Chapter 6

Business Continuity/Disaster Recovery Plan Development

Solutions in this chapter:

- **Phases of Business Continuity and Disaster Recovery**
- **Defining BC/DR Teams and Key Personnel**
- **Defining Tasks, Assigning Resources**
- **Communications Plans**
- **Event Logs, Change Control, and Appendices**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Introduction

The bulk of your work in developing your business continuity and disaster recovery plan is complete when you get to this point. Granted, you may be reading this book through from start to finish before developing your plan (recommended) and therefore you will have none of the actual work completed. However, things move quickly in the business world and there are some of you who are doing the work as you read each chapter. Either way, this is where everything comes together. The risk analysis you performed led you into your vulnerability assessment. That data helped you develop an assessment of the impact various risks would have on your business. Finally, you took all your data and identified mitigation strategies—actions you could take to avoid, reduce, transfer, or accept the various risks you found. With that, you now have to develop a plan that takes your mitigation strategies and identifies both methods for implementing those strategies, and people, resources, and tasks needed to complete these activities.

In Chapter 7, we'll go over emergency activities including disaster response and business recovery, so we'll refer only briefly to those elements in this chapter where appropriate. In Chapter 8, we'll discuss training and testing and in Chapter 9, we'll discuss maintaining the plan. All of these are elements that should be included in your BC/DR plan as well.

The plan basically needs to state the risks, the vulnerabilities, and the potential impact to each of the mission-critical business functions. For each of these, there should be associated mitigation strategies. In some cases, there will be multiple mitigation strategies; in other cases, you may have elected to simply accept the risk. However, all of this should be clearly laid out in your documentation thus far. Next, you need to determine how and when those strategies are implemented and by whom.

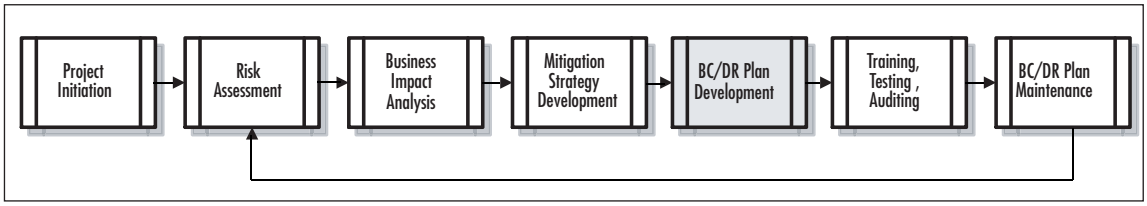
Your work breakdown structure will look something like this:

1. Identify risks *(complete)*.
2. Assess vulnerability to risks *(complete)*.
3. Determine potential impact on business *(complete)*
4. Identify mission-critical business functions *(complete)*.
5. Develop mitigation strategies for mission-critical functions *(complete)*.
6. Develop teams.
7. Implement mitigation strategies.
8. Develop plan activation guidelines.
9. Develop plan transition guidelines.
10. Develop plan training, testing, auditing procedures.
11. Develop plan maintenance procedures.

As you can see from this simplified list, you should already have items one through five completed. We'll discuss developing teams in this chapter as it relates to carrying out the BC/DR plan, not the planning team that you should already have in place (and who hopefully have helped you accomplish tasks one through five). We'll cover developing plan activation and transition guidelines in this chapter before heading into Chapter 7. At the end of this chapter, you'll have items one through nine complete (or will understand how to complete them when you begin project work).

As with previous chapters, we'll begin with a review of where we are in this process (see Figure 6.1). Creating the BC/DR plan entails putting together the information you've developed so far and adding a bit more detail. We'll create the BC/DR plan document in this chapter, but keep in mind we'll have to circle back later to add detail that we develop in upcoming chapters.

Figure 6.1 Project Progress



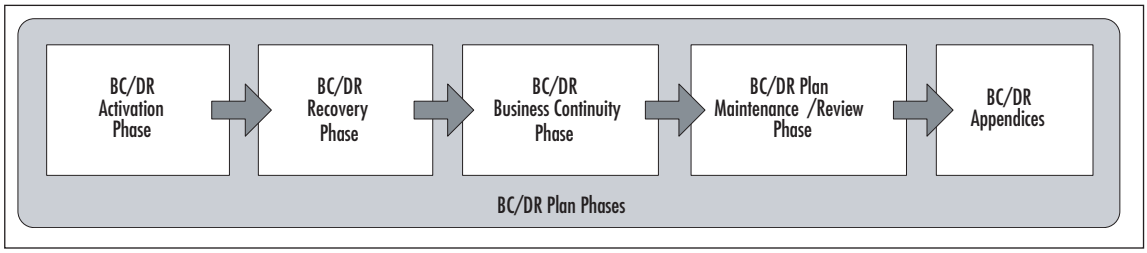
Phases of the Business Continuity and Disaster Recovery

Hopefully you'll never need to put your BC/DR plan into action, despite all the hard work you put into it. If you do need to use your plan, however, you'll need to have clear and specific guidelines for how and when to implement it. Let's begin with a quick look at the phases of the plan: activation, disaster recovery, business resumption or business continuity, and transition to normal operations.

Activation Phase

The activation phase of your BC/DR plan addresses the time during and immediately after a business disruption. In this section of your plan, you need to define when your BC/DR plan will be activated and in what manner. You don't want to activate your plan for every little glitch your business runs into, so you'll need to develop a clear set of parameters that you can use to determine if or when to activate your BC/DR plan. In addition, you will need to define how your plan is activated, including who has the authority to activate it and what steps that person (or persons) will take to initiate BC/DR activities.

Figure 6.2 Phases of Business Continuity and Disaster Recovery



Activation includes initial response and notification, problem assessment and escalation, disaster declaration, and plan implementation. After you have begun implementing the plan, you proceed into the recovery phase, as shown in Figure 6.2.

It is in this activation phase that you should define various disaster or disruption levels so that you know when, if, and how to implement your plan. For example, if you experience a network security breach, you'll have to activate different phases of your plan than if the server room is flooded. Therefore, defining various disaster types and levels is important in understanding what should trigger the implementation of BC/DR plans. You may choose to use a three-level rating system, as described here. However, make sure that whatever system you devise, it's tailored to your specific business configuration and that it gives you the guidance you'd need to make these crucial decisions based on predetermined and agreed-upon criteria.

Major Disaster or Disruption

The possibility or likelihood of this type of disaster occurring is low but the business impact is extremely high. This event disrupts all or most of the normal business operations of the company and all or most of its critical business processes. The disruptions occur because all or a majority of systems and equipment have failed or are inaccessible. This includes destruction to the entire facility; a major portion of the facility; or entire networks, subnets, or sections of the business. Once you've defined what this level of disaster or disruption entails, you should define the process for determining which parts of your BC/DR plan should be activated and which team members should be called upon. We'll discuss triggers more in a moment; for now you should attempt to define the business systems, mission-critical functions, and major operations that when affected would cause a major disruption. This will help you develop appropriate triggers to determine when and how to activate your BC/DR plan.

Intermediate Disaster or Disruption

An intermediate disaster is likely to occur more frequently than a major disaster, but less frequently than a minor disaster (hence the "intermediate" designation). Its impact will be less than a major and more than a minor event. This type of disruption or disaster interrupts or

impacts one or more mission-critical functions or business units, but not all of them. Operations will experience significant disruption, entire systems or multiple systems may fail or be unavailable, but not all of them. An intermediate event could include a fire or flood in the building that impacts IT systems and equipment, structural damage to part of the building where critical operations occur or where vital equipment is located. As with the other two levels of disruption, it's important to define not only what each tier consists of but which parts of the BC/DR plan should be activated and which team members should begin implementing BC/DR activities. As with a major disruption, clearly delineate which systems, functions, and operations would be impacted to earn an intermediate designation so you can define triggers that will address these types of situations.

Minor Disaster or Disruption

Minor disruptions occur every day in the business world and rarely, if ever, are BC/DR plans called into action. The likelihood of a minor event occurring is high, the associated disruption is low. The effects typically are isolated to one component, one system, one business function, or just one segment of a critical business function. Normal operations can often continue, almost uninterrupted, in the face of a minor disruption. Critical business functions still occur for some period of time after this type of disruption. The failure of a single system or service can typically be addressed during the normal course of business. For example, the failure of a single server, system disk, or phone system is problematic but usually does not require the activation of a BC/DR plan. There may be examples, however, where minor disruptions should be addressed by the activation of part of a BC/DR plan. If that is the case, be sure to clearly identify those disruptions along with which sections of the BC/DR plan should be implemented when and by whom.

Activating BC/DR Teams

Clearly, the BC/DR plan cannot activate itself, someone or a team of people need to make appropriate assessments of the situation and make a determination as to whether or not to activate the plan or portions thereof. Therefore, it's also important to create and maintain various BC/DR teams that handle the response to the business disruption by implementing appropriate sections of the BC/DR plan. We'll discuss the makeup of these teams later in this chapter, but for now we'll list some of the BC/DR teams you may want to define and populate as you continue in this planning process.

