

Computer Solutions

(Bill Ridgeway)

Telephone: 020 8422 7570

7 Sandringham Crescent, HARROW, HA2 9BW

Email: info@1001solutions.co.uk

Website: 1001solutions.co.uk

Backing-up

The objective of backing-up is to provide a resource from which corrupted or missing files or the whole system may be recovered. The acid test of a good backing-up regime lies in the answer to the question "how much resource can the business afford to put into installing and configuring the computer from scratch and reconstructing data whilst trying to carry on the business?". It is questionable how long a business can continue without access to its customer database, stock inventory, accounting, invoicing, banking, and standard letters. In the longer term consideration should also be given to retaining information required by HM Revenue & Customs (HMRC) for the purposes of personal tax, corporation tax and VAT.

It is commonly argued that it is necessary to back-up only 'user' files from, say, 'My Documents'. Whilst this may include the most important files to the user it is very likely that it may not include all files which may be required later as, unknown to the user, changes occur to files other than user files. These files may be -

user files which, by default or design, may not be saved in a known folder (e.g. 'My documents'). These include the address book, bookmarks, custom dictionaries, downloaded files, emails, faxes, favorites and templates; and

configuration files (generated by software) that may be modified, unknowingly, by the user. These files may be all that is needed to avoid a complete re-installation of software.

It is, therefore, highly recommended to back-up all files on a regular (perhaps weekly) basis.

The term 'back-up' is not fully synonymous with the term 'copy'. Correctly interpreted, backing-up is systematically and routinely taking a copy of files which may be used when the originals become corrupt or missing. However, the term backing-up has come to be popularly used to mean copying (in a less than systematic way) selected files onto, possibly, a limited capacity media. The term 'copy' is more correctly used to mean taking a copy of a selected file(s) perhaps for transfer to another computer or as security in the event of fault occurring when making structural changes to a file in course of development (e.g. spreadsheets, macros). There is, however, a grey area between the use (common parlance and practical) of the two terms.

Selecting a backing-up regime

Backing-up may be done on-line or in-house. It is arguable that the ability to backup and restore may be affected by the loss of either an internet connection or the backing-up media. It is, therefore, argued that using both methods provides a robust backing-up regime. Key points in comparing the two methods include -

On-line backing-up	In-house backing-up
an unknown third party is trusted with responsibility for the security of sensitive information	user retains responsibility for the security of sensitive information
sensitive information may be held on a server abroad	user retains full control of the location of sensitive information
there may be a restriction on the capacity available for backing-up	there should be no problem (if properly planned) with capacity
there may be a restriction on the period of time for which backups may be retained - which may limit usefulness as a means of backing-up historical data	there should be no a restriction (if properly planned) on the period of time for which backups may be retained
the cheapest cost for unlimited capacity is about £28 per year. There is also a possible additional cost by the Internet Service Provider (ISP) if there is a limit (cap) on the amount which may be uploaded / downloaded or due to a "fair use" policy of the ISP	the cost of a 160Gb hard disk drive is about £37. The cost of a USB hard disk drive caddy is about £31. The cost of Acronis True Image is about £38

It is important to select a backing-up regime that will be robust and meet operational requirements against threats which may be summarised as -

Loss of key data (through fire, theft or ‘user error’)

Copying key data files (to, say, a USB flash memory stick, CD, DVD or on-line) once a day will provide a short term backup resource (should a file be ‘lost’) and also a resource from which (if there is a fire or theft) the business may continue using another computer- assuming the computer has appropriate software. A template batch file is available from Computer Solutions. It is essential to ensure ALL key data is included. The USB flash memory stick, CD or DVD should, ideally, be easily accessible in an emergency evacuation.

Loss of historical data (through fire, theft or ‘user error’)

Backing up (full and incremental) say, on a weekly basis will provide a resource from which files deleted from the hard disk may be recovered. If not done on-line the recommended media required for this is a hard disk drive in an (external) USB caddy and appropriate software. The backup will include more files (including system and software files) which may not be wanted. However, it is advantageous to include all files in a backup rather than to exclude files which may be required later. If using a single hard disk drive it is recommended there should be at least two backup sets on a single hard disk drive. This avoids having to erase and loose all backups when the hard disk drive becomes full and is re-used. The hard disk drive should, ideally, be kept in another building (or, at least in another part of the building).

In order to aid identifying the version of a particular file to be recovered a record should be kept of the -

date on which a backup is made;

identification of the media used; and

type of backup (e.g. 'full', 'incremental', 'differential')

Hard disk drive failure

Cloning the hard disk to an external hard disk drive (using something like Acronis True Image) - and refreshing, say, every three months - will provide a resource which can be used in place of a failed hard disk drive. The recommended media required to achieve this is a hard disk drive in an (external) USB caddy. The hard disk drive will not be up-to-date with software, software updates, new software program updates or key data. However, it should provide a good platform from which the business may continue. It is an alternative to having to do a complete software install which (possibly at a stressful time) requires knowledge of all installed software and how it was configured. The hard disk drive should, ideally, be kept in another building (or, at least in another part of the building). It may not always be possible to boot a computer from an external USB hard disk drive. However, swapping hard disk drives is a straight-forward task.

Loss of computer

This is a threat which cannot be overcome easily other than acquiring a replacement computer. A complete knowledge of installed software, access to software CDs (and other sources of software) and knowledge of product keys and the configuration of software is the key to an easy complete software installation on a replacement computer. Access to a copy of user files taken as an insurance against ‘Loss of key data (through fire, theft or ‘user error’)' or ‘Loss of historical data (through fire, theft or ‘user error’)' above is also necessary.

Other considerations

Software on individual computers on a network should be configured so that all user files are saved to the network server (or the designated computer) from which backups are to be taken. This ensures that those user files are backed up. Also, this is more reliable than backing-up a number of computers.

It is important to note that as little as possible software should be running when backing-up. This reduces to a minimum the possibility of a file(s) 'in use' not being backed up.

If you have any further queries on this subject please contact me.

© 2010 Bill Ridgeway. Reproduction, copying, image scanning, storing or recording by any means in any form or broadcasting or transmitting through any medium of any part of this document is not permitted without the express written consent of Bill Ridgeway.