

General PC Data Protection - Overview

Why do I need a data protection plan?

The essential task of data protection is to duplicate, and thus safeguard, your data. This process should be accomplished across multiple devices and/or media to be most effective. Each added redundancy increases assurance that the data you need can be made available if the original source of data becomes inaccessible. Your protection strategy should cover the full range of availability. From the occasional need for a “good” copy of a single corrupted file, to the loss of all files due to hard-drive failure or natural disaster.

Think of the time you spend in the process of creating, refining and organizing your personal computer information. As you work in a digital medium, all of this labor is saved in complex patterns of zeros and ones to computer files stored on hard-drive. These files can be easily retrieved; updated, relocated... it's a happy digital world until that hard-drive fails. This failure is not a distant possibility, but an inevitability. All hard drives, no matter how expensive and well designed, will fail. Your personal user files and the installed programs and data that help create them, can be gone in an instant, without warning. As traumatic as this scenario sounds, it is one you must contemplate in order to build a solid data protection strategy.

Without Data Protection....

If your Programs drive fails: you will need to manually re-install your Operating System, re-do its customizations, then re-install all your application programs. This task could be multi-day. With an image backup DP strategy, your complete restore to the replacement drive should take little more than an hour.

If your User-Files drive fails: your user-created personal files are in serious jeopardy of being irretrievably lost. The cost for drive data-recovery (from a professional service with “clean room”) is in the thousands of dollars and there is no guaranty of success! With a drive-to-drive or tape DP backup strategy, your complete restore to the replacement drive should take no more than a few hours.

How much duplication is enough?

For protecting your Operating System and Programs, two levels of duplication are advised. User-created files should have three levels of duplication, on different devices or media, as insurance in case one level fails. These levels represent: session, standard, and off-site duplication, with the last as emergency security. The off-site media should be kept away from your home at an office site, a friend's house, or even a safe deposit box. If local fire, etc., wipes out your computer and data – this is your ace to rebuild.

What basic tools are recommended?

- DVD recordable device and “burn” software.
- External (USB, Firewire, or SATA) hard-drive or USB flash drive.
- Imaging, traditional backup, and/or Sync software (See addendum for details).
- Backup Log: hardcopy record of all backup/restore operations, indicating date, media type, and relevant notes. Documenting to visible log acts as both reference and reminder. Place this on a clipboard at your workstation, within view.

PROTECTING YOUR DATA

The following solutions are presented, sorted by cost, from least to most expensive. A “tools” list is included in each solution, but without recommendation for any particular manufacturer’s hardware or software – that is left up to you.

Solution1 - Minimal

Tools: Synchronization software, USB flash-drive, DVD burner and software (see Addendum).

This approach is designed only to protect user-created files. As a minimum data protection strategy your operating system and programs files would not be protected by this plan and therefore could be lost. In such case you would need to re-install your OS and all application programs, or build anew from your manufacturer’s supplied installation media. That being said, lets explore how this solution protects your personal files and data.

Organizing your personal files via folder hierarchy structures your personal information, making it easier to find and maintain. Naming your created files with a version# suffix is another good practice that helps insure more uniquely meaningful filenames. Good organization will help your day-to-day computing and also simplify backup. If all your personal files and data, for example, are kept in sub-folders off the ***My Documents*** parent or main folder, then your backup “source” is obvious. Spend some time to organize both your personal files and the data files that applications use to present personal information to you. If you use Outlook, then its “.pst” file should be located under ***My Documents*** or other source name. If you use a PIM, then its data file(s) should also be located within the source parent folder. Once your organization is ready, you are ready for effective personal data protection.

Synchronization software is designed to automatically duplicate data across multiple devices, in this case from a designated folder on your computer’s hard-drive to a designated folder on a connected USB flash-drive. Via synchronization software of choice, setup a one-way sync from your hard-drive (source) folder to (target) backup folder on your USB flash. Once the sync is in place any new or changed source files are automatically copied to the USB target. This copy “propagation” process can be immediate or it can be delayed until logout/shutdown. Many user’s find the latter advantageous as they have until the end of the current session to use the prior session’s

backup as “un-do” resource. When ready, simply click shutdown and walk away as the sync automatically propagates all of the current session’s changes before running final shutdown.

When near capacity, burn the contents of your USB sync folder to DVD then clear its contents and re-sync anew. Periodically rotate burned DVDs to your off-site storage location. This will provide three levels of duplication for your user-created files.

Note: modern sync software is capable of sophisticated multi-computer service. One option is to sync both a notebook and desktop computer from the same USB hard-drive or flash. There are many sync combinations possible, so carefully check out your software’s capabilities before purchase. Also note that USB flash-drives do have a life span and should not be used exclusively as a backup archive; they are only designed (conservatively) for about 100,000 erase cycles!

Solution2 - Moderate

Tools: Sync software, Image backup software, external USB hard-drive, DVD burner and software (see Addendum).

For just a little more cost and effort you can safeguard all of your computer’s files. The steps detailed in Solution-1 still apply except that you will be syncing to a designated folder on a USB hard-drive. Your sync software will auto-copy, at the end of each session, all newly created or modified files from their original locations to a designated folder on the USB hard-drive. When this folder is near DVD capacity, burn that folder’s files, then clear its contents to repeat the process with new data. Use imaging software to “clone” your O/S and Programs drive to a different folder on the same external USB hard-drive. Re-image after any significant updates to your OS or Programs. Periodically burn a set of DVDs from the USB image files. Rotate burned DVDs to your off-site storage location.

