Data Security and Data Protection

Most companies are totally reliant on information stored on their PCs, Laptops and Networks. If plant machinery stops working it can be replaced without too much inconvenience. If a computer stops working there may not be any means of accessing the data stored. It is, therefore, essential that data is protected and secured on a regular basis.

Here are some of the issues to consider when reviewing the security of your computer systems, and some of the compliance issues surrounding data security and data protection.

Access Security

Restricting access to computers and the computer network minimises the risks of data loss.

Access controls cover two main areas:

- **Physical access**

  i.e. who can enter the premises and who can see personal data, and
- **Logical access**

  i.e. ensuring an employee only has access to the appropriate software and data necessary to perform their particular job.

Physical access

In addition to having appropriate physical access controls to the premises, consider if people can see computer monitors when passing or from the outside of the premises, and whether material containing personal information is subject to appropriate disposal procedures.

Logical access

Logical access techniques should be employed to ensure that personnel do not have more access than is necessary to perform their role.

This should be tackled at both the system level and at applications level.

At the system level, for example, some users will not require access to the accounting software.

At the applications level, for example, with an accounting package it may be desirable that all users of a purchase ledger can access supplier details and post purchase invoices, but it may be that access to supplier payment and cheque printing routines is restricted to only a few of these users.

Passwords

Passwords are a common and effective tool when implementing access controls.

Basically, they should be **easy to remember** but **difficult to guess**.

A number of factors determine how effective they are.

Passwords should:

- be relatively long (e.g. 8 characters or more)
- contain a mixture of alpha, numeric and other characters (such as &^")
- not be the same for all applications
- be changed regularly
- be removed or changed when an employee leaves.

It is worthwhile avoiding:

- any part of your name or family members
- significant numbers, e.g. family dates of birth or car registration
- names of something important to you e.g. sports team, pop group
- names of famous people, landmarks, movies etc
- published passwords.

There are a number of online password checkers – search in your web browser for 'password checker'.

You can, if you search for 'password generator' or 'password creator', find a number of password generators, although these are less likely to create an easily remembered password.

Memorable Password

There are different methods that can be used to create a memorable password.

One such way is to take the initial letters of each word in a favourite song lyric or phrase – then improve it!

Example

The first two lines of Led Zeppelin's Stairway to Heaven are '**There's a lady who's sure all that glitters is gold**'.

This forms the password '**talwsatgig**' when using the first letter of each word.

The Microsoft password checker classes this as "weak" as it only contains lower-case letters, although in reality it is probably relatively strong due to the combination of letters.

However, replacing each occurrence of the letter 'a' with '@', each letter occurrence of 'l' with the number '1', each occurrence of letter 's' with '5' and each occurrence of letter 'g' with '9' creates '**t@1w5@t9i9**'.

The Microsoft password checker classes this as "strong".

Even just changing the A's and G's ('**t@lws@t9i9**') is enough to make the password strong and is easy to remember.

A variation of replacing I's with 1's, instead of the L's is, obviously, equally as effective, producing '**t@lw5@t919**'.

Changing one of the characters to upper-case, e.g. the initial 't', strengthens the password even more, the above examples becoming '**T@1w5@t9i9**', '**T@lws@t9i9**' and '**T@lw5@t919**' respectively.

Data backup and restore

Data backup is an essential process for security and needs to be undertaken on a regular basis.

Backups should be part of the company's overall Disaster Recovery plan. However, it is no good having lots of backups if you can't get access to them when required.

The first consideration is whether you are going to use online off-site backups (via the internet) or purchase your own physical media on which to back up your data. Or, as some businesses do, use both!

There advantages and disadvantages to both, with varying costs, but the main determining factor should be that the chosen route is the most appropriate for your business.

Cost, albeit important to all businesses, should not be the primary constraint – it is a fact that 60% of companies that lose all their data will shut down within 6 months of the disaster.

If you are thinking of the in-house option, you should also assess:

- whether you or one (or more) of your employees is capable of, and has the time required to, perform the necessary tasks

- where the backup media will be located off-site
- whether the backup media will be available if the designated person is not available through unexpected absence. Whilst holidays / business trips can be planned, sickness could cause problems.

Search the internet and/or speak to your **abacus** accountant to determine the best solution for you.

