BACKING UP YOUR PRECIOUS DATA AS A MATTER OF ROUTINE WILL PROTECT YOU FROM THE AWFUL REALISATION THAT, IN THE EVENT OF A DISASTER, YOU REALLY HAVE LOST EVERYTHING. DAVE MITCHELL HAS A PLAN OF ACTION.

Data protection act

Illustration by Paul Shorrock

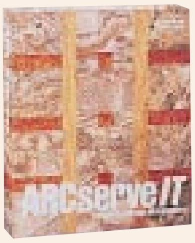
Data is just as valuable as cash to business, yet an alarming number of companies fail to take appropriate measures to protect it. It's easy to view funds, property and staff as assets, but data rarely comes into this equation. Information held on customer accounts, sales and stock is just as important to business operations and, realistically, is one asset that is not expendable. Once data is gone, it's gone for good. How long would your company survive if all customer records and details on debtors were lost? The lucky ones might get through, but many will fall by the wayside. There's been plenty of research in this area and the general finding is that over half of companies that lose their data will go out of business.

It's essential to survival that data is protected,

BACKUP SOFTWARE AND HARDWARE OPTIONS

Software

☛ **Seagate Backup Exec** NT and Novell NetWare versions. Excellent features for network backup. Fewer management tools than ARCserve but still excellent.



☛ **Computer Associates ARCserve** Another top choice for network backup run from Windows NT or Novell NetWare servers. Supports multiple tape drives and can manage backup rotation strategy.

☛ **Yosemite Technologies TapeWare** Fast becoming a main contender. Good management features, plenty of backup options and a pile of predefined backup systems are included.

Hardware

☛ **Hewlett-Packard DAT8** Digital audio tape based drive that uses cheap DAT DDS-2 format 4Gb capacity tapes. Approximate drive cost, £500.

☛ **Tandberg Data SLR6** A SCSI-based drive offering a whopping 12Gb of native storage on a single cartridge for less

than £600. Fast, with transfer rates of around 110Mb/min.

☛ **Sony SDT-9000** DAT DDS-3 format SCSI drive with 12Gb native capacity, 70Mb/minute transfer rates and all for around £800.

• *Contacts*

Seagate Software
01628 771299
www.seagatesoftware.com

Computer Associates
01737 775500
www.cai.com

Kingswall Computers (Tapeware)
01604 767636
www.kingswall.co.uk

Hewlett-Packard
0990 474747
www.hp.com

Tandberg Data
01582 769071
www.tandberg.com

Sony 0990 424242
www.sony.co.uk

and backup plays a key role in this. But, this must be seen as part of an overall plan that ensures a company can survive a disaster and get back on its feet as quickly as possible. While a lost file may be easy to restore, total data loss is not so easy to recover from. Your plan should include full disaster recovery procedures, secure off-site storage and even a contingency site to be used if access to your premises is denied.

Risk assessment

The first course of action is to assess the risk areas – identify all threats to your systems and data and take appropriate measures to protect against them. These should include human error and physical damage to equipment whether accidental or malicious. Viruses come into this grim picture as well. Even though the most common viruses can be removed safely by good anti-virus software, there is a potential for data corruption. Boot sector and macro viruses can be cleaned easily, but file viruses actually play around with program coding and often damage files beyond repair. In many cases, anti-virus utilities won't even attempt to repair the infected files and will recommend that they are restored from the last clean backup.

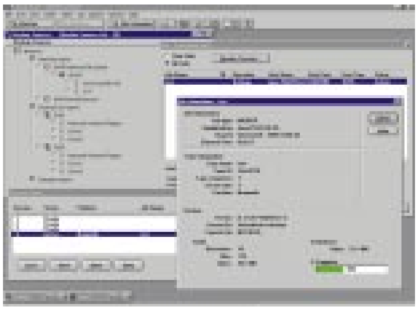
These are more common problems, but the potential disaster needs to be considered. Fire, flood and theft spring to mind, and it's here that off-site storage for your latest backup tapes becomes imperative. Hardware can be replaced easily but is of little value if all your data was destroyed as well.

Implementing a backup strategy may look expensive to small businesses on a tight budget, so perhaps they should apply some reverse logic and first consider what a disaster would cost them. How much business would be lost for every twenty four hours out of action? There's also the knock-on effects, such as potential new customers going elsewhere because essential services can't be provided. Surely it makes sense to invest a proportion of this amount to ensure it doesn't happen.

In the February issue of *PCW* we looked at networking for small businesses and how costs can be reduced by sharing devices such as printers and modems over the network. The same applies to backup: why go to the expense of having a tape drive on every desk when you could place a single drive on the server? All attached workstations can be backed up to a single location, making it far easier to manage.