- Crisis management team
- Damage assessment team
- Notification team
- Emergency response team

- Business continuity coordinator or lead
- Crisis communication team
- Resource and logistics team
- Risk assessment manager

Depending on the size and nature of your company, you may or may not need some of these functions. It's also possible that one person may fill one or more roles if you're working in a small company. We'll discuss these roles in more detail in a section coming up later in this chapter.

Developing Triggers

If you're familiar with project management, you're probably familiar with triggers. Typically, risks and triggers are identified so that if a project risk occurs, a trigger defines when an alternate plan or method should be implemented. The same is true here. If you are going to implement your plan, you'll need to define how and when that should occur—those are your triggers. For example, if you use the three categories of major, intermediate, and minor, you'll need to define what actions are taken in each case. Each level of disruption should have clearly defined triggers. Let's look at a hypothetical example. You're the IT manager of a small firm and the head of the BC/DR team. You're at home one evening just sitting down to dinner when one of the data processing operators who works until 9 P.M. calls you. She reports that there was a fire in the building, it's been evacuated, and the fire department is on the scene. You ask her a series of questions and ascertain that the fire seems to have been contained relatively quickly but that some of the networking gear may have been damaged either by the fire or by the fire containment efforts. She believes the server room is in tact but she's not sure. If you have clearly defined triggers in place, you may determine that this appears to be either a minor or an intermediate disruption and that you should most likely activate a portion of your BC/DR plan. The trigger might be defined as a series of steps such as:

1. Business disruption event has occurred.
2. Disruption to business operations has occurred.
3. Initial assessment by employees on the scene indicates intermediate level damage, including the following:
   - A portion of the network is or may be out of service.
   - One or more critical servers are or may be out of service.
   - A portion of the physical facility has been impacted by the disruption.
   - It is likely employees will not be able to resume normal operations within two hours.

This is an example of a trigger you could define for intermediate types of events. As you've done previously, using scenarios helps you define these elements more clearly. By defining three statements and four attributes, you have a good understanding of whether or not to activate the BC/DR plan for intermediate outages. You also have a defined timeline—if normal business operations cannot resume within two hours. This should be tied to your overall maximum tolerable downtime (MTD) and other recovery metrics developed earlier. If your MTD is 24 hours, an intermediate disruption might be something that will disrupt normal operations for two to six hours. You and your team will need to define these various windows, but be sure to tie your triggers to your recovery metrics.

Your intermediate activation steps are related to the trigger. Once you know you should activate your plan, you should define the immediate steps to be taken. This helps remove any uncertainty about next steps and helps begin a focused response effort. An example of the first steps for an intermediate disruption is shown here.

1. If a disruption appears to be **intermediate** on initial assessment, within two hours:
   - Attempt to gather information from the emergency responders, if appropriate.
   - Activate the damage assessment team.
   - Notify the crisis management team to be on standby notice.
2. After two hours from event notification, gather initial evaluation from damage assessment team.
3. After three hours, notify crisis management team of next steps (stand down, fully activate).
4. Within three hours of event notification, BC/DR plan should be implemented if assessment indicates intermediate or major disruption.

Notice, though, that our description of the actual disruption levels includes trigger information. How many systems are impacted? How extensive is the damage? The more clearly you can define these details, the more precise your triggers will be, and this will help you determine if and when to activate your plan. Spend time clearly defining the circumstances that will warrant plan activation at the various levels you've defined and also spend time defining initial steps to be taken in each phase so that you have checklists of next steps. We'll provide additional checklists you can use as starting points for your own lists when we go over disaster recovery steps in the next chapter as well as in the appendix materials at the end of this book.

Transition Trigger—Activation to Recovery

Another trigger to define is when to move from one phase to another. In this case, that means when to move from the activation phase to the recovery phase. This transition is one

that typically occurs fairly naturally, so you don't need to over-engineer this. However, you may want to define the transition trigger like this:

1. The damage assessment team's initial evaluation indicates an intermediate disruption.
2. The crisis management team has been called in and is on scene.
3. The immediate cause of the event has stopped or been contained.
4. The intermediate section of the BC/DR plan has been activated.

You may wish to define other triggers for your transition, from activation to recovery, suitable to your organization. When defining your triggers throughout, keep your maximum tolerable downtime (MTD) and other defined metrics in mind so that you can work within those constraints. For example, if your MTD is very short, your time between activation and recovery also should be very short. In this case, you may have to err on the side of timeliness and take action with incomplete or preliminary data. You'll have to balance your need to collect information with your need to get the business back up and running as quickly as possible (and within your MTD constraints). Rarely, if ever, is there perfect data in an emergency (or any other time). Defining these triggers and constraints clearly in your plan can help you make better decisions in the stressful aftermath of a business disruption or disaster. Help the team make the best decisions possible by spending time now to define these triggers as clearly and unambiguously as possible.

Recovery Phase

The recovery phase is the first phase of work in the immediate aftermath of the disruption or disaster. This phase usually assumes that the cause of the disruption has subsided, stopped, or been contained, but not always. For example, in the case of flooding, you may decide that if it's external flooding, you will wait until waters subside to begin recovery efforts. This may be required by local officials who restrict access to flooded areas. However, in other cases, you may be able to or choose to initiate recovery efforts while flooding is still occurring. This might include placing sandbags around the entryways to the building or removing equipment that is not yet under water. As you can tell, many of your actions will be dictated by the specifics of the situation, so there's no simple rule to follow here. However, we can say that recovery efforts have to do with recovering from the immediate aftermath of the event, whether or not the event is still occurring. This phase may also include evacuating the facility, removing equipment that can be salvaged quickly, assessing the situation or damage, and determining which recovery steps are needed to get operations up and going again. The recovery phase is discussed in detail in Chapter 7.

Transition Trigger—Recovery to Continuity

You'll learn more about recovery activities in Chapter 7, so you'll need to circle back and define these triggers after you understand the information covered in that chapter. At this juncture, you can make a note that you need to develop triggers that help you know when to transition from recovery efforts to business continuity efforts. Typically, these triggers will have to do with determining that the effects of the disruption have been addressed and are not getting any worse. For example, if you experience a fire in the building, the fire is out, the assessment has been done, any equipment or supplies that can be salvaged have been, and alternate computing facilities have been activated. Those are activities that take place in the recovery phase and when these are all complete, it's time to move into the business continuity phase, which typically includes starting up systems so that business operations can resume. Defining these points should include specific events that have occurred, milestones that have been met, or time that has elapsed. Also keep your MTD in mind as you define triggers for this transition.

Business Continuity Phase

The business continuity phase kicks in after the recovery phase and defines the steps needed to get back to "business as usual." For example, if you have a fire in the building, the recovery phase might include salvaging undamaged equipment, ordering two new servers from a hardware vendor, and loading up the applications and backup data on the servers at a temporary location so that you can begin to recover your data and your business operations. The business continuity phase would address how you actually begin to resume operations from that temporary location, what work-arounds need to be implemented, what manual methods will be used in this interim period, and so forth. The final steps in the business continuity phase will address how you move from that temporary location to your repaired facility, how you reintegrate or synchronize your data, and how you transition back to your normal operations. This detail is discussed in Chapter 7. You'll also need to define triggers here that define when you end business continuity activities and when you resume normal operations. Again, as with the other triggers, you should strive to be as clear and concise as possible. You'll have enough to deal with later if you do end up activating and implementing your plan, so spend time here to save yourself a headache later on.

Although it might seem intuitive that you'll resume normal operations when everything is back to normal, things sometimes do not return to normal after a business disruption of any magnitude. Certainly, business operations will resume, but some things may change permanently as a consequence of this disruption. For example, your company may decide as a result of a major fire or flood that it wants to move to a new location and it's going to do that while operating from the alternate site. That would complicate things because it would mean moving from the alternate site to a new site, with all the concomitant challenges inherent in both resuming normal operations and moving to a new facility. Though this

example may seem outside the bounds of normal business decision-making, be assured that disruptions can change the way companies see their businesses and the way they approach operations. Another example is developing a work-around that's used in the recovery phase that works so well that someone decides to use it full time. When do you transition back to normal operations if you incorporate BC/DR work-arounds? When do you officially transition back to normal operations if you decide that the new server role or network configuration actually works better than the original? It might be a simple matter of formally evaluating the change, agreeing to make it permanent, and declaring you're now running under normal operating conditions. You and your team can define these triggers in advance and you may need to modify them later but at least you won't be working with a blank slate.

