

Backing IT Up



A guide from Chiltern Business Computing Ltd

Every business depends on its computer systems to some degree or other. For many, systems are vital to business survival and success.

This brief guide discusses the necessity for backing up computer systems, why it is important, and the criteria for choosing backup methods and frequency. For further information or to discuss your particular needs, please contact Jim Symington – contact details are below.

- **What is backup?**
- **Can't I just copy the files?**
- **Why is backup important?**
- **What are the threats?**
- **Key backup system criteria**
- **Backup systems**
 - **On-line**
 - **Local**
- **How often should you back up?**
- **Types of backup**
- **What is Grandfather, Father, Son?**
- **I back up regularly - what else should I do?**

What is backup?

People often talk about the importance of backup, but what is it? In simple terms, it is keeping a copy of what's on your computer so you can get it back if something goes wrong.

Can't I just copy the files?

You may wonder why you might need to use backup software, rather than just copying the files. Backup is a form of copying, but there are limitations and cautions with simple file copying:

- You may miss files – it is less easy to set up an automatic routine
- Open files cannot be copied
- It may not all fit on one CD or DVD, and you have to manually split the copy process.
- You cannot use tape as backup device
- Broadly speaking, copying doesn't work unattended
- You cannot back up your system (as opposed to your data) by copying. (You cannot satisfactorily copy system registry and start-up files.)

Why is backup important?

There is hardly a business that does not use computers. And some depend on systems to function at all. Loss of systems or data will cause one or more of the following:

1. **Lost time** - getting the system going again and recreating data
2. Immediate **loss of revenue** – inability to collect cash
3. Permanent **loss of data**, which can affect everything from accounting to marketing (lost contacts or customer records).
4. **Lost customers**
5. **Extra costs.**

How serious the effect of data loss will be depends on the business and what data has been lost. However, it is a fact that a proportion of companies that suffer major disruption to their systems go bust.

What are the threats?

- 1) **Hardware failure** – your computer or its storage device (normally hard disk) may fail.
- 2) **Error** – you may mistakenly delete, over-write or accidentally corrupt a file.

- 3) **Fire, theft and flood** – your computer or storage device may be stolen or burnt
- 4) **Virus or intrusion** – either may destroy or corrupt data, or damage systems

Key backup criteria

There are many possibilities in backing up systems. You need to make the right choices for you (and you may need more than one method to cover all bases).

The requirements for secure backup are:

- 1) To be held off-site
- 2) To hold different versions – a single backup that you overwrite each time is of limited value. See Grandfather, Father, Son below.
- 3) To be readily accessible when needed.
- 4) To be quick and convenient enough to make, so that it is not an inconvenience to the business.
- 5) To ensure that open files or databases are backed up, so that these do not get accidentally left out of the backup copy. (Will you need to make sure the system is idle at the time you back up?)
- 6) To be robust. Backup that doesn't work correctly and reliably is dangerous – it just gives a false sense of security.
- 7) To be tested. If it doesn't actually work when you come to restore, you may as well not have bothered.

Backup methods

1. **Online backups.** Various providers including specialists and ISPs offer online backup services (i.e. over the internet).

Some points to consider:

- 1) How much are you backing up? Lots of data could be very slow. Remember that most internet connections are broadband ADSL – which means that upload speeds (transfers to the internet) are a fraction of the download speed, which is the nominal speed usually quoted (eg 8Mb).
- 2) How much will it cost? Some providers offer a free service for fairly small amounts of data.

- 3) Does the online service meet the criteria above, eg the ability to hold different versions of the backup?
- 4) You cannot reach your backup if your system cannot access the internet. This could be tricky in some cases, e.g. corruption, virus attack.
- 5) Is the online backup provider well-established? Do they have a good reputation, and will your data be secure?

Remember that online backup cannot help recover your **system** if for example you have hard drive corruption or failure. You will need to have other means for this, perhaps the manufacturer's recovery disk set.

Before using manufacturer's recovery process to restore system to out-of-box state, remember that this will destroy your data – if you need to try to recover that data (perhaps by using a disk recovery service), do NOT run the manufacturer's recovery process as this may irretrievably destroy the data. Having recovered your system and got back online, you will then be able to recover your **data**.

2. Local backups. Backing up to devices attached to your system

The most common options are:

- Disk drive
- Tape Drive
- CD/DVD
- To another system (in which case this too needs to be backed up).

