white paper

Managing **Data Protection**

Nightmare scenario: Your organisation maintains a database containing a lot of personal information about your clients. As part of an internal control check, your auditor asked to see some of the information, but the disks you put it on never arrived at the accountant's office.

What is wrong with this situation?

This Sage white paper sets out to explain some of the issues behind data protection, by setting out the relevant laws and regulations. It also describes precautions you can take to prevent such a situation happening within your organisation.

sage

white paper

Managing Data Protection

Contents

What you need to know about data protection

Data protection, information security and why they matter to you

You may not be a government department with millions of names on your files, but you still have a lot of important information within your control that needs to be protected. Here are some of the reasons why:

- **HM Revenue & Customs** requires you to retain VAT records for at least 6 years and other tax records for 7 years. You are now allowed to do so using digital copies.
- **Even if it is not trading**, a live company must maintain its statutory registers and minutes indefinitely to comply with the Companies Act.
- **The Data Protection Act** applies to all businesses and covers paper records as well as computer data. Any company that "controls" personal information must register with the Information Commissioner. Failing to do so is a criminal offence.
- **Business continuity** - data protection isn't just about legal compliance, it also has important practical considerations. For example, could your business still function if it was suddenly unable to access the data on its systems? If this information is essential to the organisation's continued survival, treat it with an appropriate level of care.
- **Good housekeeping.** Maintaining good data security standards, taking and testing back-ups regularly, and patching and updating application software keeps your business running smoothly and ensures it better able to prevent disruptions or intrusions.

Data Protection Act requirements

The Data Protection Act applies to any personal data your company holds about customers, suppliers, prospects and employees. The things that are covered include:

- **Your business card** collection or contacts in a Filofax.
- **HR records** on existing, potential and ex-employees.
- **Outside suppliers** - if you supply records to an outside supplier such as a payroll bureau, recruitment agency or mailing house, you must obtain a written undertaking from them that they, too, will protect the security and integrity of any personal data.
- **Customer and prospect databases** such as those held on a customer relationship management system.
- **Third party mailing lists** that you may buy or rent.
- **CCTV** - If you operate a CCTV system, you must ensure anyone visiting your premises is aware it is in operation, for example with a prominent sign. Not doing so could breach the visitor's rights.

Register with the Information Commissioner

If you are an organisation that controls personal data in scenarios similar to any of those set out above, you need to sign up to the Register of Data Controllers, which is maintained by the Information Commissioner's Office. It costs £35 a year to register, which you can do online at www.ico.gov.uk. Processing personal information without being on the register is a criminal offence.

Employee records - key principles

The Data Protection Act sets out a code of eight principles that should be applied to employee data. It must be:

- **Fairly and lawfully** collected and processed.
- **Used only for limited** and well explained purposes.
- **Relevant** to your organisation's needs, and not excessive in detail.
- **Accurate** and up-to-date.
- **Kept no longer** than is necessary.
- **Processed in accordance** with the rights of the individual.
- **Securely stored** to prevent unlawful or unauthorised processing, loss, destruction, damage or disclosure.
- **Not transferred** to countries outside the European Economic Area.

Data Protection Act checklist

- Has the company appointed a data controller to take responsibility for complying with the act? **Complete** ☐
- Have you explained the DPA to managers, and the legal duties it places on them and their data? **Complete** ☐
- Have you made staff who can access information covered by the act aware of the criminal implications of disclosing personal data? **Complete** ☐
- Have you reviewed your IT systems to make sure that the data you hold and the way it is used complies with the eight principles? **Complete** ☐
- Is personal information held in paper and electronic formats stored securely, with access limited only to relevant staff? Are file cabinet keys and computer passwords stored safely? **Complete** ☐

Information security basics

Don't be fooled into thinking that information security is all about internet firewalls and anti-virus software. Information security is more about developing a rounded view of the risks associated with your information assets, and taking appropriate measures to reduce those risks. Setting down clear policies and teaching your team good security practices is often a more effective way to reduce risk than buying IT security systems - though you will probably need to do that too.

Acceptable use policy

No matter how small the organisation, its information security strategy should start with an acceptable use policy that sets down on paper what your employees should and shouldn't do, and what will happen to them if they do not abide by the policy. The rules should cover computer use, email and internet access and be applied consistently and without favour. Enforce the rules! Don't be tempted to overlook breaches, since failing to deal with employees who break the rules will encourage others to think they can get away with it too.