Maintenance/Review Phase

The maintenance phase has to occur whether or not you ever activate your BC/DR plan. On a periodic basis, you need to review your BC/DR plan to ensure that it is still current and relevant. As operations and technology components change, as you add or change facilities or locations, you'll need to make sure that your plan is still up to date. One common problem in BC/DR planning is that companies may expend time to develop a plan but they often do not want to (or will not) expend the time and resources necessary to keep the plan current. Old plans are dangerous because they provide a false sense of security and may lead to significant gaps in coverage. If a plan is not maintained, then all the time and money invested in creating the plan is wasted as well. In addition, if you end up activating your BC/DR plan at some point, you'll want to assess the effectiveness of the plan afterward, when things settle down. You should do this relatively close to the end of the recovery and business continuity cycles so that lessons learned can be captured and applied to your BC/DR plan before memories fade and people go back to their daily routines. Reviewing the plan in the immediate aftermath of a disruption will give you valuable insights into what did and did not work. Incorporating this knowledge into your plan will help you continue to hone the plan to meet your evolving business needs. This is discussed further in Chapter 9.

Defining BC/DR Teams and Key Personnel

There are numerous people in positions that are critical to the activation, implementation, and maintenance of your BC/DR plan. Although these may not all be relevant to your organization, this will serve as a good checkpoint to determine who should be included in your various phases. You'll also need to form teams to fulfill various needs before, during, and after a business disruption or disaster. Where possible, you should specify a particular position or role that meets the need rather than specifying individuals. If your Facilities Manager should participate in the Damage Assessment Team, for example, you should specify the Facilities Manager and not Phil, who happens to be the Facilities Manager now. That will allow your plan to remain relevant whether Phil wins the lottery and leaves the com-

pany, gets hit by a bus and is out for an extended period of time, or is promoted to vice president.

Though we briefly define types of teams and their roles in the BC/DR effort, you should take time to clearly define the roles and responsibilities of each team. Having clear boundaries will help ensure that teams are not working at cross-purposes and that all aspects of the plan are covered. Gaps and omissions occur when these kinds of definitions are ill-formed. If helpful, you can create team descriptions that read like job descriptions and you can task members of your HR department on the BC/DR team to assist with or lead this activity. A good team description will identify the following attributes:

- Positions or job functions included on the team (Facilities Manager, HR Director, etc.)
- Team leader and contact information
- Team mission statement or set of objectives
- Scope of responsibilities (define what *is* and *is not* part of this team's mission)
- Delineation of responsibilities in each phase of BC/DR (i.e., when will the team be activated and deactivated?)
- Escalation path and criteria
- Other data, as needed

Crisis Management Team

In most companies, the composition of crisis management team will mirror the organizational chart. It should have representatives from across the organization and should bring together members of the company who have the expertise and authority to deal with the after-effects of a major business disruption. The crisis management team (CMT) will decide upon the immediate course of action in most cases and when necessary, they can contact senior management. They will direct the distribution and use of resources (including personnel) and will monitor the effectiveness of recovery activities. They can adjust the course of action, as needed. They should be in charge of activating, implementing, managing, and monitoring the business continuity and disaster recovery plan and should delegate tasks as appropriate.

Management

Each company has a management team or structure that oversees the business and its operations. You'll need to determine which positions from your management team should be included in your plan. Remember to review all the phases. For example, you might decide that only a member of the management team can cause the BC/DR plan to be activated.

Management might be required to decide when to transition from disaster recovery to business continuity activities or they might be the one(s) to decide how and when the BC/DR plan should be tested. Identify the positions that should participate as well as define how they should participate in each phase.

Damage Assessment Team

A damage assessment team should be comprised of people from several key areas of the company, including Facilities, IT, HR, and Operations. Your company's damage assessment team may contain other members, depending on how the company is structured and what type of business you're in. If you work in a small software development firm, you may just need the CEO, the IT manager, and the office manager to operate as the damage assessment team. In larger companies with multiple locations, you'll need to have several damage assessment teams or you may choose to create a mobile team that can fly to any site and assess damage within 24 hours of an incident. You may choose to have both a local and a mobile corporate team so that the right team can be called in. If the building floods, you may not need the mobile team to come in. However, if you have a large fire, earthquake, or other major event, you may need the support services of a mobile damage assessment team.

Operations Assessment Team

You may choose to have a separate operations assessment team comprised of individuals who can assess the immediate impact on operations. A damage assessment team may be tasked with this job, but in some types of companies, you may need a separate operations team that can assess what's going on with operations and how to proceed. The operations assessment team can also be tasked with beginning recovery phase activities, monitoring and triggering the transition from activation to recovery, recovery to business continuity, and BC to normal operations.

IT Team

Clearly, you need an IT team that can not only assess the damage to systems, but can begin the disaster recovery and business continuity tasks once the plan is activated. This IT team will work closely with the damage assessment team and/or the operations assessment team to determine the nature and extent of damage, especially to IT systems and the IT infrastructure. You may not need some of the technical specialties listed here, but this should be a good starter list for you to work from to determine exactly what expertise you'll need on your team.

- Operating system administration
- Systems software

- Server recovery (client server, Web server, application server, etc.)
- LAN/WAN recovery
- Database recovery
- Network operations recovery
- Application recovery
- Telecommunications
- Hardware salvage
- Alternate site recovery coordination
- Original site restoration/salvage coordination
- Test Team

Administrative Support Team

During a business disruption, there are a wide variety of administrative tasks that must be handled. Creating an administrative support team that can respond to the unique needs of the situation as well as provide administrative support for the company during the disruptions is important. This might include ordering emergency supplies, working with vendors arranging deliveries, tracking shipments, fielding phone calls from the media or investors, organizing paper documents used for stopgap measures, and more.

Transportation and Relocation Team

Depending on the specifics of your BC/DR plan and the type of company you work in, you may need to make transportation arrangements for critical business documents, records, or equipment. You may need to move equipment in advance of an event (like a hurricane or flood) or you may need to move equipment after the event to prevent further damage or vandalism. Relocating the company and its assets before or after a disruption requires a concerted effort by people who understand the company, its relocation needs, and transportation constraints.

Media Relations Team

You may recall that in Chapter 1, we mentioned the need to create a crisis communication plan because you will need to provide information about the business disruption/disaster to employees, vendors, the community, the media, and investors. One key area that should be well-prepped is media relations. Unlike other stakeholders mentioned, the media makes its living selling interesting stories. Since a disruption at your business may qualify as news, you might as well craft the message rather than leaving it to outsiders. Creating a team that

knows how to handle the media in a positive manner and that understands the policies and procedures related to talking with the media is vital to help ensure your company's image and reputation are maintained to the greatest extent possible. Certainly, if your company is at fault, you will have to deal with a different set of questions than if your company experiences a natural disaster. Still, you'll need to manage the story either way.

Human Resources Team

The aftermath of a crisis is an incredibly stressful time for all employees. Having an HR team in place to begin handling employee issues is crucial to the well-being of the employees and the long-term health of the company. Retaining key employees, adequately addressing employee concerns, facilitating insurance and medical coverage, and addressing pay and payroll issues are part of this team's mission. This team may also be responsible for activating parts of the BC/DR team as it relates to hiring contract labor, temporary workers, or staff at alternate locations.

Legal Affairs Team

Whether your legal experts are internal or external to your company, you should identify who needs to address legal concerns in the aftermath of a business disruption or emergency. If you hire outside counsel to assist you with legal matters, you should still assign an internal resource as the liaison so that legal matters will be properly routed through the company. If you operate in a heavily regulated industry such as banking, finance, or health care, you should be well aware of the constraints you face, but having a legal affairs team can assist in making decisions that keep your company's operations within the bounds of laws and regulations. Even if you're not in a heavily regulated industry, you may need advice and assistance in understanding laws and regulations in your recovery efforts.

Physical/Personnel Security Team

In the aftermath of a serious business disruption, you will need a team of people who address the physical safety of people and the building. These might be designated Human Resource representatives, people from your facilities group, or both. If you work in a large company or in a large facility, you may have a separate security department or function that manages the physical and personnel security for the building. If this is the case, designated members of their team should be assigned to be part of the BC/DR team. If you don't have a formal security staff, be sure that the members of this ad hoc team receive training. Someone from HR or facilities might be willing to take on the role of security in the aftermath of a disaster, but they need to be trained as to the safest, most effective method of managing the situation. Training for part-time or ad hoc security teams is crucial because if a natural disaster strikes, emergency personnel such as your fire or police department will focus on helping schools, day care centers, nursing homes, and hospitals first. Your company

may fall very low on the list of priorities, so having trained staff that can fill the gap in an emergency may literally mean the difference between life and death. We'll discuss training later in the book, but keep this in mind as you develop your teams.

Procurement Team (Equipment and Supplies)

Every company has some process in place for procuring equipment and supplies. In small companies, this might fall to the office manager or operations manager. In larger companies, there's usually a purchasing department that handles this function. Regardless of how your company is organized, you need to determine, in advance, how equipment and supplies will be purchased, tracked, and managed after a localized disaster such as a fire or in the aftermath of a widespread disaster such as a hurricane or earthquake. This includes who has the authority to make purchases and from whom, what dollar limit the authority carries, and how that person (or persons) can get authority to make larger purchases. For example, a company might specify that three people have the authority to purchase equipment and supplies up to $2,000 per order and up to $20,000 total. Beyond that, they have to have the president or vice president sign off on purchases. This predetermined purchasing information can also be communicated to key vendors so they know the three people who are authorized and what the authorization limits are. In this way, if disaster strikes, the company can turn to trusted vendors who, in turn, know the rules. This can expedite the recovery process.

