization. There are many hazards that are particularly relevant to small businesses. These include, but are not limited to, flood of the business itself, flood of access routes to the business, fire, arson, computer virus, utility outage, illness of key personnel, theft, and power surge.

Large businesses are affected by many of the same things; however, there are some differences that are more relevant to larger businesses than to smaller ones. These include, but are not limited to, denial of service attacks, hackers,

TABLE 3.2 Weighted list of hazards identified by a small business.

Hazard	Weight (1 to 5 scale)
Flood of business	2
Flood of access routes	4
Fire	4
Arson	3
Virus	2
Electrical outage	4
Catastrophic illness of owner	5
Theft	4
Power surge	3



spam, adware, interruption of supply chain, interruption of shipping channels, fire, flood, earthquake, hurricane, tornado, other natural disasters, multiple disk crashes, massive power failure at multiple key locations, data corruption, programming logic errors, malicious data alteration or deletion, and many more.

Assess and Prioritize Risks

After the risks have been identified, each of the listed risks needs to be assessed and each hazard given a weight of how likely that hazard is to affect the organization and the potential impact of that hazard on the organization. The recovery team needs to determine what the chances are of each hazard occurring, as well as determine the ramifications to the business, in a worst-case scenario, should that hazard occur. The assessment and prioritization will be a more subjective rather than objective assessment, but it's important that careful thought be given to the realistic ramifications of a disaster to the overall organization's operation and that intelligent and realistic measurements be assigned to each. Although the tendency may be to either take an overly optimistic or overly pessimistic view of what the ramifications may be, care must be taken to judge the real risk rather than either of the extremes. If you do need to choose between the two extremes, however, planning for the worst case allows you to plan for the most severe ramifications and be pleasantly surprised if that isn't the extent to which the event impacts the organization.

Once you have determined the hazards and the ramifications, you need to make a prioritized list of those hazards that are most likely to occur in your unique circumstances and which have the most serious ramifications should they occur. Using this list you can then determine the best disaster avoidance strategy to keep the hazard from affecting your organization and the best disaster recovery strategy to use in each situation. Use this list as a means to help you to work your way to a point where you determine that the cost of continuing to put avoidance and recovery strategies in place is not cost effective. Putting in fire alarms in any situation will be cost effective. Preparing for a hurricane in Minneapolis would not be.

Table 3.2 showed an example of a prioritized weighted list of risks associated with small businesses. Table 3.3 shows a similarly organized list for larger organizations.

When performing this part of the exercise you need to look at who could be hurt, and how and to what extent the injuries can impact the individual or the organization. Remember, it isn't just a cliché that your most valuable assets are people. They are the ones who know how to get the company back on its feet and who know the inherent meaning of the data. Their safety needs to be paramount in the decisions on how to limit the impact of, and recover from, any potential risks.

Also, you need to determine how to make the best use of the resources available and how to most quickly limit the impacts of any risks that you

TABLE 3.3 Partial weighed list of hazards identified by a large business.

Risk	Weight (scale 1 to 10)
Denial of service attack	8
Hackers	7
Spam	7
Adware	7
Interruption of supply chain	5
Fire	9
Flood	8
Earthquake	6
Hurricane	7
Tornado	7
Tsunami	2
Power failure at one or more locations	6
Avalanche	5
Disk crash	7
Data corruption	8
Virus	7
Interruption of outbound transport of product	6
Network failure	8
Hardware failure	8
Data deletion	8
Programming logic errors	9

determine to be significant. Any company has only a finite amount of resources and therefore needs to make intelligent decisions as to what it can reasonably accomplish with the plans and what it can't.

IN PRACTICE: The Reality of Risk

It is important that all major hazards and risks that are relevant to an organization be examined. An exhaustive analysis of every hazard that might be relevant in any way, regardless of how rare the event may actually be, might be overkill. This exercise needs to be approached in

▶▶ CONTINUED ON NEXT PAGE

**CONTINUED**

a complete manner, but with an eye on the reality of the organization and location situation. It isn't really necessary to consider snowfall as a serious risk in Houston or Miami. Although it might occasionally snow, the risk to a business from extensive snowfall is negligible.

It is always interesting when there are individuals with a sense of humor on the team. They can lighten the mood and make the meetings more interesting. They may come up with hazards like a herd of hungry rabbits attacking the data center, or the computers developing a personality and taking over the process themselves. The levity can be particularly useful when the team has decided that they will at least examine every hazard that is brought to the table. Although these ideas are far-fetched, and the people with interesting senses of humor know this as well as the rest of the team does, they can introduce a level of reality necessary when looking at potentially bad situations for extended periods of time.

Develop Controls and Make Risk Decisions

It is important to make intelligent decisions once you have completed your risk assessment. When you have determined the primary risks—the hazards and events that will have the worst ramifications and that will be most likely to occur—you need to decide what you are going to do with that information and what you can do to limit the impact or mitigate the damages.

At this point you need decide what kinds of controls you can most easily put into place that will address the largest number of hazards and events, particularly the most significant ones. Many of these controls will likely be procedural (changing passwords at the organizational level at least every 90 days, mandating that work stations be locked when users walk away from them, or allowing access to sensitive data and locations only by those with a need-to-access basis). Others will necessarily have to be physical (fire prevention and elimination in the computer room, sump systems in the basements of buildings in likely flood-prone areas, or the implementation of an automated early response system to alert all personnel in the case of an event occurring).

Additional people will need to be involved at this point in the process. Because of the nature of the decisions financial intervention on the part of the organization will often be required, and key people with the ability to make these decisions, or at least those who can assist in influencing these decisions, need to be brought into the process. It is no good determining that you need to install a fire suppression system in the server room if funding will not be provided for such a decision. These people will want hard facts, for example, the relative cost effectiveness of installing Halon over carbon dioxide over

nitrogen over simple water over dry chemical as a means to suppress a fire that may occur in a computer room. Direct (the cost of the system) as well as indirect (the cost of replacing water-soaked components should the suppression system either deliberately or inadvertently be triggered) costs need to be provided to the decision makers.

