



**dti**

**ACHIEVING BEST PRACTICE  
IN YOUR BUSINESS**

Information Security:  
Hard Facts



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.

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

Protecting information has never been more important. Organisations face a wide range of risks to their data, including virus attacks, inappropriate usage, unauthorised access and theft or systems failure

By understanding more about potential risks and putting a number of simple procedures in place, you will be able to raise the standard of your information security. Find out more about what you can do to safeguard your information.

**This brochure is for:** Any business interested in protecting its information.

**It covers:** The importance of information security, the different risks to information, preventative measures you can take, and how to deal with security breaches should they occur.

---

## Contents

- |   |                                    |
|---|------------------------------------|
| 02 Security – the right perspective       | 10 Theft – information is an asset |
| 04 Viruses – build up your immune systems | 12 Systems failure – be prepared   |
| 06 Unauthorised access – hacking away     | 13 Further help and advice         |
| 08 Inappropriate use – the danger within  |                                    |

# Security – the right perspective

It's important to get the right perspective on information security. In all likelihood, you are probably more at risk from a burglar than from computer crime, so the real issue is not the frequency of the dangers, but their potential consequences. A single break-in is not likely to bring your business to its knees, but a lapse in information security might.

## **MANAGEMENT CHALLENGE OR TECHNICAL ISSUE?**

Information security must be seen as a management and business challenge, not simply as a technical issue to be handed over to the experts. To keep your business secure, you must understand both the problems and the solutions. These vary in complexity – sometimes they are surprisingly simple – but almost all of them depend on training and staff awareness. Like practically every aspect of business, information security has a positive and a negative side. Ignore it, and you are storing up trouble. Manage it well, however, and real benefits can accrue. Think of it as a sensible health regime that not only helps prevent sickness striking but is also a benefit in itself.



## **BUSINESS BENEFITS**

- Take the opportunity to review and improve – secure systems are robust and efficient systems.
- Use security to differentiate your business – build confidence with your customers and suppliers.
- Increase your capacity – secure online ordering can boost your business, enabling you to open 24 hours a day, 7 days a week.
- Manage risk more effectively – cut down on losses and potential legal liabilities.



## **THE LATEST INFORMATION**

This brochure is only intended to alert you to potential problems and point you in the direction of their solutions. It does not provide comprehensive answers to this fast changing and growing subject. For that, visit our website at [www.dti.gov.uk/bestpractice/infosec](http://www.dti.gov.uk/bestpractice/infosec), which is free, comprehensive, and regularly updated.

# Viruses – build up your immune systems



## **THE THREAT**

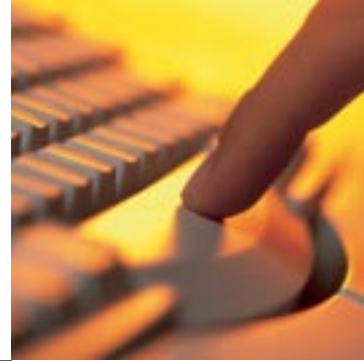
Viruses are programmes that enter your computer or network uninvited and then set out to damage it in some way. They are self-replicating – once they are released they spread without outside help. In the vast majority of cases they get into your system via e-mail, floppy discs or CD-ROM.

While some viruses are designed to destroy information, sometimes causing your systems to crash, others simply clog it up with unwanted and useless information. Signs to watch out for include the system slowing down and/or the unexpected appearance of files.

Almost every computer and network has come under virus attack – or will. Viruses vary in the levels of danger they present to your business, but like the flu, there is no such thing as a good virus – just varying degrees of discomfort and pain.

## **IMPLICATIONS**

- Commercial – loss of vital information, inability to function.
- Reputation – passing viruses on to customers and suppliers, lack of professionalism, service suffers while system is down.
- Financial – cost of recovery, cost of repair, management time.



## PROTECTION AND RECOVERY

Protection from virus attack demands a combination of technology, people and planning.

### Planning

Analyse the risk and decide on who manages virus protection. Plan for a crisis and for recovery. As soon as infection is suspected, isolate the infected server or hard disc, if possible. If your entire network is infected, isolate it until the problem is solved.

### Technology

Virus protection software is cheap, widely available and easy to manage. Manage is the key word – viruses change all the time, and software must be updated to cope with new threats.

### People

Your staff should make up the first and last line of defence against virus attacks. Backing up your system will help minimise loss. Awareness training and straightforward rules can prevent dangerous attachments being opened, for example, and ensure that floppy discs and CDs are scanned before being used.



## A VIRUS BY ANY OTHER NAME ...

Viruses can be subdivided into categories: macro viruses, file viruses and boot sector viruses. Within these categories, there are many types of virus, including Worms and Trojan Horses. The important thing to remember is that you need protection from all of them. Remember: while your Internet Service Provider (ISP) may scan for viruses, it's vital you run your own tests as well.