Keep in mind that this team needs to be large enough that there is no "single point of failure." If you authorize only one person and something happens to that one person, you'll be scrambling to obtain emergency authorization for other individuals. Instead, authorize enough people to provide flexibility but not so many as to create chaos. Also, be sure your limits are appropriate to the type of business you run. If you may need to replace computers at $1500 a piece, make sure the limits reflect that. If a purchaser has a $1,000 limit per item, that will preclude him or her from making a simple purchase needed to get the company running again.

General Team Guidelines

Though we recommend populating teams first with needed skills based on *roles* and *positions* within the company, we also recognize that ultimately *people* are assigned to the team. People should be chosen to be on teams based on their skills, knowledge, and expertise, not because someone wants to be on a team or because someone's boss placed them on a team. In a perfect world, you could choose team members solely on competence, but we all know that in the real world, that's not always the case. Occasionally, you get the people who have the most time on their hands, who sometimes are the junior members of the team, or the least competent people in the department. You have to work within your organization's constraints and culture, but also strive to populate your teams with the right people with the right skills. Ideally, these are the same people who perform these functions under normal

conditions. It doesn't make sense to have the database administrator take on media relations duties during an emergency, just as you don't want the marketing VP managing the restoration of the CRM database, if possible. Certainly, in small companies many people are called upon to perform a variety of tasks and if that's the case, the same will be true if the BC/DR plan has to be activated. The teams also should be large enough that if one or more members of the team are unable to perform their duties, the team can still function. If you have other personnel or other parts of the organization that can wholly take up the BC/DR activities, so much the better. If not, you may also choose to designate key contractors or vendors to assist as alternates in the event of a catastrophic event. These personnel should be coordinated and trained as alternates along with internal staff.

Looking Ahead...

Specialty Vendors Help BC/DR Plans

There are numerous specialty vendors that can provide tremendous assistance to your firm in the event of a business disruption such as a fire or chemical spill. Although the numbers and types of firms in your area will vary, you should consider your specific needs in advance of any disruption and search for a firm that will meet your needs, even if that firm is located across the country. These firms provide a wide and unusual assortment of services, some of which are listed here:

- Chemical oxidation
- CO2 blasting
- Condensation drying
- Contact cleaning
- Corrosion removal
- Damp blasting
- Degreasing
- Deodorizing
- Fogging for odor removal or disinfection
- Manual hand wiping
- High pressure and ultra-high pressure jetting
- High temperature steam jetting
- Hot air drying
- Low pressure jetting
- Microwave drying

Continued

- Ozone technology
- Sanitation
- Steam blasting
- Vacuum drying
- Water displacement

As you can see, this is quite a list and it's not exhaustive. Be sure to think through the various scenarios that apply to your firm and determine which specialty services might best be outsourced to a qualified third party. You'll save yourself time and money in the long run and you'll likely get up and running much more quickly with targeted, competent help than if you try to do everything on your own.

BC/DR Contact Information

After you've developed the requirements for your teams in terms of the specific skills, knowledge, and expertise needed, you'll identify the specific people to fill those roles. Part of plan maintenance, discussed later in this book, involves ensuring that the key positions are still in the BC/DR loop and that key personnel are still aware of their BC/DR responsibilities.

Another mundane but crucial task in your planning work is to compile key contact information. Since computer systems often are impacted by various types of business disruptions—from network security breaches to floods and fires—you'll need to have contact information stored and available in electronic and hard copy. It should be readily available at alternate locations and copies should be stored in off-site locations that can be accessed if the building is not accessible. However, since this list contains contact information, it should also be treated as confidential or sensitive information and should be handled and secured as such. This information should include contact information for key personnel from the executives of the company (who will need to be notified of a business disruption) to BC/DR team members to key suppliers, contractors, and customers, among others.

Develop a list of the types of contact information you need, including:

- Management
- Key operations staff
- BC/DR team members
- Key suppliers, vendors, contractors (especially those with whom you have BC/DR contracts)
- Key customers
- Emergency numbers (fire, police, etc.)

- Media representatives or PR firm (if appropriate)
- Other

After you've identified the contact information you want to include, you'll need to determine where and how this information currently is maintained. In most companies, this information is stored in a multitude of locations and is not easily compiled with a few clicks of the mouse. You may need to develop a process for maintaining an up-to-date list, both electronically and on paper, of these key contacts. For example, many of your key contacts may be in a contact management application made available to everyone in the company. However, information such as executives' cell phone numbers and home phone numbers may not be included in this companywide contact database, for obvious reasons (especially if you work in a medium to large company). Therefore, you'll need to have a copy of the contact information plus information not included there. Developing a process for gathering and maintaining that data is an important part of BC/DR readiness. If a serious business disruption occurs in the middle of the night—for example, the building catches on fire—who will you contact? How will you know who to contact? Where will you find the key phone numbers you need if you can't get back into the building and you can't access computer systems? Since notification is one of the first steps in activating your BC/DR plan, you'll need to have key phone numbers available (*you* meaning the person(s) responsible for activating the plan). Develop a process for this during your BC/DR planning project and make sure that your maintenance plan includes regularly updating this information.

In addition to developing and maintaining a contact list, you should also define a contact tree. This defines who is responsible for contacting other teams, members of the company, or the management team. That way, each team member is tasked with specific calls to specific people and the notification process is streamlined.

Common Challenges

Maintaining Up-to-Date Contacts

Maintaining up-to-date contact information can be a challenge, especially since that information seems to change so frequently. If you work in a small company, you may task your office manager or other administrative support staff with maintaining this list and preparing an updated list once per month or once per quarter, storing it in designated locations and distributing it to key personnel. In larger companies, this task becomes a bit more difficult as contact information typically becomes fragmented—the contacts needed by the marketing group are not the same contacts needed by the IT group. Therefore, you may choose to have departmental responsibility for maintaining key contacts relevant to that business function. If you choose

Continued

that route, be sure you still have someone with high-level BC/DR responsibility who oversees the maintenance of BC/DR contact information, which in this example would include the departmental representatives who have the contact information for their units. The master BC/DR contact list should be maintained by someone on the BC/DR team and should include, at minimum, contact information for key executives, department heads, regional managers (other locations), and key BC/DR vendors, contractors, and suppliers. Regardless of the method you choose for managing your contact information, be sure that it includes a process for regularly updating it. Also update the contact tree once the contact list is revised.

Defining Tasks, Assigning Resources

The tasks and resources that need to be assigned have to do both with implementing the mitigation strategies you've defined as well as fleshing out the rest of the plan. First, you have to ensure your risk mitigation strategies will be properly implemented. This may mean creating project plans to address any new initiatives you need to undertake in order to meet your risk mitigation requirements. We'll assume you've got that covered as part of your risk mitigation strategy. If not, now's the time to develop your work breakdown structure, tasks, resources, and timelines for completing any risk mitigation strategies that need to be completed in advance of a disruption. This might include purchasing and installing new uninterruptible power supplies for key servers, updating your fire suppression systems, or implementing a data vaulting solution. Other mitigation strategies such as arranging for an alternate site need to be completed in advance, but activating it requires a different set of tasks that occur later. Finally, strategies that include accepting risk mean there probably are no additional tasks at this time.

Other tasks have to do with defining your BC/DR teams, roles, and responsibilities; defining plan phase transition triggers; and gathering additional data. Let's start with tasks related to some major activities including alternate sites and contracting for outside BC/DR services. Clearly, there are other tasks and resources you'll need, but this should get you started in developing your own list of tasks, budgets, timelines, dependencies, and constraints for the remaining BC/DR activities in your plan.

As you develop these tasks, keep in mind standard project management processes:

1. Identify high-level tasks, use verb/noun format when possible (i.e., "test security settings" rather than "security settings").
2. Break large tasks into smaller tasks until the work unit is manageable.
3. Define duration or deadlines.
4. Identify milestones.
5. Assign task owners.

6. Define task resources and other task requirements.
7. Identify technical and functional requirements for task, if any.
8. Define completion criteria for each task.
9. Identify internal and external dependencies.

We're not going to go through all that detail for these next two high-level tasks, but you should include this level of detail in your plan.