Once the decisions are made, it is time to implement a plan for managing the risks to the organization and for putting the controls in place that will minimize the impact of the hazards. It is also time to put into place the meat of the DR planning.

Implement a Risk-Handling Plan and Controls

The next step in the process is to implement the risk-handling plan (the prevention steps and the recovery plan) and to put into place the controls that will, hopefully, make those plans unnecessary.

Now is when you put into place those measures and controls that will help mitigate the damages and limit the impact that any event may have on the organization. It is also the time when you determine how best to bring back the company's systems and get it back into a functional state in the quickest way possible given any constraints on the organization.

In this step you will determine the frequency of backups required for your organization to meet its SLAs and to remain a going concern. You will determine how best to test those backups, because without knowing that you can recover backups they are useless. You will also determine what systems are critical to recover and in what order they need to be recovered. This prioritization of systems will be covered to a greater extent in Chapter 4.

Now is the time that money starts to play a bigger role in the planning. This is when you purchase the redundant hardware and put controls in place that limit access to data to those who need it. You put the new rules and regulations in place in the organization and impress upon the organization the importance of adhering to those rules.

This is also when you begin the process of testing your DR plan for effectiveness. Testing will prove to you and to all stakeholders that your plans are sound and that you can recover the business to the point where you can continue as an organization regardless of the eventualities that may befall the organization.

Evaluate, Track, and Report

Finally, you need to evaluate the measures that you have put into place, track the successes and failures in your measures and in your testing, and report back to the organization as a whole on the effectiveness. These last steps will be iterative. It will never be as simple as putting measures in place to limit your exposure to emergency situations and then feeling that you are safe forever. The organization needs to periodically reevaluate the steps it has taken to control



the risk that it faces from disaster situations and determine if what is in place is still sufficient or relevant to the situation and make adjustments as necessary. There was a time that simply putting a sign on the door to a server room was sufficient to keep people from inappropriate access to the servers and the data; it then became necessary to adjust the security measures and lock unauthorized people out of the server room. Eventually, it became necessary to alter the network access to keep people from accessing the servers inappropriately from remote locations. Because technology changes, and society changes, it is important to realize that preventive measures have to change and the evaluation process needs to continue indefinitely. You must consider what has been learned, what can be done differently to do better the next time, and then test these new scenarios.

Not only is it important that you report the successes, it is even more important that you report your failures and learn lessons from what didn't work. These lessons will prove to be invaluable in the next iteration of testing and will likely prove to be just as valuable if and when the time comes that an actual disaster is declared.

During the testing phase, make notes of where you found places that you could take shortcuts, what didn't work, or what didn't work the way that you thought it should. It may even be worthwhile to add the position of scribe to the disaster recovery team roster and have someone designated to take notes during the process and own those notes until they are incorporated into the plan later.

IN PRACTICE: Not Resting on Your Laurels

It is important to note that this is an iterative process. You can't just do it once and never address it again. Although many of the hazards and risks won't change to any great degree, the steps that the organization puts in place will change over time.

At one point, limiting access to a building at Lawrence Data Archiving meant simply giving everyone who was allowed to be there a key. Once in the building, everyone was free to come and go as they liked. That was when there were 5 employees.

As the business grew, security had to grow as well. The organization identified the free and easy access to the servers as a potential security risk. Further, it was determined that providing keys to all employees to come into the building was a maintenance issue as far as tracking keys and replacing keys for people who lost theirs. An ex-employee (who had had her key replaced several times while employed) was found in the building using the bathrooms with her children. Not all keys had been turned over when the employee left.

CONTINUED ON NEXT PAGE

CONTINUED

The organization decided that, to mitigate the risk, it would provide those who needed access to the servers with an electronic key card. Further, all employees were given a key card, and security to where the employee was permitted to go was tied to that card. If the card was reported lost or a replacement was requested, the security to the lost card was terminated. That way, anyone who needed access to the servers would be given a card and only those with cards could get in. This was when there were 50 employees.

Over time, employees began to leave their cards in their desk drawers, hanging on lanyards on their cube walls, or just laying on their desk. There was an incident when someone who was not officially given access to the server room was found inside, having appropriated someone else's key card to gain access. It was time to reevaluate the risk mitigation methods that were in place. There were now 150 employees.

The organization decided that biometric options were the way to go. Fingerprint scanners allowed people into the building and into most locations where they were permitted to be. Access to the server room had pupil scan added to the fingerprint scanner as an added measure of security. This way, employees could not lose their access method, nor was it easy for someone to use someone else's security. When an employee was no longer employed by the organization, the computerized access was revoked. This was when the organization had 500 employees.

As you can see, reevaluation based on needs of the organization, over time, needs to take place. This is true of any organization and any hazard and risk combination. Needs change. Technology changes. The organization needs to change along with it.

Asset-based Risk Assessment

A second five-step approach to risk assessment is *asset-based risk assessment*. It attacks the problem more from the perspective of the assets rather than from the perspective of the disaster. Under this approach, you assess all assets, threats, vulnerabilities, and risks to come up with appropriate countermeasures for each. The following sections describe these steps in greater detail.

Asset Assessment

The first step in this particular risk assessment methodology is asset assessment. Disaster recovery team members and the asset owners identify and rank the assets that are most critical to the mission-critical operations, followed by the next levels of



operation, and finally the least critical operations. By identifying and prioritizing these assets the organization can take the first steps toward focusing its disaster recovery resources on those assets that are most important to the organization.

Typically, assets are the tangible things in the organization (people, servers, networks, or other equipment). However, these are not the only assets of an organization. The often-overlooked, more intangible assets include information and data; the processes that are particular to the organization; the reputation of the organization in the marketplace; and the goodwill that is associated with that organization by its vendors, its customers, and its partners. It may well be that the information and associated automated processes are the organization's most important assets. Tangibles are often replaceable, particularly commodity hardware and software, but the intangibles may be irreplaceable.

