

FACTSHEET

Keeping your systems and data secure



Most businesses store information in both computer and paper-based systems.

Whatever storage method you use, keeping your data secure and confidential will help safeguard the information you need to run your business successfully and ensure you comply with relevant legislation.

If your business data is lost, misused or accessed without authorisation, it can be difficult to make informed business decisions. This can also put you at a competitive disadvantage. Serious data loss can put your whole business at risk.

This guide sets out the benefits of looking after your data, the principles of business continuity and the risks associated with using technology for storage.

Why data security is important

Data security is important to most businesses. Financial information - eg accounts and tax details - or employee information - eg payroll and personnel files - could be very difficult to replace. This could expose you to certain risks that need managing carefully. If you lost data through human error, fire, theft or for some other reason, you would at the very least have to spend time and effort collecting and reproducing the information.

More seriously, your sales, distribution and the **reputation of your business** could be directly affected. Projects in progress - eg new product designs - could be delayed as the work is redone.

Losing data in a **customer database** - such as customer names, contact details and information on their buying habits - could stop you targeting customers with appropriate mail shots or informing them of new products. This could mean you lose potential sales, and revenue.

A **virus** can damage your business by making documents stored on computers unusable. As more and more business is conducted via email, a virus can also make getting in contact with suppliers and customers more difficult. This can mean delays in making purchase orders and taking customer orders.



Risk management

Risk management is a process whereby risks are identified, assessed for their impact and likelihood and then, depending on their seriousness, reduced to an acceptable level.

Risk assessment can help you identify what risks your business faces and what would happen if you lost valuable data or your systems failed.

Carrying out a risk assessment

Firstly, you need to **identify potential hazards** to your data and systems. This will include looking at:

- physical threats - eg an office fire, power cuts, malicious damage and theft
- human error - eg input error, mistaken processing of data and careless disposal of data
- threats from corporate espionage and malicious damage

You can then consider how you currently secure data and information systems and **identify areas where you are vulnerable**. Consider:

- who has access to what information
- who uses the Internet, emails, data and how they do so
- whether access is restricted to those who need data for their work
- whether passwords are used and how they are kept
- what anti-virus software and firewalls you have in place to protect systems
- your level of staff training

Once this is done, you can prioritise the data and systems that are the most critical to your business, and decide which require additional security safeguards.

It is worthwhile drawing up a **business continuity plan** that employees can follow if systems fail. You should review your risks and security safeguards regularly to allow for changes in your business' circumstances or working methods.



IT security policy

Data security is only one aspect of the wider issue of IT security in a small business. It is good practice to write an IT security policy, setting out the general rules that will be followed to minimise IT security risks. This can then be used by management and employees to help ensure good practice.

You should develop a clear policy that takes account of common risks to your data. This will allow staff to understand and adopt appropriate security measures, and help create a security-conscious culture. The policy does not need to be lengthy or complicated, but should provide a reference point for all staff.

An IT security policy should cover both external threats such as viruses and internal threats such as the theft of data.

Your IT security policy might include:

- secure login identification for using IT systems
- logical access controls - limiting access to information and restricting access to the level needed for each job
- confidentiality rules for customer and business information
- plans for business continuity management

You also need a clear policy on what you consider acceptable use of the Internet and email, as these are usually the means by which viruses get into systems. Such a policy will normally prohibit the browsing of websites likely to contain offensive material. Similarly, you should prohibit the use of email to send or receive such material.

You should have a clear policy about the transmission of sensitive commercial information via email. In addition, you should clearly state your policy on the use of business email and web facilities for private use.



Types of threat - viruses

Computer viruses are created to cause a nuisance or damage computer systems. Viruses are programs that can replicate themselves, spreading from computer to computer, and often damage files. They are usually activated by opening a program or document and are often passed on to unsuspecting users.

There are several variants of the virus idea that you may see:

- Trojan - a program that appears to do something useful, but actually has a hidden destructive capability.
- Worm - a program that spreads itself over a network, reproducing itself as it goes. Worms can cause problems by creating a lot of useless traffic on your network.

You can be infected by:

- email
- clicking on website advertisements
- using contaminated external floppy disks or CDs
- attaching a corrupted removable media storage device via a USB port

Viruses can spread rapidly through your business network via internal email, an intranet, a shared disk, or an infected media storage device. They can overload or crash your computers and network.

They can capture keystrokes - everything you type, such as confidential passwords and credit card details - and they can destroy files.

Tools for combating the problem include the following:

- Install anti-virus software to detect viruses, stop them running, help you delete them and repair the damage. Remember to update the software regularly.
- Use the surfing security functions available with your web browser to restrict specific high-risk sites.
- Have a clear IT policy for acceptable use of business systems and email. Refer to this policy in employment contracts and provide training for the procedures.

Using and regularly updating anti-virus software to scan emails is good practice and can be invaluable for protecting your systems. Ensure employees are warned not to open attachments from unknown or suspicious senders. Restricting email and Internet access to those who need it can lower the risks of your systems being infected by a virus.



