

May 17, 2007

How well are you prepared for an information & technology disaster?

*by Robin Wheaton,
IAAM State Director and chairman of the Technology Committee*

Imagine yourself conducting business as usual when suddenly a fire erupts completely destroying your office or you are stormed by the authorities with a warrant to seize certain files and all of your data processing equipment. Now imagine yourself a few hours later wondering:

What just happened?

I have nothing, absolutely nothing

What am I going to do?

How prepared would you be for such event?

Here are some suggestions on being prepared for such a disaster

Keep an offsite backup preferably in the form of external hard drives you would rotate each day. These drives are inexpensive. Look for with USB 2.0 drives or better yet, the latest eSata backup drives which are 10x faster than traditional USB 2.0 hard drives. Prices range from \$ 150 on up. If you choose an eSata drive, most computers will require an eSata interface card which costs \$40 on up. Note: You will need at least 2 drives for the best protection because you will be taking one home with you each night. For backup software, you can use Window's built in backup software or better yet, programs such as PC Backup by Stompsoft or Backup Exec will provide for more sophisticated backups that include data from all network connected workstations.

Tape drives are nice, but in a complete disaster, you better have another tape drive kept off site to install in a new machine to restore your data which hopefully was also kept off site.

Keep in mind; you can replace your computers quickly, but your data is so vital to getting back on line the fastest.

Keep an onsite and offsite printed record of:

1. Contact information for your trusted computer/network support technician

2. User login names & passwords for each computer as well as the network file server. Be sure that you know the administrative password for every computer which is important for access upon restoring your data.
3. File server user account settings, security settings, internet provider account info, printer definitions, file sharing structure and drive mappings for shared access.
4. Email settings for each user
5. Remote access codes (PcAnywhere, GoToMyPC, LogMeIn, etc.)
6. Quickbooks client data login information
7. Printout of your firm contact information (Outlook)
8. Keep payroll check clients signature cards off site
9. Keep your software CD's and all computer software CD's offsite. It works out very nice to organize your CD's in a music CD binder
10. Tech support numbers for all software vendors

#