

Information Security: A Business guide to using the Internet

dti

The DTI drives our ambition of 'prosperity for all' by working to create the best environment for business success in the UK. We help people and companies become more productive by promoting enterprise, innovation and creativity.

We champion UK business at home and abroad. We invest heavily in world-class science and technology. We protect the rights of working people and consumers. And we stand up for fair and open markets in the UK, Europe and the world.

The internet has changed the world of commerce and business. With over 600 million people already connected – and the numbers rising daily – it provides opportunities for a whole new way of doing business – reaching customers you didn't even know existed, in markets previously beyond your reach.

The internet connects around 250 million host computers around the world. It is an open environment, whose whole purpose is to facilitate the exchange of information. Using the internet and other communications services brings tremendous benefit in increasing your competitiveness and obtaining business advantage. However, its very openness also makes it vulnerable to a growing range of security threats.

This brochure is for: any business looking to put appropriate security controls in place to protect their information.

It covers: the five steps you can take to make sure your business is protected.

Contents

- 01 The five steps
- 02 Step 1: Identify your business needs
- 06 Step 2: Assess the risks
- 13 Step 3: Develop a security policy
- 14 Step 4: Implement security controls
- 19 Step 5: Manage, monitor and maintain effective security controls
- 20 Summary
- 21 Further help and advice

Achieving best practice in your business is a key theme within DTI's approach to business support solutions, providing ideas and insights into how you can improve performance across your business. By showing what works in other businesses, we can help you see what can help you, and then support you in implementation. This brochure focuses on these solutions.

The five steps

If you buy or sell products over the internet, ensuring the security of financial transactions is a particular concern. For example, you need to be sure that credit card payments can be made safely.

The internet attracts hackers – people who like the challenge of attempting to access other people’s computer systems and information, by looking for and exploiting your organisation’s weak spots. Even though only a very tiny minority of users will disrupt businesses by stealing, deleting or altering information or even attempting fraud, that risk will always be there. And as the internet becomes ever more important in business terms, the risks are sure to grow.

Consequently, it is important that you go about connecting up to the internet in the right way to meet your business needs. You can then ensure that the appropriate security controls are being implemented to protect your company’s most valuable asset – your information. This booklet explains the five steps you can take to make sure that your business is protected:

- 1 Identify your business needs**
- 2 Assess the risks**
- 3 Develop a security policy**
- 4 Implement security controls**
- 5 Manage, monitor and maintain effective security**



Step 1: Identify your business needs

A marketing presence on the internet is now becoming a commercial requirement for companies – from the very large to the very small.

UK companies are finding that the internet is a cost-effective form of marketing, an easy way of providing information on their products and services to a mass market. What is especially attractive is that it provides a shop window to a whole new world of potential customers. With a website or an online shop, you can now promote your company and its products or services to a vast audience worldwide. You can be in business 24 hours a day, 365 days a year – gaining a real business advantage over your competitors. In fact, you can use the internet for business purposes in many different ways.

SECURITY OF THE INTERNET

Security is an important issue whatever use your business makes of the internet and the following pages describe how best practice can be used to reduce security risks.

It's a mistake to connect to the internet without clearly identifying your business needs. In some cases, the decision to use the internet is an arbitrary one – perhaps you've heard a lot about it, or someone in the IT department thinks it seems like a good way to go. In some cases, business internet connections are based on nothing more than an employee who has a connection at home and wants to have the same facilities at work. Or it can be because a competitor has a connection. There are problems with this approach – without a business case and defined needs you may buy an inappropriate service. It could cost more than necessary, provide services that you do not need or want to access, and could expose you to security threats without you realising. It can also be very time-consuming, and with e-commerce becoming much more popular, the potential risks are growing. A clearly defined business requirement is essential. If you are planning a website, for example, you need to consider how you will use it, and how security will be managed.

ASK YOURSELF

- What services are needed and what will they be used for?
- Which services will you prohibit access to because they're not needed or are undesirable?
- If you are considering providing a WWW page, what information do you want to publish and how frequently will it be updated?
- Who will be responsible for the service?
- Who will carry out a risk assessment and produce a security policy?

USES OF THE INTERNET



E-MAIL

This allows you to exchange mail messages with customers and suppliers anywhere in the world in as little as a few minutes. You can also send attachments such as orders and invoices with e-mail messages.



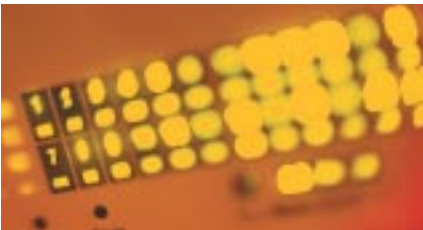
WORLD WIDE WEB (WWW) PAGES

You can readily provide or retrieve many types of information – financial, sectoral, reference and educational, or provide an online shop window for your products and services. In-depth company and market profiles can be obtained quickly.



