

IT Disaster Recovery Planning for Dummies

September 2015

The early, single mainframe data center has given way to massive data centers containing hundreds of servers and terabytes (if not petabytes) of data. Data centers have become decentralized, with companies deploying multiple data centers around the world. Networking is now just as critical as processing resources. Computer-room operators have been replaced by lights-out data centers. The requirements for outage recovery have shrunk from days to hours and in some cases even minutes.



However, many data center managers have been unable to effectively address disaster recovery. In some cases, it is because of a lack of knowledge or a lack of resources. In other cases, there has been no commitment on the part of management.

Peter Gregory's book, "IT Disaster Recovery Planning for Dummies,"¹ provides IT management with the knowledge required to develop a disaster recovery plan (DRP). Companies are largely powerless to stop disasters; but with proper disaster recovery planning, the effects of the disaster can be mitigated; and the company can survive.

Starting with an Interim Plan

The author estimates that the development of a DRP may take about three months for very small companies and one to two years for a large organization. He therefore recommends that a company start with an interim DRP.

An interim DRP can be completed in a few days by a handful of key people. It answers the question, "If a disaster occurs tomorrow, what steps can we follow to recover our systems?"

An interim DRP begins by building an emergency response team of subject matter experts and providing them with the procedures for declaring an emergency. Communication procedures are established for the emergency response team to communicate with each other and with other critical people in the organization under various scenarios of communication facility losses.

Roughed-in procedures are developed to get critical systems running again, including what to do if the building housing the systems is destroyed. The DRP must be documented and the emergency response team trained. The interim DRP should be reviewed every few months and updated to reflect changes in the business' practices and the IT system architecture until a full DRP has been completed.

An interim DRP is a poor substitute for a full DRP, but it can provide some disaster response in the short term.

¹ *IT Disaster Recovery Planning for Dummies*, Peter Gregory, *John Wiley and Sons, Inc.*; 2008.

The Full DR Project

Before initiating a disaster recovery project, it is important to ensure that there are executive sponsors. They are top management, C-level managers who fully support the effort that will be needed to complete the plan and who will supply the funding required by the project.

The Business Impact Analysis

The first step in the DR project is a Business Impact Analysis (BIA). The BIA quantifies the effect on the organization of the interruption of any critical business function. It helps to identify the most critical business processes and how quickly a company needs to recover them.

The BIA should focus on several key aspects of the organization, including business processes, information systems, other assets (machinery, etc.), people, and suppliers.

For each critical business function, several parameters should be determined. They include:

- *MTD* – the Maximum Tolerable Downtime, or how long a business process can be down before it threatens the survival of the business.
- *RTO* – the Recovery Time Objective, or the maximum period of time that an application can be down before restarting it.
- *RPO* – the Recovery Point Objective, or the maximum amount of data that can be lost.
- *Critical Personnel* – a list of all employees who are critical to the business process.
- *Suppliers* – the list of external suppliers of services or products that are important to the business process.
- *Criticality* – a measure of the criticality of the business process to the organization.
- *Risk Analysis* – the probability that various disasters will adversely affect the business process.

Based on the BIA, estimates can be made for the amount of money that would be reasonable to invest in each business process for the purpose of disaster recovery.

Mapping Business Functions to Infrastructure

In order to determine what must be accomplished to recover a business function that has been taken out by a disaster, its dependence upon the corporate infrastructure must be understood. In terms of IT, this infrastructure includes workstations, servers, storage, networks, operating systems, and application software.

Data-flow diagrams of all business processes should be generated to show the interaction of users with the applications, the interaction of applications with each other, and the flow of data between users and applications. With these diagrams, intersystem dependencies can be determined. If a particular application goes down, what business functions are affected? If a communication facility fails, what tasks can users no longer perform?

User Recovery

Users are primarily connected to IT services via their workstations. In today's technology, the workstation is generally a web browser communicating with various web sites. Replacing a web browser that has

been destroyed in a disaster is straightforward – simply give the user another terminal with a web browser and the appropriate plug-ins.

However, older applications used client/server technology. In these cases, much of the application logic is located in the client workstation. To replace such a workstation, the application logic must be available along with all the patches that have been made to it. Ensuring that these client applications are available is a key component of the DRP.

In addition, users need access to common services such as print servers, file servers, and application servers (for client/server applications). These services must be restored before the users can be fully functional.

