

Midwest Tech Group Backup Solutions Guide

Whether you have no idea what backups are or if you are an experienced IT professional, this guide will help you consider the options you have in safeguarding data on your computer systems. You will also learn about strategies to protect your data and the details that you need to plan recovery from an unforeseen failure of your computer system. A good backup plan can be your insurance policy against disaster.

What is the objective of a backup?

To facilitate restoration of data and computing capability to a computer that suffers any degree of data loss from one file to an entire array of disk storage

Backup copies of files are made so that they can be re-created in the event of data loss due to disk failure, computer hardware failure, destruction of computing equipment (lightening, flooding, fire), virus or hacker attack, human error and theft. Restoring data from backups is not just a time saver; restoring original work might be impossible to re-create. Imagine an author writing a chapter in a book. Let's say that chapter two, written two weeks ago is lost. That author might come close to re-writing the chapter, but the original text could probably never be duplicated no matter how much time was spent.

No one will disagree that backups of data are necessary for protection against data loss.

What choices do I have for backup

There are many ways to backup or *copy* data. One of the easiest ways is to click and drag a copy of a file to another location on the system's disk drive. Other strategies use software to manage selection and copying of data in bundles called backup sets. Data can be stored locally (on the same computer or within the same office) or remotely (taking a copy home with you for example).

The decision of which backup strategy to use is determined by the type of disaster you wish to avoid and how quickly you require your systems to be operational following the disaster. For the average user, being able to restore a system in an hour or two following the loss of a hard drive would be quite acceptable.

The combinations of backup configurations are infinite. At one extreme would be redundant systems replicating themselves across wide geographic areas using redundant hardware, and emergency power generation equipment. The other extreme might be the backup copies that Microsoft Word makes as you are editing a document.

The criteria you should use to make your selection for a backup method are:

- Cost
- Recovery time
- Time required to perform backup
- Time required to launch backup or load media
- Location of backup data (local or remote)
- Media format (Tape, disk, zip drive, etc)
- Level of protection (entire system or just critical files)

Cost of "Down Time"

To help you evaluate how much weight you should give the criteria listed above, try to quantify how much "down time" costs you. If your computer is used for taking orders or processing information that customers wait for, down time can be expensive. Some larger companies measure downtime in tens of thousands of dollars per minute. Most of us don't have this level of liability in our computing environments but down time does have its cost.

Ask yourself these questions:

- If a file is lost, is your solution to simply re-create it?
- If your computer disk drive fails, will you personally have to replace the disk or computer yourself?
- How much is your time worth?
- How much would it cost to have one of your staff restore the failed computer?
- How much would it cost to hire a data recovery expert to recover files on a damaged hard drive?
- How accessible is your backup data?
- Is it on site? Do you have to drive to get it?
- Is the backup data up to date?

The key is that your cost of downtime determines what your recovery time should be. Keep this in mind when you are looking at backup solutions.

Backup Basics

When backing up data, there are three things to consider:

1. What is to be backed up
2. Method of transfer (Backup)
3. Destination of backup data (where it is stored)

Step one is to decide what data you wish to back up. Any computer based data that has value *or* provides the function for processing that data should be backed up. This includes the operating system (Windows), programs like Word or Excel and data files (documents, e-mail, database data, etc.). Your backup/recovery procedure must be capable of re-creating the computing environment as well as the application data. If your system disk were to fail, you would lose the Windows environment, all your programs and any data used by those programs.

Many computers ship with an emergency recovery disk that can be used to re-create the system disk in the event of a failure. This means that the computer can be restored to its original, as purchased state. Any programs that you installed after purchase, any updates to Windows, any data that you had on your disk prior to the failure would not be restored by using the emergency recovery disk alone. You would have to have additional backups to recover optional software and data. Midwest Tech Group does not recommend depending on the recovery disks shipped with a PC.

Step two, the method of transfer, is the way in which you will capture the data to be backed up. Will you simply copy files or use a backup program to collect your data into a "backup set". Some backup programs can be configured to run automatically at pre-set times. Automatic programs are the best because people generally forget to run their backup procedures on a regular basis.

The third step is to decide where the backup data should be stored. Copying to another disk or media that stays at the same location with the computer being backed up adds risk to data security. If disaster or theft hits the office where the computer and the backup data are, both could be lost.

Backup Strategies

Working smart when backing up your data can mean the difference between a plan that is reasonable and will be easy to maintain and a plan that you won't execute because it is an inconvenience. Backup strategies can be grouped into three types:

- Image
- Full / Normal
- Differential / Incremental

The image backup is the best way to protect your computer against a major disk failure. Special software is used to create an exact copy of all of the programs and data on your hard drive. In the event of a disk failure, the faulty disk is replaced, and the backup "image" is restored to the replacement disk. This solution is thorough but usually takes hours and requires attention by someone to complete. There are other drawbacks including hardware compatibility issues if restoring to a new computer with a different hardware configuration. The advantage of an image backup is that everything can be restored – no need to re-install windows or other programs.

