

Backing Up

Backing up means making a copy in computer terms. There are a number of things that you might want to make a copy of. These include:

- information you have created (documents, spreadsheets, emails etc.) which are referred to as data;
- your operating system (Windows for example, and its settings for your computer or the server);
- and programmes (normally in the form of original disks).

Of these, data backup is normally regarded as the most important, but if you have a server, this may be just as critical.

Backups are essential for everyone. It is simply a matter of good administration and risk management. You can take out insurance against the loss of data/restoration, but in exactly the same way that a fire can destroy paper records, electronic destruction for whatever reason is just as costly and time consuming. However, electronic copying is easy and cheap nowadays.

Associated with backing up data is security. This is a separate issue, but suffice to say that the Data Protection Act applies equally to paper and electronic information. In very simple terms, this means that if you hold information on an individual which enables that individual to be uniquely identified and 'traced', then you must firstly have their permission to have the information and secondly it must be held securely.

There are many circumstances where you need to maintain records for a number of years, including for example records for the Inland Revenue and specific funders. If you keep your information electronically, then you need to maintain copies of that information and it may need to go back 6+ years! The other major reason to take backups is the "what if" scenario. Ask yourself the question "what if specific information was lost". Would it affect your organisation; would it be critical; would you have to close down? Just as importantly, think about what information that might be; for example, accounts, p.a.y.e. details, records against which you are funded etc. Then consider where that information is held; for example, on an individual's machine, on the server, on a memory stick. Then consider the risk attached to holding the information there, for example; a power surge destroying data, malicious attack (from a disgruntled member of staff or a virus), from your technical support (who by accident re-formatted your data drive), fire, flood or theft. This forms a risk assessment which should be part of your organisation's quality processes. You can then address this with a backup and security policy, some of which may need to be included in job descriptions or staff handbooks. You are particularly at risk if you don't have a server.

Focussing on data backup, it is important that whatever system you employ, it works. In order for it to work, you must first ensure that it also doesn't get destroyed (perhaps by the risk you were protecting against). So, to put a backup tape or disk on top of your computer/server defeats the object if there is a theft or a fire! In other words, you need to locate your backup somewhere safe, preferably at a different location.

There are many options when it comes to backing up data and choosing the right one for you will depend on a number of factors which you will need to consider;

- cost of setting it up
- ease of operation
- amount of time the backup takes
- how much data is to be backed up
- amount of staff time involved
- how technical it is

The possible backup options include:

Floppy disk	1.4Mb	becoming rarer – 50p
Zip disc	750Mb	becoming rarer - £7/disk
CD-Recordable	600ishMb	15p/CD
DVD-Recordable	4.7Gb	25p/CD
External hard drives	up to 1Tb (and growing)	£60 for 500Gb USB
Network Attached Storage	up to 1Tb (and growing)	£136 for 500Gb
USB Memory stick	up to 32Gb (and growing)	£35 for 16Gb
Tape	10 – 800Gb	around £20
Online back up services	as much as you want (ish)	£50-£100 p.a.

The commonest backup systems involve using tapes which are reliable, can be done overnight and can hold a reasonably large amount of data. However, they are not necessarily the cheapest option. You can find out greater detail about the different types of backup up and their advantages/disadvantages at:

<http://www.ictHubKnowledgebase.org.uk/backingupyourdata>

For a comprehensive list of backup software to suit all needs and pockets:

http://en.wikipedia.org/wiki/List_of_backup_software

The solution that's right for you is dependent on all the factors previously mentioned and it is their balance which is important (i.e. time/cost/capacity/resources/importance). Virtual Riders can advise you accordingly free of charge. Call 0845 337 2949.

There is no point in having a backup system in place unless you use it: and if you're not there, that someone else does it. This requires a simple and straightforward policy backed up (sic) by a clear procedure.

First of all decide the following:

- What is backed up
- Where it is being backed up to
- Who is in charge of performing backups and verification
- When backup will be run
- Which software will be used to manage the backup process

Write this down and make sure people are aware of it! Create a review period (e.g. every year or whenever a new project is set up for example).

Now create the procedure/protocol. This means determining the frequency of backup, how many prior copies there are and where the backups are stored. The example below (from LASA) uses tapes, but could apply to any media.

- There are four tapes for days of the week - Monday, Wednesday, Thursday and Friday.
- For Tuesdays, there are a further four tapes - for the second Tuesday of the month, the third Tuesday, and so on.
- There are five more tapes, each for the first Tuesday of month - these get overwritten every five months.

This schedule enables the restoration of data from the previous evening or from five months ago as required.

Added to this needs to be a pragmatic approach to where the tapes are stored. For example, the daily and weekly tapes could be stored on site in a fire proof safe, with the monthly tapes being stored off site.

An example protocol can be found at:

<http://www.brightonandhovepct.nhs.uk/healthprofessionals/generalpractice/policies/electronicrec/documents/backuppolicy.doc>

If of course you don't have a server you may need to do little else than make sure that all staff have a copy of their work which they give to you once a week (for example) on a memory stick (£10 for 2Gb will normally suffice).

You may think that all of this is overkill for your organisation. If you think this is the case, just ask yourself what happens if you lose all your data in the next 10 minutes....

Additional information:

<http://www.techsoup.org/toolkits/disasterplan/index.cfm?cg=searchterms&sg=backup>

<http://en.wikipedia.org/wiki/Backup>

<http://www.onlinebackupreviews.com/index.html>

<http://www.volresource.org.uk/samples/ITpolicy.htm>