Organizations, from a security perspective, need to protect sensitive and proprietary information, and may face HIPAA ramifications if proper security measures are not taken. HIPAA, the Health Insurance Portability and Accountability Act, provides for the privacy of an individual's medical information. Disaster-impacted organizations need to not only maintain and protect the sensitive and proprietary information, but also protect information about the functions of the organization and its employees, the critical processes that are centrally unique to the organization, and information connected to the disaster itself.

For each asset that the company identifies, it needs to identify all the events that could impact each of the assets. This needs to include the damage or destruction of the asset, or damage that could impact the information or functionally provided by the asset. An estimation of what the effect of the loss of the asset would be to the organization, both short term and long term, needs to be provided.

A worksheet is typically used to record the results of this assessment. An example of this can be seen in Table 3.4. Because it is the foundation of the remainder of the assessment, the asset assessment is the most important step in this process. The rest of the steps build upon its foundation.

Threat Assessment

The threat assessment step focuses on the adversaries or events that can in any way adversely affect the identified assets of the organization. In this step, it's important to find a means to quantitatively assign a value to what may appear to be a qualitative judgment of the department or the individual involved in the assessment. This quantitative measure can be inferred from the data and information gleaned from the research and interviews done. A threat is usually considered in terms of other adversaries or events. It's important to remember that in order to be an adversary, one must possess both the ability and the intent to cause unwanted events. Natural threats to the organization, such as hurricanes, tornadoes, or fire, do not possess intent that has the capability to cause great harm.

Caution

HIPAA

It is critical for an organization with health-related information to protect access to data during a disaster, throughout the recovery, and even while testing its systems. Records may be accessible to unauthorized personnel, locks may be circumvented, and alarm systems may be inoperable. HIPAA-impacted organizations must be extra cautious when its information is housed offsite, as it may be accessible to people who are not authorized to view it. These situations can leave you open to violations simply due to poor planning.

TABLE 3.4 Asset assessment list.

Asset	Location
mysroracle1	Denver
mysroracle2	Denver
mysroracle3	Austin
mysroracle4	Austin
mysroracle5	Pittsburgh
mainframe	Denver
mysqlserver1	Pittsburgh
mysqlserver2	Pittsburgh
myfileserver1	Austin
myfileserver2	Austin
mymailserver1	Denver
mymailserver2	Austin
mywebserver1	Denver
mywebserver2	Austin

IN PRACTICE: Serious Threat

Freeman was a developer on a Windows system at Westin Walker Company. The developers in this company had access to all development servers but no one was supposed to have access to move programs into the production servers. Freeman was angry at the idea that he was not able to move one program in because the administrators didn't think it had been tested thoroughly.

He decided that he had done a complete job with the testing and he would circumvent the system to get his changes into production because he knew better than the administrators what was important to the users and that his code would not affect any of the data other than what was intended.

Freeman copied his program into the production server that he had access to that no one knew about. No one knew about the change until a week later when extensive data corruption in the database was discovered. It took several weeks to recover the data back to the original state and reapply the changes. The damage that was done to the organization's reputation was immeasurable.

The intent was not to cause data corruption, but the malicious intent to put into place something that was not authorized did cause data corruption.



In order to determine whether adversaries pose a serious threat to the organization, you must determine if they have both the intent and the capability to cause the unwanted events. Further, you must determine or infer their history by a track record of successful attacks against assets similar to those found in the asset assessment. Similar steps can be made for events rather than adversaries because you can determine whether a given event has a historical track record for causing detrimental effects to assets and organizations similar to those involved in the assessment.

What's more, there are certain events—most particularly connected to viruses, denial of service attacks, and other cyber events—that may be treated as independent threats rather than adversaries. Because you cannot track the ability of the attacker or determine the history of the attacker to cause adverse effects for an organization, you may need to handle these threats somewhat differently than threats that can be viewed historically.

Again, all assets must be considered, including information and automated processes. Organizations that rely heavily on critical networks connected to the Internet must be cognizant of different events in the larger environment than organizations that don't rely as heavily on these features.

Again, an effective way to handle threat assessment is to make use of a worksheet. By expanding on the asset assessment worksheet, and including the relevant additional information, Table 3.5 shows an example of what might be

TABLE 3.5 Threat assessment worksheet.

Asset	Threat
mysrvoracle1	hacking
	destructive statement
	crashed database
	crashed server
mysrvoracle2	hacking
	destructive statement
	crashed database
	crashed server
mainframe	hardware failure
	server room fire
	destructive program
	hacking
mysqlserver1	hacking
	destructive statement

» CONTINUED ON NEXT PAGE

CONTINUED

Asset	Threat
mysqlserver2	crashed database
	crashed server
	hacking
	destructive statement
	crashed database
myfileserv1	crashed server
	hacking
	virus
	spyware
	hardware failure
myfileserv2	hacking
	virus
	spyware
	hardware failure
	hacking
mymailserver1	spam
	virus
	hardware failure
	hacking
	spam
mymailserver2	virus
	hardware failure
	hacking
	spam
	virus
mywebserver1	hardware failure
	denial of service attack
	virus attack
	hacking
	hardware failure
mywebserver2	denial of service attack
	virus attack
	hacking
	hardware failure
	hardware failure



found in a threat assessment worksheet. The worksheet lists the assets along with the undesirable events that could adversely affect the performance of the assets without making concrete reference to particular adversaries. Included in this worksheet should be information that might be known about adversaries' capabilities to cause undesirable events. In the case of an event rather than an adversary, you can make use of information relevant to the chance that an undesired event will occur and infer the ramifications of the event occurring to the assets.

The deliverables from this step will be an overall threat level for each asset for each adversary, with the worksheet allowing the assets and threats to be efficiently and effectively organized and documented, and all information later to be organized integrated into a single complete analysis.

