Making a Disaster Recovery Plan



Firstly, why do we need a disaster recovery plan? Simple, many events even apparently trivial ones can cause a business to be unable to trade and close down. Causes can be a spectacular natural disaster like Hurricane Katrina, terrorist attack such as 9/11 in New York or 7/7 in London or flooding such as was encountered in the UK in 2007. Causes can also be much more mundane such as a toilet cistern leaking flooding a server room or a virus attack on the network that corrupts a key database. Add fire or major equipment failure and it’s easy to see how a thriving business can be brought to a halt.



Cost is critical here; you may have a detailed plan to protect everything and keep the company up and running, but if it is too expensive and will bankrupt the organization it’s a nonstarter.

The business has to have its own business continuity plan that must integrate with the IT disaster recovery plan and there is clearly a great deal of detail you can go into here but we need to focus on the basics of the IT plan.

## Step 1. Set Objectives

We need an IT plan that is part of the organization’s overall business continuity plan and meet the same needs for protecting crucial data, access, and continued function.

We also need to understand the maximum time the business will survive without IT; what is my maximum tolerable outage?

Also where do I need to recover to? Options are:

* zero data loss, recovery to the point of failure
* start of the current business day (SoD)
* end of the previous business day (EoD)
* intraday, a point between the last available backup either SoD or EoD and the failure e.g. midday
* period end weekly/monthly backup



## Step 2. List of Critical Needs

Next identify the critical needs of IT organization, how they impact the organisation and how they allow it to continue to function. This is an outline at this stage, i.e., backups of data, redundancy for connectivity, power and equipment, plus potential alternative sites. Again this is general view not the specifics. Each organization keeps different types of data and in varying amounts all of which needs to be backed up. We need to develop categories as this will drive the amount of storage required and the frequency of backups required.

In no particular order typical types of data would include:

* Financial Data
* Emails
* Audit Data
* Applications
* Organizational documents
* Customer lists
* User data files
* Operating System backups
* Databases
* Transaction files
* Website data

Then list critical services, their recovery objectives and recovery priorities, this will create the following recovery process plan.

##

## Step 3. Recovery Process Plan.

Now you can decide what services are to be recovered, the order in which they to be recovered and the extent of that recovery. Part of this process is to assign roles to named individuals allocating specific responsibilities to each. Also a list of the third party contact details; your secondary data centre plus location of backups, spare equipment etc.

## Step 4: Backup Equipment

This should be both on and offsite, with the offsite location being a significant distance from the main site so as to be unaffected by any local disaster (fire or flood for example). The plan must include the design of the architecture, with key consideration given to performance (backups must not interfere with day to day operations), growth in data volume, and on-going supportability of the backup applications.

Again, it’s critical to be mindful of the budget involved!

## Step 5: Investigate Alternate Sites

An option for the organization is to consider a fall-back site to allow the organization to temporarily function in the case of a disaster. When reviewing these consider cost, size and supportability for the organization and IT plus network and phone connectivity.

## Step 6: Test

Will it work when you need it? Obviously you must test the plan!

You need disaster drills and test recovery of data, failovers, and access to remotely stored data.