Online off-site backups

There is an ever-increasing number of dedicated storage bureaus (and even some banks) who offer online offsite backup facilities. The dedicated storage bureaus also tend to copy files to at least one different location in another part of the country so your data is more likely to be recoverable even in a regional disaster situation. However, you wouldn't, for example, want to use a storage bureau located in the building adjacent to your premises!

When you use online backup services, you are basically entrusting your personal files and confidential documents to them. This means that you have to check on the security features that they implement in order to protect your files. Often packages offer a combination of file storage and computer backup, and files can be downloaded on any internet connected device – not just back to the server – subject to suitable authentication.

You tend to select a certain storage capacity with the price depending on the amount of storage selected and it is often easy to change to a different package if required.

Each evening, at a scheduled time, your computer will connect to the 3rd party computer via the internet and the pre-selected folders and files downloaded. The files are encrypted prior to transmission and are password protected.

The initial download can take a long time, and if there is a lot of data to download, some companies will send an external hard drive on which to take the initial backup, which is then loaded on their machine much faster than can be obtained via the internet. Once the initial backup has been achieved only the 'changed' files are downloaded so the backup runs relatively quickly out-of-hours.

Restoring folders or individual files tends to be quick and easy, with bureaus often having both online videos and helpdesks to assist.

On-site backups

Backup media

There are a number of different backup media available: CD, DVD, Solid-State Drive (SSD), External Hard Drive and tape cartridges, all of varying sizes (although CD and DVD have limited capacity).

Most server backups will use either use tape cartridges or SSD drives. For more temporary forms of backup, a USB memory stick/pen (which is a small SSD) might be considered.

Backup frequency

A cycle of backups should be retained for a period of time, a value judgement has to be made in this respect – see backup retention below).

Overwriting the same backup media day after day is not recommended.

Example 1

Using 20 different media devices the following strategy could be implemented:

- Separate media for Monday, Tuesday, Wednesday and Thursday, overwritten on the same day each week. Total: 4
- Separate media for each Friday of the month, overwritten on the same Friday of each month. Total: 4 (noting on 4 occasions in the year there will be a 5-Friday month)

- Separate media for each month, taken on the last working day of the month, and overwritten on the same month-end each year. Total: 12
- To complement the above, an annual backup taken on the last working day of the year and kept indefinitely.

Example 2

Using 32 different media devices the following strategy could be implemented:

- Separate media for each working day of a four-week period, overwritten by rotation. Total 20
- Separate media for each month, taken on the last working day of the month, and overwritten on the same month-end each year. Total 12
- To complement the above, an annual backup taken on the last working day of the year and kept indefinitely.

The type and number of media selected determines the outlay incurred, but remember that having backups may be one of the best investments made in the company.

Backup retention

Ideally not all backup media should be stored in the same location, although in practise that is not particularly easy to achieve. Obviously, the safest place is off-site.

Some firms rent secure storage space. If storing your own media (off or on-site) ensure it is in a data-safe rather than purely a fire-safe. A data-safe is fireproof but also protects against magnetism which can erase data. There is increased chance of magnetic corruption if a building is fire damaged causing metal structural supports and/or cables to collapse. Note that data and fire-safes vary in the length of fire protection that they guarantee. The length of protection should be appropriate to the location.

Issues such as how long certain type of records accounting records, for example, need to be legally kept for, also need consideration.

Backup media degradation/decomposition

CD/DVD media is noted as being particularly prone to degradation, and should not be relied upon for long-term storage. However the low cost of external hard-drives and SSDs effectively now make these a non-starter. However, if using CD/DVD media it is worthwhile creating a new copy each year to replace the previous copy.

External hard-drives contain a spinning drive and so have the same potential problems as the computer's internal drive.

Solid State Disks do not have any moving parts and therefore less prone to failure. They are much more resilient to knocks and can be written to in excess of 1 million times.

Backups should be checked on a regular basis for signs of digital decomposition.

Backup strategy

Backing up 'system state' files in addition to data files makes for easier recovery should the server's hard-drives fail and the server needs resetting to its pre-delivered state. Failure to back up the system state files will mean a longer set-up of the new/repaired server.

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 the majority of cases, when using well-designed off-the-shelf software, data can be relocated to the server, either during the initial set-up of the application software or on creation of data.

If not, separate backups may be required for both the server and one or more PCs. Some server backup software can access PCs provided they are left switched on, although additional licences are normally required.

