

Importance of disaster recovery planning

As IT systems have become increasingly critical to the smooth operation of a company, and arguably the economy as a whole, the importance of ensuring the continued operation of those systems, or the rapid recovery of the systems, has increased.

It is estimated that most large companies spend between 2% and 4% of their IT budget on disaster recovery planning, with the aim of avoiding larger losses in the event that the business cannot continue to function due to loss of IT infrastructure and data. Of companies that had a major loss of business data, 43% never reopen, 51% close within two years, and only 6% will survive long-term.

As a result, preparation for continuation or recovery of systems needs to be taken very seriously. This involves a significant investment of time and money with the aim of ensuring minimal losses in the event of a disruptive event. – Wikipedia

“Disaster Planning Essentials for Small Business Network”

✓ Document your hardware, software and network

System documentation can provide an introduction and overview of systems. New Administrators, contractors and other staff may need to familiarise themselves with a system; the first thing that will be requested is any system documentation. To avoid staff having to waste time discovering the purpose of a system, how it is configured etc system documentation should provide an Introduction.

Many systems are supported by disaster recovery arrangements, but even in such circumstances, the recovery can still fail. There may be a need to re-build a system from scratch at least to the point where a normal restore from backup can be done. To make a rebuild possible it will be necessary to have documentation that provides answers to the configuration choices. For example it is important to re-build the system with the correct size of file systems to avoid trying to restore data to a file system that has been made too small. In some circumstances certain parameters can be difficult to change at a later date. When rebuilding a system it may be important to configure networking with the original parameters both to avoid conflicts with other systems on the network and because these may be difficult to change subsequently.

Even when a disaster has not occurred, there may be times when it is necessary to reload an Operating System or Application; this can either be as part of a major version upgrade or a drastic step necessary to solve problems. In such circumstances it is important to know how an OS or Application has been configured.

The benefits of good system documentation, when trouble shooting, are fairly obvious. A comprehensive description of how a system should be configured and should behave can be invaluable when configuration information has become corrupted, when services have failed, or components have failed.

Good system documentation will include a description of the physical hardware and its physical configuration, which can avoid the need to shutdown a system in order to examine items such as jumper settings.

When planning changes or upgrades it will be necessary to assess the impact of changes on existing systems. A good understanding of existing systems is necessary for assessing the impact of any changes and for this good system documentation is required.

System documentation can be used for many purposes including Auditing, Inventory, Maintenance, etc. The documentation of individual systems forms an important component of the overall network documentation.

✓ **Develop an emergency contact list**

Who will you call if you have to replace a part or computer immediately? Who can best get you up and running again in case disaster strikes? Make a list. You'll probably have several different vendors on your list. Include any account numbers along with full contact information (vendor company's name, service rep's name, phone numbers, pagers, after-business-hours contacting instructions, and so on).

Also put your computer maintenance contact on this list. Be sure your documentation contains how to contact each person any time, any day, anywhere, since disasters don't keep regular business hours. "If you're not comfortable with your computer maintenance firm now, when everything's running smoothly, you'll probably be very unhappy with them if a catastrophe occurs," Lasky says. "It's best to have on call a firm you can trust to react quickly and with expertise. And have them on board before you really need them."

✓ **Back up and store all data files off-site**

The importance of an offsite backup is absolutely crucial to any business. While most business owners perform data backups, the storage location of backups is often overlooked. Losing your primary data storage can be devastating enough, but losing your only backups could be extremely detrimental to any business.

✓ **Proactively monitor your equipment and data**

Maintain Your System. One of the most important ways to avoid disaster is by maintaining the security of your network. While fires, floods, theft and natural disasters are certainly a threat, you are much more likely to experience downtime and data loss due to a virus, worm or hacker attack. That's why it's critical to keep your network patched, secure and up-to-date. Additionally, monitor hardware for deterioration and software for corruption. This is another overlooked threat that can wipe you out. Make sure you replace or repair aging software or hardware to avoid this problem

✓ **Develop Disaster Recovery Plan**

The primary objective of a Disaster Recovery plan (a.k.a. Business Continuity plan) is the description of how an organization has to deal with potential natural or human-induced disasters. The disaster recovery plan steps that every enterprise incorporates as part of business management includes the guidelines and procedures to be undertaken to effectively respond to and recover from disaster recovery scenarios, which adversely impacts information systems and business operations. Plan steps that are well-constructed and implemented will enable organizations to minimize the effects of the disaster and resume mission-critical functions quickly.

✓ **Have a communications Plan**

If something should happen where employees couldn't access your office, e-mail or use the phones, how should they communicate with you? Make sure your plan includes this information including MULTIPLE communications methods.

✓ **Foolproof your Disaster Recovery Plan**

A study conducted in October 2007 by Forrester Research and the Disaster Recovery Journal found that 50 percent of companies test their disaster recovery plan just once a year, while 14 percent never test. If you are going to go through the trouble of setting up a plan, then at least hire an IT pro to run a test once a month to make sure your backups are working and your system is secure. After all, the worst time to test your parachute is AFTER you've jumped out of the plane.