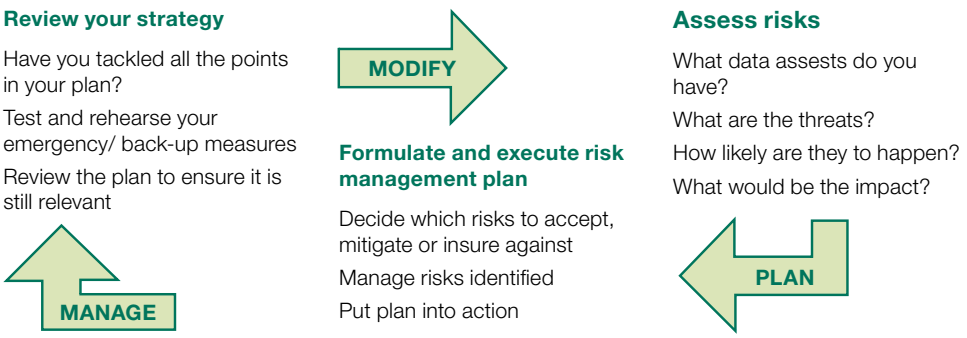
Management systems

Information and its security need to be managed, so make someone responsible for it, and ensure appropriate systems are in place to keep it safe. This can be as simple as applying the rule of "least privilege" and only allowing access to people who need to use the data - for example by keeping paper records in locked filing cabinets, with designated key holders who will only give the key to authorised employees. Within a computerised system, the system Administrator can control file access privileges with user IDs and passwords.

Risk assessment

Safe computing starts with documenting all the information assets you hold and defining their function within the organisation. Prioritise the protection of those assets according to the risks they present - either from unauthorised access, which might incur legal or regulatory action, or the impact on your business if you were to lose any of them.

Information security risk management cycle



Training

It's surprising how few companies bother to train employees in this vital area. Training reduces your exposure to many threats and will stand you in good stead should you ever be caught up in any legal or enforcement action. Don't limit training to a long list of things not to do, but cover good practice - some of which are documented in the following sections of this whitepaper.

Preventive technologies

Firewalls and anti-virus software can help reduce intrusions from hackers, but are not much use if they are installed then neglected, or used in isolation. An internet firewall behaves like a computerised security guard, checking to see if incoming data has a valid reason to enter the premises and keeping an eye on what goes out. Anti-virus software is more like an x-ray scanner, checking whether electronic packages coming into the building contain any malicious or dangerous material. Even if you have these systems, they will only work if you keep them up to date by regularly downloading and applying virus signature and system updates.

IT security checklist

- Have you set up your email server or firewall to block attachments such as .exe, .pif and .scr that are commonly used to carry malicious code? **Complete** ☐
- Have you configured the firewall to stop viruses/worms going back out from your network? **Complete** ☐
- Have you downloaded and applied the most recent security patches and updates for your operating system and anti-virus software? **Complete** ☐
- Have you trained users on safe email and surfing practices, such as not clicking on unknown attachments or links in emails purporting to come from their bank? **Complete** ☐
- Have you trained users to look out for suspicious occurrences and to report their suspicions to IT support? **Complete** ☐
- Have you set down an acceptable use policy restricting high-risk or non-work activities such as peer-to-peer file sharing, Skype accounts, downloading MP3s or pornography? **Complete** ☐

Business continuity planning

Besides the possibility of losing your data through misuse, virus infection or theft, your risk assessment should have identified physical and mechanical threats such as fire, flood, civil disorder and more common occurrences such as spontaneous system and disk crashes, or power failures.

Business continuity planning is all about taking steps to ensure you can cope with any of these disruptions. It is not practical to plan for every worst-case scenario, so you should try to work out how long you could keep going without a particular system or data source, and invest a sensible amount in insurance, back-up services or facilities to bring it back into operation within that time span. Thinking through the scenarios that could affect your organisation and devising suitable recovery plans could save your company from going out of business.

What your business continuity plan should cover

- **The circumstances** in which it would be applied.
- **Emergency procedures** - what to do when disaster strikes.
- **Fallback procedures** - how you would bring business processes back on-line and how long it would take.
- **Back-up systems** and premises to enable you to resume normal operations.
- **A schedule for testing**, reviewing and updating the plan.
- **Training** to make staff aware of the plans and their responsibilities in the event of any disruption.