It is often advantageous, particularly for smaller organizations where financing for extensive software or external assistance is not available, to store this information in a spreadsheet workbook or in a word processor document so that it is portable, inexpensive, and so that a couple of different types of backups are available in the case of a disaster.

Vulnerability Assessment

The next step in the analysis is the vulnerability assessment. This is similar to what might be conducted in a traditional security survey in that the team members identify and characterize vulnerabilities in the organization related to the specific assets and undesirable events. It is important to address these vulnerabilities as a combination of factors. For instance, you cannot simply say that people are vulnerable to death; in fact, 100 percent of people are likely to die at some point. Although this is accurate in relationship to the risk assessment and disaster recovery plan, it's important to assess the combination of the person and the event. For example, people are 20 percent more likely to die in a tornado in Tornado Alley during June, July, and August. It's important during this assessment to look for the exploitable situations in an organization that are created by a lack of adequate security measures, personal behaviors, or commercial construction.

Vulnerabilities will likely include the absence of adequate security personnel; poor access controls, software controls, or contractor access to systems; and often unscreened or unsupervised visitors in secure areas.

Again, it's important to look at the combination of threats and assets and determine the vulnerabilities that are directly associated or able to be associated with each combination. In this way you can more appropriately assign discrete and measurable controls to each combination and make the end task of protecting the organization or recovering from an attack more defined and easier to implement.

It's also important at this level to look at each asset and threat not only from an internal view looking out at what you perceive to be the dangers, but with an eye toward how an adversary or external event might view the same asset-threat combination. Those involved in this assessment should ask

themselves, “If I wanted to physically harm this asset, I would . . .”, “If I were <insert natural disaster> I would affect this asset by . . .” or “If I were a <hacker, virus, worm, or other attacker> I would attempt to break into this asset by . . .” In this way you can put yourself more into the position of the adversary and find different ways that an asset may be compromised.

During the vulnerability assessment, it’s important that you take into account the *severity* of each vulnerability. Compiling this information gives the team more complete information, so combinations of threats can be analyzed.

Risk Assessment

The risk assessment step is the point in the process where all previous assessments, assets, threats, and vulnerabilities are combined and evaluated. By looking at all previous worksheets and asking the following questions you can determine the weighted lists of assets, threats, and vulnerabilities to use as a basis for identifying necessary controls:

- What’s the likely effect to the organization if this asset is harmed by one of its relevant unwanted events?
- How likely is it that this adversary or adversaries can and will attack one of the assets to which they are associated?
- What vulnerabilities is this adversary or adversaries most likely to take advantage of connected to this asset?

The purpose of this step, and the end result of proceeding with this step, is an evaluation of how all the ratings interact to arrive at an overall level of risk for each asset. Using the risk analysis worksheet is extremely helpful in this step as it will assist you with organizing the information and presenting it in a readable and understandable format.

By making effective use of this worksheet, you should be able to determine the major vulnerabilities and threats in the organization, where they will lay, and what assets they affect that compare the overall risk across the spectrum of assets. You will then be able to determine the physical and cyber risks as well as which of the risks will require the most immediate attention and controls.

Initially, the terms used to describe the ratings of severity for each component may be qualitative and imprecise. Verbal ratings such as medium are often subjective and hard to combine to get an overall understanding of complete risk to the organization. However, users and subject matter experts may be more comfortable in using brief, subjective terms rather than attempting to objectively assign a number to the process.

In situations where subjective measures are being used, it is typically preferable to assign a numeric value to each subjective measure. For example, you may be able to assign a numeric rating scale of 1 to 10 or 1 to 5 that can then be used to combine all weights in an analysis to come up with an overall weighted scale.



In order to arrive at the weighted scale you need to compute the following equation with the values derived from each table. The equation for deriving risk in the case of this analysis follows:

$$\text{Risk} = \text{consequence} * \text{threat} * \text{vulnerability}$$

What you come up with is the overall weighted scale. After this step is completed, the disaster recovery team leaders or managers will determine the threshold where the cost of further analysis and controls becomes more costly than the benefits that are derived from it. For example, although the threat of a hurricane to a server in some situations is severe, the benefit of ensuring that a server in Montana is hurricane proof is not likely cost effective because hurricanes don't typically occur in the state of Montana.

Some of the analysis will end at this point. However, in many cases counter-measures must be put into place to mitigate the risk to the organization of the threats and vulnerabilities to the assets. By determining the point at which diminishing returns occur, and the point at which the organization is no longer willing to fund the mitigation of the risk, the final step in the risk assessment process can be taken.

Controls

You can now identify the countermeasures that may be necessary in order to provide the organization with the steps to follow after a disaster. Using the worksheets as a guide you can determine the most significant vulnerabilities, threats, and consequences that need to be addressed and the assets to which these are attached. You can find the most cost-effective options for mitigating the risks associated with the combination. You may want to consider planning for more than one contingency for each combination, based on differing severities and consequences.

The completion of this step is the basis for decision makers to develop an appropriate disaster recovery plan. Keep in mind, however, that the process must be continual not just a one-time exercise. Threats change, assets change, and processes and abilities within the organization change. It's important to remember that this is an ongoing process, one that needs to be revisited periodically to ensure that the organization is both secure and covered in the event of a disaster.

New threats will emerge from new sources. Threats may appear quickly and may require the organization to do a "quick and dirty" version of the risk assessment to determine how to handle the new threats. Organizations that use a process of continual assessment will be better able to adapt to unanticipated threats as they occur.

The Business Impact Analysis

Another risk assessment process is the business impact analysis (BIA). In this process, rather than identifying the assets and driving the process from that perspective, you address the whole organization from the perspective of the

perceived threats. We will start out by taking a more in-depth look at what we mean by business impact, and then look at an outline of how this assessment process works.

