Chapter 1

Understanding Disaster Recovery

In This Chapter

- Understanding how the many kinds of disasters affect businesses
- Starting your disaster recovery plan
- Getting your DR project going
- Taking a whirlwind tour through the DR planning lifecycle

Disaster recovery (DR) planning is concerned with preparation for and response when disaster hits. The objective of DR planning is the survival of an organization. Because DR planning is such a wide topic, this book focuses only on the IT systems and users who support critical business processes. Getting this topic alone to fit into a 400-page book is quite a challenge.

In this chapter, I describe why you need disaster recovery planning and what benefits you can gain from going through this planning. You may be pleasantly surprised to find out that the benefits go far beyond just planning for disaster.

I also take you through the entire disaster recovery planning process — from analysis, to plan development and testing, to periodic plan revisions based on business events. If you've never done any work in disaster recovery planning before, this chapter's a good place to start — you can get the entire story in 20 pages. Then, you can branch out and go to the specific topics of interest to you elsewhere in this book.

Disaster Recovery Needs and Benefits

Stuff happens. Bad stuff.

Disasters of every sort happen, and you may find getting out of their way and escaping their consequences very difficult. If you're lucky enough to avoid the direct impact of a disaster, dodging its secondary effects is harder still.

Here are some of the disasters that can assail an organization:

- Fires
- Floods
- Tornadoes
- Hurricanes
- Wind and ice storms
- Severe storms
- Wildfires
- Landslides
- Avalanches
- Tsunamis
- Earthquakes
- Volcanoes
- Security incidents
- Equipment failures
- Power failures
- Utility failures
- Arson
- Pandemics
- Sabotage
- Strikes and work stoppages
- Shortages
- Civil disturbances
- Terrorism
- War

Each of the scenarios in the preceding list has unique primary and secondary effects that you need to take into consideration when developing a disaster recovery plan.

The effects of disasters

The events that I list in the preceding section have the potential to inflict damage to buildings, equipment, and IT systems. They affect people, as well — killing, injuring, and displacing them, not to mention preventing them from reporting to work. Disasters can have the following effects on organizations:

- **Direct damage:** Many of these events can directly damage buildings, equipment, and IT systems, rendering buildings uninhabitable and systems unusable.
- **Inaccessibility:** Often, an event damages a building to such an extent that it's unsafe to enter. Civil authorities may prohibit personnel from entering a building, even to retrieve articles or equipment.
- **Utility outage:** Even in incidents that cause no direct damage, electric power, water, and natural gas are often interrupted to wide areas for hours or days. Without public utilities, buildings are often uninhabitable and systems unable to function.
- **Transportation disruption:** Widespread incidents often have a profound effect on regional transportation, including major highways, roads,

bridges, railroads, and airports. Disruptions in transportation systems can prevent workers from reporting to work (or going home), prevent the receipt of supplies, and stop the shipment of products.

- **Communication disruption:** Most organizations depend on voice and data communications for daily operational needs. Disasters often cause widespread outages in communications, either because of direct damage to infrastructure or sudden spikes in usage related to the disaster. In many organizations, taking away communications — especially data communications — is as devastating as shutting down their IT systems.
- **Evacuations:** Many types of disasters pose a direct threat to people, resulting in mandatory evacuations from certain areas or entire regions.
- **Worker absenteeism:** When a disaster occurs, workers often can't or won't report to work for many reasons. Workers with families often need to care for those families if the disaster affects them. Only after they take care of their families do workers consider reporting to work. Also, transportation and utility outages may prevent them from traveling to work. Workers may also not know whether the organization expects them to report to work if the disaster damages or closes the work premises.

These effects can devastate businesses by causing them to cease operations for hours, days, or longer. In most cases, businesses simply can't survive after experiencing such an outage. Businesses supply goods and services to customers who, for the most part, just want those goods and services; if the customers can't obtain those goods or services from one business, they often simply go to another that can provide them. Many businesses don't recover from such an exodus of customers.

Minor disasters occur more frequently

Don't make the mistake of justifying your lack of a DR plan by thinking, "Hurricanes rarely visit my neck of the woods," or "Earthquakes occur only every one hundred years," or "No country has ever invaded our country," or "Mt. Rainier hasn't erupted in recorded history." All of these statements may be true. However, disasters on smaller scales happen far more frequently, often hundreds of times more frequently, than the big ones.

