



ICT

Data Security

Although it does not show on the balance sheet as an asset, the data stored on the PC or PC Network can be invaluable to a business – small or large.

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

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
- Logical access – controls to ensure employees only have access to the software necessary to perform their particular job.

Logical access

An example of logical access would be that all staff will probably need access to e-mail and calendar software, but not all staff will need to access the accounts package.

Some software packages also have internal logical access controls to prevent employees exceeding their authorisation – for example in an accounting package it may be desirable that all users can access supplier details and post purchase invoices – but it may be that only some of these users also have access to supplier payment 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
- contain a mixture of alpha and numeric characters
- not be the same for all applications
- be changed regularly
- be removed if related to an individual employee who 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

Where the key applications data files are stored needs to be determined. This is relatively easy if there is only one PC involved but in a network environment some data files might be stored on the server and other data files stored on local drives.

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 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, you will need to understand how to use and maintain this software.

Key areas to consider include:

- who is responsible for this procedure and
- what data is actually being backed up and what (if any) criteria the backup software uses (ie which files/folders are actually backed up)?

The person responsible needs to be able to:

- adapt the criteria as new applications are added
- interpret backup logs and react to any errors notified
- restore data from backup media.

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 a network backup) on a regular basis and always just before period end updates.

Local PCs

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

Continued >>>

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 tape cartridges or CD/DVD reader/writers. For more temporary forms of backup, or just moving large files around, a memory stick or USB 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). Overwriting the same backup disc/tape day after day is not advised.

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 all systems require software to filter these items out of the system. This software will require regular updating, along with any relevant software repairs (patches) to the PC operating and network systems.

Additional network security in the form of firewall software is also required.

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.

Other matters

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 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.

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.