Some imaging software can create an exact copy of the system disk onto another disk. It still takes a while to perform the "image" process but the system can be restored to it's backed up state in the amount of time it takes to replace the hard drive in the computer.

A "full" backup has varying definitions depending on vendors of backup software. In the world of Microsoft Windows, it is called a "normal" backup. The term simply means that all files selected for backup will be copied regardless of whether they have been backed up before. This will become clear with the explanation of the incremental backup.

The "Incremental" or "Differential" methods copy data modified or created after the last backup. An incremental backup will safeguard files created or changed since the last "Full" or "Incremental" backup (An image backup would qualify as a "Full" Backup). The objective is to make copies of only that data that has been added or has been changed since the last backup operation. In the case of an image backup, all files modified or added since that backup could be used to restore the system disk to it's pre-failure state by restoring the "image" and then adding the elements from the incremental backup(s).

A backup of only data files protects against loss of things like Microsoft Word documents, spreadsheets, e-mail messages and contact information. If data is lost, it can be replaced from the standard backup. If the system disk is lost, however, Windows and all related programs must be restored first.

What should I do?

The best way to backup a computer is a combination of strategies: Image and differential backups. Having an image backup available is great but what if it is a month old? The differential backup data is used to bring the incremental backup up to date. An image backup should be made any time there is a major change to the operating system (Windows). Following this change, differential backups save any data that has changed since a point in time or a previous backup. Incremental backups can be used as well, backing up data changed since the last backup.

Choose your backup destination:

Your data needs to be stored somewhere and you have many choices:

Local backup: using the hard drive on your computer to make a duplicate copy of a file already on the disk. Microsoft Word uses this method to keep copies of documents as they are being worked on.

Floppy disk: Floppy disks are becoming remnants of the past. Many computers today aren't even built to include floppy drives. They only hold 1.4 MB of data and can be used to save only the smallest of files. The floppy disk is not a viable backup solution in today's environment.

Network disk: The target for your data can be a disk on another computer within your network. This provides safety for your data in the event that something happens to your computer. Your data will be kept safely on the other computer. If the local network is damaged (lightening, power surge, etc.) you run the risk of losing data because both the original and the backup could be lost.

Removable disk: Data stored on a removable disk can be carried away from the local computer location and stored "off site". This method provides additional security in the event that all data is lost at the computer site. Restoring from offsite media presents an additional problem because someone must go get it in order to restore from it.

Magnetic Tape: Still a standard in data storage, magnetic tape provides a way to copy large amounts of data and to store multiple versions of backups. Tape media can be expensive and restoring files from a tape can be involved if the tapes are stored off site. Restoration can also be time consuming if you are trying to restore only one file because the information on the tape cannot be accessed directly as with disk based storage. Tape media can easily be stored offsite. Offsite storage can be costly if a courier service is used.

USB memory device: A small, pack of gum sized device can be used to store or transfer data files. It is totally solid state so it is fast. Storage capacities average about 150MB per device. They are handy and can be used to "take the data with you". These type of devices can cause security issues for companies trying to control how data might be removed from their offices. Keep this in mind if you are developing security policies at your company.

CD/DVD: This type of media tends to be slower than others. Some recording formats are not compatible with others and reliability can be questionable. Large backups can be awkward when many DVD's or CD's start stacking up. A CD can hold about 640 MB while a DVD can hold about 4 GB. Multiple DVD's would have to be used to backup the average hard drive of today.

OnLine Backup: Backups are performed using "client" software on your computer to transfer data to a server located in a secure location accessible through the internet. Storage is offsite thus adding the security of offsite storage without costs of transporting tapes or other media. Backups are set up once and performed automatically after that. Restoring files is easy and multiple versions of files are instantly available. Online backup satisfies the current and anticipated compliance requirements, such as Sarbanes-Oxley, SEC 17a-4, HIPAA and other Federal regulations.

Backup Method	Additional Hardware Cost	Offsite Storage Possible	Automatic Backup	Time For recovery	Capacity
Local Computer	0	No	Yes	Fast	Large
Disk to disk	\$100	No	Yes	Fast	Large
Removable Disk	\$200	Yes	No	Mount disk	Large
Tape	\$500-2000	Yes	No	Slower to access	Large (Price Dependent)
CD/DVD	\$100	Yes	No	Slower than disk	Limited
USB Memory Device	\$50	Yes	No	Fast	Limited
Online Backup	0	Yes	Yes	Limited by Internet connection speed	1 GB

Procedural issues

A good backup plan will anticipate the types of failures that could be expected in a computing environment. Downtime should be calculated to determine how quickly data can be restored and how much work would be lost between backups. The key factors to consider are:

- How often should backups be performed?
- How to verify that backups are done
- Ensure that new files are included in backup
- Restore files periodically to test procedures

Services

To make sure that data at your site is secure, consider outside resources to help you:

- On site evaluation and planning
- Midwest Tech Group's Remote support center
- Midwest Tech Group's backup consultation
- Off site data storage
- Online Backup service