Smaller disasters — such as building fires, burst pipes that flood office space, server crashes that result in corrupted data, extended power outages, severe winter storms, and so on — occur with much greater regularity than big disasters. Any of these small events can potentially interrupt critical business processes for days. In time-critical, service-oriented businesses, this interruption can be a fatal blow. *Contingency Planning and Management Magazine* indicated that 40 percent of companies that shut down for three days or more failed within 36 months. An unplanned outage may be the

beginning of the end for an organization — everything starts to go downhill from that point forward. That sobering thought should instill fear in you. You might even put that chilling thought on a sticky-note and attach it to your monitor as a reminder.

Recovery isn't accidental

From a DR perspective, the world is divided into two types of businesses — those that have DR plans and those that don't. If a disaster strikes businesses in each category, which ones will survive?

When disaster strikes, businesses without DR plans have an extremely difficult road ahead. If the business has any highly time-sensitive critical business processes, that business is almost certain to fail. If a disaster hits a business without a DR plan, that business has very little chance of recovery. And it's certainly too late to begin planning.

Businesses that *do* have DR plans may still have a difficult time when a disaster strikes. You may have to put in considerable effort to recover time-sensitive critical business functions. But if you have DR plan, you have a fighting chance at survival.

Recovery required by regulation

Developing disaster recovery plans used to be simply a good idea. These plans are still a good idea, but they're also beginning to appear in standards and regulations, including

- **PCI DSS (Payment Card Industry Data Security Standard):** Although not really government legislation, it's required for virtually every merchant and financial services firm. PCI is a great example of what I call *private legislation* — laws made by corporations instead of governments. All the major banks and credit card companies impose PCI.
- **ISO27001:** This international standard for security management is gaining considerable recognition. Many larger organizations require their IT service providers to be ISO27001 compliant.
- **BS25999:** The emerging international standard for business continuity management.
- **NFPA 1620:** The National Fire Protection Association standard for pre-incident planning. It's a recommended practice that addresses the protection, construction, and operational features of specific occupancies to develop pre-incident plans that responders can use to manage fires and other emergencies by using available resources.

- **HIPAA Security Rule:** This U.S. law requires the protection of patient medical records and a disaster recovery plan for those records.

Over time, more data security laws are certain to include disaster recovery planning.

The benefits of disaster recovery planning

Besides the obvious readiness to survive a disaster, organizations can enjoy several other benefits from DR planning:

- **Improved business processes:** Because business processes undergo such analysis and scrutiny, analysts almost can't help but find areas for improvement.
- **Improved technology:** Often, you need to improve IT systems to support recovery objectives that you develop in the disaster recovery plan. The attention you pay to recoverability also often leads to making your IT systems more consistent with each other and, hence, more easily and predictably managed.
- **Fewer disruptions:** As a result of improved technology, IT systems tend to be more stable than in the past. Also, when you make changes to system architecture to meet recovery objectives, events that used to cause outages don't do so anymore.
- **Higher quality services:** Because of improved processes and technologies, you improve services, both internally and to customers and supply-chain partners.
- **Competitive advantages:** Having a good DR plan gives a company bragging rights that may outshine competitors. Price isn't necessarily the only point on which companies compete for business. A DR plan allows a company to also claim higher availability and reliability of services.

A business often doesn't expect these benefits, unless it knows to anticipate them through its development of disaster recovery plans.

Beginning a Disaster Recovery Plan

Does your organization have a disaster recovery plan today? If not, how many critical, time-sensitive business processes does your organization have?

If your organization has no DR plan at all, you might be thinking that even if you start now, you can't finish your DR plan for one or two years, leaving your business exposed. Although that may be true, you can start with a lightweight interim plan that provides some DR value to the organization while you complete your full-feature DR plan.

Starting with an interim plan

You can develop an interim DR plan, which you design as a stopgap plan, rather quickly. It leverages current capabilities and doesn't address any technology changes that you may need over the long haul.

An interim plan is an emergency response plan that answers the question, "If a disaster occurs tomorrow, what steps can we follow to recover our systems?"