INFORMATION EXCHANGE (FILE TRANSFER)

You can exchange information in the form of data files, often appended to e-mail messages as attachments.



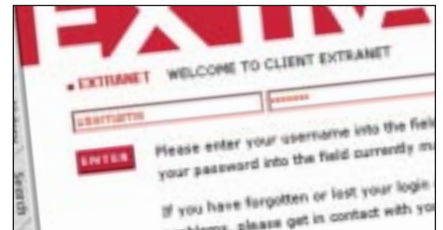
E-COMMERCE

More and more companies are using the internet to sell their products directly to customers. Everything from books to computers can now be bought by browsing through an online catalogue, and ordering with a secure credit card payment.



INTRANET

An intranet is a network – or a group of networks – which can be accessed by only those individuals who have been authorised to do so. It is an excellent way of sharing information, for example in a company which has sites in different parts of a city, or across regional, national and international borders.



EXTRANET

An extranet extends the concept of the intranet to encompass trusted trading partners. However, access is still restricted so that only those with a need to do so, and who have been authorised, can access the network.

SELECT YOUR INTERNET CONNECTION

There are several different ways of connecting to the internet. These range from:

- Connecting to the internet using a standard modem and telephone line (ie a narrowband/ dial-up connection) can be sufficient for a new business that requires e-mail and occasional use of the internet.
- Broadband is a term used to describe a range of high-speed connections to the internet. A broadband connection can send and receive data up to 10 times faster than a standard modem connection.
- Mobile connection using mobile devices and wireless connections provides new opportunities for increased flexibility and productivity, and can be very cost effective. Wireless networks provide a quick way of connecting devices without cables. They range from full Local Area Networks (LANs) to the connection of small local devices using methods (protocols) such as Bluetooth, which enables wireless communication using short-range radio technology.
- Third Generation Cellular is an emerging technology, sold mostly by mobile telephone companies. It enables users to send high-capacity items (for example, images, e-mail and music) to mobile devices using broadband speeds.

Unless your company is large, you are most likely to connect to the internet via a third-party service provider. Third party service providers are directly connected to the internet. In order to get connected, you will need a PC, a modem, and some communications software. You then dial in to your service provider's system, which acts as your connection into the entire global internet. Many service providers give telephone access via a local telephone number that allows you to reduce call charges. A basic internet service will provide you with an e-mail address and the facility to send and receive e-mail messages. You may also receive some free 'web space' which you can use to set up a website.

If you need a more advanced site giving details of your company's products and services, or want your company's name to appear in the web address, you will need a 'web hosting' account. This provides the extra facilities required to run a sophisticated website, such as an online store. Organisations with very busy websites may want a dedicated service, where the service provider dedicates a server to running a particular customer's site. Many large organisations prefer not to use a service provider; they have a direct connection to the internet either via a standalone PC or a networked PC.



WAYS TO GET ONLINE

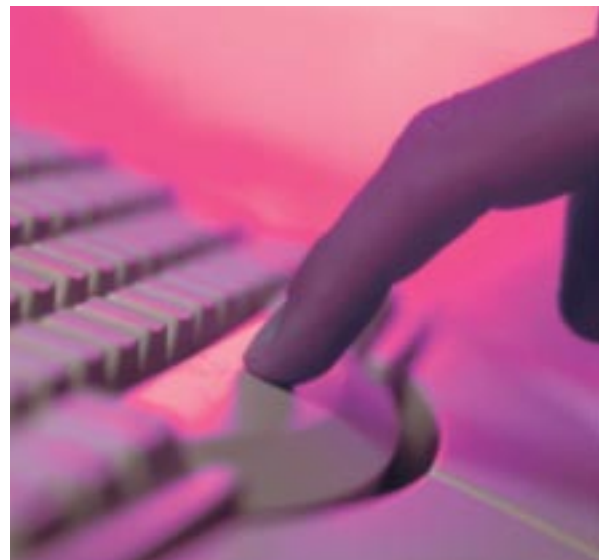
Today, everyone from supermarkets to banks is offering internet access services. There is a greater choice of service providers than ever before, but that means you must select very carefully. When choosing a service provider, you should find out if they provide security advice. Some of them provide security controls with their services. Similarly, some of the network suppliers offering Value Added Networks (VANs) – those typically used for financial information – offer strong security. However, some suppliers don't offer security controls at all. You should ask suppliers what security protection they provide, and ask them for details of reference sites. If you decide that you require some specialist advice on security, there are a number of companies that can help you. You should always establish the credibility of the company and its consultants.

