

## Data Security and Data Protection

Although data does not show on the balance sheet as an asset, many companies are totally reliant on the information stored on their PC's, Laptops and Networks.

Here we look at 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

Good access controls to the computers and the computer network minimise the risks of data loss.

Access controls can be divided into two main areas:

- Physical access – controls over who can enter the premises and who can see personal data
- Logical access – controls to ensure employees only have access to the appropriate software and data necessary to perform their particular job.

#### *Physical access*

As well as having appropriate physical access controls to the premises – there are other considerations such as can people see screens from the outside, and is material containing personal information 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 desirable that only a few of these users also have access to supplier payment and cheque printing routines.

#### *Passwords*

Passwords are one of the measures which can be used to implement access controls.

However, to be at all effective they should:

- be relatively long (i.e. 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.

## Data backup and restore

Data backup is an essential process for security and needs to be undertaken on a regular basis. There are a number of points to consider.

### *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 PC's.

### *Backup strategy*

There is likely to be a need for two parallel backup procedures; one to cover a complete systems backup and another to cover the backing up of individual applications' data files.

### **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 disc. In this case, the whole of the hard disc 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. It is a good idea to use these (as well as full server backup) on a regular basis, and always just before period end, or pay period end, update routines.

### *Local PCs*

Remember that some users will have applications data files exclusively on their local drives (such as payroll data for example) and these will all require their own regular backup regime.

### *Backup media*

There are about half a dozen different types of backup media available – from the writable CD capable of storing up to 1gb, through the DVD reader/writer (5gb) up to the mighty external hard drives (1000gb). Most server backups will use either use tape cartridges or CD/DVD reader/writers. For more temporary forms of backup, a USB memory stick/pen (1gb) might be considered.

### *Backup frequency*

A cycle of backups should be retained for a period of time (probably going back at least 12 months – but see Backup retention below). Overwriting the same backup disc/tape/cd/dvd day after day is not advised.

### *Backup retention*

Backups should be stored in a variety of locations. Obviously, the safest place is off-site.

Physical backup media can be stored in a separate location, whilst some firms may rent disc space on a service provider's server, to backup files to.

Issues such as how long certain type of records, accounting records for example, need to be kept for, should be borne in mind.

### ***Backup media degradation/decomposition***

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

DVD's are particularly sensitive to light (i.e. they are photosensitive) for example, so ensure that they are stored in a dark environment.

RW media is noted as being particularly prone to degradation, and should not be relied upon for long-term storage.

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

## **Restoring data**

As with backup, 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 identified.

## **Virus/Spam protection**

The prevalence of e-mail 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 on-going 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 firms' security procedures and the consequences of abusing these. You might wish to refer to our factsheet which sets out a model internet and e-mail 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 is required. That will then mean on-going compliance with the principles of information handling and information security. We 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 mail shots.
- 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 we can help

We 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.