Although a full DR plan takes many months or even years to complete, developing an interim DR plan takes just two to four days from start to finish. The procedure for developing an interim DR plan is simple: Take two or three of the most seasoned subject matter experts and lock them in a room for a single day. Usually, these experts are line managers or middle managers who are highly familiar with both the critical business processes and the supporting IT systems. Using existing capabilities, the team develops the interim DR plan by following these procedures:

- **Build the emergency response team.** Identify key subject matter experts who can build the environment from the ground up if the business has such a need.
- **Procedure for declaring a disaster.** A simple procedure that the emergency response team can use to decide if events warrant declaring a disaster.
- **Invoke the DR plan.** The procedure for getting the disaster response effort under way.
- **Communicate during a disaster.** Whom the disaster response team needs to communicate with and what to say. This list of personnel might include other employees, customers, and the news media.
- **Identify basic recovery plans.** Roughed-in procedures that can get critical systems running again.
- **Develop processing alternatives.** Ideas on how and where to get critical systems going, in case the building in which you now house them becomes unavailable.
- **Enact preventive measures.** Steps the organization can take quickly, in advance, to make recovery easier, as well as measures to prevent a disaster in the first place.
- **Document the interim DR plan.** Write down all the procedures, contact lists, and other vital information that the team develops during the planning process.
- **Train the emergency response team members.** Train the emergency response team members that the team chooses.

The two or three subject matter experts/managers should develop all the points in the preceding list in one day, and then one of those people should

spend the next day typing it up. The other people review the plan to make sure it's correct, and then the experts take half a day to train the emergency response team.

Don't let the organization rely on this lightweight plan as *the* DR plan. It's a poor substitute for a full DR plan, but it can provide some disaster response capability in the short term. The interim DR plan isn't a full DR plan, and it doesn't deliver the value or confidence of a real plan. Have the experts who create the interim DR plan review that plan every three or four months until you complete the full DR plan. Then, you can put the interim plan in a display case in the lobby so passers-by can see it and think, "Gee, that's the first DR plan the company had . . ."

Beginning the full DR project

As soon as possible after you develop the interim DR plan, you need to get the *real* DR project started. The time you need to develop a full DR plan varies considerably, based on the size of your organization, the number of critical business functions, and the level of commitment your business is willing to make.

I estimate that developing a DR project takes three months for the very smallest organization (less than 100 employees and only one or two critical applications) and two years for a large organization (thousands of employees and several critical applications). But you have many other variables besides company size to consider. I don't have a formula to give you because I don't think one exists. My advice: Don't get hung up on timeframes — at least, not yet.

You need to take care of a number of steps before you can begin a DR project, as I discuss in the following sections.

Gaining executive support

DR projects are disruptive. They require the best and brightest minds in the business, taking those minds away from other projects. From a strictly financial perspective, disaster recovery planning doesn't provide profitability, nor should you expect the organization to become any more efficient or effective (although both can happen).

You may find selling the idea of a DR project to management difficult. A DR project doesn't have a ROI (return on investment), any more than data security does. Both disaster recovery planning and security deal with preparing for and avoiding events that you hope never happen (and if you do your job correctly, the fact that the events don't happen *is* your return on investment!). Still, you may need to convince management that DR planning is a worthwhile investment for any (or all) of the following reasons:

- **Disaster preparation and survival:** The most obvious benefit of a completed DR plan is the organization's survival from a disaster — survival that comes as a result of planning and preparation.

- **Disaster avoidance:** Disaster recovery planning often leads to the improvement of processes and IT systems that makes those processes and systems more resilient. Events that would result in a severe business interruption before you had the DR plan in place become, in many cases, just a minor event after you enact the plan. Table 1-1 includes many examples of events and their impact on organizations with and without DR plans.
- **Due diligence and due care:** Few organizations have never experienced an accident or event that resulted in the loss of data. Neglecting the need for disaster recovery planning can be as serious an offense as neglecting to properly secure information. DR planning protects data against loss. If your organization fails to exercise this due care, it could face civil or criminal lawsuits if a preventable disaster destroys important information.