Some questions you may wish to ask them include:

- What is their experience of your type of business?
- What is their track record in this field?
- Have they had recent experience of similar tasks?
- Can they provide reference sites?

More information on how to manage your connection securely is given in Step 4 – Implement Security Controls.

For comprehensive advice on all aspects of Information Security including specific sections on *Getting started with a computer system*, *How to choose an ISP*, and *Online trading*, see our dedicated business advice pages at www.dti.gov.uk/bestpractice/infosec



Step 2: Assess the risks

The internet is an unmanaged environment and consequently there are potential risks in using it. Therefore businesses need to take precautions and implement appropriate security controls to minimise these risks. However, before you can implement the right controls for your company, you need to understand exactly what the risks are.

UNDERSTANDING THE REALITIES

First, you need to understand the potential threats to your computers and information. Here is a summary of the realities:

- The internet is inherently insecure because it is a public network that has no central management or control.
- A company using the internet is responsible for the security of its own network, systems and information.
- There are people on the internet – hackers – who can attack your computer systems and information and who enjoy the challenge of attempting to gain unauthorised access.
- These hackers are well organised, often sharing news of hacks on special websites.
- Internationally agreed technologies for protecting financial transactions over the internet are available today.
- It is possible for messages to be read or modified.
- If you download any information from the internet, including e-mails and attachments, you are vulnerable to virus attacks.
- Unless properly encrypted, credit card payments can be intercepted and manipulated or stolen.
- Downloading of illegal or inflammatory material (eg pornography) could have legal consequences.



THE MYTHS ABOUT INTERNET SECURITY

There are many myths about the security of a connection to the internet. These are a few of the most common security misconceptions.

- The service provider is responsible for the security of your information, systems and network connections – No. It is your responsibility.
- Nobody would want to access the information you send across the internet – No. There are a number of people who are interested in this information and capable of accessing it.
- All systems connected to the internet are secure – No. Many are inherently insecure.
- Nobody can divert, copy or modify the information you send across the internet – No. There are people who are capable of doing this.
- Business financial transactions are safe when transmitted across the internet – No. This is only true if you take precautions to protect your information. Internationally agreed technologies for protecting financial transactions over the internet are available today.

IDENTIFYING THE RISK OF EXPOSURE

To understand the extent to which your business is exposed, you should assess the potential risks. You will need to consider:

- The value of the information
- The harm to the business which could result from a security breach
- The realistic likelihood of a security breach occurring, taking account of both current threats and existing controls.

Once you have assessed the level of risk you can then determine the controls that are needed to reduce the risks to an acceptable level. Security controls will help avoid:

- Breaches of confidentiality
- Invasion of privacy – personal and business
- Theft of information
- Unauthorised modification of information
 - denial of access and availability
 - vandalism or malicious damage to systems or information
 - financial loss resulting from credit card fraud, etc.

Further guidance on Risk Assessment is contained in the following publication: 'Information Security: Business Assurance Guidelines', available to download or order from the DTI, quoting reference URN 04/625 (please see the Further help and advice section).

TYPES OF RISK

The following table lists some of the risks commonly associated with use of the internet:

RISK TYPE	RISK DESCRIPTION
<p>Unauthorised access</p>	<p>There will always be cases of internal users trying to gain unauthorised access to applications and information, just as there will always be people outside who are keen to see what your systems are like, or what they contain. Risks are increased if you have something of interest or value. For example:</p> <ul style="list-style-type: none"> • Payment systems • Research information (especially if you are trying to develop things that will require patents or copyright to protect them after they become public) • Desirable software that can be downloaded • Politically and commercially sensitive information, such as salary levels, marketing plans and sales prospects.
<p>Viruses and worms</p>	<p>A computer virus is a programme designed to alter the way a computer operates, without the knowledge or consent of the user. There are two key aspects of a virus:</p> <ul style="list-style-type: none"> • They are self executing. Typically, a virus will attach itself to another programme on your computer, so that it is activated when that programme is used. • They are self replicating. Viruses are designed to spread from machine to machine and across networks. To achieve this, a virus will usually copy itself to other programmes on a computer, before executing any intended tasks. <p>There are a huge number of viruses in existence, carrying varying degrees of risk. Some are extremely malicious, with the ability to delete or damage files and programmes. Others are less destructive, but prove debilitating by jamming resources, causing systems to crash with consequent loss of data.</p> <p>A worm is a programme that is designed to replicate and spread throughout a computer system. It will usually hide within files (for example, Word documents), and distribute those files through any available network connections. Worms are often used to drain computer resources such as memory and network access, simply by replicating on a large scale. In addition, worms sometimes delete data and spread rapidly via e-mail.</p>
<p>Spam</p>	<p>Unsolicited commercial e-mail (UCE) or unsolicited bulk e-mail (UBE), generally known as 'spam', is a major concern for internet users.</p> <p>Spam is e-mail sent to a large number of e-mail recipients, without their agreement to be contacted, by the sender. This also includes those messages sent after a recipient of an initial e-mail has asked a sender not to send on any more e-mails, or has not indicated a wish for additional e-mails.</p> <p>Spam messages are usually commercial in nature, often containing 'get rich quick' schemes and illegal product information, but the term spam can also refer to any message that a user receives from a sender with whom they have no relationship.</p>
<p>Frauds and scams</p>	<p>Increasing numbers of frauds and illegal scams are directed at small companies and individuals. Greater use of the internet is one reason for this increase, although it is not the only factor. Improved technology has aided the development of new frauds whilst existing frauds have been adapted to exploit these improved technologies. Some common frauds include:</p> <ul style="list-style-type: none"> • Telemarketing frauds Offers which suggest an individual has 'won' a prize or is entitled to a 'free' trial of some product sound too good to be true, and often are. This type of scam can be an attempt to get you to divulge credit card or bank details, or may ask you to phone a premium rate number for more information.