Alternate Site

Although this should be part of your BC/DR plan, it's worth calling it out separately due to its importance and the need for advance work. If part of your risk mitigation strategy is to develop an alternative site or off-site storage solution, you should develop a number of details before moving forward. These should be tasks (or subtasks) within the WBS just discussed, so let's look at some of the details you might include. Also keep in mind that you need to develop a trigger that helps you determine if or when you fire up the alternate site. You probably don't want to activate the alternate site if you have a minor or even an intermediate disruption, so how do you define when you should? When all systems are down or when some percentage of systems down? You have to take your MTD into consideration along with other factors such as the cost of firing up the alternate site and the cost of downtime. If your downtime is estimated to be 12 days and that cost is $500,000 but the cost of firing up the alternate site is three days and $250,000, is it worth it to activate the alternate or should you just hobble along until you can restore systems at the current location? There's no right or wrong answer, it's going to depend on your company's MTD, potential revenue losses, cost of starting up the alternate site, and so on. Have the financial folks on your BC/DR team prepare some analyses to determine metrics you can use to help determine your trigger point. As you're going through the activities listed in this section, keep these factors in mind.

Selection Criteria

Selection criteria are the factors you develop to help you determine how to select the best alternate site solution for your company. This includes cost, technical and functional requirements, timelines, quality, availability, location, and more. Be sure to consider connectivity and communications requirements in this section along with your recovery requirements such as maximum tolerable downtime.

Contractual Terms

Determine what contractual arrangements are appropriate for your company. Many vendors have predetermined service offerings and contracts are fairly standard. Other companies can

accommodate a wider range of options and will work with you to develop appropriate contractual language. In either case, be sure to run these contracts past your financial staff and your legal counsel to make sure you are fully aware of the financial and legal consequences of these contracts in advance of signing them. If you're not clear what they mean operationally, be sure to talk with the vendor and add clarifying language to the contract. Do not simply take the vendor's word that a particular paragraph or section mean something. Verbal agreements are always superseded by written contracts, so make sure the contract spells it out clearly. You don't want to rely on verbal commitments made by employees no longer with the company when it comes to implementing your BC/DR solutions, so be sure to put everything in writing in advance.

Comparison Process

Be sure to specify what process you'll use to select the vendor. This might include a list of technical requirements the vendor must meet, but it might also include an assessment of the vendor's geographical location, financial history, and stability and industry expertise, among other things. Selecting the right vendor for an alternate site or off-site storage is a very important aspect to your BC/DR success and should be undertaken with the same rigor as your other planning activities.

Acquisition and Testing

Once you've selected your alternate site or off-site storage vendor and completed the contract, you will need to make whatever additional arrangements are needed for developing this solution so that it is fully ready in the timeframe you've designated. This might include purchasing additional hardware and software, setting up communications channels, and testing all solutions implemented. Create a thorough acquisition and testing plan for this phase so you can transition to it as seamlessly as possible in the event of a business disruption. During your testing phase of the BC/DR plan (see Chapter 8), you should test the process for firing up this solution on a periodic basis.

Contracts for BC/DR Services

Although we highly recommend you involve your purchasing, finance, and/or legal professionals in executing your BC/DR contracts, you should also have a general understanding of some of the elements to consider. As with alternate site considerations, keep your MTD, your costs, and potential losses in mind. Have your financial folks help you with performing financial analyses to determine what makes financial and business sense for your company. If a firm wants to charge you $50,000 for some sort of contract but your downtime estimate with associated revenue and collateral loss is only $40,000, the contract might not be worth entering. Additionally, determine your triggers for calling upon these contractual arrange-

ments so you don't prematurely fire up these contracts or avoid using them during times when they should be activated.

Develop Clear Functional and Technical Requirements

You know from project management fundamentals that developing functional and technical requirements is often what defines the difference between success and failure. The same is true here. If you have not clearly and fully defined your functional and technical requirements, you'll get all kinds of vendor responses. The more specific you are, the more fully a vendor can address your needs. In addition, if you leave too many elements open to discussion, you'll endlessly discuss possibilities without being able to identify appropriate solutions. Have these discussions in advance, and then come to a firm agreement about the requirements. If some requirements appear to be optional or "nice to have," then list them as options and not as requirements. Pare down your requirements to the elements you absolutely must have. Remember, the more options you include, the higher the cost is likely to be. Therefore, if cost is an issue (and it almost always is an issue), be sure to list what you require and what you desire as separate items. When this information has been finalized, write up formal requirements documents that you can provide to potential vendors. Also, be sure that your requirements documents are reviewed by subject matter experts, including IT experts and those in your company who understand regulatory, legal, and compliance issues. Your requirements should meet all these needs before going out to the vendors.

Determine Required Service Levels

Service levels are typically part of technical requirements, but we've listed them separately because they are vitally important when developing Requests for Proposal (RFP) or Requests for Quote (RFQ) from vendors. You may have contractual obligations to provide certain levels of service to your customers, so you may need to specify requirements for your vendors that meet or exceed these metrics. Even if you have no externally facing service level agreements (SLA), you should still specify SLAs in your contracts with vendors. If you're contracting for Internet connectivity, you should specify bandwidth, minimum upload and download speeds, and maximum downtime per specified period, for example. These may sound like technical requirements, but let's look at how this can play out in a contract. You write up your requirements, which include bandwidth, minimum upload/download speeds, and maximum downtime. Three vendors respond to your RFQ to provide backup Internet connectivity to your company in the event of an outage from your main vendor or in the event that your company's facilities are damaged. All three companies give you quotes that indicate they can meet or exceed those three requirements (bandwidth, speed, availability). However, those are not contractual terms, those are the company saying they *can* meet or exceed those metrics. If it's not in the contract, it's just a statement of capabilities, not a commitment. A service level agreement will specify minimum bandwidth availability during

a 24-hour period, 7 days a week. It would state that you will have access to [insert bandwidth metric] 24 hours a day, seven days a week until [insert termination metric or trigger]. This way, the vendor can't provide you the bandwidth you requested only from 11 P.M. to 6 A.M. on Saturdays and Sundays and short you the rest of the time. Granted, most vendors are on the level and want to provide the services to you they've agreed upon, but that's why contracts exist—to clearly define who does what, when, and at what cost. This keeps the guess work (and the finger pointing) to a minimum.

Compare Vendor Proposal/Response to Requirements

Once you receive vendor responses to your proposals, you should evaluate how closely each vendor comes to meeting the requirements of your plan. Any vendor that does not meet the requirements should not be considered further. There may be two exceptions to this. First, if your requirements are unique enough that no single vendor can meet your needs, you may have to circle back and find two or more vendors who can work together to meet your unique requirements. Second, you may discover from vendor responses that your requirements were too broad, inclusive, or vague, and that none of the vendors' responses meet your requirements exactly. In that case you may have to refine your requirements and go back out for bid. Assuming your requirements are well written, your next step is to eliminate vendors that cannot meet your needs and focus only on those vendors who addressed your requirements fully in their responses.

Identify Requirements Not Met by Vendor Proposal

If there are one or more requirements not met by any vendor, you may need to find two or more vendors to work together to provide the full range of services you need. If none of the vendors met a particular requirement, you may also choose to review that requirement and reassess it in light of vendor responses. Remember, you contract with vendors in order to leverage their specific expertise. If none of them meet a particular requirement, you may wish to talk with several of your short-list selections to find out why they did not address that aspect. It might be redundant or otherwise unneeded. In that case, you should revise your requirements to reflect this new information.

Identify Vendor Options Not Specified in Requirements

Vendors also may offer additional options not specified in your requirements. Again, based on the vendor's expertise, they may offer additional choices that can round out your requirements or plan. Utilizing their expertise can be a good way of ensuring you have the best solution in place. For example, the vendor might say (in essence), "Everyone who's asked for A, B, and C also has found that D was an extremely important option they'd overlooked. Perhaps you'd like to add D to your plan as well." They may be sharing industry expertise and best practices with you, or they may simply be trying to up-sell you. You'll have to look

carefully at these options and perhaps do some independent research to determine whether these options are "must have," "nice to have," or "useless add-ons." If you have an established relationship with these vendors, they'll more than likely offer you additional options but won't put pressure on you to upgrade unless they feel it's vital to your success. However, we all know there are sales people that will try to sell you every option they can think of just to make a bigger sale, so you have to be an active participant in the transaction. Know your options, know what makes sense, do some additional research, and determine if any of the additional options would enhance your plan or fill in gaps you didn't realize existed. Don't be forced into upgrades and options you don't really need just because you have a very persuasive sales person in front of you.

From the Trenches…

Managing the Sales Process

Sometimes your purchasing department manages the purchase of goods and services, but when you're talking about the purchase of backup, storage, or alternate site services for your BC/DR plan, there's a good chance you will be directly involved. If you haven't been involved with the sales process in the past, you might find yourself being swayed by excellent sales people—the ones who can convince you that you need something you really don't. Most sales people are honest and are trying to balance their need to sell with your need for the product or service they're selling. They also realize that loyal customers are borne out of an honest sales experience, not out of strong-arming someone into purchasing more than they need. In order to be successful in the process, take time to be clear about *your* objectives *before* a sales meeting. If you intend on making a purchasing decision at that time, write down the terms or parameters you will accept. Keep these to yourself but know that this is your bottom line. If the sales person cannot or will not meet your bottom line objectives, there is no deal to be struck.