Table 1-1 Examples of Events without and with a DR Plan

Event	*Without a DR Plan*	*With a DR Plan*
Server crash and data corruption	Several days to rebuild data from backup media	Recovery from backup server or disc-based backup media
Hurricane, volcano, or tsunami	Several days' outage	Transfer to servers in alternate processing center
Earthquake	Damaged servers, outage of more than a week	Little to no outage because of preventive measures and backup power
Fire	Servers damaged from smoke or extinguishment materials; several days to rebuild data from backup media	Early suppression of fire, resulting in minimal damage and downtime
Severe weather, resulting in extended power outages	Insufficient backup power capability, resulting in several days' downtime	Sufficient backup power or transfer to servers in alternate processing center
Sabotage	Several days' outage to repair corrupted data	Recovery from recent backup media
Wildfire or flood	Evacuation of personnel; servers shut down due to lack of on-site management	Transfer to servers in alternate processing center

Understanding the frequency of disaster-related events

Getting an accurate idea of how frequently certain disaster-related events can occur may be difficult. Some events, such as volcanoes and tsunamis, happen so rarely that you may find quantifying the probability, not to mention estimating the impact, next to impossible. You can statistically predict other events, such as floods, a little more easily (primarily because they occur somewhat more frequently and predictably), but even then these events vary in intensity and effect.

If your organization has any sort of insurance policy that covers disasters, the insurance company might have some useful information about coverage for disasters. Also, insurance companies may offer a premium discount for organizations that have a disaster recovery plan in place, so you should ask your provider whether it offers such a discount.

Civil disaster preparedness authorities in your area may have some helpful information about the frequency and effect of disasters that occur with any regularity in your region. Where I live, many rivers flood in the fall and winter; earthquakes occur fairly regularly; and Mt. Rainier, an active volcano, sits a scant 20 miles away from my residence. Perhaps your location is blessed with hurricanes, tornadoes, or ice storms; regardless, local authorities should have some clues as to the frequency and severity of natural disasters in your area and how businesses can prepare for them.

Completing important first steps in a DR project

After you gain executive support, you probably just want to get started on your DR plan. But you need to take some important first steps before you launch your DR project:

- **Create a project charter.** A *charter* is a formal document that defines an important project. A typical project charter includes these sections:
  - Project definition
  - Names of executive sponsors
  - Project objectives
  - Project scope
  - Key milestones
  - Key responsibilities
  - Sources of funding
  - Signatures

  Chapter 16 contains a more detailed description of a DR project charter.
- **Select a project manager.** An individual with project management experience and skills — someone who can develop and track the plan, work with project team members, create status reports, run project

meetings, and (most importantly) keep people on task, on time, and within budget.

- **Create a project plan.** A highly detailed description of all of the steps necessary to complete the DR project — the required sequence of steps, who'll perform those steps, which steps are dependent on which other steps, and what costs (if any) are associated with each step.
- **Form a steering committee.** The executives or senior managers who are sponsoring and supporting the project should select members for a formal steering committee. The DR steering committee has executive supervision over the DR project team. While you develop the DR project, the DR steering committee may need to meet as often as one or two times each month, but after you complete the DR project, they probably need to meet only two to four times each year.

After you put these initial pieces in place, you can launch the formal DR project, which I talk about in the following section.

Managing the DR Project

Begin your DR project with a kickoff meeting that can last from one and a half to three hours. The entire DR project team, the members of the DR steering committee, all executive sponsors, and any other involved parties should attend. The steering committee should state their support for the DR project.

After the initial kickoff meeting, the DR project team should probably meet every week to discuss progress, issues, and any adjustments you need to make to the project plan. The project manager should publish a short status report every week that you can review in the meeting. You can send the status report to the steering committee members to keep them up to date on how the project is progressing.

You need to identify and manage many more details to manage a project that spans many departments, which a DR project usually does. If you need more details on project management, I recommend you pick up a copy of *Project Management Planning For Dummies* (Wiley), by Stanley E. Portny.

The following sections discuss the sequence of events for an effective disaster recovery planning project.

Conducting a Business Impact Analysis

The first major task in any disaster recovery project involves identifying the business functions in the organization that require DR planning. But you also need to conduct risk analysis of each critical business function to quantify

the effect on the organization if something interrupts each of these functions for a long time. This activity is known as the Business Impact Analysis (BIA) because it analyzes the impact that each critical process has on the business.

Setting the Maximum Tolerable Downtime

For each critical process, the team needs to determine an important measure — the longest amount of time the process can be unavailable before that unavailability threatens the very survival of the business. This figure is known as the *Maximum Tolerable Downtime (MTD).* You may measure an MTD in hours or days.

On the surface, setting the MTD for a given process may appear arbitrary — and, to be honest, it might be at first. Get members from the DR steering committee involved in setting the figures for each MTD. Committee members' somewhat arbitrary estimates may be more educated than estimates you could get from other sources, such as senior management and outside experts.

