

10 Common Disaster Recovery Gotcha's - Part 1

Contributed by Gareth Eagar
Tuesday, 08 August 2006
Last Updated Sunday, 03 December 2006

The first part of an article looking at 10 common issues that you need to be aware of when planning for Disaster Recovery

More and more, IT executives are realizing that having a plan for recovering from potential disasters is no longer an option, but a necessity.

Disasters do happen, and they occur in many different ways. Your critical IT systems could be made unavailable by a hardware failure, flooding, fire, theft, an extended power outage or countless other unexpected events. And while the cause may be unexpected, you need to have a plan to get your business systems up and running again, reliably and quickly.

Whether you have a contract to recover your systems at a commercial disaster recovery site or make use of your own backup systems and site, there are some common “gotcha’s” that you need to be aware of before a disaster strikes.

Firstly, and I believe most importantly, if you haven’t tested your recovery plan recently (that means at least once in the last 6 months), you cannot have confidence in your ability to recover. You will also not have an accurate idea of how long it will take you to get your IT systems running again. To be really prepared for a disaster and confident in your ability to recover, you need to test your DR plan and you need to test regularly.

When you do a test recovery of your systems, ensure that you recover to the expected recovery hardware, as this will often be a different system type to your production hardware. You may, for example, have a 2 CPU IBM server in production but a lower spec single CPU HP server as your recovery system.

As most backup and recovery software restores the system fully, including the configuration that applied to the original hardware, restoring your system on different hardware can be a complex and time-consuming process. Therefore, ensure you get some experience of these issues during your DR testing and make sure that you have built in adequate time in your recovery plan for hardware dependency problems. Alternatively, review some of the software solutions that are available from various vendors that automate the process of recovering to different hardware configurations (such as the Indigo Stone HomeBase solution)

Another common ‘gotcha’ that many companies experience when recovering their systems in a real disaster situation is that they had not planned for and tested the worst-case scenario. I recently worked with a company that experienced a hardware failure on a critical system. They were contracted for recovery at a commercial disaster recovery site and regularly tested their recovery plans. However, their disaster recovery rehearsals were based on a ‘best-case scenario’ and in performing the recovery after the hardware failure they found that the disaster had not occurred according to their best-case scenario planning. Perform both best-case and worst-case scenario testing. For example, don’t only test recovery of a full system backup, but also test recovery of the incremental level 1 backups and database log file backups and plan for a disaster occurring during your financial year end processing, just for good measure!

We all know that our business systems are constantly evolving and changing - we seldom have the 5-year upgrade cycles for our servers that were perhaps more common 20 years ago. Therefore, your disaster recovery plans and procedures need to be ‘living’ documents – it’s not a WORM (write-once read-many) type of document. Your Disaster Recovery documentation needs to be updated on a regular basis and you need to ensure that whoever performs your recovery testing strictly follows the procedures outlined in the documentation (rather than ignoring the procedures and working from experience as many people do). As they work through the documentation they need to constantly update the procedures, clarify parts that may not be clear, etc.

There are many different disaster scenario’s, from isolated hardware failures to a major incident rendering your entire site unavailable. So even if you do have updated procedures based on regular testing, it’s not going to help you if the next disaster to hit your company is a major incident type disaster and the latest backup tapes and recovery documentation isn’t available off-site. Arrange to store your backup tapes securely offsite and ensure that you have a process for keeping the latest version of your recovery procedures, contact lists, etc offsite but easily available (a good way to store the required documentation is electronically on a secure Internet site that you don’t host).

Having your documentation and tapes available off-site is great, but you also need to make sure that you aren’t heavily dependent on a few key resources that could potentially be unavailable at the time of a disaster. Murphy’s Law states that if you need to recover your systems, the staff members who have the technical skill and have performed

the recent recovery testing will be on holiday in a remote outback part of Australia without phone signal. Although you won't achieve this on the first test, you do need to work towards having procedures detailed enough that other technical staff that have never worked in your IT environment could perform the recovery of your systems based on your documentation. So ensure that your procedures make no assumptions about the reader having experience in your specific environment.

You may perform test recoveries of the worst-case scenario to different hardware using other technical staff regularly and have great updated procedures stored off-site with the backups, but you also need to make sure that you review your entire DR plan from all levels (including high-level objectives) on a regular basis. That way you will minimise the risk of a recovery 'gotcha' when Murphy's Law catches up with you at 2am during your next financial year-end run.