Good backup software comes into play as well. Network versions of popular products allow you to view the resources on each workstation, select the files you want backed up and send them across the network to a tape drive attached to a server. Users don't have to be involved, as backup can be run out of hours and the whole strategy can be managed by the software itself.

The type of hardware will be determined by the amount of data that must be backed up and the time available. Tape is the only sensible choice as it combines high performance and low storage costs. Devices such as Jaz drives may seem



▲Seagate's Backup Exec uses agent software loaded on each workstation so hard disks can be remotely backed up to a tape drive on the server

GOOD BACKUP PRACTICES

- **Schedule** backups for a specific time each day. If you back up when time permits, it may not get run at all.
- **Appoint** one member or a team of staff with full responsibility for the entire backup and recovery strategy.
- **Don't rely** on one copy of vital data. Run the backup job a second time to create a copy instead of copying one tape to another, as this may transfer errors.
- **Check** your data by including verification as part of your backup.
- **Retire** old tapes from the system. Ensure tapes stored for long periods are regularly re-tensioned if specified by the manufacturer.
- **Make** off-site storage an essential part of your backup strategy and use it.
- **Tapes** to be retained on-site should be labelled and stored in a fireproof safe.
- **Recovery** plans should be regularly tested to ensure they'll run smoothly if disaster strikes.
- **If continued business operations** are critical to survival, consider using a contingency site where essential operations can be restored during a crisis.

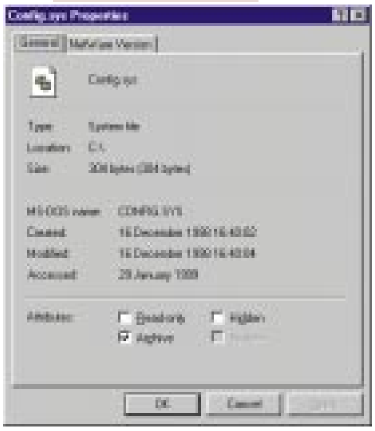
a good idea, but the high cost per megabyte of storage far outweighs its superior performance. Choose a tape drive that can store all the day's backup data on a single tape.

One of the reasons data doesn't get secured is because backup is about as exciting as watching paint dry. If you have to sit around waiting to change tapes as they fill up, the chances are you won't bother in the first place.

It's far easier to start a backup at the end of the day and walk away knowing it will be finished when you next come in. Be wary of manufacturers' claims, as they invariably quote the performance and capacity of their products with a 2:1 compression ratio applied. Most modern tape drives can pack more data on the tape by compressing it as it is being read. However, the type and variety of data on today's networks makes this almost impossible to achieve, so it's far safer to use the uncompressed, or native, figures quoted for a tape drive. If possible go for a SCSI-based drive. Parallel port and IDE drives might be much cheaper, but they are too slow and have insufficient backup capacity to be of use for network backup.

When it comes to choosing the best backup strategy you'll be faced with three main options — full, incremental and differential. A full backup is obvious; but what do the others mean? They are both types of partial backup and their differences come down to a file property called the archive bit, a feature that is fundamental to correct backup software operation. You can see this by choosing a file from Windows Explorer and viewing its properties. Below the dates for creation and modification is a section called Attributes. Here you can see whether it is a system file, marked as read only, hidden, and the status of its archive bit. Whenever a file is created or modified, the archive bit is switched on automatically to show that it is either a new file or its contents have changed. When your software runs a full backup, each file copied has the archive bit switched off to indicate that it has been secured to tape. If any file is subsequently modified, the archive bit is automatically switched back on again, indicating that its contents have changed since the last backup.

▼The Archive attribute is vital to backup software as it shows whether a file has been created or updated since the last backup


Config.sys Properties

Config.sys

Type: System file
Location: C:\
Size: 206 bytes (384 bytes)

MS-DOS name: CONFIG.SYS
Created: 16 December 1998 16:40:02
Modified: 16 December 1998 16:40:04
Accessed: 28 January 1999

Attributes: □ Read-only □ Hidden
☑ Archive □ System

When an incremental backup is run, it checks the status of each selected file's archive bit and only copies those that have had it switched back on — hence the term 'partial backup'. Once the backup candidates have been secured, the archive bit is switched off again. The next day's incremental backup will also check the archive bit of the same group of files and copy any that have been changed. Consequently, the tapes produced by each incremental backup will only contain those files that were modified in the twenty four hours prior to them being run.

Differential backups, on the other hand, don't change the archive bit after copying a file. Any file that was created or modified after the last full backup will be copied to each day's tape until the next full backup is run. As you go through the week, each day's differential backup will be larger than the previous one as the number of files modified or created increases.

Backup or recovery?