Again, some points to consider:

- 1) How much are you backing up? Will your chosen method cope? Will it all fit on a single tape, disk or whatever media you are using?
- 2) How much time will it take to back up? Can it be set to back up unattended?
- 3) Where will you store off-site copies?
- 4) How many versions of backup will you keep? See Grandfather, Father, Son, below.
- 5) What do you have to install on a fresh system (eg new computer, or after hard drive replacement) in order to be able to access your backup? You need to have copies of any software required for the backup process in a secure, fire-proof place.

- 6) How much will it cost? There may be costs for the backup device itself, backup software required, and media (tapes, CDs, removable drives).
- 7) How robust is the backup media? Careless handling can damage portable disk drives. Memory sticks can be unreliable. Tapes can wear or jam.

How often should you back up?

This question can be turned round to say

- How much work are you prepared to lose?
- and if you lose it, how long will it take you to reinstate it?

The practical answer for most businesses is daily backup, usually done automatically during the night. (In sophisticated business systems, databases may have inbuilt mechanisms enabling you to “Roll-back” transactions if there’s a problem.)

You may wish to take additional backups beyond the routine daily ones if:

- 1) You are installing new software
- 2) Doing upgrades to the system
- 3) Running major processes – eg a Payroll year-end.

It is quite acceptable for *extra* backups for the sorts of purpose above to be done within the system you are working on. You might do this by copying data to a backup folder. After all, if the whole system fails or there is a disaster, you can still go back to the backup from the night before.

Types of backup

If you don’t have too much data, don’t worry about this bit – back it all up every time. However, if you have a lot of data, it may be too time-consuming or expensive to back it all up every run – after all, most of it doesn’t change from day to day. So there are methods of reducing backup volumes to deal with this.

There are three basic types of backup process:

- **Full** – as it says, everything is backed up

- **Differential** – Everything that has changed since the last *Full* or *Incremental* backup
- **Incremental** – Everything that has changed since the last *Full* or *Incremental* backup. You may use a succession of *Incremental* backups between each *Full* backup.

(It is not usual to mix *Differential* and *Incremental* backups in a backup routine.)

- To restore completely from a **Differential** backup, you need the last *Differential* backup AND the last *Full* backup (and all the *Incremental* backups, if there were any in between).
- To restore completely from an **Incremental** backup, you need ALL the *Incremental* backups since the last *Full* backup, and the last *Full* backup itself.

What is Grandfather, Father, Son?

Grandfather, Father, Son is a hierarchy of backups. The purpose of the hierarchy is simple:

If something goes wrong on the system, how long will it be before you notice? Will you have a backup set old enough to restore a sound copy?

- In some cases, you will notice immediately, and therefore last night's backup will get you out of trouble.
- In other cases you may not notice for a week, a month or more, depending on your business routines.
 - For example, you have a key spreadsheet you update every month for the monthly accounts. You come to use it this month, and it won't open. Somehow the file is corrupt. So you need to get back to a copy of the file before it was damaged, perhaps 3 weeks ago.

One standard solution (explained in the context of local backup) is a routine that goes like this:

- **Daily** – Monday to Thursday – Rotate 4 sets of backup media, one for each day

- **Weekly** – every Friday – Rotate 5 sets of backup media – Week 1, Week 2 etc
- **Monthly** – last working day of every month – Rotate 4 sets of backup media – Month 1, Month 2 etc
- **Yearly** – preserve the backup from the last day of the year indefinitely.

The above routine will require 13 sets of media plus one for every year that goes by. It will give you the maximum chance of recovering lost data, whenever the problem occurred.

I back up regularly - what else should I do?

This is actually one of the most important bits. There's little point in having good backups if you can't use them.

Once you have a backup routine, you need to make sure you will be able to use the backups should the worst happen. In making these preparations you should assume that you cannot get at anything at all on your present system, at least to start with. You will therefore need to have available:

- ✓ Printed emergency instructions – e.g. Hardware and software support phone numbers and support website logins, supplier contact details, software installation and option instructions.
- ✓ A Source of replacement hardware (compatible with your original).
- ✓ A Device to read your backups (if you used tape, you will need a suitable drive).
- ✓ Media for reinstalling your backup software (whatever software you used to create the backups).
- ✓ System recovery disk set for your computer(s). Key service packs.
- ✓ Software installation media for your applications.
- ✓ Details of setup and login for your Internet and email services – with these at least you can collect your email from another computer and use the Internet.

If you have any questions arising from this guide, or to discuss the backup needs for your business, please contact:

Jim Symington

Chiltern Business Computing Ltd

Tel: 0845 521 1555

Mob: 07813 080053

Email: Jim@ChilternBusinessComputing.co.uk

Web: www.chilternbusinesscomputing.co.uk