For detailed information, suggested procedures and important links visit [www.dti.gov.uk/bestpractice/infosec](http://www.dti.gov.uk/bestpractice/infosec)

# Unauthorised access – hacking away

## THE THREAT

Unauthorised access – or hacking – involves someone breaking into your system without your consent. The danger can come from outside your business, with the hacker gaining access to your office system or internet site over the telephone network, or inside your business, when the hacker is often an employee. It can involve obvious damage: your website vandalised, files altered and damaged; or less obvious: files can be copied and taken without your knowledge.

Some businesses are more at risk than others. Clearly if you rely on IT to generate income, your level of risk is highest because a hacker can shut down your entire operation. Equally, e-commerce is vulnerable to operational damage and damage to consumer confidence. But any organisation that deals in, or holds, sensitive information may find itself targeted.



## IMPLICATIONS

- Commercial – loss of e-business due to damage, loss of confidential customer information such as credit card details, theft of essential information.
- Reputation – brand damage through appearing vulnerable, damage to consumer confidence, service suffers as a result of vandalism.
- Financial – negligence and compensation claims, cost of repairs.



## PROTECTION AND RECOVERY

Protection from unauthorised access demands a combination of planning, technology and people.

### Planning

You need to be clear about the nature of the risks, and how much impact they could have. Planning must also involve clear awareness of roles and responsibilities, and proper training for using defensive technology. Recovery steps should be in proportion to the potential for harm. Develop a recovery plan before the worst happens and be sure that it includes measures to help repair damage to your reputation.

### Technology

Anti-hacking technology is dynamic – as soon as barriers are developed, hackers will find a way around them. So while software has been developed both to prevent hacking and to alert you to the risk, it must be maintained.

**Firewalls** sit between your internet access – the point of attack – and your network or server – the target. They can be installed on networks or individual servers.

**Intrusion detection systems** will alert you to people entering or testing your defences, and need regular updating.

**Vulnerability assessments** test your system for weakness and direct you to appropriate remedies.

**Hardening** involves checking your operating system to make sure that all defences are up and passwords enabled.

### People

Training should be used to build security awareness into your business culture. Passwords must be used intelligently, and access to sensitive terminals monitored and controlled.



## E-COMMERCE: PLAYING IT SAFE

Most browsers and servers support an encryption standard known as SSL (Secure Socket Layer). If you store customer details, you will need to encrypt the database, and monitor access. For high value transactions, you and your customers may want to create digital signatures for confidence and security.

For detailed information, suggested procedures and important links visit [www.dti.gov.uk/bestpractice/infosec](http://www.dti.gov.uk/bestpractice/infosec)

# Inappropriate use – the danger within



## **THE THREAT**

As a rule of thumb, assume that e-mail and internet access will be misused unless you have measures in place to prevent this. The most commonly cited misdemeanour at disciplinary hearings is e-mail and/or internet abuse.

The issue is complicated by three factors.

Firstly, the term covers a huge range of activities – from surfing the net during office hours through to e-mailing material that is obscene, offensive and damaging to your firm's reputation and prospects.

Secondly, everyone has a different view on what is obscene or offensive, and e-mail, with its potential for mass, instantaneous mailings, can magnify the problem.

Finally, moving digital information is dangerously easy. Someone who would never dream of accidentally sending sensitive information to the wrong postal address may accidentally click on the wrong e-mail address without even realising.

## **IMPLICATIONS**

- Commercial – loss of confidential information, loss of customers.
- Reputation – brand damage, evidence of poor management or lack of awareness of sensitive cultural/political issues.
- Financial – cost of disciplinary action, possible litigation, time-wasting by employees.



## PROTECTION AND RECOVERY

Protection from inappropriate use demands a combination of planning, technology and people.

### Planning

Being able to demonstrate that you have measures in place to stop inappropriate use of digital media is the first step to recovery – lack of these will damage your reputation still further. If the offence is going to trigger disciplinary action, it is important to gather evidence. Any incident should trigger a review of guidelines and training.

### Technology

Content checking software is triggered by words that suggest that your system is being used to transmit obscene or racist material, for example. It can also be used to help spot virus infected attachments. Usage filtering requires constant monitoring and is based on complex lists that offer guidance on what is and what isn't allowed. Monitoring usage is legally extremely complex and demands compliance with a wide range of legislation.

### People

Policy and training should be your first line of defence. Guidelines for e-mail and internet use must be practical, clear and realistic. Remind people of their responsibilities, their role within the organisation and how its success, and their future, depends on maintaining a good reputation with customers and suppliers.



## DIGITAL AUTHORITY

Remember: an e-mail carries the same authority as headed company notepaper. Make sure that staff understand the sensitivity of e-mail documentation, and how far and how fast it can spread through the system. Once you send an e-mail, it is beyond your control.