Which type of partial backup will suit you best will be determined by one of two factors: whether you want fast backup or fast recovery. As incremental backups are only copying data that has changed during a comparatively short space of time, they'll be a lot quicker. Many companies whose operations extend beyond the standard 9-to-5 day frequently opt for the incremental purely because the network administrator has less time available to run backup. The downside will be revealed when the time comes to restore data.

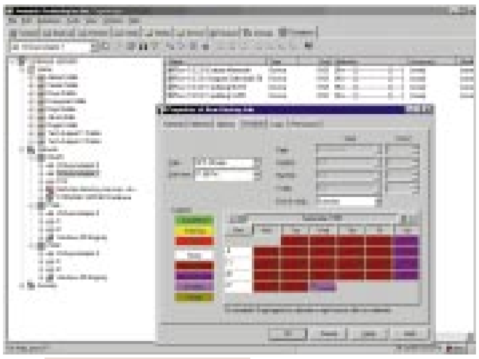
Recreating an entire system will require the most up-to-date full backup to be copied back first, followed by all subsequent incrementals.

Say you're running a full backup every Friday and a disaster occurred on the following Thursday: you'd need to restore five different tapes and each incremental must be applied in the order they were created.

The differential backup wins out here, as full system restoration would take far less time and will be easier to manage, as only the latest full backup plus the last differential will be needed. However, each day's backup will take longer as the week progresses. In situations where large amounts of data are changing frequently, it is not unknown for the week's final differential to be almost as large as the full backup.

Getting it taped

Now that we know what types of backup are possible, a suitable tape rotation system needs to be implemented. This will reduce the amount of media to a manageable level and the type will depend on the choice of backup horizon. If you only want to keep a copy of your data for one week, then do a full backup run on Friday, along with incrementals or differentials for Monday through to Thursday. The tapes are then all re-used the following week. Although tape life is reduced due to the frequent usage, it's a simple system that's easy to manage and can be modified to suit. Say you want a backup horizon that extends back two weeks. Instead of recycling the end-of-week full backup, remove it from the system over to secure storage and use a new tape. The following Friday sees the tape held in storage swapped over and returned to the system.



▲ TapeWare looks complex but it has a wide range of pre-defined strategies included to help with network backup

This method of regularly removing tapes from the system and replacing them with fresh media gives a wide range of options. Most companies will need to retain copies of their data for at least a year so month-end backups can be introduced into the system. The tapes used for mid-week partial backups are still recycled, but each weekly full backup is removed to secure storage. The first three tapes are returned to the system the following month, but the fourth is removed permanently and a new tape used in its place. When you reach year-end, you'll have twelve tapes containing data for the entire period.

This one year system is often referred to as a Grandfather/Father/Son (GFS) rotation where the daily backups are the Sons, the weekly backups the Fathers and the monthly backups the Grandfathers. It is one of the most commonly used backup strategies because it is relatively easy to administer and provides good, long-term data protection. There are, however, potential pitfalls that need to be avoided. Say you decide to carry out some housekeeping on a server or workstation because disk space is running out. If you run this in the middle of the month, the deleted files will not be on the month-end copy. They will be on the weekly copies but these will be recycled the following month.

If possible, leave all housekeeping tasks until after the month-end backup has been taken, or take a separate copy and store it permanently. The difference between a backup and a copy is that the latter leaves the archive bit alone, otherwise it would interfere with the tape rotation system. Also, for your backup strategy to work properly, the tapes being rotated out of the system must be stored off-site and must remain there until they are required. If your business premises gets burnt down, flooded or all your computer equipment is stolen, you will still have access to your data. Servers and PCs are replaceable but data is not; once it's gone, you've lost it for good.

Contingency plan

As backup is an integral part of a data protection policy, so is disaster recovery. If your computer equipment is stolen then you need a decent insurance policy so it can be replaced as quickly as possible. However, that won't help in the event of a fire or flood or even a gas leak. You also have to consider the possibility of being denied access to your premises by the emergency services.

In these situations a business continuity plan using a contingency site is the answer. You move the necessary personnel to a pre-prepared remote location, recreate critical systems using your off-site data, and maintain reduced business operations until you can re-enter the main premises. A contingency site is probably the most difficult part of the strategy to create as it can be expensive. However, it is not unknown for non-competing companies in the same geographical area to cooperate with each other and provide assistance if disaster strikes. If this is not feasible, then consider a third-party specialist.

Companies that already have a data protection plan in place are thinking ahead. They'll have it fully documented and will regularly test the procedures to ensure there are no foul-ups if it has to be run for real. Unfortunately, many firms still have their heads in the sand and will consider it a waste of money: why pay out large sums of money for something you hope never to use? They are living on borrowed time: Murphy's Law states that whatever can go wrong, will go wrong, and when least expected. Are you prepared to risk your company's future that he's wrong? It's called false economy. □