You may run into some problems setting an MTD:

- Strictly speaking, an MTD is hypothetical. If a given business process in the organization *had* been unavailable for that long, you wouldn't be sitting around talking about it because the business would have failed.
- You may have trouble finding valid examples of peer organizations that failed because of a critical outage.
- You're dealing with degrees of failure. A business could suffer a lengthy outage, resulting in a big loss of market share that leaves the organization a shadow of its former self. Do you consider that failure?

Setting the MTD for each critical process is at least somewhat arbitrary. But the team has to establish *some* figure for each process. And don't worry — you can always adjust the figure if later analysis shows it's too high or too low.

Setting recovery objectives

After you set the MTD for each critical process, you need to set some specific recovery objectives for each process. Like the Maximum Tolerable Downtime (which I talk about in the preceding section), recovery objectives are somewhat arbitrary. The two primary recovery objectives that you usually set in a BIA are

- **Recovery Time Objective (RTO):** The maximum period of time that a business process will be unavailable before you can restart it. For instance, you set an RTO to 24 hours. A disaster strikes at 3 p.m., interrupting a business process. An RTO of 24 hours means you'll restart the business process by 3 p.m. the following day.

  The RTO must be less than the MTD. For example, if you set the MTD for a given process for two days, you need to make the RTO less than two

days, or your business may have failed (or put failure in its destiny) before you get the process running again! In other words, if you think that the business will fail if a particular business process is unavailable for two days, you must make the target time in which you plan to recover that process far less than two days.

- **Recovery Point Objective (RPO):** The maximum amount of data loss that your organization can tolerate if a disaster interrupts a critical business process. For example, say you set the RPO for a process to one hour. When you restart the business process, users lose no more than one hour of work.

In the final analysis, arriving at an MTD (as well as an RTO, RPO, and so on) is a business decision that senior management needs to make.

Developing the risk analysis

After you set recovery objectives (see the preceding section), you need to complete a risk analysis. For each critical business process, you need to determine the following:

- **Likely disaster scenarios:** List the disasters that can possibly strike. Include both natural disasters and man-made disasters. You might end up with quite a long list, but you don't need to go overboard. Don't get too detailed or list highly unlikely scenarios, such as a tsunami in Oklahoma City or an alien spaceship crash landing.
- **Probability of occurrence:** The probability of each scenario actually happening. You can use a high-medium-low scale, or you can get more detailed if you want.
- **Vulnerabilities:** Identify all reasonable vulnerabilities within each business process. *Vulnerabilities* are weaknesses that contribute to the likelihood that an event such as a flood or earthquake will result in a significant outage.
- **Mitigating steps:** For each vulnerability you list, cite any measures that you can take to reduce that vulnerability.

The risk analysis takes quite some time to complete, even for a smaller-organization that has only a handful of critical business processes.

You may be able to take a shortcut in the risk analysis: Instead of developing a list of all disaster scenarios for *every* business process, you may want to list all scenarios for each business location.

Seeing the big picture

After you complete the MTD, RTO, RPO, and risk analysis for each business process, you need to condense the detailed information down to a simple spreadsheet so you can see all the business processes on one page, along with their respective MTD, RTO, RPO, and risk figures.

If you sort the list by RTO, you can see which processes you need to recover first after a disaster. If you sort by RPO, you can see which processes are the most sensitive to data loss.

You can add a column on your big-picture spreadsheet that expresses the cost or effort you need to upgrade each process so that you can recover it in the timeframe set by its RTO and RPO. You can express these needs roughly by using symbols such as $, $$, $$$, and $$$$, where each $ represents thousands of dollars. A $ represents thousands of dollars, $$ means tens of thousands, and so on.

With this high-quality spreadsheet, you can easily see all critical business processes and the key measures for each. When you rank the processes, you can instantaneously see which processes are the most critical in the organization. Those critical processes — of course — require the most work in terms of disaster recovery planning.