The same holds true in any negotiation—know what your bottom line is and work toward meeting (or exceeding) that bottom line. If you have developed clear requirements and you know your bottom line, you should be able to successfully navigate the sometimes tricky sales process. Negotiation skills can help you in all aspects of life and they'll certainly help you in the business world. If you're interested in learning more about the art of negotiation, there are thousands of helpful books, courses, and seminars you can turn to for more information.

Communications Plans

Earlier in this book, we discussed the need for various communications plans. In this section, we'll define various communications plans you should develop and identify some of the common elements in such a plan. If you already have communications plans in place, you can use this section as a checkpoint to ensure you've got all your bases covered. For each plan, you should define specific steps just as you would for any other process in your BC/DR plan. You should define the following:

- Name of communication team, members of team, team lead, or chain of command
- Responsibilities and deliverables for this team
- The boundaries of responsibilities (what they *should* and *should not* do)
- Timing and coordination of communication messages (dependencies, triggers)
- Escalation path
- Other information, as appropriate

Communications plans can be assigned to other, existing teams. A good example of this is that the employee communication plan may be the responsibility of the HR team. There's no need to create additional teams to execute communications plans if these activities fall within the scope of defined teams. However, in some companies, it might make sense to have most of the communications come from one dedicated communications team in order to maintain control over communications and to ensure that a single, consistent message is delivered to all stakeholders. The decision is yours and usually is based on how large the company is and how it currently operates.

Internal

The internal communication plan is really part of the BC/DR activation and implementation plan. If a business disruption occurs, you need to have a process in place for notifying BC/DR team members. This is done as part of BC/DR plan activation and is a critical aspect that should be clearly delineated. How will team members be notified and updated? What processes, tools, and technology are needed? Are these included in your plan yet? If not, add them to your WBS or in a section called Additional Resources so they are captured and addressed in advance of a business disruption.

Employee

Employee communication is also internal communication but differs because it is any communication that goes out to employees who are not part of the BC/DR implementation. If a business disruption occurs, you'll need to know how to notify all employees. You'll also

need to let them know answers to the most basic questions including what happened, what is being done to address the problem, and who they should go to for more information. For example, if the building burns down overnight, employees may show up for work in the morning as scheduled. The BC/DR team may already be in action but the general employee population needs information. How this information is communicated and by whom should be identified. It often makes sense to develop an information tree so that key communicators know to whom they should go for updates and official information. For example, in a small company, you may designate the HR manager as the person who will communicate with employees on all BC/DR matters. The HR manager should know who to go to for information on the status of the BC/DR activities. This might be the Facilities manager or the BC/DR team leaders (who should be identified in the activation plans, discussed earlier in this chapter).

Customers and Vendors

Customers and vendors typically require different types of communications but the information is often similar. They may need to be notified of the business disruption, the basic steps being take to rectify the problem, the estimated time to recovery and any work-arounds needed in the meantime. If you are developing crisis communications plans for the first time, be sure to read the case study that follows this chapter, entitled "Crisis Communications 101," for more information on how to communicate in a crisis.

Shareholders

If you have shareholders of any kind (debt or equity investors, shareholders, etc.) you must communicate the nature and extent of the disruption. In most cases, they are concerned with the ongoing viability of the company and possibly the short-term financial impact of the disruption on the company. Therefore, communication with this group requires that specific issues be addressed. As you can tell, these issues are very different than, say, employee issues, so someone well-versed in investor relations should be charged with this communication. In most companies, this task falls to the CEO or a high-ranking corporate officer who can specifically address the concerns of those who have a financial stake in the company.

The Community and the Public

In addition to communicating with all the other stakeholders we've mentioned, you also will need to communicate with the general public. Local newspapers, TV, and radio stations will certainly take an interest in a localized business disaster such as a fire or flood. National and international media may also take interest if the event is unique in some way or is part of a widespread disaster. Members of the local community may also have more than just vicarious interest—they may need to understand the impact your business disruption may have on them. Businesses in communities don't exist in isolation, and what happens to one busi-

ness may have a ripple effect on other businesses even if those other businesses are not customers or suppliers.

Communicating with the media is a tricky proposition and many executives at large firms go through extensive media training sessions in order to learn how to deal with the media. Although an extensive discussion of this topic is outside the scope of this book, you will learn the basics by reading the case study that follows this chapter. Additional media relations training resources are readily available online and there are hundreds of excellent books on the topic as well. As the leader of the BC/DR project plan, you may or may not be called upon to communicate with the media, but being prepared is always a good idea.

This plan should be well thought-out and you may wish to seek legal counsel with regard to what must be disclosed, to whom, and in what time frame. As you learned in the case study presented earlier in this book ("Legal Obligations Regarding Data Security" by Deanna Conn), there are numerous legal requirements regarding notification and remediation that must be met in certain circumstances. To ensure you comply with regulations and laws in your industry, be sure to seek appropriate input from subject matter experts as you craft your shareholder communication plan.

TIP

Many public relations firms specialize in crisis communications. You can work with this type of firm in advance to develop appropriate communications plans. You can also contract with these kinds of firms to assist with communications in the aftermath of a major event. In most cases, they can advise you on the best course of action, potential communications pitfalls, and provide guidance regarding certain legal issues. You may also need to get a legal opinion in certain matters, especially if death or injury occurred on your company's premises or as a result of company action. The PR firm you work with can help you understand how to communicate effectively and when to seek additional input before, during, and after your business disruption.

Event Logs, Change Control, and Appendices

In traditional IT, event logs track a variety of system and network activities. In a broader sense, you may choose to create a BC/DR event log for tracking various events and milestones. For example, your decision to activate your BC/DR plan may be based on two or three event types occurring, either simultaneously, in quick succession, or within a specified time period. These events may trigger the activation of the BC/DR plan itself, or they may signal the point in time when it's appropriate to move to the next stage in your plan. Having

a chronological log of events can help clarify circumstances so appropriate decisions can be made in a timely manner.

Event Logs

As an IT professional, you're probably well versed in reviewing event logs as they pertain to systems and security events. However, in BC/DR, event logs are not necessarily logged by a computer system. In many cases, event logs are hard copies developed sequentially over time by making notes on what happens when. Event logs help you track events, in order, over time, and can help in identifying appropriate triggers for key activities.

Keep in mind that these logs establish who knew what and when, so they may become legal documents at some point in the future. You have to balance the need for timely information with the potential for litigation. As unfortunate as it may be, sometimes too much documentation leaves the company open to lawsuits, even when the company has acted as best it could given the circumstances. We don't suggest you do anything illegal or unethical—quite the opposite—but you may want to talk with your legal counsel to understand what can and cannot become evidence in the event there is a lawsuit that stems from some sort of business disruption. If something can become a legal document or be used as evidence in some manner, you should be aware of that going in. Your legal counsel may have recommendations about how to record data to minimize the possibility of litigation while maintaining accurate, useful logs.

In the absence of specific legal advice on how to develop logs, the best general advice is to record only the relevant information and stick to the actual facts, not conjecture. Instead of "Barnett seemed confused by the request to review the equipment," you might simply say, "Barnett was contacted regarding reviewing the equipment at 11 P.M., 2/22/07" or "Barnett had numerous questions regarding the request to review equipment. Issue escalated to Barnett's boss, Martina." All these statements are true but the first statement contains conjecture—was Barnett confused or did you just assume he was because of the look on his face? If you state in your log that Barnett was confused, this might be the basis of a lawsuit claiming that appropriate action was not taken in a timely manner. Stating only the facts keeps everything moving forward and does not unnecessarily open the door to legal problems down the road.

On the other side of the legal coin, there may be legal or regulatory requirements to log certain events or make notifications within a certain timeline. Event logs can help you operate within these legal requirements as well. If you operate under these constraints, be sure to include these requirements in your BC/DR plan, perhaps with hard copy templates of the event logs, so that your team knows clearly what the logging or notification requirements are in the stressful aftermath of a business disruption.

Change Control

Change control is a necessary element in any project and BC/DR planning is no exception. There are two types of change control you'll need to develop. First, you need to devise a method of updating your BC/DR plan when change occurs in the organization that impacts your plan. Second, you need a method of monitoring changes to the BC/DR plan to ensure they don't inject additional uncertainty or risk into your plan. Let's look at both of these scenarios briefly.

As companies grow and expand, numerous changes occur to the organization's infrastructure. This can include departmental reorganization, the creation of new departments, the expansion to additional facilities, and more. It also comes with changes to the IT infrastructure including the location and duties of servers, the implementation of new applications and technologies, and the reorganization of existing infrastructure components. All these kinds of changes impact the existing BC/DR plan. These elements should be addressed in the plan maintenance activities, which we'll discuss in Chapter 9. You can't control the change that occurs in the organization, but you can put in place a system for assessing change and how it impacts your BC/DR plan. In most cases, this occurs during the periodic review of the plan and we'll remind you of that in Chapter 9.

