

Disaster Avoidance Planning



Elizabeth M. Smith
President
Technology Services Group, Inc.

In the wake of the dreadful hurricanes of the last two seasons, taking a long look at your information security and disaster planning processes may be very prudent. It goes without saying that disaster avoidance is much preferable than disaster recovery. Resources invested in disaster avoidance garner a much higher return than resources spent recovering from a disaster.

Surge protectors and uninterruptible power supplies (UPS) help protect systems against power related problems. Firewalls, anti-virus and anti-spam applications and security policies are critical for protecting information assets from the ever-increasing threats of malicious human generated data losses. Frequent, routine data backups are generally adequate insurance against accidentally deleted files, hard drive failure or data corruption. But for a major weather event, flood, fire or other catastrophic occurrence, you need a well-considered plan for securing and recovering the information and systems necessary to conduct your business.

How long has it been since you did a thorough audit of the information redundancy, backup and recovery systems of your company, or even your critical personal information for that matter? For most businesses, the most valuable assets are residing somewhere on a computer hard drive. How long can your business survive without access to certain systems and information? If the answer is shorter than the several days required to obtain, rebuild and reinstall systems and archived data, then you need to make sure your information security processes provide for system redundancies in secure and offsite locations in such a way that they can be “plug-and-play” somewhere else should disaster strike your business location.

Have you audited your data and backup configurations to ensure that all data is in fact being backed up? Are database files closed during backup routines? If not, do you have proper software agent modules for your backup application that are able to properly replicate open files? What about local drives of employee laptops? Are important files stored there? Is there a process in place to audit local folders for updated, essential data files? Have you performed routine test restores of data to ensure backup media are still good? Do you have multiple copies of backup software in several locations so that you can quickly install the application required to restore data on another system? Is your tape drive technology such that you could obtain a compatible one immediately should yours become non-functional, or is it so archaic (or proprietary) as to make your backup media unusable in the immediate term?

If your responses to some of these questions do not leave you feeling confident, here are a few tips that may help:

1. A good way to archive critical data is to burn archival CDs or DVDs periodically and routinely in addition to your tape backup systems. Data can be retrieved from these archives on almost any PC or laptop in an emergency.
2. Run head-cleaning tapes routinely on tape drives and monthly (or more frequently) test restores on randomly selected files to make sure data can be retrieved.
3. Archive static data onto DVD or CD, make copies and store in several off-site locations. Since this is relatively non-changing data, you don't have to swap these out frequently, as you do with your nightly backup media. (Another option is to mirror the data to a hard drive that is stored in an off-site vault.)

4. Inventory and Document:

a. Identify your mission critical data - client contacts/address books, financial databases, personnel databases, e-mail - what else? Then document where this data is stored on your network, the hardware and software system requirements, where the installation software is, the serial numbers and vendor contact information. How and where can you quickly obtain replacement systems that meet the technical requirements for running these mission critical applications? Store this information securely offsite.

b. Computer and network systems - LAN architecture, configuration and diagrams, hardware configurations and serial numbers, software version and serial and/or license numbers, vendor information and what systems support which services. Store this information securely offsite.

c. Server administrative login IDs and passwords including any third party or remote e-mail and Internet domain hosting administrative login credentials. Store this information securely offsite.

5. Need to copy some of this documentation offsite in a hurry? Secure it with a password (in Microsoft Word[®], WordPerfect[®]) and e-mail it to your personal account if you have one (i.e. Comcast[®], Earthlink[®], AOL[®], Sprint[®], etc.).

6. Review the backup job configuration and compare to data repositories. Confirm that all data identified as mission-critical and essential is included in backups. Make sure new drives, folders, etc. are included in the backup. Check for exclusion options in the job configuration to insure erroneous settings are not excluding the backup of important data.

7. Have your IT staff configure laptops so that changed files in data folders are mirrored to server drives upon network login or at other specified times.

8. Test UPS devices on servers and other essential systems to make sure they function properly and provide enough battery power.

9. Investigate backup applications that have immediate disaster recovery capabilities that allow you to boot from a removable drive, recognize the tape drive and restore directly.

10. Interview vendors of mission-critical systems regarding disaster recovery services they may offer.

11. Investigate options for humidity, temperature and water controls/gauges as well as UPS and other systems gauges for computer rooms that can notify someone of alert situations.

12. What is the plan to remain in contact with your key IT staff in the event of communications systems failures? In the event of a major hurricane where they will need to provide for their family's safety?

In summary, make sure your data protection and recovery plans and processes are commensurate with the value of the information to the ongoing operation of your business.