10

Disaster Recovery

In previous chapters you have looked at how you would launch a business continuity (BC) program within your organization, understand the risks, and prepare to deal with an emergency. The next step is to discover what you need to do to ensure the recovery of your information technology (IT) systems and electronic data together with your communications technology.

This chapter will help you to:

- ☑ Identify the critical equipment and the services on which you depend.
- ☑ Prepare to be able to rebuild or restore your data systems.
- ☑ Determine what you need to have in place to accommodate your system users.
- ☑ Initiate a sound backup regime to ensure reliable data recovery.
- ☑ Ensure that you have adequate recoverable and accessible backup for all your essential data, information, and records.

10.1 What is Disaster Recovery?

Disaster recovery is that essential element of the BC management program which aims to restore the essential support services, thus enabling the core business functions to provide continuity of service to clients and client functions. Typically, disaster recovery plans cover the procedures to restore the technical services such as computing, Internet connectivity, and telecommunications, but the same principles can be applied to other types of equipment and services.

10.1.1 Characteristics of Disaster Recovery Plans

Disaster recovery plans tend to be technical, specific, and detailed, with little or no room for interpretation or deviation. Because they are concerned with technical and mechanical matters, things often have to be done in a particular sequence and approximation is not good enough. Such plans will include specific instructions, sequential task lists, and detailed procedures. There will be a tendency to avoid generalities and focus on the specifics.

…the main thrust is the resilience of the service and availability of the data to the users.

A disaster recovery plan takes an approach different from a BC plan. For example, a BC plan might suggest "access to office accommodation for 6 staff will be needed as a matter of some urgency." In contrast, a disaster recovery plan may state "6 desks in 360 square feet of ground floor office space with 120-volt single phase power should be available within 12 hours."

10.1.2 Aspects of Disaster Recovery

There are two distinct aspects of disaster recovery:

- Satisfying the ongoing need for business support systems through the recovery and restoration of essential facilities and resources.
- Preserving the integrity and availability of critical information through backup and recovery procedures.

These two aims are interdependent; there is no point in achieving one without the other. You need the systems and equipment in order to run the applications and provide the services, but they are ineffective without the data behind them. In addition to the regular issues of data security, confidentiality, access control, performance, and compatibility, the main thrust is the resilience of the service and availability of the data to the users.

As you saw in Chapter 6, a number of continuity strategies can provide resilience in various degrees. However, your actual choice of strategy will be influenced by a number of factors which will be covered in this chapter. Cost may or may not be a major factor, but you do need to get a clear perspective on financial implications. Factors to be considered include:

- The resilience, or the recovery, of technology and support services in general.
- Systems recovery, which includes the recovery or restoration of operating systems, software, and data.
- Network and Internet connectivity.
- Disaster recovery sites or services, the facilities and resources necessary to enable a recovery to take place.
- Work area recovery, providing suitable accommodation and resources for the general user population.
- In-house or third party options, the choice between having a contract with a specialist service provider and setting up your own independent solution.

Once you have explored the continuity options, return to the subject of establishing and maintaining the *backup regime*, which is the other essential ingredient of disaster recovery.

10.2 Technology and Support Services

One of the most important tools of modern business is communications systems. Without communications, there is no business activity. Communications technology, along with almost all of your other support services, is computer-based. Indeed, a modern telephone exchange is nothing more than a large computer with lots of remote users. Therefore, it makes sense to integrate the development and management of our telecommunications and data networks with your IT services. This integration makes life much easier than a set up in which two separate groups of technicians attempt to work in parallel or in competition with each other.

In most business operations, the majority of such services are provided and managed by an external organization. It is only the very large institutions, or those with specialized needs, that can justify developing their own dedicated services. Thus, it may be safe to assume you are able to rely on the support of your external service providers in a disaster recovery situation.

If you are seeking to provide total resilience within your own facilities, you will need to cover a number of services and utilities in some detail during your investigations and subsequent protection program. On the other hand, if you intend to make use of an alternative site or service provider, then you will be able to regard service failure as one of the effects with which your plans can cope, as long as your alternate site is not subject to the same interruption.

10.2.1 Range of Services

The range of services you may need to consider within your disaster recovery planning can be divided into two main groups. Technical services usually come under the control of an IT manager. All the other services are commonly called facilities, run by a facilities manager.

10.2.1.1 Technical Services

- Telephony, which includes the external service as well as the internal switchboard and communications network. If you have a call center, then you might regard this as an extension of the telephony system or perhaps as a separate function which requires its own dedicated disaster recovery plan.
- Internet, which includes the cabling and distribution network as well as the actual service from your service provider. This can be a very critical function in any organization which does a large proportion of its business over the Internet.
- Intranet, which is your own private version of the Internet which may be run by your own technical people or it might be outsourced to a specialist service provider.
- News and information services, which may be essential tools for some business units where trading and decision-making are dependent upon up-to-date information.

10.2.1.2 Facilities

- Electricity, which is essential to power all of your technology, heating, lighting, and electromechanical equipment together with conveniences such as elevators and escalators.
- Air conditioning, which may be used to maintain an effective working environment as well as protect equipment, such as servers, from overheating.
- Water supply, which may be required for drinking, hygiene, cooking or as a coolant or an ingredient in processing operations.