Time for decisions: In or out

Sometimes, a DR team can become overwhelmed by the number of critical processes and the cumulative estimated cost of getting each process to a point at which the organization can recover it within the targeted timeframes. And if the team isn't intimidated by the cost, they may be daunted by the sheer number of IT applications that require work. In this situation, I suggest several remedies:

- **Revise recovery objectives.** When you see the recovery objective and the estimated investment side by side, senior managers can make some decisions about a reasonable amount of investment for a given process. Early estimates can place the cost of upgrading recoverability at a higher figure than the value of the process itself. Senior managers or executives can help to place limits on what you can reasonably spend.
- **Combine recovery capabilities.** You can probably combine the investment for improving the recovery time for several applications, which can reduce costs. For instance, investment in a single large storage system costs far less than separate storage systems.
- **Sharpen those estimates.** The project team can do more detailed work on the investments required to improve recovery times for applications by drawing up actual architectures and plans and then obtain actual estimates for investment. If you proceed with those investments, you need those more detailed numbers, so you can prepare these more accurate figures now and save yourself time later in the DR planning process.
- **Make a multi-year investment in recovery.** After obtaining accurate estimates for improving application recovery, you may reasonably plan for a multi-year investment that improves the most critical applications in the first year and less-critical applications in subsequent years. Or you can use staged investments to incrementally improve recoverability.

For example, if critical applications' RTO is 24 hours, investment can improve applications' RTO to 48 hours in the first year and to 24 hours in the second year.

- **Do the most critical now and the rest later.** The team can draw a line on the chart, handling processes above the line (those that are most critical) in the current project and processes below the line (those that are less critical) in future DR projects.

DR teams often find that their first set of RTO and RPO figures are just too ambitious, perhaps even unrealistic. You may need to revise the objectives and the investment requirements up or down until you reach reasonable figures.

Chapter 3 describes the end-to-end development of a Business Impact Analysis in detail.

Developing recovery procedures

After the DR planning team agrees on recovery objectives (primarily RTOs and RPOs) and chooses the list of in-scope processes, you need to develop disaster recovery procedures for each process.

Mapping in-scope processes to infrastructure

Before you can start preparing actual recovery procedures for applications, you need to know precisely *which* applications and underlying infrastructure support those processes. Although you probably did some of that work when you made cost estimates for recovery in the BIA (which I talk about in the section "Conducting a Business Impact Analysis," earlier in this chapter), you need to go into more detail now.

Many organizations have equipment and component inventories, so you can use those inventories as a good place to begin. Getting an accurate inventory of all equipment and then mapping that inventory to individual business processes definitely takes some time. But without this information, how can you approach the task of developing a viable recovery plan for a business process?

You can find inventory information and get a better understanding of applications' system support from technical architectures, especially drawings and specifications. Technical architectures give you an invaluable look at how systems and infrastructure actually support a business process. If these architectures don't exist for your organization, consider developing them from scratch.

When you know all the parts and pieces that support an application, you can begin developing plans for recovering that application when disaster strikes.

Developing recovery plans

When you think about it, you have to do an amazing amount of up-front work and planning before you can take pen to paper (or fingers to keyboard) and begin drafting actual recovery plans. But you do eventually get to the plan-writing point.

Disaster recovery has many aspects because you may need to recover different portions of your environment, depending on the scope and magnitude of the disaster that strikes. Your worst case scenario (an earthquake, tornado, flood, strike, or whatever sort of disaster happens in your part of the world) can probably render your work facility completely damaged or destroyed, requiring the business to continue elsewhere. So, you can logically approach DR planning by considering recovery for various aspects of the business and infrastructure:

- **End users:** Most business processes depend on employees who perform their work functions. Those employees' workstations may need recovery after a disaster. In the worst case scenario, all those workstations are damaged or destroyed (by water, volcanic ash, or whatever), and you have to get new ones somehow. Chapter 5 discusses user recovery in detail. Employees also need a place to work, but because this book primarily focuses on IT and systems recovery, *where* you put the employees' replacement workstations is beyond the scope of this book.

  

  When you develop contingency plans for locating critical servers, include work accommodations for your critical employees, also.

- **Facilities:** You need to recover the building(s) in which your organization houses its IT systems. If those buildings are damaged, you need to repair them. But if they're beyond repair, you need to identify alternate facilities. No, don't go shopping for space during a disaster — you have to work it all out in advance. Do you need a cold, warm, or hot site? You need to consider that and may more details. I cover all these considerations in exquisite detail in Chapter 6.

- **Systems and networks:** The core of IT system recovery is the servers that applications use to do whatever they do. In worst case scenarios, servers are damaged beyond repair, so you need to build them from scratch. And no server is an island, so you also need to recover a server's ability to communicate with other servers and end-user workstations. Chapter 7 goes into these tasks in detail.