Solution3 – Optimal (Single Drive)

Tools: Sync, Image, and traditional backup software, USB/Firewire DAT or DLT tape, Blu-Ray DVD external drive + blank media, or hot-swap chassis + prepared drives (see Addendum).

A single drive-unit can be effective for the full range of data protection as long as its media is removable. Tape systems, once dominant, are still excellent backup/restore solutions. They have the advantage of inexpensive media and mobility. A single USB DAT/DLT backup can service multiple computers. The disadvantages are relatively slow performance compared to hard-disk based systems, unless you invest in high-end DLT that can cost thousands of dollars. High-capacity DVD, with Blu-Ray at the lead, has similar performance to standard tape, can also be mobile, but has equivalent-capacity media priced at twice that of tape. One advantage to Blu-Ray is that a single device can burn media from CD-R to BD-RE. Additionally, the price for Blu-Ray devices and

media should continue to fall. A general disadvantage to single-drive tape/DVD systems is that, because of their relatively smaller capacity, larger backup jobs will be “spanned” across multiple media, requiring periodic manual eject and load.

A third removable option is hard-drive chassis, where a hot-swappable drive is inserted into a designated USB/Firewire or ATA enclosure, allowing for high-speed backup and restore. Sync software could be used to effectively “mirror” files from your user-files drive to such an enclosure, providing your second level of data protection. A big advantage to any removable media is that it greatly simplifies “off-site” backup, as you can periodically rotate out a media-set for this purpose (see Addendum). You will still need both imaging and traditional backup software for complete computer protection, storing the image-sets to removable media. This DP approach can service multiple computers but is moderately expensive.

Addendum

Below is a chart comparing various attributes of the media covered in this overview. I have tried to come up with “real world” statistics that could provide a solid basis for judgment. Capacity and speed ratings are for a single device without data compression.

	<i>Capacity</i>	<i>Cost per GB</i>	<i>Backup Speed</i>	<i>Data Retention</i>
DLT	160gb	25 cents	40gb per hour	20 years
SSD	128gb	200 cents	100+ gb per hour	10 years
Blu-Ray	50gb	55 cents	20gb per hour	5 years
DAT	30gb	50 cents	10gb per hour	10 years
Flash	16gb	250 cents	50+ gb per hour	10 years
DVD+r	4gb	10 cents	20gb per hour	5 years
Hard-drive	1tb	15 cents	100+ gb per hour	*(see notes)

* modern large-capacity hard drives are designed primarily to store data while spinning, though If used in periodic backup rotation they can provide many years of service via USB enclosure, etc. Drive backup to SSD is preferred, especially as off-sight media, because of superior data retention “life span”.

Using Both Imaging and Traditional Backup Software

Image backup is sector-by-sector, effectively enabling an exact “clone” of your hard-drive. While this provides the most reliable means of copying and restoring an OS drive it does have the limitation of insisting that the restore target boot under similar hardware, especially motherboard/chipset. It is also unaware of the file “archive” bit which is essential to traditional backup software applications.

Traditional backup is file-by-file, utilizing the “archive” bit and other file-based info to check each file’s backup status. The O/S drive requires both imaging and traditional backup

strategies to insure its complete data protection. The first provides a sector-by-sector base, while the second adds the ability to include modified files to insure the latest customizations and backup catalog are restored atop the clone. Other drives can usually be protected by traditional backup software alone.

The three basic types of backup/restore offered by traditional software.

1. Full: backup of all selected files (often targeting an entire drive).
2. Differential: backup of all selected files that have been modified or newly added since the last Full.
3. Incremental: backup of all selected files that have been modified or newly added since the last Full or Incremental.

Software Restore and Copy Protection

Copy protection mechanisms should only pose potential problems in restore of the O/S (Programs) drive.

BEST: USB Master-dongle, such as used by VSL. This one (Syncrosoft) USB dongle can authorize all compliant manufacturers software products. When invoked, these applications will look to the USB dongle for access authorization. In the event of OS/Programs drive failure, an image of this drive can be restored to a new drive and all the residing master-dongle apps should function perfectly without need for software re-installation.

ACCEPTABLE: Challenge/Response variant of "signature" based copy protection, such as deployed by Spectrasonics. With this method the "Response" code is the signature authorizer, based on the Challenge code issued during software install. This approach allows for cloned applications to function perfectly on their newly imaged drive, as long as the Challenge/Response procedure alone is redone.

WORST: Hard-drive "signature" (as used by "brand X"). This creates a unique reference from low-level hard-drive info concatenated with application serial# to create an authorization reference for each application. The purpose of this approach is to prevent software piracy. Unfortunately, it severely cripples cloning/imaging as a legitimate means of data protection for fully licensed users. In the event of OS&Programs drive failure, an image of this drive when restored to a new drive will disallow access to any "signature" based application. The user will be forced to uninstall and re-install such applications. A more humane, "lite", version of this copy protection is used by Native Instruments, where application serial# is combined with hardware component info, such as CPU, to provide a unique reference. Simple drive replacement should not be a problem here, as only major changes to low-level hardware require full re-authorization.

John O'Mahoney

DAW-solo.com © 2008

V1.11 (12/01/08)

Disclaimer: I offer this guide as a free service to the community. Use it at your own risk. I make no guarantee or warranty about its results, though I have made every effort to carefully research its subject material.