

# First Steps for System Administrators tasked with DR

Contributed by Gareth Eagar  
 Tuesday, 08 August 2006  
 Last Updated Saturday, 21 October 2006

So you're a sys admin that has been tasked to sort out DR for your systems and you're not sure where to begin? This article will get you started.

So you've been tasked to sort out DR for your IT systems and you're not sure where to begin?

Firstly, Disaster Recovery should be a component of a Business Continuity plan that has been established by the business. The IT systems are just a tool for the business (though obviously it's a critical tool) and so a full Business Continuity plan should be created that addresses issues such as facilities, human resources, crisis management, public relations and so on.

If you don't have business buy-in from top management, you're going to have a tough time and then even if you're successful, if a major incident hits your organisation, getting IT systems recovered will only be of limited usefulness if the rest of the business cannot continue (if your building is destroyed where are your users going to work from to access the systems you've so lovingly rebuilt?)

So let's say that you do have business buy-in, then your first step is to find out from your business continuity planner the Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) for the IT systems. The business needs to tell you what the priority is of the applications you're running and how long they can survive without these systems (RTO) and how much data they could afford to lose (RPO).

Once these are determined you'll know whether you need a high-availability / fail-over solution, data replication or if rebuilding systems and recovering data from the last backup is acceptable. What you're likely to find is that some systems require high availability while others can be recovered from backup within a larger time period.

Irrespective of whether you're using high-availability or traditional recovery solutions, there are certain key elements to having a successful disaster recovery program.

- Test, test and test some more. If you don't test your recovery regularly (and that means at least once every 6 months you do a full recovery test to your off-site location) you can't have confidence in your ability to recover. IT environments are very dynamic these days with daily changes, so you need to test regularly to ensure that you can still recover after changes in your environment.
- Audit your backups. Your backup (whether replicated or to disk/tape) is obviously critical to recovery so ensure that you are backing up everything you need and that the backups are actually working. For more help, read the article "How good are your DR backups"
- Integrate Change Control with your Disaster Recovery planning. You need to ensure that you evaluate each change in your production environment for how it may affect your recovery environment and procedures. For example, if you're doing traditional recovery and you change your tape technology, you need to ensure that you have the new type of tape device available at your recovery site. Or, if you install a new application, you need to ensure that it is fully backed up, you may need to send a copy of the install CD off-site and you may need to add new procedures to your recovery documentation.
- Write yourself out of the procedures. You need to make sure that you (and the rest of your system administrators) are not the only people that can perform the recovery. You need a documented recovery plan and technical procedures and these should be clear enough that another competent technical person that has never worked in your specific organisation could perform the recovery &mdash; so don't assume any knowledge of your environment, make the procedures clear. Some people feel that the procedures should be detailed enough for the secretary to perform, but I disagree. Your organisation will always be able to find some technical resource to perform the procedures, it just may not be you (with a bit of luck, you may be blissfully unaware of the disaster as you sit on some remote island with no phone signal on holiday).
- Keep it off-site. You need to plan for the possibility (no matter how remote you may think it is) that your entire data centre could be destroyed one day (along with your offices). If this ever happens to you, you don't want to be the one running into the burning building to grab a copy of your backup tapes and the latest procedures. You need to ensure that you keep your data tapes and the latest version of your DR related documentation securely off-site (and by securely, I don't mean on the back seat of your car!).
- Do regular reviews of your DR strategy and BC plan. Over time, applications that were critical may become less critical and systems that were being used by a small new division with low priority may have become critical as the division has grown in importance. I don't believe this is the system administrators job directly, but check that somebody is reviewing your Business Continuity and Disaster Recovery objectives from a high-level on a regular basis. You don't want to sweat it out with recovery of a system that over time has become less important to the business, while ignoring another system that the business now views as important. In addition, changing RTO and RPO objectives for specific systems may require a change to the strategy for recovery (high availability vs rebuild and restore).

Let's look at the different recovery strategies and some ideas around planning for how to actually recover these systems.

#### HIGH-AVAILABILITY / FAIL-OVER SOLUTIONS:

This is generally the most expensive solution as you're going to require duplicate systems and probably substantial bandwidth between your production site and the recovery site. Depending on the platforms you're running, there are different products out there that can deliver what you need.

Firstly find out what the budget is, how much bandwidth you have available and then make a list of the functionality that you will require (such as instant and automatic fail-over or a solution that requires manual steps in order to get the new systems up and running). Depending on your environment, you may be able to find a solution that runs both systems as production, therefore allowing load-sharing between the servers. This enables you to benefit from your DR solution on a daily basis rather than only getting the benefit when you hit a disaster.

After that you need to do your research to find relevant products that meet your functionality requirements, budget and bandwidth constraints. Obviously Google is a good place to start and then once you have a short-list of products, I strongly recommend that you search Internet news groups to research the issues and experiences that others may have found with the products you're looking at.

When testing solutions, ask the vendor what the process is for performing fail-over testing. Some products allow you to go into a test mode so that you can test fail-over without affecting production, while others don't make this very easy and if you can't test your DR plan regularly, you can't trust it!

#### REBUILDING YOUR SYSTEMS AND RESTORING DATA

For those systems that have a RTO and RPO that allow for rebuilding of the systems and restoring the data, you can either do this using traditional methods or by purchasing a software solution that automates to some degree the rebuild and restore process.

One of the most important points to remember is that for certain disaster scenarios, you're likely to be recovering the system to dissimilar hardware. This means that simply doing a system state restore along with the data restore is not going to work.

The traditional method for recovery is therefore to reinstall the operating system, customise the operating system (add users, create filesystems / partitions, configure networking, etc), reinstall the applications (and service packs) and then restore the data. This requires a copy of all relevant software to be kept off-site and requires extensive and regularly updated documentation on the system and application configuration and re-installation procedures.

Luckily various vendors have come up with products to enable you to recover your system to dissimilar hardware (such as the Indigo Stone HomeBase solution). If your budget allows for such a solution (and I strongly recommend that you go this route - traditional recovery is highly unreliable because of all the manual processes and these solutions are still a lot less expensive than most high-availability solutions) then you won't need to keep hundreds of CD's off-site and spend half your life updating system configuration documentation and recovery procedures.

Before purchasing such a solution however, make sure that you try-out the solution yourself with recovery to different hardware - while a number of solutions claim to offer dissimilar hardware support, some work better than others.

There is a lot of work involved in getting your DR project started and unfortunately, the work never ends. You have to constantly review the plan, update the procedures and test, test and test. But if you do this properly, you'll definitely sweat less when you're woken up in the middle of the night at some point and told that the computer room you so loved has gone up in smoke.