Data protection

A practical guide to IT security

Ideal for the small business

ico.
Information Commissioner's Office

The Data Protection Act states that “appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data”. This is known as the seventh data protection principle and is explained in more detail on our website, www.ico.gov.uk

Keeping your IT systems safe and secure can be a complex task and does require time, resource and specialist knowledge. If you have personal data within your IT system you need to recognise that it may be at risk and take appropriate technical measures to secure it. The measures you put in place should fit the needs of your particular business. They don’t necessarily have to be expensive or onerous. They may even be free or already available within the IT systems you already have.

We have produced this guide to give small businesses practical advice in the area of IT security.

What's in it for you?

Breaches of data protection legislation could lead to your business incurring a fine – up to £500,000 in serious cases. The reputation of your business could also be damaged if inadequate security contributes to high profile incidents of data loss or theft.

However, there are measures that you can put in place to prevent security breaches or limit the damage if they do occur.

The first step: assess the risk to your business

Before you can establish what level of security is right for your business you will need to review the personal data you hold and assess the risks to that data. You should consider all processes involved as you collect, store, use and dispose of personal data.

Consider how valuable, sensitive or confidential the information is and what damage or distress could be caused to individuals if there was a security breach.

With a clear view of the risks you can begin to choose the security measures that are appropriate for your needs. The next step is to begin putting them in place.

Use a layered approach to security

There is no single product that will provide a 100% guarantee of security for your business. The key to effective security is to have a layered approach, combining a number of different tools and techniques. If one layer were to fail then others are in place to catch the threat.

Checklist: Use a layered approach to security

- [ ] **Physical security**

  Equipment containing personal data could be stolen in a break-in. You should ensure that personal data on your systems is protected against these threats. Your servers should be in a separate room with added protection. Back-up devices should not be left unattended and should be locked away when not in use.

- [ ] **Anti-virus and anti-malware**

  You should have anti-virus or anti-malware products regularly scanning your network to prevent or detect threats. You will also need to make sure they are kept up-to-date.

- [ ] **Intrusion defence**

  You need to be able to stop breaches happening before they penetrate deep into your network, for example, by using a well configured firewall.

- [ ] **Access controls**

  Restrict access to your system to users and sources you trust. Each user must have their own username and password.

  A brute force password attack is a common method of attack, perhaps even by casual users trying to access your Wi-Fi so you need to enforce strong passwords, limit the number of failed login attempts and enforce regular password changes.

  Passwords or other access should be cancelled immediately a staff member leaves the organisation or is absent for long periods.

Employee awareness and training

Employees at all levels need to be aware of what their roles and responsibilities are.

Train your staff to recognise threats such as phishing emails and other malware.

Segmentation

You can prevent or limit the severity of data breaches by separating and limiting access between your network components. For example, your web server should be separate from your main file server. This means that if your website was compromised the attacker would not have direct access to your central data store.

Policies

A policy will enable you to make sure you address the risks in a consistent manner. Well written policies should integrate well with business processes.

Device hardening

Remove unused software and services from your devices. Older versions of some widespread software have well documented security vulnerabilities. If you don't use it, then it is much easier to remove it than try to keep it up-to-date.

Make sure you have changed any default passwords used by software or hardware – these are well known by attackers.

Secure your data on the move

What is the problem?

You need to ensure that the same level of security is applied to personal data on devices being used away from the office. Many data breaches arise from the theft or loss of a device (eg. laptop, mobile phone or USB drive) but you should also consider the security surrounding data you might send by email or post. You can take steps to reduce the effects of the theft by ensuring that personal data is either not on the device in the first place or that it has been appropriately secured so that it cannot be accessed.

What can I do?

- Encryption is a means of ensuring that data can only be accessed by authorised users. Typically, a password is required to 'unlock' the data. You can find more information on our website, www.ico.gov.uk
  - Full disk encryption means that the all data on the computer is encrypted.
  - File encryption means that individual files can be encrypted
  - Your encryption password should be a mix of upper and lowercase, numbers and special characters (i.e. #, &, !) and be kept a secret.
  - Some software offers password protection to stop people making changes to the data but this may not stop a thief reading the data. Make sure you know exactly what protection you are applying to your data.
- Some mobile devices support a remote disable or wipe facility. This allows you to send a signal to a lost or stolen device to locate it and, if necessary, securely delete all data.
  - Your devices will need to be pre-registered with a service like this.

- Only transfer personal data to mobile devices if you actually need it and remove it when you have finished.

Keep you and your systems up-to-date

What is the problem?

Computer equipment and software needs regular maintenance to keep it running smoothly and to fix any security vulnerabilities. Security software such as anti-virus and anti-malware needs regular updates in order to continue to provide adequate protection.

What can I do?

