Data Security - Backup

Many companies are now completely reliant on the data stored on their network servers, PCs, laptops, mobile devices and in the cloud. Some of this data is likely to contain either personal information and/or confidential company information.

Here we look at some of the issues to consider when reviewing the security of your computer systems and data.

Data backup is an essential disaster recovery procedure and should be undertaken on a regular basis. A business should view regular backups as a form of insurance policy against disaster, theft or cyber attacks.

There are a number of points to consider.

Systems and applications software installation media

Ideally, once the software has been installed, the original media should be stored securely off-site, unless the software was downloaded. Similarly, any activation keys/ codes should be stored securely.

Data file locations

In a network environment some data files might be stored on the server and other data files stored on local drives. In which case, separate backups may be required for both the server and one or more PCs.

Ideally, a network solution should be provided, which ensures that all data is re-copied back to the server from local drives.

One strategy would be to use a synchronisation service such as Microsoft OneDrive, or even Sharepoint, instead of more traditional network disk storage.

Backup strategy and frequency

There is likely to be a need for two parallel backup procedures. One to cover a complete systems backup of servers, usually as an image, and another to incrementally (or differentially) backup any data files that have been updated since the previous backup.

The most common backup cycle is the grandfather, father, son method. This consists of a cycle of four daily backups, four or five weekly backups and 12 monthly backups.

Remember that some data has to be preserved for many years - for example accounting records need to be kept for a minimum of six years.

Certain backup media, such as tape or CD/DVD can be reused many times, but they do not have an infinite life and will need replacing after two to ten years depending on the quality and number of times used. Some additional points are made on this issue in the section on backup media degradation.

Solutions such as disk-to-disk, or disk-to-disk-to-tape, and cloud-based backup services do away with the need to worry about degradation.

Backup responsibilities

A specific staff member should be given responsibility for the backup procedures. This person must be able to:

- regularly ensure that all data files (server and local) are incorporated in the backup cycle(s)
- adapt the backup criteria as new applications and data files are added
- modify the backup schedule as required
- interpret backup logs and react to any errors notified
- restore data if files are accidentally deleted, or become corrupt
- regularly test that data can be restored from backup media
- maintain a regular log of backups and the locations where backup media are stored.

Applications backup routines

Many accounting and payroll applications have their own backup routines. It is good practice to use these on a regular basis (as well as conventional server backups) and always just before critical update routines. These backup data files should be stored on the server drive so that they are backed up along with the server.

Local PCs

Certain users will have the data files of applications exclusively on their local drives, for example payroll data. These will require their own regular backup regime, which (as mentioned in the previous paragraph) may consist of a combination of backing up to media and backing up to

the server. Consideration should also be given to whether this data should remain on the local PCs, or whether it should be moved elsewhere.

Backup media

The selection of the right media to use for backups will depend on criteria including, the available budget, the volume of data requiring backup and the networking operating software. External hard disks, or a NAS box with cloud backup, may provide good solutions. If an external service provider, or cloud option is being used, they should have their own backup regime. However, do not rely solely on this and ensure any third-party supplier meets or exceeds your backup needs.

Other media types such as tape or optical storage (CD/DVD/Blu-Ray) may also be considered as a cheaper alternative, but capacity and lifespan may be limited.

External hard disk drives are another option. However, any disk that must go off site for backup reasons should also be encrypted in case of loss or theft.

Backup location

Backups should be stored in a variety of both on-site and off-site locations. On-site backups are easily accessible when data has to be restored quickly, although they are at risk from emergencies, such as fires or floods.

A large number of businesses use on-site safes. However, in a recovery situation these could be inaccessible for a period of time.

Off-site backups have the advantage that they will be recoverable following an emergency, but storage must be both secure and accessible.

Backup retention

Finally, certain types of records, such as accounting records for example, need to be kept for a minimum period of time and this must be considered when developing the data backup strategy (also see below regarding degradation).

Backup media degradation/ decomposition

Backup media degrades and the data stored on them decomposes over a period of time.

Optical media such as CD/DVD and Blu-Ray are particularly sensitive to light (photosensitive), so ensure that they are stored in a dark environment. They are also prone to physical damage when being handled. Finally, CD-Rs and CD-RWs will last anywhere between five and ten years, whereas DVD-RWs and LTO tape media can last up to 30 years.

Backups should be checked on a regular basis for signs of digital decomposition, and tested to check that data can be successfully restored.

In-house or cloud?

Many internet service providers and third-party IT service organisations, now offer off-site data repositories and also complete online application solutions, either as standard or as a chargeable extra. This removes the need to internally support a server and its operating and applications software. However, there are a significant number of key security issues which should be covered as part of the contract/service level agreement (SLA). These should include:

- level of encryption
- the countries in which the data is processed and stored (as this has potential issues with data protection laws)
- data deletion and retention periods
- the availability of audit trails, covering who is accessing the data
- ownership of the data if the provider goes into administration/receivership.

Where data is stored in the cloud, try to ensure that as little personal data as possible is processed and stored in this way. If this is not possible then at least anonymise the data so that individuals cannot be identified.

Ensure you can manually take your own backup copies of data stored with a third-party, and that this data is in a readable format and can be restored onto other services and applications.

How we can help

We can provide help in the following areas:

- performing a security/information audit
- drawing up a suitable backup regime
- training staff in security principles and procedures.

Please do contact us if we can be of further help.

For information of users: This material is published for the information of clients. It provides only an overview of the regulations in force at the date of publication, and no action should be taken without consulting the detailed legislation or seeking professional advice. Therefore no responsibility for loss occasioned by any person acting or refraining from action as a result of the material can be accepted by the authors or the firm.