

Disaster Recovery – IT VOAD – 1/15/2008

Perry Christensen



The importance of hardware and Software in a Disaster Recovery Plan:

- “A Company that experiences a computer outage lasting more than 10 days will never fully recover financially. 50 percent will be out of business within five years.”
- An estimated 25 percent of businesses do not reopen following a major disaster
- 70 percent of small firms that experience a major data loss go out of business within a year.
- Of companies experiencing catastrophic data loss: 43% of companies never reopened and 51% of companies closed within 2 years
- 80% of companies that do not recover from a disaster within one month are likely to go out of business.
- 75% of companies without business continuity plans fail within three years of a disaster
- Companies that aren't able to resume operations within ten days (of a disaster hit) are not likely to survive.
- Of those businesses that experience a disaster and have no emergency plan, 43 percent never reopen; of those that do reopen, only 29 percent are still operating two years later.

Source: Score.org http://www.score.org/pdf/HP_Download_ImpactofDisaster.pdf

Disaster Recovery, the process an organization uses to recover access to their data, software and hardware to resume normal and critical business functions after a disaster, is part of a larger process called **Business Continuity Planning** .

Both are critical to ensure your organization can respond to the community in times of disaster. Let's be honest, creating a disaster recovery plan (DRP) or an even more comprehensive business continuity plan (BCP) takes a lot of work and is often so daunting a task that most of us put it off. Experience has taught me that the best way to tackle this humongous task is to take a small portion and work on it. It is like the joke about eating an elephant one byte at a time.

Here are five small tasks that you can undertake and by documenting them begin to create a disaster recovery plan for your data, software, and hardware.

Install and use antivirus software:

Make sure you have a reliable highly rated antivirus program on each computer and server.

You must use and keep definitions up to date.

Make sure everyone runs the virus scan on a regular basis.

Backup your data – keep a copy off site:

Tape backup:

Pros: Currently the most robust method; Easy to maintain and store off-site

Cons: Expensive

USB hard drives:

Pros: Inexpensive; 2.5” drive can be stored in a safety deposit box

Cons: Easily damaged, must manually plug in the device, Data may not be encrypted

USB Flash Drives:

Pros: Easy to use; small; Capacity is increasing all the time

Cons: Easy to lose

Online back-up:

Pros: Easy to use

Cons: Slow; Expensive; stability of provider may be an issue

Test your backups every so often; most companies only find out that they have a bad backup when they are trying to restore important data.

Backup your installation CDs – keep the original copy onsite:

Don't forget to document your registration keys

Sharing agreements for computers with at least one other organization:

Seek out compatible organizations that are in a different location. Consider for profit partners.

In an emergency using your data on another computer may allow you to continue your operation.

Require and use strong passwords on each of your computers:

An ounce of Prevention is worth a pound of cure.

Check your password = <http://www.microsoft.com/protect/yourself/password/checker.msp>

If you will start doing these five things you will have taken a large step in creating a positive response to disasters both large and small. By documenting where backups will be stored and who is responsible for these activities. You will begin the process of creating a disaster recovery plan.

TTS offers a free 1 hour evaluation of your existing network at no cost to you. An analysis of your network, servers, workstations, and readiness for disaster can be addressed in this evaluation. Call or visit our website to arrange an evaluation.