Computer misuse and hacking

Unauthorised access, known as hacking, involves someone breaking into your IT systems without consent. The threat can come from inside or outside your business. There are various legal penalties for hackers, but you should not rely on these to act as a deterrent.

If your IT systems connect to the Internet then you need to take special precautions against hacking, including the following:

- **Firewall** - this checks what goes into and out of your systems and blocks things that could be a threat according to a set of rules.
- **Intrusion detection systems** - these look for the signs of a hacking attempt on your systems and warn you if such an attempt is seen. Intrusion detection systems software can be obtained from a number of suppliers. You can find one using a web search. However, you will need some understanding of networks - or external support - to install and use them effectively. You might take action based on the warning, eg shutting down systems at risk.

Just as important as these tools is to keep your software up-to-date, as hackers will try to take advantage of older software that contains known weaknesses.

It is an offence to gain unauthorised access to a computer, even if no damage is done and no files are deleted or changed. It is also an offence to **purposefully change files** on a computer with intent and without authorisation, eg deleting files or even changing computer settings. If there is the intent to commit a further offence, eg access your bank account online to transfer money, then an individual could face five years imprisonment and/or a fine.

Don't rely on the law to protect your IT systems. It is a deterrent to hackers, but you must also take your own precautions. You must also ensure that your employees do not use your system to hack other organisations.



Internet and email issues

The inappropriate use of email and the Internet, eg using the Internet for non-work purposes, can have significant consequences for your business. This could be in terms of:

- damage to your business' reputation
- loss of productivity
- increased risk of liability and legal action, eg as a result of sexist or racist emails
- increased risk of virus attack

To avoid inappropriate usage, it is a good idea to clarify exactly what is and is not permitted at your business in a written record. You could ask employees to sign to confirm that they have understood the email and Internet policy.

You may also wish to consider putting guidelines in place regarding the use of online diaries, detailing the kinds of comments that are acceptable.

You certainly should prohibit the use of your business' IT systems for the distribution of information (perhaps via a website) that has no relevance to your business. For example, the distribution of music and video tracks might well result in civil action against your business.

It is also worth introducing electronic safeguards. You should ensure that all email that enters or leaves your business passes through virus checking. You can install filtering software that searches emails for specific words or phrases, normally obscene or discriminatory, or monitors which websites your employees are accessing, or filters the type of websites they can access. You can extend this filtering to block access to sites that are known to carry obscene or racist material.

These measures are not infallible. You should not rely on filters alone to protect your business.

Before monitoring your employees' email and web usage it may be worthwhile seeking legal advice as there are data protection issues to consider.



Data back-up and disaster recovery

The extensive use of computer systems makes business operations vulnerable to major problems, ranging from the accidental loss of data to deliberate sabotage. Storage systems, whether computer or paper-based, can be at risk of theft or physical damage through a fire or flood.

If computer systems are out of action due to any of these reasons, you may face problems in paying staff, complying with data protection law, taking customer orders, or having deliveries cancelled because you have not paid your suppliers.

Backups allow you to continue trading even if computer data has been lost. Backups consist of copies of data from your key systems. These copies are made to portable media like magnetic tapes or CD-ROMs. You should have a back-up routine (often done every day) as part of your **IT security policy** and you should check that this is being correctly carried out.

Best practice for backing-up data includes:

- giving one person the main responsibility for backing up, and designating a second to cover for absence
- using a different tape or disk to back up each day of the week and have a schedule for rotating them
- keeping backups secure - preferably off-site from the main business premises, eg in a bank box

Disaster recovery is intended to provide cover for really serious incidents such as fire or flood. It is good security practice to work out in advance how your business could survive and recover from such an incident, recording this in the form of a disaster recovery plan. Good data security and data backups are essential requirements for disaster recovery.

You should train your staff in business continuity methods - safeguarding essential functions. You should also consider IT security - see the page in this guide on **IT security policy**.



Staff training and data security awareness

Communicating security policies and procedures to employees, and getting their commitment to adopting such methods, is an important way of lowering the risk of loss or damage to your data and systems.

If your staff regularly use and process data, make them aware of data security and protection principles, and what actions might infringe on security or confidentiality.

Staff who use IT for their work need to know how to use systems and how to be security-conscious. If staff know the procedures to follow when systems fail, it will be easier for them to get back to work in such an event.

To create awareness about data security issues, it may be helpful to consider the following:

- Train staff to use systems correctly and give responsibility for backups.
- Communicate data security procedures and principles - consider obtaining signed declarations from anyone handling sensitive information.
- Plan how particular tasks will be carried out manually if technology breaks down.
- Set out IT good practice, including use of email, software and the Internet, and the use of passwords. Draw staff attention to it by referring to it in employment contracts.
- Involve staff in a risk assessment and in regular reviews of your procedures. See the page in this guide on **risk management**.