Business Impact

All disasters and emergencies—regardless of size or severity—have a business impact. The level of impact, however, will vary. Assessing the level of harm that may occur from any given threat or risk is essential to designing a disaster recovery plan. The response to any level of emergency, disaster, or event needs to fit the type of disaster or emergency, and the danger that event presents to the business.

The potential impact is assessed using several criteria. The following sections address many of these criteria and will provide you with a better idea of how different people play their parts in the overall assessment.

Service Level Agreements One of the first considerations is the service level agreements (SLAs) that the organization has to meet. When formal (or even informal) agreements are in place with internal or external customers, those have to be taken into consideration early in the disaster recovery planning effort.

An SLA is defined as “a contract that spells out the terms of service that an outsourcer will provide.” (<http://guide.darwinmag.com/technology/outsourcing/sla/>) In setting SLAs, two things need to be uppermost in the minds of the negotiators:

- Can the SLA be reasonably fulfilled?
- Can the SLA be reasonably enforced?

An SLA that does not meet both of these criteria will result in problems for both parties at some point in the agreement's lifetime. If the provider does not have a full understanding of how the SLA is to be fulfilled, it may not be able to provide the service in a timely manner. Further, if the criteria can't reasonably be fulfilled, the consumer may be accused of knowing beforehand that it could not be fulfilled and taking advantage of the provider. If it is not reasonably enforceable, it is possible that there could be lengthy court battles over exactly what is to be expected and how the parties are to work together to achieve the goal. Consumers may not understand their role in the success of the contract and providers may not fully understand what is expected of them in the event that their services are required. This can also lead to the inability of the organization to recover from a disaster.

SLAs, as well as being established between the organization and each of its vendors, should also be set between the IS department of the organization and with each of the business units. These agreements define the guidelines that will allow the planning of disaster recovery by allowing timelines to be built upon the various SLAs; Each step along the line will be taken in



order of its necessary completion depending on the disaster that invokes the plan.

SLAs need to be constructed with input from all business units on the needs that each unit must have met and from all the functional areas on what services they are able to provide.

IN PRACTICE: Service Level Agreements

Conceptually, service level agreements are fairly easily defined—a contract that spells out the terms of service that one party can expect from another party. But in an organization, this can mean a lot of things and, unless it is spelled out, can remain a great definition but one that is not practical.

One company claims that they need to have “five nines” availability of its systems to its customers (internal customers as well as external customers) for their tier 1 production systems. Five nines is 99.999 percent, or about 315 seconds of downtime a year. This is not in writing anywhere, and when pressed they claim that the 99.999 percent is only for the time when they don’t schedule outages for maintenance. That means that the five nines that they demand in availability is only for unplanned outages, but nowhere is this defined or written down. Further, when pressed to provide SLAs on any of its systems, it relies on rough estimation to determine how much downtime it can withstand and when the appropriate people are called in. It calls in upper-level support after a system has been down about an hour or so. It can withstand downtime of about 2 or 3 hours. There is no way to hold anyone, internal or external vendors, to such broad generalizations.

Another company has SLAs that say that it will have maintenance done on nonproduction systems within a 48-hour window. It requires at least 48 hours notice of an upcoming window and a written statement of work to be done in those 48 hours. There are hourly financial ramifications (typically \$1000 an hour for every hour it exceeds 48, charged on the quarter hour) for missing the SLAs unless the reason for the delay is attributed to the customer not providing adequate feedback in a timely manner. This is spelled out in writing in every contract (internal as well as external) that the company maintains. Any deviation from the normal contract is written, especially for the client, and is flagged as different whenever maintenance begins so that all involved know the timelines and the ramifications for missing them.

Functional Area Input The role that each area in the organization plays in the overall functioning of the business needs to be carefully assessed. Each functional area needs to be able to define its own place in the organization as well as be able to elaborate to the disaster recovery team what it believes it will take to recover its systems. The people in these areas will know best what systems they use regularly, which systems they use during different periods of the month or the year, and what systems can be allowed to be pushed out into later in the recovery efforts. This not only helps with the definition of the organization as a whole, but allows each of these units within the organization to realize its worth to the organization and to the disaster recovery effort.

By allowing each area to have input to the total process you allow them both to take ownership of their part of the plan and to buy into the overall plan and the cooperation necessary to successfully complete the steps outlined in the plan. How each functional area fits together to fashion the whole recovery plan needs to be coordinated by the head of the planning team. Encouraging the functional areas to be a part of the planning and testing will foster a feeling that the team is working to actually allow them the ability to do their job the way that they are used to and will encourage them to tell you things that they may have otherwise forgotten.

How the Assessment Works

The purpose of the business impact analysis process is to assist the organization and its management with understanding the impacts associated with all possible threats to the organization. It also assists with the use of that information to calculate the maximum tolerable downtime for the organization based on the time-critical services and resources that the organization relies upon. For most organizations, the resources involved in the time-critical assets include the following:

- Personnel
- Facilities
- Technology, including all computer systems
- Software
- Data
- Networks and network equipment associated with data communication
- Networks and network equipment associated with voice communication
- Paper document records and electronic records
- Plant and equipment
- Inventory, for both internal use and external sale



It is important to note that with the business impact analysis, as with all the analyses, the approach that is taken by the organization is customizable to both organization and situation. Because the needs and resources of a small business are often exceptionally different from the needs of a large organization, even though many of the underlying basic needs are similar, flexibility must be considered at all levels of the disaster recovery planning process.

There are many ways to conduct the information gathering that's required in BIA, including one-on-one interviews with subject matter experts and brainstorming with individuals across the organization. It's helpful to meet with a cross-section of people, as each offers a unique perspective on the organization, its processes, its assets, and data. The information can be gathered face to face, or through the use of electronic data transfer such as emails or central Web sites. The use of a formal or semiformal questionnaire in these cases is often useful, so similar answers can be compared to each other rather than trying to glean information from a freeform discussion. In a group setting these questionnaires can be discussed at length while allowing for the same questions to be answered in all arenas, and again the answers can be compared with each other on equal footing.