RISK TYPE	RISK DESCRIPTION
<p>Frauds and scams (continued)</p>	<ul style="list-style-type: none"> <p>• Advanced Fee Frauds AFFs often (but not exclusively) originate from parts of Africa. Nigeria is notorious for this type of scam, so much so that AFFs are often called '419 Schemes' after Section 4.1.9 of the Nigerian penal code. This type of fraud usually involves e-mails from 'officials' claiming to represent a foreign government agency and wanting to transfer very large amounts of money into your bank account on a temporary basis and for which you will receive a generous fee. Again, this is usually an attempt to gain your bank details.</p> <p>• Lottery scams As the popularity of lotteries has increased in recent years, so too has the number of lottery-based scams. A well-known example is the Canadian lottery scam. This involves people (based in Canadian call centres) telephoning potential victims and advising them that they have won money on the lottery but before they can claim the prize, they must send money to cover processing fees. More than 80% of victims are aged over 65 and many are told not to use credit cards as these "can be traced" and prizes would be liable to local taxes.</p> <p>• False billing In a false billing scam, the fraudster sends a professional-looking invoice for products or services that were never ordered or received, hoping that it will be paid without investigation. This type of scam is usually aimed at larger organisations with big billing/ payment systems, in the hope that smaller invoices will go through unnoticed. In some cases, false billing is pre-empted by a telephone call from the fraudster, intending to make targets think that they may have bought something from the fraudster at some point.</p> <p>• Financial fraud If your business offers any form of online trading there are many ways you could be targeted by fraudsters. One of the simplest is the use of stolen credit cards to pay for goods or services. While card issuers carry much of the risk in such transactions, you are obliged to ensure that transactions are validated in accordance with your bank's contractual instructions. This is even more important when dealing with 'cardholder not present' transactions, especially when the delivery address of the items purchased is different from that of the cardholder.</p> <p>• Identity theft Identity theft is when someone uses information about a person (or an organisation) to assume his or her identity. They will then try to obtain goods or services using that identity – for example, jewellery, electronic items, bank loans and credit cards. There are many ways in which an identity can be assumed. Some fraudsters read formal death notices in local newspapers and seek to assume the identity of someone who has recently died, while others scour rubbish bins behind offices and shops, looking for credit card slips. There are also cases where fraudsters set up websites to elicit information as part of a seemingly legitimate transaction – a technique known as web spoofing.</p> <p>• Phishing 'Phishing' is the term used for the practice of sending false e-mail messages to a wide audience (using spamming lists) in the hope that some people will reply to them. Phishing e-mails are designed to look as if they come from a bank or similar organisation asking recipients to confirm their account details (including account numbers and online banking security information). They usually give a plausible reason for requesting such details – for example, to maintain an account.</p>

