



If disaster strikes, will you be ready?

Written by: Paul Songaila
Founder
Twin Systems Plc

Date: November 2004

If disaster strikes will you be ready?

If there is one thing that is certain in the world of IT it is that at some point your systems will fail. Admittedly hardware is becoming ever more reliable but outside interference is a real threat, whether it's a virus, unauthorised entry or a system crash, the affect on your business can be catastrophic.

The good news is that you can do a lot to protect your IT infrastructure should an unplanned outage occur.

Integrate

Disaster recovery should be an integral part of your business strategy most of all someone needs to own it and the more senior that person is the better. If business strategy changes then your disaster recovery plans must keep pace.

Big Picture

It can be very easy to concentrate all your efforts on Head Office, The Data Centre or the Server Room. What about a remote user who customises their work and adds a disproportionate value to the organisation? All these areas need attention and no stone should be left unturned even if there seems a remote risk of failure.

Prioritise

Some of your systems will be much more crucial than others. For instance the e-mail system may need to be up and running before the database system depending on business need. By default the IT department may be given this task but they may not be business aware enough to make a balanced decision.

Hardware

Your systems themselves can be protected from failure. Consider duplicating storage by RAID, Mirroring or completely replicating critical systems. Avoid single failure points such as power supplies, communication lines and even the office you are in.

Most companies will not survive a complete outage for more than a few days if they have not made contingency plans.

Data backup

This area is crucially important to your business. You need to decide what you are going to back up and when, plus a process for undertaking the task. Most organisations perform a full back up at the beginning of the week then back up the changes each day until the whole process starts again.

The changes can take two forms - the first is **differential**, this is where the complete difference from the first tape is backed up every day. The second is **incremental**, which means only the changes from the last days backup are stored. The incremental method is quicker on a day to day basis but all tapes are involved in a restore, whereas the differential requires only two tapes.

Offsite data backup is also crucial. It is important that risk is spread and a process exists to ensure data is up to date at any given time and can be used for restoration with relative ease. Whether the method is tape, CDR's or VPN access is crucial and should not be down to an individual.

Be secure

Protect yourself if it's data sensitive and take measures to prevent it from being stolen. One note of warning - if your back up is encrypted or has access control like Fort Knox, can it be easily restored if a key user is not there?

Test! Test! Test!

Test your plan. How many businesses think their back ups are running smoothly only to discover not all the information is there or their new systems cannot even read it!

How long will it take to restore? If it is 24hrs, do you have a contingency in the meantime? What is the minimum required to keep your business alive? When deciding on new systems back up strategy should be a major focus ensuring if something does go wrong restore time is minimal.

When things change

Reorganisation, infrastructure changes etc can all affect the robustness of your plan so make sure all data that is likely to be required can be restored easily. Make sure all your suppliers have effective disaster recovery plans. Key personnel details should be kept up to date and every employee should be aware of their role in any disaster.

These are just a few of the issues that need consideration and remember any disaster recovery plan needs to be linked to a Business Continuity arrangement for the organisation.