

# Disaster planning for your computer systems

If someone stole your server tonight, how long would your business be out of action? If you cannot immediately answer this question, you need to review your disaster planning strategies.

The fact is, more than nine out of ten businesses have seriously insufficient disaster recovery plans. They don't realise that the average time it takes to get a business operational again ranges from **THREE DAYS** to **NEVER**, even if they have good backup systems.

So why do professional businesses fail to properly plan for IT failures? There seems to be three common reasons:

## (1) Time/Not Wanting to Deal with it

The first is a combination of time and not wanting to deal with the issue: They know disaster planning is important, but they keep putting it on the back burner, dealing with more urgent day-to-day issues.

It is probably the same psychology that delays people visiting the doctor to get an unusual lump or mole checked out. For some people, the delay is immaterial. For others it is the difference between preventing a health disaster and dealing with the terrible consequences.

## (2) Lack of Understanding

The fact is many small and medium businesses simply do not understand IT Disaster Planning. The problem is compounded by the reality that many small IT support companies do not understand it either.

Many believe that having 'redundant hard disks' and a 'tape backup' are sufficient. For reasons that will become clearer when you read the 'How to Plan for a Disaster' section, this belief is misguided and misinformed.

## (3) Cost

The third reason is often cost. Yes, putting in place the necessary hardware, software and processes to plan for a computer system disaster requires an investment. But the cost is often a lot lower than people think.

On the other hand, the cost of a disaster can be huge: For a 10 person organisation, a three day business outage would result in lost wage expenses of at least \$10,000. The cost of restoring your IT systems could easily be another \$10,000. But, the largest and hardest cost to calculate is the damage to your organisation from not being able to service your clients during the downtime.



**Do you have a Disaster Recovery Plan?**

## How to Plan for a Disaster

Planning for a disaster simply means understanding what can go wrong, what impact it will have on your business and what steps you are currently taking, or could be taking, to mitigate the risk or damage.

### What could go wrong?

The most common events which can lead to a disaster include:

- Hardware failure.
- Theft of a server.
- Fire or water damage (flood or sprinkler systems).
- Electrical damage (surge from lightning).
- Malicious intentional damage.
- Extended Power Outage.
- Telecommunications / Internet Outage.

### What could the impact be?

You should think carefully about the impact on your business resulting from a computer system outage.

Usually, an outage of a few hours is relatively minor. What if the outage was one business day? What if it were two, three or even a full week?

## What am I / could I be doing to mitigate the risk of a disaster or reduce the impact?

Lets now look at the various ways of either avoiding a disaster or reducing the impact on your business should one occur.

### **Suggestion 1: Have Redundant Systems**

Redundancy is about keeping systems operational, even in the event of a single hardware failure.

The most common components of a server which fail are the two with moving parts – the hard disks and power supplies.

Hard disk redundancy is provided through 'RAID' – a Redundant Array of Independent Disks. RAID 1, often called Mirroring, consists of two hard disks. Each is an exact copy (or mirror) of the other. If one hard disk fails, the other continues to operate without downtime or loss of data. RAID 5 consists of three or more disks. Again, any one disk can fail without downtime or loss of data. RAID 5 is more reliable and also permits additional disks to be added if you run out of hard drive space.

Power supply redundancy can be provided on some servers through the addition of a second power supply.

### **Suggestion 2: Take Backups**

Redundancy is a preventative step, but there are still many events which can lead to downtime and loss of data. Backup systems essentially take a copy of the data from your server and store this copy on some other media, usually a tape.

In any backup system, it is essential that you:

- (1) Backup **all** data, including emails and databases.
- (2) Keep multiple backups of varying age so that you can recover older files, not just files from yesterday.
- (3) Take backups off site, because there are certain events (fire, theft, flood etc) that could destroy both your server and any backups stored within your office.
- (4) Check and test backups regularly.

Tape is still the most common backup standard and larger capacity tapes are being developed to cope with ever increasing data storage requirements. Alternative technologies, including remote backup, are slowly emerging.

### **Suggestion 3: Have Good Hardware Warranties**

An often overlooked element of a Disaster Plan is the repair time for your hardware.

If your server is a 'no-name brand white box', you may be in real trouble here. Does your machine have a warranty? Who will fix the machine? Is the warranty issued by the person who supplied the machine, or the companies that manufactured the components? Is the warranty onsite, or do you need to ship the parts back and wait for a replacement?

If you have a name-brand machine (IBM, HP, Dell etc), what exactly does the warranty provide? Most standard warranties are *Onsite Next Business Day*. This means that a system which fails on Monday morning will not necessarily be attended to until Tuesday afternoon. An onsite, 4 business hour warranty should be considered at a minimum.

Worse though, if your machine (name brand or otherwise) is not covered by a warranty, what process will you follow to get the machine repaired? Spare parts availability, particularly for older servers, can be limited and parts can take weeks to arrive.

### **Suggestion 4: Recovery onto Different Hardware**

What many people fail to realise is that most backups need to be recovered onto identical or highly similar hardware. Recovering a backup to new hardware can be troublesome.

With identical hardware, it is often possible to restore the programs and data at the same time. Without identical hardware, restoration can easily take at least an additional 8-16 hours because all software needs to be manually installed.

### **Suggestion 5: Can you access your building?**

Physical access to your building must also be factored into your plans. Some events including flooding and electrical outages can prevent you accessing your building.

Consider where you and your staff would go in such an event. What access to computers, data, internet and email would you have during this time?

### **Suggestion 6: Don't forget the phone system**

Finally, include your phone system in any disaster recovery plan. If your building is inaccessible or phone lines are damaged, what is your backup plan? How quickly can you have phone numbers switched to a new location or mobiles?

## Conclusion

Disaster Recovery Planning is not difficult, time consuming or costly, but it does require that management recognises the risks and involves people with sufficient experience and expertise to help develop, implement and test the strategy.

As the saying goes, "*There are two types of people in this world; those that have lost data, and those that are about to*". Really, you don't want to be in either category, so start your disaster planning process today.

*Adam Feldman is the Managing Director of VISITS, a leading provider of IT services to Small and Medium Businesses in Australia. He can be contacted on 1300 300979 or via email: [adam.feldman@visits.com.au](mailto:adam.feldman@visits.com.au)*