Business recovery checklist

- **Have you documented** the information and systems that are critical to continuing the operation? **Complete** ☐
- **Have you taken** out business interruption insurance and checked that it provides adequate cover for the situations you might face? **Complete** ☐
- **Do you have back-up** computers on which you can restore your data and business systems? **Complete** ☐
- **If you have IT systems** on site, are your machines and networks protected by an uninterruptible power supply (UPS)? **Complete** ☐
- **If you use any external hosting** or bureau services, have you confirmed and tested that they have robust back-up and recovery processes in place? **Complete** ☐
- **Would you be able to** use your email/website/phone and fax lines in the event of a disaster? **Complete** ☐
- **Do you have access** to back-ups of the application software you use? **Complete** ☐
- **Have you filed copies** of all important user names, passwords and software licence keys in a safe place? **Complete** ☐

Good IT housekeeping

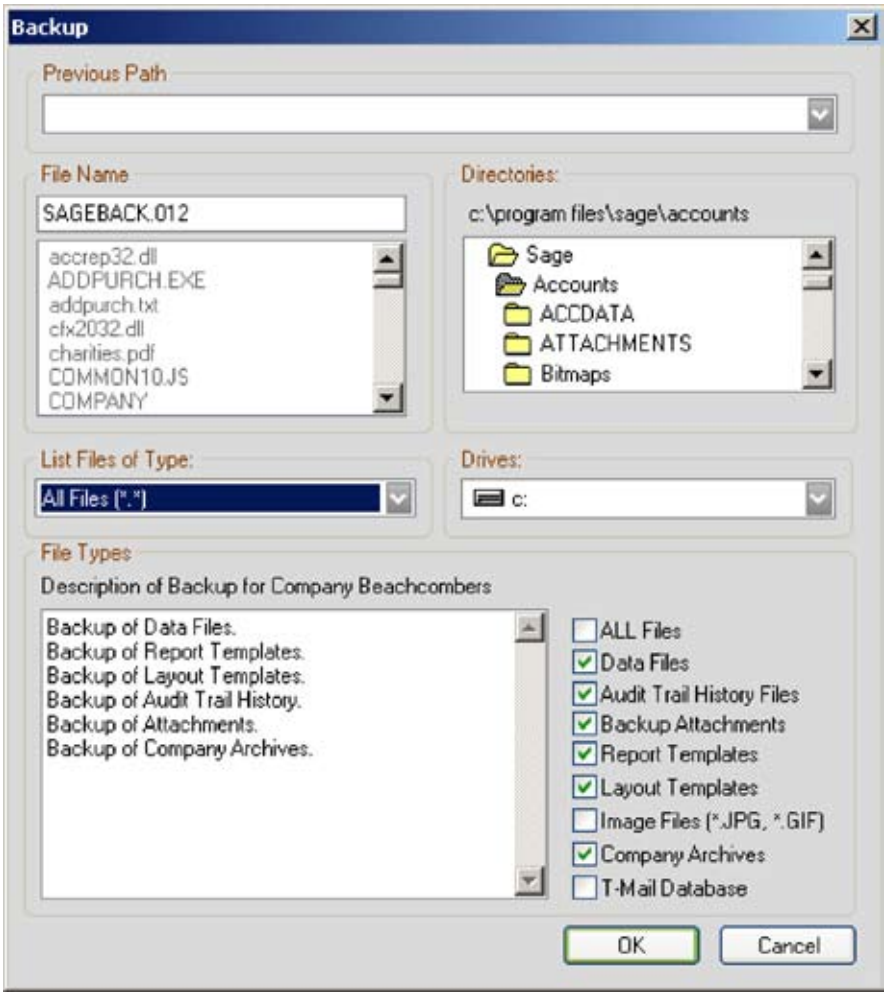
Based on the principles set out so far, it should be obvious that regular housekeeping is a critical component of your security policy. This section sets out some practical things you can do to protect your data and keep your business systems running smoothly.

Patching and updating

Because new viruses and vulnerabilities are appearing all the time, updating software is now a critical part of looking after any computer system. Make sure the person responsible for managing IT and data security has signed up with your operating system, anti-virus and application software suppliers to receive their security alerts. And make sure all updates are installed.

Data back-ups and recovery

The basic strategy for protecting electronic data is to make back-up copies on a regular basis and to store a copy off site. How often you take copies and how many you keep should be determined by your risk assessment and business continuity plans. But unless you have very low processing volumes, consider making daily back-ups. If you only hold weekly backups, you could lose up to a week's work.