A subset of change control is version control. Be sure to include a process for managing revision history for your BC/DR plan. Many people choose to simply put a small table at the beginning of the document outlining the changes in chronological order. Table 6.1 shows an example of a revision history table that might be used in your BC/DR plan.

Table 6.1 Revision History Table

Revision Number	Revision Date	Detail
1.0	02.22.07	Finalize first version of BC/DR plan
1.1	03.20.07	Modify network diagrams in Section 4.2
2.0	06.05.07	Revise plan to include acquisition of ABC Co.
2.1	11.05.07	Include new specifications and contract for alternate site.

You can define what constitutes a major and minor revision. Typically, going from 1.0 or 1.1 to 2.0 is considered a major revision (when the number to the left of the decimal point increases); going from 1.0 to 1.1 or 2.11 to 2.2 is considered a minor revision (when the number(s) to the right of the decimal point increase). Clearly, the numbering scheme is not quite as important as keeping track of revisions, unless you work in a company that has a very formal system for revision control in place. A quick note in the Detail section can help clue you in to the changes in the revision. Some people also like to document more extensive information about the changes and this can be done in the beginning of the document.

For example, you could create paragraphs labeled, "Changes in Revision 1.1," and note the key changes made to the document. This helps you see at a glance how the plan has changed without reading the entire document. There are numerous systems for managing revisions and you should select one that is consistent with the way your company operates. Don't make it into a huge production or it may be circumvented, but do use some system for tracking changes so you don't have to compare two documents side by side to figure out what changed between revisions.

Distribution

Although the plan is not yet complete, you should devise a strategy here for distributing and storing the final BC/DR plan. The revision history will help you and the team with version control, but you will still need a method of distributing the latest revision or notifying the team that a new version exists. In some cases, the plan may be stored in a software program that performs version control and revision notification. In that case, you're pretty well set other than adding team members to the notification list. If you're not using such a program, you can still maintain the plan on a shared, secured network location and provide team members or team leads with access to the folder. Keep in mind that this document is a very sensitive document and all precautions should be taken to ensure it does not fall into the wrong hands, is not leaked to competitors or to the media, or otherwise compromised. Use standard security and encryption where this document is concerned. Distribute the document in soft copy via e-mail only as needed. If possible, simply e-mail a notification that a new version is available while maintaining the document in the secure location. Remind people that the document is sensitive and should not be copied, distributed, or otherwise handed out. The document should only be distributed to those who have a defined need to know.

Finally, be sure you create a process or method for *printing* the updated plan so you have a hard copy version available if systems go down. The BC/DR team lead or leads should all have a paper copy in a secure location, both on-site and off-site. When new versions are available, old versions should be shredded or destroyed in a secure manner.

Appendices

Any information relevant to your plan that does not belong in the body of the plan should be attached or referenced as an appendix. There are no strict rules about what should or should not be included in the appendices, but it's usually detail required for successful implementation of the plan that may pertain to only one group or subset of BC/DR teams. For example, you might include the technical specifications of mission critical servers in an appendix. As servers are moved, updated, or decommissioned, you can easily update the related appendix without modifying the plan itself.

Contracts with external vendors should be kept as appendix items so that they are located in one central place for reference. Your finance and/or legal departments may want to retain originals of these contracts, which is fine, but be sure to include copies in your BC/DR plan. If you have to activate your plan, you don't want to have to run around looking for someone from finance or legal to determine how and when you can activate your external contracts.

Templates for event logs, communications, and other predefined processes can be included. In event log templates, be sure to include time, date, event, notification requirements, legal, or compliance issues and other requirements so they're easily accessible in the event of a business disruption or disaster.

Key contact information should be included in the plan, but you may choose to include it as an appendix, especially if it changes frequently. If you choose to do this, you should include key contacts within the body of the plan and use the appendix for additional contact information, as appropriate. The reason for including the key contact information within the body of the plan is twofold. First, key contacts are integral to the successful activation and implementation of the plan. As such, that information should be incorporated into the body of the plan. Second, if that information changes, it should trigger a BC/DR plan revision. Key personnel need to be trained, they need to understand their roles individually and as part of the BC/DR team, and they need to be given the tools, resources, contacts, and information needed to do so successfully. If a key member of the BC/DR team leaves, for any reason, the person replacing them needs to be brought up to speed. This should trigger a quick review of the plan. If the successor has been assigned by virtue of position (the Facilities manager resigns and a replacement is hired), the replacement needs to be trained in all aspects of their duties with regard to the BC/DR plan. If the successor is not assigned and needs to be found, looking through the roles and responsibilities of this position can help you select the right person to fill the gap.

Any other information that is related to the plan that needs to be updated, maintained, and correlated to the BC/DR plan itself should be included as an appendix. Don't throw everything you can think of into an appendix and think you're covered. More is not necessarily better in this case, but do be sure to include key information you'd want to have quick access to in the event of a natural disaster or other significant business disruption. To give you a few ideas about what else might be attached to your plan in an appendix, we've provided the following list. Not all of these elements are needed by every company, but you can pick and choose based on your unique situation.

- Critical work space equipment and resource information and related vendor data
- Critical IT hardware, software, equipment and configuration information, and related vendor data
- Critical manufacturing, production and warehousing information and related vendor data

- Critical data and vital records information, including storage and retrieval information
- Alternate IT or work site information
- Crisis management center resources and information
- Insurance information including all relevant policies, policy numbers, and insurance contact information
- Service level agreements (that you must provide to customers or that vendors must provide to you)
- Standards, guidelines, policies, and procedures
- Contracts related to BC/DR
- Forms
- BC/DR Plan distribution list
- Glossary

Every company and every BC/DR plan is different, so there is no hard-and-fast rule about where information belongs, as long as critical data is included in a logical manner. If writing a plan or organizing data is not your strong suit, be sure to recruit assistance to draft a plan that makes sense. It should follow a logical progression and match the way your company does business to the greatest extent possible.

Additional Resources

What other resources do you need to successfully implement and maintain your plan? In the next chapter, we'll discuss emergency and business recovery plans, so some of this may come up in that context. However, if there are communication tools, equipment, or resources you think of as you develop your plan, they should be noted in a section called Additional Resources (or other similar heading) and they should be added to your WBS to ensure someone takes ownership of gathering these needed resources.

What's Next

When you complete the work in this chapter, you should have a fairly robust BC/DR plan in the works. It will have gaps related to specific emergency and disaster recovery efforts (see Chapter 7), and in training, testing, auditing, and maintaining the plan (see Chapters 8 and 9), but other than that it should be well on its way to completion. If not, step back and review your data, your plan, and your company to determine what is missing and how you can address those gaps.

Summary

Putting your business continuity and disaster recovery plan together requires pulling together the data previously developed and adding a bit more detail. Understanding the phases of the BC/DR plan helps you develop strategies for managing activities if you have to implement your plan. The typical phases are activation, disaster recovery, business continuity, and resumption of normal activities. The plan must also be tested and maintained, regardless of whether it's ever implemented.

Potential disruptions need to be categorized and we discussed three levels: major, intermediate, and minor. By clearly defining these for your organization, you can ensure you understand what recovery steps should be implemented. This will define how and when you activate your BC/DR plan. After the plan is activated, a trigger should define when disaster recovery tasks begin. These recovery tasks should be well defined in your BC/DR plan and we'll cover these in detail in the next chapter. The transition from disaster recovery to business continuity should also be well defined so that you can begin to resume business activities, though things will not be back to business as usual at this juncture. This is also discussed in detail in the next chapter.

Developing your BC/DR teams is a vital part of your planning. There are numerous roles and responsibilities in each phase of your BC/DR work and defining these and populating your teams in advance is crucial to your success if the plan is ever activated. In addition, these teams will need to be trained in implementing the BC/DR activities. Training is discussed in detail in Chapter 8.

After you've created your teams, you can further develop your planning tasks and assign resources, timelines, and budgets. You can identify task dependencies, develop milestones, and create completion criteria for key tasks. Since each company's set of tasks will vary widely, we presented only a sampling of high-level tasks related to acquiring an alternate computing site and contracting with vendors.

Communications plans are part of the BC/DR process because if a business disruption occurs, many different groups of people will need status updates and information. This includes employees, management, shareholders, vendors, customers, and the community, among others. You'll need to decide who needs to know what and when they'll need to know it. Then, you'll need to develop distribution methods appropriate to those groups (and to the circumstances of the disruption).

Event logs can help you manage the business disruption from start to finish, but remember that these may become legal documents later on. You may wish to consult with your legal counsel regarding what should and should not be included in the event logs. For example, it's generally considered fine to include facts but not conjecture or opinion. Sticking to the facts helps keep the log clear and concise and can avoid misinterpretation of data. In addition, there may be legal or regulatory requirements for event logging or notifi-

cation, so be sure to include this in your process and make a note of it in any log files you develop (whether soft or hard copy).