In constructing the questionnaire remember that custom questions can be created based on the needs of the organization and the scope of the business and the analysis.

Quantitative questions can be used to assess the economic impact of potential organizational disruption. These are often measured in monetary terms and can be extrapolated from other man-hour type information or forecast loss of business for the duration of an outage. An estimation of the impacts at this level will assist the organization with understanding fully the potential loss not only in terms of loss of income but also increased incurred expenses. Loss in terms of quantitative categories may include the following:

- Lost revenue
- Lost sales
- Lost trade discounts
- Lost accounts payable discounts
- Incurred accounts payable penalties
- Interest paid on borrowed money
- Interest lost on loans
- Contractual fines and penalties for missed SLAs
- Unavailability of funds to the organization
- Penalties due to late deliveries
- Canceled orders due to late deliveries
- Added expense of relying on outside services

- Cost of temporary employees
- Cost of rental or lease equipment
- Need for emergency purchases, often priced at a premium
- Salaries paid to idle staff
- Cost incurred for temporary relocation of employees
- Transportation costs for backup to an auxiliary site
- Replacement cost of key employees

Although this is not an exhaustive list, it gives you an idea of the types of costs that can be incurred in the event of an outage. These are only the immediate quantitative costs directly associated with the disaster and the time immediately following the disaster. The financial ramifications can often be long reaching in the event of a disaster lasting longer or having greater impact than anticipated.

Although the economic aspects of a disaster can be easily understood, and can be measured in terms of dollars and cents either lost or incurred, it's important to also ask qualitative questions to estimate the potential loss impact in terms of emotional understanding and feelings. Although in today's business uncertainty is a daily fact, extended uncertainty and the feelings associated with and surrounding a disaster situation can often provide convincing arguments to the organization's management and a disaster recovery team for shorter recovery windows than may be provided for otherwise. Typically, qualitative questions include the loss of customer service capability, the loss of customer confidence, the loss of vendor confidence, and the loss of employee confidence in the organization.

Questionnaires should also make use of specialized questions, if such questions are relevant to the organization. For example, one question for accounting might be: If you had to process invoices manually, rather than through the system, how much longer would it take you to accomplish this than it does now? Or how would the necessity of having to process invoices manually for several days at month end affect your comfort level in doing your job? If the questions are couched as a means to weigh the relative importance of a system rather than a judgment on a person's ability to perform his or her job in a different manner, valuable information can be gathered not only on the relative importance of systems, but the comfort level that people have when faced with high stress change.

Once the questions are compiled to create questionnaires, the organizational chart for the organization will drive the questioning process. In an organization of any significant size, representatives from all levels of the organization must be involved to obtain the broadest picture of the situation. It's important to not rely entirely on the formalized management structure as the only means of gleaning



information because much valuable information is found at lower levels of the organization, and much of this information never flows to the top management. The people who work with the system day to day provide valuable information on how the data relates to each other and how the systems function within the organization; they may also have valuable information on how to quickly recover from problems. These may be situations and solutions that upper management has not thought of.

Identifying the Threat The first thing that BIA does is to identify the threats rather than the assets. By looking at the threat first you can limit the number of assets to those that are directly affected by the given threat. Although this may lead to certain assets not being addressed, the most vulnerable assets should quickly rise to the top of the list. These are going to be the assets that need to be addressed first. The lesser important assets will be discovered through the process.

The deliverable from this step will end up being a list of all realistic potential threats to the organization. This list should remain realistic and not reflect reactionary attitudes. Again, there's not much chance of a hurricane in Minnesota, and there's not much chance of an avalanche in Houston. Once you have the list, you can then proceed to the next step in the process, which is assessing the risk of the threats to the organization.

Assessing the Risk to the Organization Once you have the list of threats to the organization, you can then proceed with determining the risk that those threats pose. This will give you both the statistical chance that the risk will occur as well as the ramifications to the organization should the risk occur. If you can come up with a weighted list of both the chances that the disaster will befall the area or the organization and a weighted list of the ramifications or consequences to the organization, you can provide an overall ordered list for each scenario.

You can then proceed with the most likely and most serious threats and vulnerabilities and address those with respect to avoidance or mitigation.

Identifying Business-Critical Activities Now that you've determined the threats to the organization and the weighted list of the ramifications of those threats, you can determine the business critical activities performed by the organization and assign those activities and their associated assets to the weighted list and come up with an overall process, assets, threat, and ramifications list that will allow you to further prioritize your avoidance and mitigation plan.

Providing Required Support from Information and Communications

At this point in the process you can start assigning people from the disaster recovery team connected to information and communications systems to addressing the

disaster recovery plan as it relates to the most serious concerns. This will be an iterative process as you address the most serious concerns remaining and apply the solutions to all relevant processes and assets.

OCTAVE Risk Assessment

There is one more assessment process that we should address. Created through Carnegie Mellon University, the OCTAVE risk assessment process is a flexible and simple process that is easily adaptable to an organization of any size, type, and complexity. It can provide an overview that is relevant and valuable not only for disaster recovery planning purposes, but also for internal security audits and revelations.

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a risk-based strategic assessment and planning technique used primarily for security but which can also be used for disaster recovery planning purposes. Because it addresses threats, assets, and vulnerabilities, it is similar to the other evaluations; however, it is less focused on information technology and more targeted on the ability of small teams from an operational and business perspective to work with the IT department to address the needs of the organization. This small team identifies, based on the knowledge of many employees, the current state of the organization with respect to security and its risk sensitivity and in relation to critical assets within the organization.

This highly flexible assessment strategy can be tailored to nearly any organization and can be very effective in identifying those areas where the organization is most likely to be affected by a disaster situation. Because it focuses on the organizational risk rather than just the technological risk, and is targeted toward balancing operational risk, security practices, and technology, it is often a better fit for many organizations.