- **Data:** Data is the heart of most business applications. Without data, most applications are practically worthless. You may find recovering data tricky because data changes all the time, right up until the moment a disaster occurs. You can recover data in many different ways, depending on how much data you need to recover, how quickly that data changes, and how much data you can stand to lose when a disaster strikes. I cover data recovery in its entirety in Chapter 8.

- **Preventive measures:** Within the context of developing recovery plans, you have many opportunities to improve applications, systems, networks, and data to make them more resilient and recoverable. An ounce of prevention is worth a pound of cure, and this saying really does apply to disaster recovery planning. You can prevent or minimize the effects of a disaster by taking certain measures, and you should identify those measures. I cover the topic of prevention in Chapter 5 through Chapter 8, as well as in Chapter 12.

Writing the plan

As you prepare to actually develop and document the recovery plans for the components that support critical business processes, you should know what exactly goes into a plan, how to structure it, and how to manage the contents of the plan.

A disaster recovery plan should include the following sections:

- Disaster declaration procedure
- Emergency contact lists and trees
- Emergency leadership team members
- Damage assessment procedures
- System recovery and restart procedures
- Transition to normal operations
- Recovery team members

After you write the plan, you need to publish it in forms that make it available to recovery personnel. You can't just put the DR documents on your organization's intranet or the file server because the intranet may be down and the file server unreachable when the disaster strikes. In order to make DR plans available and usable, you need to distribute them in multiple forms (including hard copy, CD-ROM, USB drive, and so on) so emergency response personnel can actually access those plans from wherever they are, without having to depend on the same IT systems that they may be expected to recover.

I cover the details on writing DR plans and more in Chapter 9.

Testing the plan

After you develop the DR plan, you need to put it through progressively intense cycles of testing. If an organization needs to trust its very survival to the quality and accuracy of a disaster recovery plan, you need to test that plan to be sure that it actually works. In disasters, you rarely get second chances.

You need to do several types of tests:

- **Paper tests:** Staff members review and annotate written procedures on their own.
- **Walkthrough tests:** A group of experts walks and talks through a recovery procedure, discussing issues along the way.
- **Simulations:** A group of experts goes through a scripted disaster scenario to see how well the procedures work.
- **Parallel testing:** The recovery team builds or sets up recovery servers and runs test transactions through those servers to see if they actually can.
- **Cutover testing:** The ultimate test of preparedness. The recovery team builds or sets up recovery servers and puts the actual business process workload on those systems.

These tests move from simple reviews of DR procedures to simulations to the real thing.

Chapter 10 covers DR plan testing in detail.

Understanding the Entire DR Lifecycle

After you write and fully test the DR plan, you're still not done. Business processes and IT systems change with regularity, almost as often as the sun rises and sets. In even a short period of time, disaster recovery plans can get out of sync with the systems they're supposed to protect, and after enough time, the DR plans have little value.

The time spent on the original DR plan will be a waste if you don't update that plan!

Disaster recovery planning is a lifecycle proposition: After you establish a DR plan, you need to regularly review, revise, and test that plan.

I discuss all the topics outlined in the following sections in Chapter 11.

Changes should include DR reviews

To protect and preserve the value and relevance of your DR plan, you need to modify the plan's coverage of several business processes when changes occur to these processes:

- Technology changes
- Business changes
- Personnel changes
- Market changes
- External changes

When any of the events in the preceding list occur in your organization, you need to review and revise your DR plan so that the plan stays up to date and can continue to protect the business.

Periodic review and testing

Establish a calendar of review and testing to ensure that your DR plans are up to date. For instance, set up a calendar for your disaster recovery procedures like this list:

- Review monthly
- Walkthrough test quarterly
- Parallel or cutover test annually or semi-annually

How often you perform these reviews and tests depends on many factors, including the value and risk associated with supported business processes and the rate of change that occurs.

Training response teams

The stakes are high in disaster recovery planning: The survival of the business may hang in the balance if disaster strikes. Periodically train the likely disaster response team members on recovery procedures. In fact, you should train even staff members who aren't likely to end up on the disaster response team — you never know who'll be available when a disaster hits.

Training, if you do it right, doesn't overburden personnel. Because you should perform testing regularly, that testing can serve as the bulk of the training effort. By including the right personnel in paper tests, walkthrough tests, simulations, parallel tests, and cutover tests, you train them simply by exposing them to the recovery plans in these levels of testing.