Security and the Internet

Your IT system, and the information you hold on it, is valuable. Accidental or malicious damage is at best inconvenient and at worst disastrous.

Simply using a computer to hold and process business information creates a security risk. Connecting the system to the Internet increases the threats to which it is exposed and the potential damage from a security breach.

This briefing covers:

- The basic security features every computer system needs.
- The additional security required for systems linked to the Internet.
- Assessing how secure you are.

1 Basic protection

1.1 Physically protect computer equipment.

- Physical access to a computer is the most direct way of getting hold of the information stored on it.
  It can also be the easiest way to discover how to gain remote access at a later date.
- Portable computers are at particular risk. Consider restricting the information held on them and make employees personally responsible for their own laptops.

1.2 Design your **network architecture** to control security risks as far as possible.

- Use passwords to restrict inappropriate access across the network (see **2**).
- Focus on high-risk information and systems eg confidential and financial information.
- Standardise the configuration of your PCs. Use as few different types of operating system and application as you can.
- As far as possible, isolate or protect computers with direct access to the Internet from the rest of the network. But remember that the benefits of networking computers, to allow employees to share information and access the Internet, often outweigh the security risks.

  Restricting Internet access to a single PC can be an effective solution for businesses that make little use of the Internet.

1.3 Control any **point of entry** through which viruses or other problem material could enter your system.

- Make sure any material entering your

system is automatically checked for viruses.
- Run a regular virus scan of the entire system.
- Keep virus-protection software up to date.

1.4 Create a robust **back-up** system.

- Set up a procedure for taking regular partial and complete back-ups.
- Store back-ups off-site. Keep them away from heat, moisture and magnetism.
- Have a different tape for each day of the week. Replace tapes every few months.
- Conduct regular tests to make sure you can restore data from your back-ups.
- Make contingency plans for disaster recovery. For example, what would you do if both your system and your back-ups became infected by a delayed-action virus?

2 Passwords

2.1 Use passwords to control **access** to your system and the information held on it.

- Every employee must have a unique user ID and password.
- Set up the network so that employees can only access authorised parts of the system.
- Consider installing tracking software. This produces a log showing which users have accessed which information.
  Get legal advice before taking such a step.

2.2 Establish **password control** procedures.

- Avoid obvious passwords (eg birthdays).
- Consider only allowing passwords issued by the network administrator.
  Passwords should be given to employees in person, rather than distributed by internal email.
- Make sure passwords are kept secure. Employees often save their passwords on the system, or keep copies by their PC.
- Ban employees from telling anyone else their password, and from using another employee's user ID and password.
- Do not allow users to log in to more than one PC at the same time.
- Ask employees to log off when they leave their computers for more than a set period of time. For example, an hour.
  Or install password-protected screensavers.
- Change passwords regularly. You may want to set them to expire every 30 days so that users are forced to change them.
- Change passwords when an employee leaves, or when a security breach is suspected.
  Delete the accounts of former employees.

2.3 Set up procedures and train employees to use built-in **file protection** features of individual software packages.

Typically, these use passwords to control which users have access to, and can modify, a particular file.

3 Software control

3.1 Any **software** from outside your system can create a security risk.

- The software itself may have security weaknesses.
  For example, a hacker may be able to decipher the password which has been used to protect a word-processing file.
- The software may create security weaknesses in your system.
  For example, software which allows external dial-in access to your network.
- The software may be infected with a virus.

3.2 Control software **installation**.

- Ensure that only designated employees install software.
- Do not install unnecessary software.
  For example, free plug-ins which allow web-browsers to read audio and video files

➨ If you hold personal or financial data on your computer system, you will need to consider legal compliance issues. See **Website and email law**.

Security policy

A Your security will not work unless you set up good **procedures** and follow them.

- Make security a key element of the Internet and email policies you distribute to all employees.
  See **An email policy for your employees** and **An Internet policy for your employees**.
- You may want to make failing to follow procedures a disciplinary offence, although you should take legal advice before doing so.
  But the risk is that employees will cover up honest mistakes for fear of being disciplined, making matters worse.

B Assign clear **responsibility** for security.

- Your network administrator will usually have responsibility for selecting and implementing security solutions.
- Top management must take overall responsibility, including monitoring the network administrator's performance.
  Directors can be held legally liable for the security of certain types of data.

(unless you need them).

- Computer games, particularly free downloads from the Internet, are a major source of viruses and other problems.

3.3 Control software **configuration**.

- The way software is set up affects security. For example, you can set up Microsoft Word to check documents for macros before opening them.
- Where possible, configure software when it is installed, and do not let employees make changes to it.
  Secure configuration of Internet access software is essential (see **5.2**).

3.4 Regularly check for software **updates**.

- Major software suppliers issue patches to fix identified security weaknesses and other problems in their software.

4 Employees

Create a culture of security awareness among employees.