Keeping track of document revisions is a bit of a "housekeeping" task but an important one when it comes to your BC/DR plan. Use a simple, concise method of ensuring that the plan is updated and that everyone has the latest plan. Develop a method for distribution and storage of the plan so that it's accessible to key personnel in the event of a disruption. Finally, include additional data such as technical requirements, service level agreements, and vendor contracts as appendices to the main BC/DR plan. Keeping all relevant data with the plan can make plan implementation and maintenance much easier.

Solutions Fast Track

Phases of Business Continuity and Disaster Recovery

- ☑ The various phases of the BC/DR cycle include activation, disaster recovery, business continuity, maintenance/review. Plan maintenance and review occurs periodically, regardless of whether or not the plan has ever been activated.
- ☑ The activation phase occurs when a disaster or business disruption occurs and it is determined that the plan should be implemented. Clear directives on how and when to activate the plan should be included.
- ☑ The disaster recovery phase includes the tasks that must be undertaken to stop the impact of the event and to begin recovery efforts. This includes damage assessment, risk assessment, salvage operations, as well as the evaluation of appropriate alternatives and solutions.
- ☑ The business continuity phase entails the activities required to restore the company to business operations. This assumes disaster recovery has been completed and that the business is up and running in a limited mode. This is not yet business as usual, and may involve the use of temporary solutions and work-arounds.
- ☑ Maintenance and review are similar phases. Maintenance requires a review of the plan from time to time to ensure everything is still current and that changes to the company or its infrastructure are reflected in the plan.
- ☑ Review occurs after the plan has been activated and implemented. Gathering lessons learned and updating the plan with new information gleaned from the experience helps the organization avoid making the same mistake twice and helps the organization learn from the experience.

Defining BC/DR Teams and Key Personnel

- ☑ You should have already identified key personnel, positions, skills, and expertise needed for your BC/DR activities. In this phase, you should form your BC/DR teams based on those stated needs.
- ☑ There are many different types of teams you may need. In smaller companies, people may take on multiple roles. Be sure teams are large enough to accommodate the potential that one or more team members may be unavailable during or after a disaster (for a variety of reasons).
- ☑ Key personnel should also be identified at this time. This may include certain members of the executive or management team, people or vendors with specific skills needed, and the like.

Defining Tasks, Assigning Resources

- ☑ Tasks, owners, timelines, budgets, dependencies, and completion criteria are among the details that should be developed for BC/DR plan activities. Additional detail and checklists are provided in Chapter 7.
- ☑ All the tasks needed to activate, implement, manage, and monitor the BC/DR plan in action should be defined. You can create project plans for each subsection of work or develop detailed checklists.
- ☑ Be sure to note key internal and external dependencies for tasks. Milestones should be added to your project plan or as items on a checklist.
- ☑ Maximum downtime and other time-based objectives should be noted and addressed within the project plan or checklist.
- ☑ Contracts for alternate sites, equipment, and other products/services should be defined in the BC/DR plan as well. The finalized contracts can be added as appendices to the final BC/DR document. Include service level agreements, where applicable.
- ☑ Address MTD and other constraints along with legal or regulatory requirements that must be met in the aftermath of a disruption to ensure continued compliance.

Communications Plans

- ☑ There are many different kinds of communications needs during and after a major event, disruption, or disaster. You should develop plans for communicating with various stakeholders in these cases.

- ☑ Management and employees require communication regarding the current status of the business, where/when/how to report to work, who to contact for information, and so on. This often is handled by the HR team, who can be tasked with managing the employee communication plan.
- ☑ External communications are needed to contact key customers, vendors, suppliers, and contractors to notify them of the event and the company's next steps.
- ☑ Communications with local, national, and international media may be required. In these cases, it's best to have someone from the company who is trained in media relations handle these communications. PR firms often offer plan development, training, and guidance in the aftermath of an event.
- ☑ In some cases, the information communicated can become the basis of legal action in the future. Therefore, you should consult with your company's legal counsel or an expert in media relations to determine how, what, when, and where information should be communicated. This should be done before any emergency communication is needed.

Event Logs, Change Control

- ☑ Event logs, like emergency communication, can become the basis of legal action, so be sure to understand the requirements and constraints various kinds of emergency reporting may have on your company.
- ☑ Event logs help you keep track of what's going on, what's been done, and what needs to be done next. Keeping detailed logs in real time helps keep track of details that might later be lost.
- ☑ Your company may be required to meet certain legal or regulatory reporting requirements. Event logs can be helpful in ensuring you meet those requirements. Consult with legal counsel if necessary and include these requirements in soft or hard copies of your logs.
- ☑ Changes to the BC/DR plan should be tracked and noted so that team members can easily determine if they have the latest revision of the document as well as the general nature of those revisions. Be sure to develop a distribution system that notifies team members of new revisions, provides a method for accessing new documents, and reminds teams to print and store the documents in locations accessible both on- and off-site.
- ☑ BC/DR plans should be treated as confidential documents. They should be handled and stored in a secure manner and old copies should be destroyed appropriately.

Appendices

- ☑ Information that should not be included in the body of the plan but that is nonetheless vital to the plan should be included at the end as an appendix.
- ☑ Appendix data can include event log or other document templates, vendor contracts, technical specifications, service level agreements, customer contacts, or any other relevant data that would be useful to have along with the BC/DR plan if/when it's activated.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: Our IT department consists of three people and our company has one location with 50 employees. It seems all the information in this chapter is a bit of over kill. Any comments on that perspective?

A: Yes. There is a lot of information in this chapter and some of it may not apply to all companies, including small companies like yours. However, it's important that you review and consider all this information so that you can develop a comprehensive plan appropriate to your organization. When it's all said and done, you may not include the bulk of what's included here, but you will most likely feel confident you're not missing something major. Because each company is unique, there really is no one-size-fits-all solution. Instead, we have to raise as many potential points as we can and allow you to incorporate or exclude that data as you see fit. If you're in a small company, your plan may be very short. It might include plans for storing your backups off site, plans for buying or renting new computers after a disaster, and a contact list—if that's what you and your company feel is important. At the end of your planning process, you should have a plan that you're comfortable with—a plan that will enable you to recover from a minor or major business disruption in the time and at the cost you've designated.

Q: Our planning process has gotten bogged down in this very step. We managed to perform the various analyses, but now no one seems to have the time or energy to actually develop the plan—to actually define what we'll do, step by step. Any suggestions for how to move forward?

A: It can be difficult to maintain momentum, especially when the analysis activities take a fair amount of time and effort. Teams can lose participants or simply lose focus and

motivation. As the team leader for the project, you have several options. First, you should understand the current environment in your company. Are there competing pressures for time and resources? Are these impacting your project? If so, it might be time to check in with your project sponsor and get his or her assistance in reigniting the interest in this project. Second, you should look at the project as a whole. In some cases, the project begins looking so large and overwhelming at this juncture that people just sort of melt down. If this appears to be the case, you can find ways to break these steps down into smaller chunks of work so that people can see progress. For example, you can develop plans for what you would do in light of a minor disaster or event. This is usually a manageable task to consider and can provide a sense of accomplishment to the team.

Once these steps or procedures are defined, you can move on to intermediate and then major events. Building upon prior work can help teams feel they are making progress and make each subsequent task seem a bit less daunting. You can also spend time breaking the project down into smaller subprojects. For example, have the IT team work on their response to minor, intermediate, and major events. Have the communications team and the other subteams do the same. Then, you can convene meetings to have these teams sync up or coordinate their plans. You may have other tried-and-true methods you use to get a stalled project back on track, but understanding the underlying cause is the first step. In the case of BC/DR planning, the usual suspects are lack of continued corporate commitment or focus and the sense of unending, daunting or overwhelming work for the team. Addressing these underlying causes often gets the project moving forward again.

Q: Someone in the job before me created a BC/DR plan but it doesn't track at all with what you've presented so far. I'm not sure the best course of action at this point. Any suggestions?

A: Yes. The key is to ensure that the needed data is included in the plan. In reading through your old plan, even if it doesn't track at all with the way we've presented the material, you should be able to get a sense of whether or not the plan contains the necessary data. In essence, ask yourself if you had to use this plan if you would know how to recover from a major disaster. If the answer is no or maybe, then you don't have all the information you need and the plan is incomplete. You can decide to scrap it and start from scratch or you can try to fill in the holes while updating it with the most current information. Sometimes it's easier to start from scratch but you can make this determination. A detailed review of the plan to be sure it contains the necessary elements and the most current information will probably suffice. There is no single "right" way to develop your plan. The bottom line is this: Will your plan provide you enough guidance during the stressful aftermath of an emergency, disaster, or disruption to get the business up and running again? If the answer is yes, you're in good shape. If the answer is no, you need to perform a gap analysis on your plan and find out what's missing and how to address those gaps.