Backups

PB/INFO/016

Most computer users will have been very grateful for the existence of backups. Although they are often seen as a way to recover files lost due to typing errors or misplaced mouse clicks there are other reasons to make and keep secure copies of files. However each of these purposes creates different requirements for the backup and recovery system, so it is important to be clear which purpose is involved and choose an appropriate backup strategy and technology to deliver it.

Why backups?

There are at least four reasons to want to recover the past state of a file or file system:

1. System Recovery – these backups are used when a hardware or other failure has made a disk or computer unusable. The aim is to restore the disk or computer as it was before the failure, so what is needed is a complete snapshot of its content. To minimise lost work, the snapshot should be as recent as possible – there is little benefit in keeping older snapshots. Since restoring a complete system may take a long time, backup and recovery processes and formats should be designed to be as fast as possible.
2. Recovery from Ransomware – if a device or filesystem is encrypted by ransomware then a complete backup (as for System Recovery) may be the safest way to restore it. However the most recent full backup may not be appropriate, since it may already include the ransomware. This new threat may mean that multiple “System Recovery”-type backups need to be kept.
3. File Recovery – here the aim is to recover one or more specific files that have been deleted or damaged, typically by user error. Files are chosen for recovery by filename or directory, so both backup and recovery processes need to be able to navigate file systems. This is likely to make them slower than the pure snapshot systems above. Users may also want to recover previous versions of files, so multiple copies may be needed. Organisations can choose how long to keep backups depending on how long after the event a file should be recoverable, though practical and legal issues (see below) may limit the retention period.
4. Archiving – backups protect against accidents and attacks, but archives keep a record of organisational history. Archives should be part of the records management process, containing only a subset of the organisation’s information but including detailed metadata about that information to allow much richer searching. An archive might be searched for “all information about building X” or “reasons for decision Y”. For most archived information the retention period will be set (or at least influenced) by law and may be years or decades.

These different requirements are unlikely to be satisfied by the same solution. An archive will

not have all the information needed for system or file recovery and is likely to be too slow for those purposes; a system recovery backup will not provide the types of search required of an archive or perhaps even for file recovery. Indeed the different types may require completely different media – redundant disks may be an effective way to provide system recovery but archiving requires highly durable media kept under controlled conditions with regular checks and format conversion.

How backups?

Many organisations have central backup and archiving services, which can be joined by completing a form, making a small payment or merely storing files in a particular location. A well-run central service provides access to expertise and technology: a huge benefit both in time saved when things do go wrong and in peace of mind when they do not. If your organisation has a service that meets any legal requirements on your data then there are few arguments for doing archives or backups any other way.

Many organisations now use cloud services for data storage. These may cover some of the backup purposes listed above: for example a cloud service may well provide storage that is resilient against hardware failures (purpose a) and/or automatically keep previous versions of files (purpose c) subject to some time/number/size cap. Archiving (purpose d) is less likely to be provided automatically, and cloud storage may even make Ransomware incidents (purpose b) worse if the entire cloud filestore is encrypted. Check carefully to see which processes your cloud solution does, and does not provide, and ensure you make separate provision for the others

If you do have to make your own backups, then there are a number of options depending on the amount of information to be saved and the length of time for which it may need to be kept. Tapes, high-capacity removable disks and writeable CD or DVD-ROMs are all available for most desktop machines. Good quality media should always be used. If you have sufficient bandwidth then, rather than physical media, you can encrypt the result of your backup and store the resulting file on a cloud service. Catalogue and store the media in a safe, ordered fashion so the correct one(s) can be found when required. If sensitive information is being backed up, ensure that the backups are stored as securely as the originals. To ensure information remains available after a physical incident such as a theft, fire or flood, consider keeping a copy in a different, but still secure, location. Make sure backups are taken at appropriate times to give the best chance of preserving information: backups taken at the end of a working session give better protection than those taken at the start.

For ransomware protection in particular (and also helpful for other purposes) it is good practice to ensure that one backup is always “off-line” so that errors and malicious acts are not automatically replicated onto it. NCSC-UK have a helpful article [1]. Consider how the integrity of your backup and restoration processes will be affected by a persistent compromise of your infrastructure. A sophisticated attacker may be able to tamper with your backups and authentication systems over several months before their intrusion is noticed. To ensure information remains available after a physical incident such as a theft, fire or flood, consider processes that ensure a copy is always kept in a different, but still secure, location.

Whether you make your own backups or subscribe to a central service, they will be of little use if you cannot recover files quickly when needed. It is much easier to learn how to retrieve

files calmly, before it becomes a matter of vital importance. Document how to recover files for each of the four purposes, ensure that more than one person is familiar with doing this, practice regularly following an agreed schedule, and keep a record of when (and who) has done this. To get more of a “real-world” experience, use of backups should also be included in exercises. This can reveal dependencies on people, systems or data before they become critical: for example if the recovery instructions are on the filesystem that needs to be recovered!

Legal Issues

The law makes significant distinctions between archives and backups. For most organisations, keeping archives is a legal requirement [2], keeping backups may not be. If a request is made under the *Freedom of Information Act* or *Freedom of Information (Scotland) Act* then the organisation will be expected to search for the information in its archives and storage but, at least according to the Information Commissioner’s guidance [3], perhaps not its backups. An Information Tribunal case [4] indicates that a fixed policy and practice of reusing (i.e. overwriting) backup tapes should support an argument that they are not being used as off-line storage. Being clear which information needs to be kept and which does not, and implementing appropriate processes and technology, can save a lot of time and effort.

Summary

These eight steps can help you make effective use of backups:

- be clear about their purpose and choose a format and content appropriate to that;
- join a central backup/archive service if you can and always use it;
- if a central service is not appropriate, plan your own backups;
- get enough suitable media;
- leave time to backup at the end of a session;
- check the backup has worked;
- label media and store them safely and securely;
- document your recovery processes and practise them before they become critical.

Links
[1] https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world
[2] https://www.jisc.ac.uk/guides/records-retention-management
[3] https://ico.org.uk/media/for-organisations/documents/1169/determining_whether_information_is_held_foi_eir.pdf
[4] https://community.ja.net/blogs/regulatory-developments/article/information-commissioner-backups-and-deleted-files