RISK TYPE	RISK DESCRIPTION
<p>Inappropriate usage</p>	<p>Inappropriate use can cover a wide range of activities. At one end of the scale:</p> <ul style="list-style-type: none"> • employees shopping online during work hours. <p>At the other end of the scale:</p> <ul style="list-style-type: none"> • criminal activity, such as selling secret corporate information. <p>One of the most obvious forms of inappropriate use is the viewing, downloading or distribution of pornographic material. A number of high profile incidents have proved severely embarrassing for household name companies, but it is a risk for any company, irrespective of size. Inappropriate use is not just about embarrassment. Other effects include:</p> <ul style="list-style-type: none"> • loss of productivity • reduction (or loss) of network bandwidth • increased risk of virus infection and other malicious code • increased risk of liability and legal action.
<p>Personal e-mail</p>	<p>Many companies allow staff to use company e-mail systems for 'reasonable' personal use. Common sense is the only yardstick that you can use to measure what is 'reasonable'. Such an approach is difficult to police consistently, for example:</p> <ul style="list-style-type: none"> • employee receives a joke via an external e-mail from a friend • employee forwards the joke to a colleague via internal e-mail • that employee forwards the joke to an internal distribution list • another employee forwards the joke to a friend externally • the joke is sexist/racist. <p>Your company could be held liable for any offence caused by the joke.</p>
<p>Deliberate disclosure of sensitive information</p>	<p>The following scenarios are examples of serious, deliberate abuse of e-mail:</p> <ul style="list-style-type: none"> • sending of sensitive data out of the organisation • private use or disclosure of customer lists • disclosure of price lists. <p>These examples are not exclusive to e-mail (anyone can carry printed copies of a price list in their briefcase). But e-mail certainly makes it easier, potentially less traceable, and allows distribution of huge volumes very quickly.</p>
<p>Inadvertent misuse</p>	<p>Most occurrences of inappropriate use are inadvertent, and often happen because people are trying to be helpful. For example:</p> <ul style="list-style-type: none"> • sending company documents to a home e-mail account for work at home • sending company documents back to the office from home • sending large files • cc-ing (copying) to excess.

RISK TYPE	RISK DESCRIPTION
<p>Inadvertent misuse (continued)</p>	<p>The first two points can expose company information to risks that are unlikely to happen in the workplace. Family members might see confidential information - few homes have the same physical security controls as offices.</p> <p>The last two points are simple errors that can make e-mail less efficient, and at worst, grind an entire enterprise to a halt.</p> <p>Other activities may not be seen as obvious misuse, but can cause considerable loss in terms of resources and time. For example:</p> <ul style="list-style-type: none"> • 'for sale' adverts • "who is coming to the pub after work?" • using e-mail rather than face-to-face or telephone conversations • sending e-mails to the next desk • poor housekeeping, such as not deleting old/unwanted messages.
<p>Damage to reputation</p>	<p>It takes years to build a good reputation but just a few seconds to lose it. There is no scientific way of demonstrating the negative effect on a company's reputation due to an information security incident or inappropriate usage. It is probable that the cumulative effect is greater than other more measurable ones, such as fines for breaching legislation or industry regulations.</p> <p>Business partners, customers, suppliers and associates may well disassociate themselves from an organisation that is seen to have behaved inappropriately.</p> <p>Potential employees may decide against joining such companies, and current employees may leave. The media may continue to make references to a company's past difficulties, making it even more difficult to rebuild confidence and reputation.</p> <p>Remember, companies are often liable for damage caused by the misuse of systems by staff; therefore the company's reputation is at stake if steps are not taken to prevent inappropriate use.</p>
<p>Broadband</p>	<p>There is some confusion about the term 'always-on', eg as it might apply to broadband, and what it means as far as security is concerned. It does not mean that:</p> <ul style="list-style-type: none"> • your computer has to be constantly switched on • your computer is vulnerable when it is switched off. <p>It does mean that:</p> <ul style="list-style-type: none"> • there is no need to dial out for a connection to the internet • an internet connection is always available when the computer is switched on. <p>If you have a broadband connection and your computer is switched off, there is no risk to your computer. However, if you have broadband and your computer is on, you may be vulnerable to malevolent attacks if appropriate security measures are not in place. The risks to users of broadband services are not new. Most already exist in one form or another but it is the 'always-on' technology and increased communication speed that makes it important for users to be even more aware of these risks.</p>