In many cases, users also use their workstations as local computers. They may use standard applications such as Microsoft Office, or they may use custom applications. Custom applications must be available for reloading into replacement user workstations. In addition, word documents, specialized spreadsheets, and other work products created by standard applications such as Microsoft Office must be replaced. As part of the DRP, there should be methodologies for all of these specialized applications and work products to be safely stored externally so as to survive a disaster.

End-user communications must also be restored. This includes Internet connections, email, voice, and fax facilities.

Facilities Protection and Recovery

Facilities that must be recovered include information processing facilities (data centers) as well as work locations for personnel.

Disaster recovery planning for facilities starts with protection to avoid severe damage in the first place. Facility protection includes:

- Physical access control
- Electric power (UPS and generators)
- Fire detection and suppression
- Avoiding chemical hazards
- Water/flooding protection

Physical access control can include key-card or biometric entry controls, man-traps (dual doors), video surveillance, security guards, locking cabinets, and equipment cages. A hardened facility might include no windows or the use of bulletproof glass, fences, and equipment bracing.

Electric-power protection includes a UPS system to cover short electrical outages and a generator system to provide power for extended outages.

Fire detection systems include smoke detectors, heat detectors, and ionization detectors. Fire suppression systems should use gas to smother the fire. Water-based suppression systems will damage the IT systems.

If a company works with hazardous materials, the materials should be safely stored with plans for handling accidental spills or other releases.

Water detectors should be installed in the lowest places in the IT facility. All equipment should be positioned on floors well above any flood threat. This includes backup generators.

For critical applications, a remote site should be provided in case the primary site is destroyed. The remote site could be a:

- *hot standby* – with applications loaded, a current database, ready to go
- *warm standby* – servers and storage in place but no applications loaded
- *cold standby* – empty processing centers

System and Network Recovery

The BIA defines the critical business processes and the applications and databases that are required to support these business processes. The detailed configuration information for each server should be recorded, kept updated, and stored in a secure facility that can be accessed following a disaster. The same requirement applies to operating systems, storage, network components, security components, and user authentication and authorization information.

The reconstruction of networking facilities can be particularly complex if network diagrams do not exist or if the configuration parameters for the various network devices are not available.

There are additional considerations for distributed computing environments if a data center is destroyed and must be rebuilt at another location. If there are custom interfaces between applications, these must be recovered and deployed. Communication latency must be controlled so that applications do not time out due to communication delays. The new facility should be positioned so that personnel can commute to it reasonably.

To the extent possible, the IT architecture should rely on standard components with common configurations. This will ease the replacement process, which is otherwise made complex by having to configure each system according to specialized configuration parameters.

During this recovery effort, it is important to continue to protect data. Many security laws and regulations govern the privacy and security of data, and these requirements are not lifted due to a disaster.

Many data centers today use clusters for high availability. The clusters may be local, or they may be geographically distributed. They depend upon a common database that may either be a single instance or multiple distributed instances kept synchronized via mirroring or data replication. They may be operating in an active/passive mode (some servers are acting as idle backups) or in an active/active mode (all servers are processing data). The DRP must contain procedures for recovering part or all of a cluster.

Data Recovery

The most valuable IT asset is the organization's data. Data in all likelihood will be lost in a disaster. It is therefore imperative that procedures be established to recover that data. The RPO in the BIA indicates the amount of data for each business process whose loss is permissible following a disaster.

Even in the event of no disaster, disks fail and can lose data. Therefore, critical data should be stored on resilient storage such as RAID or mirrored disks.

There are several methods available to back up data so that it is recoverable. The classic technique is magnetic tape. The tapes can be stored offsite so that they will not be affected by a disaster. When data is to be restored, the tapes are accessed and are used to reload the database. Backing up data via magnetic tape is the least costly of all of the backup methods. However, its biggest disadvantage is that it can take days or even weeks to reload a large database, making tape backup viable only for those business processes with a suitably long RTO. On the other hand, magnetic tape is used to store data that has a requirement for a long retention cycle.

Data can be protected by creating a copy via mirroring or data replication. With mirroring, the storage system copies every new block to a remote system to create a backup copy. Mirroring is synchronous, so the distance between the primary copy and mirrored copy is typically limited to a few kilometers.