IT housekeeping essentials

- **Create a register** of the applications and anti-virus software you use and check regularly for security or virus signature updates. Install them as soon as they arrive.
- **Test that you can restore** the data back-ups that you make, preferably by loading them into an off-site machine.
- **In addition to your regular back-up routine**, create a monthly archive by making and storing a separate copy for each month; this would be an opportunity to do a test restore.
- **If you use a commercial data protection service**, do not leave back-up media for them lying on the desk in reception.
- **Rotate your media** and never use the same tape or disk on consecutive nights.
- **Tapes and disks** do not last forever, so replace them every year.
- **Destroy or erase media** that you no longer use. Putting them in the rubbish is not secure.
- **Consider whether** you need to take measures to prevent unauthorised copies being made on to USB memory sticks or floppy disks. Software controls and hardware locks can do this, or you can even glue up the USB ports on your computers.

Data storage and back-up options

Hard disk drives

Hard disks lie at the heart of the vast majority of office systems and do occasionally break down. In the old days, hard drives were not favoured for backing-up data, but prices have come down so much that it is possible to set up servers to “mirror” your primary business database. Archive back-ups can be made from the second machine without affecting the speed of the main network. External, network attached storage disks are also a convenient, low cost way to make back-ups.

Tape

Magnetic tape has been the traditional medium for storing back-ups since the 1960s. It is a high-capacity, low cost option, but can take a lot of time if you are trying to restore an entire system, or to locate an individual file.

Solid state (“flash”) memory

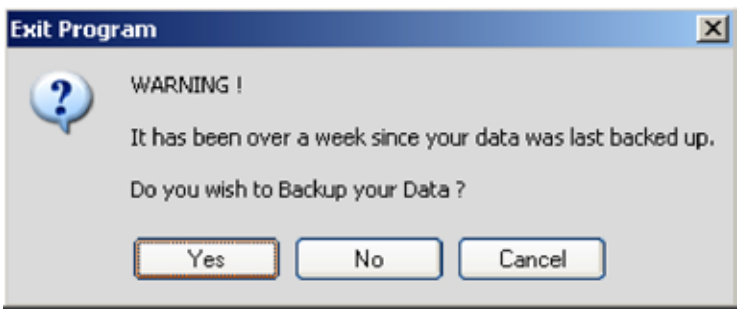
Digital camera memory cards, USB flash drives and some MP3 players are effectively giant random access memory chips and are very popular portable storage devices. Flash memory chip prices continue to fall, so they are increasingly being used for data back-ups. But being so portable, USB memory sticks are very easy to lose and some have flimsy connectors. They are more suited to smaller data transfers - for example to pass your accounts to an accountant - and should not be relied on as your primary backup device.

Optical disks

Recordable CDs and DVDs come in write-once (CD-R, DVD-R) and rewritable (CD-RW, DVD-RW, DVD-RAM) formats with capacties up to 9.4Gb of data - more than the average memory stick. They can be relatively slow to write, but offer very quick access and transfer times, and are frequently used for back-ups in smaller organisations. As with any other medium, watch for compatibility problems. A DVD written on your PC may not be readable on another machine, so test this before committing yourself to this route.

Online storage solutions

The principle here is basically the same as using a hard disk, but one that is hosted externally that you access over the internet. Online back-up can be a cost-effective way to manage your IT infrastructure, especially if you lack in-house expertise. You simply rent storage space from the hosting company by the gigabyte on a monthly basis, so issues such as disk size, type, operating system and so on are no longer your problem and the online archive can grow with you. As part of any online back-up strategy, check that the hosting company’s security and backup facilities are adequate.



Data protection resources

Information Commissioner's Office (ICO)
library - general guides, specialist industry advice and online tools
http://www.ico.gov.uk/for_organisations.aspx

ICO Register of data controllers
http://www.ico.gov.uk/tools_and_resources/register_of_data_controllers.aspx

AccountingWEB Focus on data protection
http://www.accountingweb.co.uk/item/176223

Wikipaedia on Acceptable use policies
(with links to several sample documents)
http://en.wikipedia.org/wiki/Acceptable_use_policy

Microsoft security site for the latest updates and advisories
http://www.microsoft.com/security

Windows Update - download operating system security patches
http://windowsupdate.microsoft.com