RISK TYPE	RISK DESCRIPTION
Broadband (continued)	<p>External risks</p> <p>Computer hackers seek to damage other people’s equipment and information just because they can, or because of a grudge. In some circumstances, people gain access to machines and use them as platforms for further illicit activity. Common activities carried out by hackers include:</p> <ul style="list-style-type: none"> • Denial of service attack. An attacker will flood a system with messages and data to prevent the target system from operating. • Eavesdropping. An attacker will ‘listen in’ to network traffic to find information that helps them to break into a system, or to gain valuable information. • Network intrusion. An attacker attempts to gain control of a system at a very fundamental level, avoiding a range of commonly used control systems and techniques. • Port scanning. An attacker uses a programme that automatically scans the internet for machines that have certain vulnerable configurations. Once found, the attacker tries to exploit these vulnerabilities for his/her own gain. <p>Single point of failure</p> <p>Smaller companies and individuals often combine their data and telephone lines using broadband. If the connection were to fail for any reason, all remote communication would be affected - hence there would be a ‘single point of failure’.</p> <p>System overload</p> <p>If your organisation has previously used low-speed (narrowband) connections for remote access (perhaps for salespeople or home workers), there is a potential impact when you switch to broadband. Connecting to the internet at low speed can be an unattractive option, so usage is kept to a minimum. However, the convenience of broadband may result in more people connecting more often, for longer periods. In turn, this could affect the performance of central servers and networks.</p>
Use of mobile technology	<p>Existing mobile technology is vulnerable to a range of threats. For example:</p> <ul style="list-style-type: none"> • Standard networks are usually installed within buildings, which automatically provide a degree of physical protection. In these circumstances, ‘tapping’ into cables requires physical access, whereas a wireless network is potentially open to anyone within range of the network access points. • Bluetooth and similar radio-based devices can be ‘hijacked’ and used maliciously. • Portable devices are easy to steal and were never designed to be secure. Any company information stored on a device is outside your control and can provide the means for unauthorised access to your core systems. • Some devices lose all stored data if their batteries are allowed to run down. • Mobile devices are susceptible to virus infection. Although the number of viruses that can infect such equipment is small (about 20 compared to the 55,000 that are known to threaten main systems), this is still a genuine threat. If a mobile device is infected, the equipment itself may not be affected. However, if it is used to communicate with desktop machines (e.g. for synchronising calendars), the virus could spread to larger systems.

Step 3: Develop a security policy

An internet security policy is a broad statement of your aims and intentions regarding connection and use. This is necessary to ensure that your business information and assets are protected from an attack via the service.

The policy will probably be quite short, perhaps one or two pages. Typically it should specify:

- the services that can be used
- who authorises connections
- who is responsible for security
- what standards, guidelines and practices should be followed
- users' responsibilities.

A fundamental issue is to decide who in your company will have responsibility for security. All users will have a role to play but ultimately senior managers are responsible for ensuring that appropriate security controls are implemented and maintained. An effective policy will help directors demonstrate that they have discharged their 'duty of care' in relation to information assets. The following steps will help you produce your own policy:

- research the content for the policy
- draft the policy
- obtain senior management approval
- issue the policy to all staff.

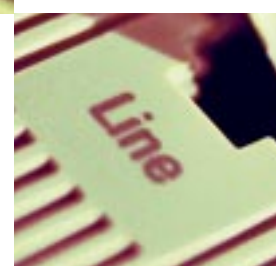
There are some documents that may help you in developing your policy.

The British Standards Institution (BSI) publishes an ISO/IEC standard entitled 'A code of practice for information security management' (BS ISO/IEC 17799). This provides best practice on information security management and on the content of a security policy. To obtain a copy, contact BSI on 020 8996 9001 or at www.bsi-global.com. The DTI publication, 'Information Security: A Business Manager's Guide' contains a draft Information Security Policy Statement and is available to download or order from the DTI, quoting reference URN 04/623 (please see the Further help and advice section).

Step 4: Implement security controls

As with all security management, a number of procedural, technical and people controls will be needed. Their complexity will depend on the service you decide to use.

The British Standard 'A code of practice for information security management' (BS ISO/IEC 17799) describes a number of controls that could be considered as guiding principles providing a good management framework for implementing information security. This will help you ensure that your internet connection meets your security requirements. You may also need specialist advice for some security requirements. The following table shows a correspondence between the internet risks discussed earlier and some of the control principles specified in BS ISO/IEC 17799.



RISK TYPE	WHAT TO DO – BEST PRACTICE
<p>Unauthorised access</p>	<p>You can minimise the risks by a combination of technology, procedures, policies and user awareness:</p> <ul style="list-style-type: none"> • install a properly configured firewall for your internet connection • make sure you have virus and content scanners (for e-mails and attachments) in place • establish policies for checking that your protection systems are working properly and that their logs are being examined appropriately • make sure your systems (especially firewalls) are updated on a regular basis with patches and hot fixes to ensure the latest known intrusion techniques are countered • employ basic housekeeping measures like regular backups, and disable logon accounts of people as they leave your company • make sure your staff are trained to spot any unauthorised access • review physical security on a regular basis.
<p>Viruses and worms</p>	<p>You can minimise the risks by a combination of user vigilance and awareness, and the use of anti-virus software. Make sure you have at least the following in place:</p> <p>Anti-virus software</p> <ul style="list-style-type: none"> • anti-virus software should be installed on your computer system • scan all incoming e-mail file attachments • update your anti-virus software on a regular basis. <p>User vigilance and awareness</p> <ul style="list-style-type: none"> • Operational environment <ul style="list-style-type: none"> – keep the office physically secure; intruders using infected floppy discs have been known to introduce viruses deliberately – ensure you (and your staff) know how to identify likely sources of viruses and worms – ensure you know who to call if your machines become infected. • E-mail <ul style="list-style-type: none"> – do not attempt to open any suspicious e-mails or attachments; treat as suspicious e-mails from: anonymous senders; strangers addressing you in a familiar manner and non-standard addresses – be especially wary of any of the above that contain attachments with .EXE, .SCR or VBS file extension names.