4.1 The **biggest risk** for most businesses comes from their employees. Deliberately or accidentally, an employee may:

- Fail to follow security procedures.
  For example, using another employee's password to save time.
- Load potentially harmful software onto computers.
- Reveal confidential security information.

  Only give Internet access and email accounts to those who really need them.

4.2 Where appropriate, make security a **recruitment issue**.

- The network manager, who controls your password and security procedures, is the greatest risk.
- Test attitudes to security in interviews and check the qualifications and references of IT employees carefully.

4.3 Make security a part of employees' **contracts**.

- Clearly set out your security procedures and policies. (See box, page 2.)

  Include training in computer security in a new employee's induction.

4.4 **Train** employees how to handle email attachments. See Email and An email policy for your employees.

- If you do not know the sender of an attachment, delete it.

4.5 Contractors and **temporary** workers are a particular risk.

- Issue them with their own passwords, and give them the absolute minimum of access to your system.
  Providing a temp with a permanent employee's password is a common error.
- Set temps' passwords and accounts to expire automatically.

5 Remote access

Once you are connected to the Internet, you need to control remote access to your system.

5.1 Protect yourself from downloading viruses by installing recognised **virus-checking** software and updating it regularly.

- Set up the software to scan all downloads and attachments automatically.

5.2 **Configure** your browser and email software to maximise security.

- Downloaded files should be saved and checked before you open them.
- Make sure dialling software automatically connects you to your Internet service provider (ISP). Keep your password secure.
- Set up a rigorous control procedure for dial-up connections to other computers. Any computer to which you connect represents a possible security risk.

5.3 Installing additional **firewall** software will improve security.

Firewall software varies from free to expensive. You will need computer expertise to use and manage it effectively.

The software can be used to:

- Make it difficult for unauthorised outsiders to gain access.
  A firewall is essential if you allow direct access to your system. For example, if you host your own website.
- Restrict data flowing into and out of your system.
  For example, to stop access to unauthorised websites and to control or prevent downloads.
- Produce a log of Internet traffic.

5.4 Choose an **ISP** that offers adequate security. See Internet service providers.

- Once you are connected to your ISP, anyone who manages to breach its security might gain access to your system.
  If your ISP hosts your website, anyone who gets past their security measures may be able to hack into your website.
- If you use your website for e-commerce, your ISP must be able to handle secure transmission of information and payments (see **6.2**).
- A good ISP will have software to minimise the risk of a denial-of-service attack. This occurs when hackers bombard you with high volumes of emails or hits on your website so that your system, or the ISP's, crashes.

5.5 Minimise the risk of **confidential information** being intercepted by email.

- Send highly confidential information using some other means (eg by post).
- Consider installing encryption software.

6 E-commerce

6.1 Treat transactions made on your website with **caution**.

It is easy for customers to assume a false identity online, or use someone else's credit card.

- Follow your normal procedures.
- Consider using digital signatures and certification to confirm someone's identity.

6.2 You need a secure **payment** mechanism.

- Ensure that payment details handled over the Internet are processed using secure technology (eg secure socket layers).
- Consider handling payments using traditional methods.
  For example, include product and ordering information on your website, but handle the final payment by post or telephone.

6.3 Building **trust** is important.

- Advertise the security features of your website on the site.
- Apply to join a Trust-UK affiliated scheme, such as Which? Web Trader.
  The schemes set certain standards for e-commerce that will give consumers added confidence when buying from your site.

See Trading on the Internet.

7 Planning security

Look for the right balance between physical, technical and procedural controls.

7.1 Start by **assessing the risks** you face. Ask yourself:

- How sensitive is the information you hold?
- How important is your system to your business operation?
- Is there any reason why someone would want to target your system?

Take into account any possible legal liabilities, particularly those under the Data Protection Act (see Website and email law).

7.2 Decide **how much** it is worth spending on security. Unless you are involved in e-commerce, or heavily dependent on your system, you may not want to spend much.

- Good procedures and virus-checking software will be sufficient for most small businesses.

7.3 Review the **effectiveness** of your security on a regular basis.

- For some companies, this could form part of an annual audit.
- If employees are not following procedures, take steps to enforce them or change your security measures.
- Consider using external suppliers to assess or test your security.

7.4 The British Standards Institution's Information Security Management System standard (BS 7799) can be a useful **tool** for identifying and managing threats to your information security.

- Achieving the standard can be expensive, but you can choose to use it as a benchmark without undergoing the certification process.

For more information, visit www.bsi-global.com.

Further help

There are other Directors' Briefing titles that can help you. These briefings are referred to in the text by name, such as Website and email law.

Published by BHP Information Solutions Ltd, Althorp House, 4-6 Althorp Road, London SW17 7ED
Tel: 020 8672 6844, www.bhpinfosolutions.co.uk