OCTAVE is driven by operational risk and security practices. Technology is addressed only as it applies in relationship to the security practices and operational risk. This enables the organization to not only gain a better understanding of current risk and security practices, but to examine how breaches in these can affect the organization as a whole. Because disaster recovery is, at its source, a breach of security (whether by human instigation or natural intervention) at some level, this approach can be systematically used to determine an organization's vulnerability to security breach and thus to disaster.

By making use of this alternative approach, an organization can make information protection decisions that are based almost entirely on the risks to the confidentiality, integrity, and availability of critical information-related assets. Again, physical assets are less important because they are easily replaceable, whereas less tangible assets are often irreplaceable. All aspects of risk are factored



into the process and by extension into the decision-making process. This allows an organization to adapt its security and protection practices in real time. These aspects include the assets, threats, vulnerabilities, and organizational impacts that have played a part in all these analyses.

Where other evaluations typically look at systems and approach the problem from that perspective, OCTAVE provides a framework in which to perform organizational evaluations. It focuses on the security practices surrounding the data and data-related assets rather than focusing strictly on the technology and adds components of data and security where necessary. Other approaches often are seen as tactical (self-directed) rather than strategic (directed by external entities) in nature, and they may have a lack of subject matter experts who can provide the necessary skill.

One of the reasons why this approach is often more successful than others is because interdisciplinary teams lead the evaluation and make critical determinations regarding the assets and discretionary measures that need to be taken. These teams include people from both the business units and the IT departments because, to effectively address business process recovery and continuity planning, both perspectives are critical when addressing and observing the global, local, organizational, and departmental security risks and vulnerabilities.

Because OCTAVE is an asset-driven approach, the analysis teams identify those information-related assets that are critical to the organization (for example, the information in the systems on which those permissions reside), focus the risk analysis activities on those assets that are judged by the teams to be most critical to the organization, and consider all relationships among the critical assets as well as the threats to those assets and vulnerabilities (organizational, human, technological, and environmental) that can expose those assets, threats, and vulnerabilities. The team further evaluates the risks as they exist in the operational context. They look at how the assets are used to conduct the organization or business, and with the exposure to risks are existing and potential security threats. As a result, the team creates a concrete, practice-based strategy for improving the organization's security and risk management.

OCTAVE requires three steps, thereby enabling the organizational personnel to quickly and efficiently assemble comprehensive pictures of the organization's information security. Following are the phases on which OCTAVE is based.

Phase 1: Create a Threat Profile

Phase 1 is to create an asset-based threat profile for the organization. This is very similar to phase 1 in the previous five-phase processes, in that it identifies the assets of the organization. It then addresses what is currently being done by the organization to protect those assets. The team then selects those assets that are most important within the organization, or that are considered critical, and

provides the existing or suggested security requirements for each asset. Finally, it's the team's responsibility to create a threat profile for each asset.

Phase 1 is typically subdivided into three processes.

1. **Identify senior management knowledge.** Identification of important assets, security requirements, threats, and organizational strengths and vulnerabilities from a representative set of upper management and documentation of the findings are relevant outcomes of this phase. These can then be combined with the information gathered in subsequent processes.
2. **Identify the operational area knowledge by collecting information about the important assets, security requirements, threats, and current organizational strength from lower-level managers in selected operational areas.** This information is combined with the information gathered in process 1 and should be gathered from managers across the organization in all mission-critical areas of business.
3. **Identify staff knowledge about the important assets, threats, and security requirements, as well as organizational strengths, weaknesses, and vulnerabilities from staff of the business areas and IT staff members in the organization.** These inputs are combined with the information from the previous processes to create the threat profiles. The analysis team selects the top critical information-related assets and defines for those assets the threat profiles for the organization.

It is interesting to discover the differences pointed out by senior management, middle management, and the IT and operational staff. They may well see the company's important assets very differently. Phase 1 is often educational to all involved because of these differences as much as it is in learning information about the different critical processes and information assets in the organization.

Phase 2: Identify Infrastructure Vulnerabilities

Phase 2 involves identifying infrastructure vulnerabilities. In this phase, an evaluation of the information infrastructure is conducted. The analysis team examines the network, assesses patterns to the information deemed critical to the organization and classes of IT components that are directly or closely related to each asset. It is then determined to what extent each cluster of components is resistant to threats against the physical assets and those associated with the informational assets.

Phase 2 is subdivided into two processes. The first process identifies the key components. The set of key components that either support or process the critical information-related assets are identified and a means by which these physical assets can be evaluated is defined. Once the key



components and physical assets are defined, the evaluation of the selected components can begin. Evaluation needs to be done at this point on the selected components as far as threats and vulnerabilities to these assets and the ramifications to the organization continuing should physical assets be compromised.

Phase 3: Develop a Security Strategy

During Phase 3, the team identifies those risks to the organization's critical assets that are most likely to affect the organization, and determines the processes that will limit the impact of the potential hazards and help recover from those hazards that are realized. The protection strategy and mitigation plans address the risks to the critical assets and the vulnerabilities to the threats based on the analysis of the information that was gathered.

3

Phase 3 can be broken down into two processes:

1. **Conduct a risk analysis.** The deliverable from this analysis is a set of impact evaluation criteria that is defined by the organization and the team to establish a common basis for determining the impact value—high, medium, or low—that is attributable to threats against the mission-critical assets. Any and all realistic risks are evaluated for impact. Probability can also be assigned at this point to further refine the process and determine the probability of the high impact, highly likely threats and vulnerabilities to the organization.
2. **Develop the protection strategy for the organization.** The strategy focuses on improving organization-wide security practices and provides a plan for mitigating the impact of the risks to the critical assets.

Further information, including detailed processes and analyses used in the OCTAVE analysis method, can be found at <http://www.cert.org/octave>. Much of the documentation is included on the companion Web site.