RISK TYPE	WHAT TO DO – BEST PRACTICE
Spam	<p>If you receive a spam message, contact your ISP to report the abuse of your e-mail service. Most ISPs will have a specific e-mail address to which abuses (including spam mails) can be reported. If you don't know what this e-mail address is check the home page of your ISP for information. Tips for combating spam:</p> <ul style="list-style-type: none"> • take care who you disclose your e-mail address to • consider using different e-mail addresses for different uses, eg one for e-mail and one for internet browsing • be aware that spammers target chat rooms and websites as sources for e-mail addresses • make use of blocking and filtering products available both direct to subscribers and via Internet Service Providers • do not respond to spam messages even if the sender promises to take your name off their list • use the opt-out box; when filling in online forms, always look for and complete any data protection opt-out boxes if you do not wish to be contacted regarding advertisements and promotions of any products or services.
Inappropriate usage (including personal e-mail, deliberate disclosure of sensitive information, inadvertent misuse and damage to reputation)	<p>Any organisation, irrespective of size, can take a few basic steps to minimise the risks from inappropriate usage. You should make sure you cover at least the following:</p> <ul style="list-style-type: none"> • appropriately configured virus defence software • a facility for checking, quarantining and managing e-mail attached files • a way of checking who has accessed what site on the internet • a legal disclaimer automatically attached to outgoing e-mails • a clear and unambiguous policy on e-mail and internet use • a means of communicating your policy to those who need it • awareness of legal implications for monitoring staff activity – this is a tricky issue that needs careful management.
Broadband	<p>There are a number of steps that you can take to reduce significantly the security risks associated with broadband. These include:</p> <ul style="list-style-type: none"> • Installing a firewall. These range from large-scale devices for companies to personal firewalls for installation on single machines. A firewall isolates a computer or a network from the public internet and inspects incoming data to determine whether it should be allowed to pass through or whether it should be blocked. • Configuring firewalls to protect ports (the entry points of a computer used by hackers) so that only authorised parties can gain access. • Ensuring that plans and procedures are in place which detail contingency measures in the event of your broadband service being lost. • Avoiding the creation of a 'single point of failure'. For example, if your telephone system operates through broadband it is a good idea to have a completely separate line that could be used if the broadband connection should fail.

RISK TYPE	WHAT TO DO – BEST PRACTICE
Broadband (continued)	<ul style="list-style-type: none"> • Using well constructed user names and passwords. • Installing anti-virus software and keeping it up to date. • Considering a Virtual Private Network for highly sensitive information and applications.
Use of mobile technology	<p>Mobile devices might be viewed as high-risk but this is not always the case. They do provide a challenge, but appropriate security can be implemented to protect files and information. For example:</p> <ul style="list-style-type: none"> • It is important that company policies are amended to address the risks associated with mobile technology. They should state the types of information that can be stored on mobile devices and the implications of doing so. • Find out who is using mobile devices (especially PDAs). Take a positive approach to educate users. • Portable devices are easy to steal and were never designed to be secure. Any company information stored on a device is outside your control and can provide the means for unauthorised access to your core systems. • Security packages (if available) should be installed on mobile devices. For example, most devices have an option to request a password as soon as the equipment is switched on. This is not often utilised. The use of passwords should therefore be mandatory in any company policies. • If you handle sensitive information on mobile devices, it may be sensible to investigate authentication and encryption software from third-party experts. • Mobile devices are getting smaller and many will be lost or stolen. Anticipate the loss of devices (and therefore data) and put relevant controls in place to reduce the impact of such an event. • If devices are loaned to employees, make sure they are returned when staff leave the company. • Ensure that company equipment is appropriately insured for use away from the premises. • Keep wireless network access points away from interference - for example, standard cordless telephones can affect them. It may be worth having your premises checked to ensure there are no interference 'hotspots'. • Wireless equipment often has security default settings - don't assume that these are appropriate for your needs. Always ensure that such settings and configuration files are checked and changed where appropriate. • If you are handling sensitive information across a mobile connection, consider using a Virtual Private Network (VPN) to ensure privacy.

The table on the previous pages suggests some security solutions for each of the services described under Step 1 – Identify your business needs. You will need to consider the alternatives and you may wish to seek specialist advice to help you. In each case, you will need a security policy, plus staff and management training and awareness.

CHOICE OF SOLUTION

The solution that you use must not only meet your business needs but also the requirements of your security policy. For many smaller companies, connection to a third-party service provider from a standalone PC will invariably be the best solution in terms of security protection and management.

