In Case of a Crash ... Computer Backups

by Carol Ann Quinsey, RHIA, CHPS

If you ever experience significant problems with—or the outright death of—your computer's hard drive, you will most likely suddenly remember how much material you saved in assorted folders that you did not back up. With luck, friends in your information technology department may be able to help you retrieve critical documents such as work in progress. But some documents may simply be lost to you.

While most of us know we need to back up our computers, few of us actually get around to it. Whether the loss is personal or professional data, protecting information on your computers can save time, pain, and frustration in the event of a crash or other problem. Backing up your data at home is just as important as doing so at work—and even less likely to be carried out regularly.

First Line of Defense: Archives and E-Mail

There may be backup options available through your work for archiving copies of important files. These systems create duplicate files in a second location apart from your hard drive. E-mail is often stored on separate servers that may not be involved in a hard drive failure. Thus you may be able to retrieve documents that were originally attached to e-mail messages. This will not help you recover everything, but it may take care of part of the dilemma.

Choosing the Right Backup System

There are many options commercially available for backing up the content of your computer. Some software requires you to drag and drop files onto a recordable CD at designated intervals. Some backup systems are automatic and run in the background once the initial set-up is complete. You must determine exactly what kind of backup system will work best for you.

One of the decisions to make in determining your backup process is whether you want a full or incremental backup. There are pros and cons to both methods, and software you purchase must be able to accommodate your preference.

Full or "archival" backup usually involves duplicating everything on the hard drive (including operating systems and utilities) to your chosen backup media. Full backups can be very lengthy and use considerable resources.

Incremental backup targets only files that have changed since the last backup. This method may be preferred as it uses fewer resources by not backing up files that have not changed since the last backup.

Other necessary decisions fall into several categories: media, software, reliance on software embedded in the computer's operating system, and use of Internet backup services. Unless you can be counted on to remember to routinely archive individual documents, an automated backup process will probably work best.

Regardless of which type of backup you choose, the most important factor is that the backup is routinely scheduled and carried out. This will be more likely to happen if it does not require a lot of effort.

Your Backup Plan

Your backup plan should include where and how backups will be stored. Backups will be useless if they are destroyed in a widespread disaster such as a house fire. You should consider storing backups someplace other than near your computer. Alternatives include such simple options as a fireproof container or file cabinet. You may also choose to store your backups off-site in a secure location.

Choices and costs of backup media vary widely. You can back up to recordable CDs, DVDs, or other optical media. You can use Zip or Jaz drives. You can use tape drives. Even floppy diskettes may serve you well if all you want to do is back up a few small but critical documents or spreadsheets.

If you cannot realistically use CDs, DVDs, or other such systems due to limitations of cost or file size, there are Internet services available that offer backup protection. Such services may also prove advantageous to "road warriors" or those who want to be able to access critical data or files from multiple locations. These services store copies of your files on the Web using servers protected by firewalls and uninterrupted power supplies. Internet backup services vary widely in price and capacity.

Testing, Testing…

One last step is easily overlooked. Remember to verify periodically that your backup procedures are working properly. You do not want to discover that your files and documents were not really backed up after you have had a system failure and are trying to restore them.

References

Amatayakul, Margret, Steven Lazarus, Tom Walsh, and Carolyn Hartley. *Handbook for HIPAA Security Implementation*. Chicago: AMA Press, 2004, p. 60–61.

Baker, Tracy. "After the Disaster." *Smart Computing* 14, no. 10 (2003): 64–66.

Baker, Tracy. "It's the Software: All about Backup Utilities." *Smart Computing* 14, no. 10 (2003): 57–59.

Hodge, Brian. "There's More Than One Kind of Backup?" *Smart Computing* 14, no. 10 (2003): 54–55.

Krutz, Ronald, and Russell Dean Vines. *The CISSP Prep Guide: Gold Edition*. Indianapolis: Wiley Publishing, 2003, 93–97.

Scapicchio, Mark. "Alternative Backup Strategies." *Smart Computing* 14, no. 10 (2003): 67–69.

Scapicchio, Mark. "Back up That Data: Bad Things Happen to Good Files." *Smart Computing* 14, no. 10 (2003): 60–62.

Segan, Sacha. "Play It Safe: Why You Should Make Regular Backups." *Smart Computing* 14, no. 10 (2003): 52–53.

Carol Ann Quinsey *(carol.quinsey@ahima.org) is a professional practice manager at AHIMA.*

Article citation:
Quinsey, Carol Ann. "In Case of a Crash…Computer Backups." *Journal of AHIMA* 75, no.5 (May 2004): 60-61.