Protecting your business against IT disasters

Preparing for IT disasters requires considerable planning, but is essential to keep your company going in times of crisis. The closely regulated nature of business today combined with statutory obligations concerning customers' data protection, means that having a disaster recovery system in place is essential.

Many companies have historically failed to prepare properly for IT disasters, and the fact is that IT disaster recovery is complicated. Doing it well requires a lot of planning, and plans need to be continually updated if they aren't going to be totally useless by the time they're needed. Testing the plan properly is rarely done, as it has a tendency to be time-consuming.

Traditionally IT disaster recovery solutions have been complicated and expensive, or cheap and ineffective. This has left many with either inadequate provisions or worse, expensive provisions that fall short of protecting the business.

Should the worst happen, it's worth thinking about whether you want to be solely reliant on your own IT team. In many cases they will be busy trying to deal with the cause of the disaster or, worse, may actually be caught up in it themselves. Here are some of the current options for protecting critical IT systems in your business.

1. Have a plan to replace and rebuild your systems

This is probably the most popular form of disaster recovery provision. Unless you've got a detailed, documented plan of how you'd replace and rebuild your critical systems, then your backups, even if done regularly, may not necessarily help. After all, what really matters to you is not that your data is 'safe' but that it's useful. If you can't interact with it, then it's not doing any useful work for you.

The fact remains that rebuilding your systems is a highly complex and time consuming process, it can easily take up to seven days. Unless you've done it from a realistic starting point a couple of times, it is unrealistic to expect it to work when you need it.

2. The development of virtualization

As a recent technological development, virtualisation has a lot to live up to but when it comes to disaster recovery, it really does show some promise. In fact, it should be able to solve both the drawbacks of traditional disaster recovery approaches by dramatically reducing costs for vastly more effective, fast recovery solutions.

Virtualisation's promise comes from its ability to provide a consistent computing environment regardless of the underlying hardware. This means that a system image can be made to work on any hardware and because of the consolidation advantages of virtualisation, multiple workloads can be run on single physical machines.

Virtualisation can deliver significant advantages for disaster recovery because it can dramatically reduce the hardware costs for the recovery platform. As a result you can now purchase products that would allow you to make a virtual warm standby solution from a physical live server.

3. Online backup options

Online backup is basically no different to a local backup but has some definite advantages. Not having to keep moving tapes around is a step forward and you can make an argument that your data is more secure in encrypted form than in plaintext on tape in somebody else's offsite storage. However, depending on your online backup solution, if you start thinking about recovery, it's not all roses.

If your online backup product doesn't keep a local copy of all of your data, how long would it take you to download a complete set of all the data on your biggest server, using a sensible proportion of your internet connectivity? If you've got a better online backup product that does keep a local copy, what happens if it's your entire building and IT systems that are out of action?

4. Warm and hot standby solutions

Finally, we start to get to solutions that actually stand a reasonable chance of delivering quickly when you need them. 'Warm' and 'hot' standby solutions take a starting point that you need to have properly provisioned, permanently available, configured, and working systems in another location, ready to take on your workloads, as and when you need them.

Where they differ is in terms of the currency of the data on them. Typically, a 'warm' system will be fed data periodically, so should you need to press them into service, you'll see your data go back in time somewhat. A 'hot' standby system is continually replicating data, so you should see minimal data loss when you need it.

The downside of both of these approaches is the same, the cost. Depending on your solution, the level of importance of your data and the importance of keeping up to date with every last transaction, prices can range from the inconveniently pricey to the truly legendary. Bear in mind that these solutions aren't a replacement for a good backup regime, they're an addition to them, and so you still need to pay attention to your backups.

REMEMBER !!!

In these technological times, very few companies can survive without their computer systems. Most businesses do not have paper copies of everything that their IT systems produce, so if that data is lost or becomes unavailable, even for a relatively short period of time, a company can be damaged very quickly.

When looking at the cost of putting a data recovery system in place, consider the cost of NOT doing so. If you lose all of your data, how much is your business worth?