Data replication replicates data (usually transactions) asynchronously to a remote site. The application is unaware of the replication activity, and the remote site can be hundreds or thousands of miles away from the production site. Data replication is often used for electronic vaulting, in which a copy of the data is stored at a remote facility where it is available to upload to a system following a disaster. Data replication is also used to keep the database of a remote hot-standby system up-to-date so that the standby system can take over processing on a moment's notice should the primary system fail.

Writing and Managing the Disaster Recovery Plan

Documentation

The author, Peter Gregory, goes into great detail on the content of the written disaster recovery plan. It should include:

- a procedure for declaring a disaster.
- emergency contacts.
- emergency leader (may depend upon the effects of the disaster).
- damage assessment procedures.
- system recovery and restart procedures.
- procedures for the transition back to normal operations.
- recovery team selection (depends upon the effects of the disaster).

The documented DRP must be stored in a secure facility that will not be affected by a disaster so that it is always available. It also may be desirable to distribute hard and soft (USB) copies to the recovery team. One suggestion is to provide laminated wallet cards with all of the emergency contact information on it.

Testing

A DRP is useless if it doesn't work. It is therefore important to test it periodically. Five levels of testing may be incorporated:

- *Paper tests* – Individual staff members review the DRP on their own. Corrections and suggestions for improvement are passed to the DRP project manager for updating the DRP.
- *Walkthrough tests* – Similar to a paper test, but the walkthrough test is performed in a common meeting with a group of experts rather than experts working alone.
- *Simulation tests* – A walkthrough test under a specific disaster scenario. The disaster is scripted over a period of time, and the disaster response team reacts to the unfolding scenario according to the DRP.
- *Parallel testing* – Disaster-response personnel actually perform the steps in the disaster recovery procedures. This includes such activities as building servers and bringing up applications. However, this testing has no impact on actual IT services.
- *Cutover testing* – Cutover testing is the real thing. The production systems are taken down and recovered to the backup systems. This testing carries with it a great deal of risk. If the cutover is unsuccessful, IT services are down.

The following test schedules are suggested:

- *Paper tests* – as often as procedures change
- *Walkthrough and Simulation tests* – quarterly
- *Parallel tests* – annually
- *Cutover tests* – annually or biennially

Keeping DR Plans and Staff Current

The need to update the DRP is affected by many factors. The IT infrastructure may be updated with new servers or other equipment. Business processes may change. Key personnel may leave. The organization's market may evolve.

Any of these conditions will require that the DRP be updated. Anytime the DRP is updated, the key emergency response team members must be retrained.

It is important to make disaster recovery planning a key element in corporate restructuring, such as IT changes and business process modifications. As these moves are considered, the effect on disaster recovery procedures should be an inherent topic for discussion.

Planning for Disaster Scenarios

The book continues with discussions related to surviving a multitude of disaster types. The first line of defense is prevention. Prevention methods can be applied to site selection, fire prevention, HVAC (heating, ventilation, and air conditioning failures), power-related failures, civil unrest and war, industrial hazards, hardware and software failures, people errors, and security incidents.

The book concludes with planning for disasters. Natural disasters discussed include earthquakes, wildfires, volcanos, floods, wind and ice storms, hurricanes, tornadoes, tsunamis, landslides and avalanches, and pandemics. Man-made disasters include utility failures, civil disturbances, terrorism and war, and security incidents.

Appendices

The book contains several lists of significant resources, including:

- Disaster recovery planning tools
- Disaster recovery planning web sites
- Essentials for disaster planning success
- Benefits of disaster recovery planning

Summary

"IT Disaster Recovery Planning for Dummies" carries on the Dummies-series tradition of books that are easy to read and complete in their detail. The over 300 pages of this book offer a detailed insight into disaster recovery planning. It becomes clear that the creation of a good DRP requires a great deal of time of many subject-matter experts in the organization and therefore must be supported actively by upper management. Furthermore, the DRP requires continual updating and therefore a continuing commitment on the part of upper management.

The other major consideration in a good DRP is testing. Disaster recovery procedures are not of much value if they do not work. However, testing a DRP can be a risky venture. Therefore, several levels of testing are described. The final level is a full cutover that, if unsuccessful, could take down IT services. However, the alternative is to rely on faith and hope when a disaster hits.

Acknowledgement

Our thanks to our subscriber, Terry Critchley, for pointing us to this book.