For detailed information, suggested procedures and important links visit [www.dti.gov.uk/bestpractice/infosec](http://www.dti.gov.uk/bestpractice/infosec)

# Theft – information is an asset

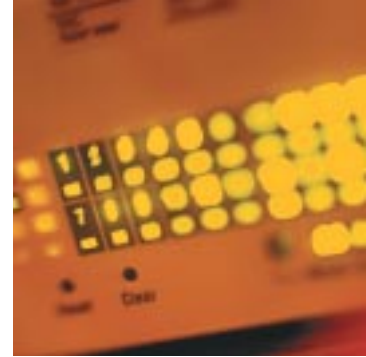


## **THE THREAT**

While everyone accepts that information has value, gauging the appropriate level of protection depends on accurate evaluation. The threat comes in various forms. Customers' financial records may be of interest to fraudsters, while research and development and copyright material could benefit your competitors. But even personnel records pose a risk. You may be obliged to hold these securely and in confidence, and loss can result in fines and litigation.

## **IMPLICATIONS**

- Commercial – loss of product information, client lists and/or essential business information.
- Reputation – trust and relationships with staff, customers and suppliers compromised.
- Financial – fines and litigation if confidential information is lost, cost of recovery.



## PROTECTION AND RECOVERY

Protection from information theft demands a combination of planning, technology and people. While the best protection is informed and well trained staff, you must coordinate this with physical security and technical/software controls.

### Planning

Analyse risks. Recovery benefits from a structured approach that allows you to identify quickly the extent of the theft, measures taken to block access and whether or not the authorities need to be involved. Back up training with robust non-disclosure contracts with staff and suppliers.

### Technology

Encrypt sensitive information, harden systems and make sure anti-hacking software is effective.

### People

Make sure you and your staff know what information is sensitive, and where it is stored. The easiest way to access sensitive digital information is from within your organisation, so you must ensure that internal access is appropriately monitored.



## DATA PROTECTION: IT'S YOUR RESPONSIBILITY

The Data Protection Act requires you to prevent unauthorised or unlawful processing of information you hold, and obliges you to prevent accidental loss or damage to the information. You must also tell the Office of the Information Commissioner what measures you have taken.

The international standard on information security BS ISO/IEC 17799 will help you formulate a policy, and reaching the standard will help reassure customers and suppliers.

# Systems failure – be prepared



## THE THREAT

The more use you make of IT, the more vulnerable you are to the system breaking down. This may not be immediately catastrophic but the loss of key information and the difficulty of performing relatively simple tasks will damage efficiency, productivity and customer relations – all the factors that give you a competitive edge.

Potential causes range from viruses to software problems, accidental fire to deliberate sabotage. For real security, you will need to guard against all of them.



## PROTECTION AND RECOVERY

Protection from systems failure demands a combination of planning, technology and people. Balance maintenance overheads against the cost of systems failure.

### Planning

Build safety into all your processes, from choosing secure premises to meticulously following back-up procedures. Successful recovery is impossible without thorough preparation, and this can involve agreements with hardware and software producers, and reciprocal arrangements with other businesses.

### Technology

Recovery sometimes involves high-level technical knowledge, so it is important to identify key personnel with the right skills before any problems occur.

### People

Ensure training involves crisis anticipation/prevention. Roles and responsibilities should be clearly defined.

## IMPLICATIONS

- Commercial – loss of vital information, inability to produce or process orders, possible collapse of business.
- Reputation – inefficiency, inability to deal with suppliers and customers.
- Financial – expensive counter measures, reduced efficiency.

## CHECK YOUR INTERNET SERVICE PROVIDER

Your ISP should have a clear security policy and be prepared to enter into a written agreement with you. BS ISO/IEC 17799 provides good guidance.

# 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](mailto: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](http://www.dti.gov.uk/industries/information_security)

Or look at our information security business advice pages at: [www.dti.gov.uk/bestpractice/infosec](http://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, providing ideas and insights into how to improve performance across your business. By showing what works in other businesses, we can help you see which approaches 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](http://www.dti.gov.uk/bestpractice)
- call the DTI Publications Orderline on 0870 150 2500 or visit [www.dti.gov.uk/publications](http://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](http://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](http://www.businesslink.gov.uk)

### Scotland

- Call Business Gateway on 0845 609 6611
- Visit the website at [www.bgateway.com](http://www.bgateway.com)

### Wales

- Call Business Eye/Llygad Busnes on 08457 96 97 98
- Visit the website at [www.busesseye.org.uk](http://www.busesseye.org.uk)

### Northern Ireland

- Call Invest Northern Ireland on 028 9023 9090
- Visit the website at [www.investni.com](http://www.investni.com)

Examples of products and companies included in this leaflet do not in any way imply endorsement or recommendation by DTI.

Published by the Department of Trade and Industry. [www.dti.gov.uk](http://www.dti.gov.uk)

© Crown Copyright. URN 04/619; 04/04