Summary

This chapter explains how to assess an organization to determine its vulnerabilities, what hazards are risks to its continuation, and how to begin to mitigate the risks and plan for recovery should an event occur to interrupt operations.

We have further seen that an important place to start is with developing the team. The chapter provides examples of important team members to consider when developing the disaster recovery plan. Now that we have a basis for the team we can begin to explore further what tasks that team will need to undertake and the process of developing the disaster recovery plan.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. What two features of disasters impact the response that the organization has to an emergency?
 - A. Type of disaster and location of the organization
 - B. Location of the organization and time of the emergency
 - C. Time of the emergency and extent of impact presented
 - D. Type of disaster and extent of impact presented
2. What two considerations need to be taken into account when establishing service level agreements?
 - A. Can the agreement reasonably last a lifetime and can the agreement be reasonably fulfilled?
 - B. Can the agreement be reasonably fulfilled and can the agreement be reasonably enforced?
 - C. Can the parties reasonably agree and can the agreement reasonably last a lifetime?
 - D. Can the agreement be reasonably enforced and can the parties reasonably agree?
3. What of the following is not a result of gathering functional area input?
 - A. Helps with the definition of the organizational emergency
 - B. Allows each business unit to realize its worth to the organization
 - C. Allows the functional area to take ownership of its part of the DR plan
 - D. Helps the functional area to buy into the plan
4. What is the definition of risk used in this chapter?
 - A. The possibility of a person or entity suffering harm or loss
 - B. The amount that an insurance company stands to lose
 - C. The variability of returns from investment
 - D. The chance of nonpayment of a debt
5. Why are risk assessments done?
 - A. They are the first step in the DR plan
 - B. To determine if enough precautions have been taken to protect the organization from harm or loss of revenue
 - C. To find out what emergencies might befall an organization
 - D. To give the DR team something constructive to do



6. What is the most important thing to look at in a risk assessment?
 - A. Who is doing it
 - B. If the area is prone to flooding
 - C. If a hazard is statistically significant
 - D. The cost associated with the assessment
7. What is a hazard?
 - A. A risk associated with an event
 - B. The chance that something can cause harm
 - C. A disturbance in operational flow
 - D. Anything that can cause harm
8. What is not an emergency situation cited in the text?
 - A. Terrorist attack
 - B. Bankruptcy
 - C. Environmental disruption
 - D. Fire
9. Which of the following is not considered to be a disaster?
 - A. Terrorist attack
 - B. Hurricane
 - C. Theft of information
 - D. Fire
10. Which of the following is an example of malicious disruption?
 - A. Earthquake
 - B. Denial of service attack
 - C. Electrical fire
 - D. Loss of utilities to a data center
11. What is the first step in a five-step risk assessment?
 - A. Identify hazards
 - B. Identify people to do the assessment
 - C. Identify controls to put into place
 - D. Test and evaluate
12. The most valuable assets in any organization are the _____.
 - A. people
 - B. revenue streams
 - C. physical assets
 - D. data

13. What are OCTAVE's primary drivers?
 - A. Operational risk and security practices
 - B. Organizations and hazards
 - C. Technology and environments
 - D. Data and hardware
14. Which of the following is not one of the phases of threat profile in OCTAVE?
 - A. Identify key components
 - B. Identify staff knowledge
 - C. Identify operational area knowledge
 - D. Identify senior management knowledge
15. What are the two processes in the security strategy of OCTAVE?
 - A. Risk analysis and asset analysis
 - B. Asset analysis and evaluation of selected components
 - C. Protection strategy and risk analysis
 - D. Evaluation of selected components and risk analysis

EXERCISES

Exercise 3.1: Equipment and System Failure

1. Search for information on system and equipment failure on your favorite search engine.
2. List what might be done to provide fault tolerance for a single system.
3. List what might be done to provide fault tolerance at a data center level.

Exercise 3.2: Utility Loss

1. Make a list of utilities required by a data center.
2. Consider and list what events might occur to interrupt each of these utilities.
3. Consider and list what might be done to mitigate each loss.

Exercise 3.3: Risk Assessment

1. Using the risk assessment method associated with Table 3.1, put yourself in the position of assessment analyst.



2. Choose one department in an organization.
3. Complete the table based on that position.

Exercise 3.4: Small Business Hazards

1. Look at the list of small business hazards in Table 3.2.
2. Expand the list by an additional five hazards.
3. Write a description of each of the five additional hazards.

Exercise 3.5: Large Business Hazards

1. Look at the list of large business hazards in Table 3.3.
2. Expand the list by an additional five hazards.
3. Write a description of each of the five additional hazards.

Exercise 3.6: Asset Assessment

1. Look at your personal computer system or at a system in the computer lab.
2. Perform an asset assessment for all the assets.
3. Write a detailed description of the assessment.

PROJECTS

Project 3.1: Functional Area Input

1. Decide on a functional area of an organization.
2. Put yourself in the position of the manager of that functional area.
3. Consider what you may see as your department's most important functions in the organization.
4. List these functions.
5. Determine what level of risk can be attributed to these functions and the kind of events that may impact the functional area.

Project 3.2: Localized Hazards

1. Pick a location in the world.
2. Write an introduction to this location.

3. Research the hazards that are inherent with the location, natural as well as man-made.
4. Determine the risk that each hazard may happen.
5. Order the risks and hazards from most likely to least likely in the location chosen.

Project 3.3: Security

Security is of paramount importance in the information industry. This project will look at the hazards and risks through the lens of security.

1. Choose a type of disaster.
2. Describe the disaster.
3. Determine if there may be potential security issues associated with the disaster.
4. Describe the issues and the potential risks associated with the disaster and security issues.
5. Provide information on what might be done to mitigate the risk.

Case Study

You are responsible for performing a risk assessment. Choose one of the types of assessments in the chapter or find another type of risk assessment and describe that new assessment type. Perform a risk assessment using the chosen type of risk assessment for a home office. Detail all the hardware, software, and information assets that might be affected.