Complete systems backup

On a network, some form of server backup software should be used to take a complete copy of the network drive(s). This can normally be set to run overnight. However, someone will need to be given responsibility for these procedures.

Key areas to consider include training in how to:

- use the backup software
- alter backup schedules and
- change backup file criteria.

The person responsible needs to be able to:

- adapt the backup criteria as new applications are added
- interpret backup logs and react to any errors notified
- restore data from backup media
- maintain a regular log of backups and where these are stored.

Finally, be aware that some backup utilities only take a mirror image of the hard disk. In this case, the whole of the hard disk has to be restored even if there is a problem with just one file or just one folder.

Applications backup

Many accounting and payroll packages have their own backup routines – some automatic – that may be taken without the users' knowledge.

Application backups will default to the same location as the original data and therefore will also be lost should a hard-drive failure occur. They should only be relied on to recover following a human error in the processing rather than as a secure backup. A full data file backup should be taken on a daily basis.

Note that these automatic backups will build up over time and start to fill the daily backup media. Therefore a decision has to be made on how many are to be kept and who is to administer the deleting of redundant ones. For example, Sage Payroll automatically takes a copy of payroll files before any updates are done. If the payroll is weekly and updated once per week, by the end of one year the daily backup will contain one copy of each of the live files and one copy of each of the 52 backups that Sage itself makes. If the payroll is updated on more than one occasion per week then all of these additional automatic backups will also be backed up! If using an online off-site backup facility, these files will continue to accumulate and unless deleted from the off-site backup will eventually push the selected package to the next price-band.

Whilst most people would automatically think about backing up data it is also essential to back up email files. In some professions there is a legal responsibility, but even if this doesn't apply, email applications can contain a huge amount of information which may not be able to be recreated, for example attachments that haven't been saved to the network.

Local PCs

Remember that some users will have applications data files exclusively on their local drives and these will all require their own regular backup regime.

However with most applications, if the pc is used on a network, the data can be stored on the network rather than on the local drive. This is recommended as servers have a better build quality and are more resilient than PCs.

If the data cannot be stored on the server, some server backup software can access PCs provided they are left switched on, although additional licences are normally required.

An alternative would be to create a .bat file, which when executed would copy the data to the server (and be backed up). However this relies on the user manually executing the 'job' before disconnecting from the network.

Restoring data

As with backups, there are a number of issues to consider.

- Total systems restore

  This can be a complex procedure in a network environment and may require specialist network engineers to provide assistance.

- Application restore

  We recommended above (see Applications backup) a separate cycle of backups to cover individual applications. If it is necessary to restore the whole application from these backups, then the restore utility within the package concerned needs to be used and the correct backup media loaded.

- Individual data-file(s) restore

  These are generally less complex, but nevertheless care is needed. If the required data files are on the server backup then the restore utility will need to be used, the correct backup media loaded and the file or files to be restored correctly identified.

Virus/Spam protection

The prevalence of email viruses and unsolicited spam means that software is required to filter these items out of the system.

This software will require regular updating, along with all relevant ongoing software security patches that need to be applied to the operating and applications software.

Additional network security in the form of firewall software is also required to protect the network from unauthorised access and potential network attacks.

Employees

All employees should know and understand the firm's security procedures and the consequences of abusing these. You might wish to refer to our factsheet which sets out a model internet and email access policy.

Staff dealing with personal data also require training in the principles of data protection and good information handling practices. Staff specifically involved in marketing also need to be aware of the Privacy and Electronic Communications Regulations 2003.

Compliance issues

Most businesses process personal data to a greater or lesser degree. If this is the case, then notification under the Data Protection Act may be required. If so, ongoing compliance with the principles of information handling and information security is necessary. **abacus** can help you with this process to ensure compliance.

As well as the Data Protection Act, there are various other Acts and regulations, which have a bearing on data security. These include:

- Privacy and Electronic Communications Regulations 2003 – which cover spam and mass-marketing mailshots
- Copyright Design and Patents Act – amended 2002. One of the main themes of the amended Act was to increase the power of the police to pursue criminal charges against employees, directors and companies for software theft.

How abacus can help

abacus can provide help in the following areas:

- defining and documenting security and logical access procedures
- performing a security/information audit
- drawing up a suitable backup regime
- training staff in security principles and procedures
- notification and/or compliance with regulations as applicable to the type of organisation.