- Make sure any security software you have is switched-on and monitoring the files it should be.
- Keep your software up-to-date by checking regularly for updates and applying them. Most software can be set to update automatically.
- If your system is a few years old, you should review the protection you have in place to make sure that it is still adequate.
- You should also keep your knowledge of threats up-to-date by reading security bulletins or newsletters from organisations relevant to your business.
- You should also let your staff know about possible threats to your organisation. This could include alerting employees to the risks involved in posting information relating to your business activities on social networks or ensuring they know how to recognise phishing emails.

Keep an eye out for problems

What is the problem?

Cyber criminals or malware can attack your systems and go unnoticed for a long time. Many people only find out they have been attacked when it is too late even though the warning signs were there.

What can I do?

- Check your security software messages, access control logs and other reporting systems you have in place regularly.
- Make sure you can check what software or services are running on your network. Make sure you can identify if there is something there which should not be.
- Run regular vulnerability scans and penetration tests to scan your systems for known vulnerabilities – make sure you address any vulnerabilities identified.

Do you know what you should be doing?

What is the problem?

Some organisations do not have adequate levels of protection because they are not correctly using the security they already have, and are not always able to spot when there is a problem. You need to make sure that all your employees are aware of their roles and responsibilities and that they are clear about when action needs to be taken. You should also consider what actions you should put into place should you suffer a data breach.

What can I do?

- Take the time to review what personal data you currently have and the means of protection you have in place.
- Make sure you are compliant with any industry guidance or legal requirements.
- Document the controls you have in place and identify where you need to make improvements.
- Once any improvements are in place, continue to monitor the controls and make adjustments where necessary.

- Consider the risks for each type of personal data you hold and how you would manage a data breach. This way you can reduce the impact if the worst was to happen.
- You should also have an acceptable-use policy and training materials for staff so that they know their data protection responsibilities.
- Get a security expert to review your systems. This will highlight where your security vulnerabilities are and how best to address them.
- Don't forget about backups of your data. Backups should be made regularly, kept secure and properly deleted when no longer required.

Minimise your data

What is the problem?

The Data Protection Act says that personal data should be accurate, up to date and kept for no longer than is necessary. Over time you may have collected large amounts of personal data. Some of this data may be out-of-date and inaccurate or no longer useful.

What can I do?

- Decide if you still need the data. If you do, is it stored in the right place?
  - If you have data you need to keep for archive purposes but don't need to access regularly, move it to a more secure location. This will help prevent unauthorised access.
- If you have data you really no longer need, you should delete it. This should be in line with your data retention and disposal policies. You might need specialist software or assistance to do this securely.

Make sure your IT contractor is doing what they should be

What is the problem?

Many small businesses outsource some or all of their IT requirements to a third party. You should be satisfied that they are treating your data with at least the same level of security as you would.

What can I do?

- Ask for a security audit of the systems containing your data. This may help to identify any vulnerabilities which can then be addressed.
- Review copies of the security assessments of your IT provider.
- If appropriate, visit the premises of your IT provider to make sure they are as you would expect.
- Check the contracts you have in place. They must be in writing and must require your contractor to act only on your instructions and comply with certain obligations of the Data Protection Act.
- Don't overlook asset disposal – if you use a contractor to erase data and dispose of or recycle your IT equipment, make sure they do it adequately. You may be held responsible if personal data gathered by you is extracted from your old IT equipment when it is resold.

Where can I get more information?

What is the problem?

As illustrated by the range of topics covered in this guide, keeping an IT network safe and secure can be a complex task and does require time, resource and specialist knowledge. However, there are a range of organisations offering advice and guidance appropriate to your business.

What can I do?

It is difficult to provide a simple answer as each organisation processes personal data differently and is at risk from different threats. However, there are a number of organisations which provide advice specifically for small businesses.

You should encourage general security awareness within your organisation. A security aware culture is likely to identify security risks. The ICO provide a range of resources which you can order from the website, www.ico.gov.uk

Get Safe Online (www.getsafeonline.org)

A joint initiative between the government, law enforcement, leading businesses and the public sector to provide computer users and small businesses with free, independent, user-friendly advice that will allow them to use the internet confidently, safely and securely.

Business Link (www.businesslink.gov.uk)

Business Link is the government's online resource for businesses. The site contains information relating to IT security and e-Commerce and is specifically targeted at businesses.

A number of security vendors also offer seminars, webinars, newsletters, blogs and advice on their websites in addition to offering formal security audits and security testing services.

Action Fraud (www.actionfraud.police.uk)

Action Fraud is the UK's national reporting centre for victims of fraud or financially motivated internet crime.

Action Fraud records and refers these crimes to the police and provides victims with a crime reference number, support and advice.

If you would like to contact us please call 0303 123 1113

www.ico.gov.uk

Information Commissioner's Office,
Wycliffe House, Water Lane,
Wilmslow, Cheshire, SK9 5AF

April 2012

ico.
Information Commissioner's Office

Upholding information rights