STAFF AND MANAGEMENT TRAINING AND AWARENESS

If everyone understands why security controls are needed and their own responsibilities for them, you are less likely to have a security breach. People are your best line of defence – especially if they are well trained and informed. Any information security initiative should be accompanied by an appropriate education and training initiative.

Don't forget that if you hold personal information about any individuals, you will need to take account of the 1998 Data Protection Act and you may be required to register with the Information Commissioner. For further information please refer to the website at www.informationcommissioner.gov.uk or telephone 01625 545745.

Further practical advice on the Data Protection Act can be found on our website

www.dti.gov.uk/bestpractice/infosec

A publication entitled 'Information Security: BS7799 and the Data Protection Act' provides advice on how BS7799 can help you comply with the security requirements of the Act and is available to download or order from the DTI, quoting reference URN 04/621 (please see the Further help and advice section).



Step 5: Manage, monitor and maintain effective security

You should regularly review the risks to your business and the controls you have implemented to ensure that they are being used properly, and that they still provide a level of protection that meets the business needs and reduces the risks the business faces.

The technical configuration of some solutions – firewalls, in particular – is critical to protecting your information. Unauthorised changes can provide a security loophole that can be exploited. It is important that the internet connection is continuously monitored to record all security-related events, alarms and incidents. These records should be reviewed regularly. This is necessary to detect whether anyone has attempted to breach your security controls.

Many companies find that with use of the internet, their initial business reasons for using the service change – particularly where the initial connection provides only basic services. For example, companies that started using the internet simply for e-mail have gone on to develop websites, and may now be moving into e-commerce.

With confidence and experience in using internet services your requirements may well change too. If they do, then you need to go through the cycle again – from defining the business needs to implementing security controls. This is necessary to ensure that your security is appropriate, and that it will meet the changed business needs. The steps you need to take are illustrated below:

- revise the business case to incorporate the changed business need
- assess the risks
- revise the security policy to cater for any changes in the levels of risk
- implement the security controls that meet the policy requirements
- monitor and maintain the effectiveness of the security controls.

Summary

The use of the internet has radically changed the way in which companies do business. For most companies, the internet is now a basic business requirement and its use has brought increased efficiency and improved customer service. This increased connectivity has brought greater exposure to security issues. However, security concerns should not prevent companies from enjoying the business benefits of the internet. It is about ensuring that the risks your business faces are properly assessed and the appropriate controls are put in place to manage those risks.



Further guidance and a full listing of all our information security publications can be found at:
www.dti.gov.uk/industries/information_security

Further help and advice

INFORMATION SECURITY ISSUES

For help and advice on information security issues contact:

The Information Security Policy Team
Department of Trade and Industry
151 Buckingham Palace Road
London SW1W 9SS
Tel: 020 7215 1962
Fax: 020 7215 1966
E-mail: InfosecPolicyTeam@dti.gsi.gov.uk

Further guidance and a full listing of all our information security publications can be found at:
www.dti.gov.uk/industries/information_security

Or look at our information security business advice pages at: www.dti.gov.uk/bestpractice/infosec

ACHIEVING BEST PRACTICE IN YOUR BUSINESS

Achieving best practice in your business is a key theme within DTI's approach to business support solutions, providing ideas and insights into how you can improve performance across your business. By showing what works in other businesses, we can help you see what can help you, and then support you in implementation.

To access free information and publications on best practice:

- visit our website at www.dti.gov.uk/bestpractice
- call the DTI Publications Orderline on 0870 150 2500 or visit www.dti.gov.uk/publications

SUPPORT TO IMPLEMENT BEST BUSINESS PRACTICE

To get help bringing best practice to your business, contact Business Link – the national business advice service.

Backed by the DTI, Business Link is an easy-to-use business support and information service, which can put you in touch with one of its network of experienced business advisers:

- Visit the Business Link website at www.businesslink.gov.uk
- Call Business Link on 0845 600 9 006.

GENERAL BUSINESS ADVICE

You can also get a range of general business advice from the following organisations:

England

- Call Business Link on 0845 600 9 006
- Visit the website at www.businesslink.gov.uk

Scotland

- Call Business Gateway on 0845 609 6611
- Visit the website at www.bgateway.com

Wales

- Call Business Eye/Llygad Busnes on 08457 96 97 98
- Visit the website at www.busesseye.org.uk

Northern Ireland

- Call Invest Northern Ireland on 028 9023 9090
- Visit the website at www.investni.com

Examples of products and companies included in this leaflet do not in any way imply endorsement or recommendation by DTI. Bear in mind that prices quoted are indicative at the time it was published.

Published by the Department of Trade and Industry. www.dti.gov.uk
© Crown Copyright. URN 04/624; 04/04