



Protecting our information systems

Working in partnership for a
secure and resilient
UK information infrastructure



Contents

	Page no
Summary	3
Introduction	5
Why do we need to protect information systems?	6
What are the risks facing information systems?	7
Why is Government concerned with protecting <i>all</i> information systems?	8
Who is involved?	9
What are we doing to protect information systems?	10
Combating hi-tech crime	11
Promoting education and awareness	13
Increasing protection	16
Addressing training and skills for professionals	19
Developing international co-operation	20
What you can do to make your information systems more secure	21
Conclusion	24
Glossary	25
Useful links	26

Summary

This document sets out the Government's approach to dealing with the various risks and threats facing information systems across the UK. It supports the UK Government Strategy for Information Assurance which aims to assure Government that risks to the information systems underpinning key public interests are appropriately managed. It outlines why and how the public sector and private sector, as well as individuals, must play a role in protecting the nation's information systems.

This document contains key messages for all those who need to consider measures for protecting information systems, from central government departments and board-level managers in large enterprises to small businesses and home users.

Organisations and individuals must take responsibility for the effective management of the risks facing their information systems. If these risks are not managed appropriately the effects could be detrimental to the continuity of government and national security as well as the social and economic well-being of the nation.

Key audiences and messages

Public sector

Trust and confidence in information systems are essential to ensure uptake of online public services.

- Your organisation must ensure senior (board level) responsibility for the risks facing your information systems.
- Your organisation must ensure that good risk management systems and procedures are developed and maintained to ensure the confidentiality, availability and integrity of its information systems.

- You must encourage awareness of information security issues within your sector in order to protect your ability to deliver public services.

Private sector

Businesses must adopt good information security practices in order to protect their own business interests as well as the overall economic and social well-being of the nation.

- Board-level managers must take responsibility for the effective management of your organisation's information systems to protect both your organisation and your customers.
- Good information security practices will help to inspire trust and confidence in the products and services you provide and therefore build a better business for you.
- If you are a small business, you must protect your information systems from various threats as the damage they cause can be costly to put right as well as affecting your organisation's reputation.

Home users and home business IT users

The Internet provides us with access to a vast supply of information and services; however, there are certain risks associated with going online which need to be addressed.

- You can go online safely by taking some simple security steps.
- Protecting yourself and your family online does not need to be time-consuming or costly.
- Poorly protected systems are not only a risk to you but also to others as they can be used as a platform to launch electronic attacks.

What needs to be done

Government is concerned with enabling the public and private sectors as well as individuals to achieve secure and resilient information systems. In order to achieve this we must all work in partnership to address the following five key areas in relation to protecting information systems, the information they carry and their users:

- Combating hi-tech crime.
- Increasing protection of information systems.
- Promoting education and awareness of information security.
- Addressing training and skills for professionals.
- Developing international co-operation.

Who is involved

There are a number of key government departments and agencies involved in developing the various strands of work relating to these five key areas. These include the Cabinet Office (Central Sponsor for Information Assurance), Home Office, NISCC (National Infrastructure Security Co-ordination Centre), the DTI (Department of Trade and Industry), the NHTCU (National Hi-Tech Crime Unit) and CESG (national technical authority for information assurance).

Introduction

The UK is an 'information society'. Information systems are now an essential part of the way we live. They enable us to communicate faster and in more diverse ways than ever before – by mobile phone, e-mail, instant messaging, 'Bluetooth' or wireless Internet connection. Not only do they provide us with the ability to indulge ourselves, such as booking holidays, but they run the critical systems behind our access to essentials such as water, electricity and even food. Information systems are so deeply embedded in our everyday lives that we tend to simply take them for granted.

The confidentiality, integrity and availability of information systems and the information they handle are essential if we are to have trust and confidence in 'cyberspace'. The continuous provision of goods and services to citizens depends on the smooth running of the information systems supporting them – particularly in the event of a crisis. Importantly, Government cannot make the UK's information systems secure by itself. Most information networks are neither owned nor operated by Government so we must each play a part in protecting *all* our information systems – from home computers and the IT networks behind large companies to local and central government systems.

In government, it is our duty and responsibility to ensure that the systems underpinning key public services are as secure as possible. For business, it makes commercial sense to protect yourself and your customers from any risks affecting your ability to provide the best possible service. As an individual, you should protect yourself and your family from problems such as computer viruses which can be costly to put right or indecent material which can cause distress. As well, it is important to consider that you may not simply be putting yourself at risk. Your unprotected computer could be used as a means of attacking other systems.

Who should read this document?

The UK Government aims to assure itself that risks to the information systems underpinning key public interests are appropriately managed. Due to the complex nature of today's networked society, the public sector cannot achieve this kind of assurance on its own.

This document is intended for the whole spectrum of information systems users and providers from the individual home user to any organisation, whether small or large, government or non-government. It is designed to give you an overview of why we need to protect information systems and what Government is doing, as well as to provide some key pointers to how we can work together to safeguard the UK's information systems.

Why do we need to protect information systems?

Any information that an organisation holds, whether it is simply a list of bank account numbers, client contacts or the formula for a best-selling pharmaceutical product, is an important asset and needs to be treated as such. Many home users may not be aware that they store enough information about themselves on their computers for criminals to impersonate them if they gain access to it, with such information as bank accounts and credit card details. Just as you would put a lock on the door to your home or office, perhaps install an alarm or even employ a security guard, so you should ensure that the information held on your computer system is sufficiently protected.

Technological advances in Internet connection introduce a new element of risk. The introduction of high-speed Internet connection (Broadband or ADSL) has been a great enhancement for business – particularly those small businesses that are able to access these services. However, it is important to recognise that because you are ‘always on’ then this exposes you to greater risk. Hackers can use an open ‘back door’ to get into your computer unless you have the right software installed to prevent them from doing so. Additionally, wireless networks, sometimes referred to as WLANs, enable a user to access the Internet via an organisation’s network. Yet at the same time they can also give a hacker access to your systems without them even having to enter your building.



What are the risks facing information systems?

Both businesses and government are increasingly dependent on the Internet for performing day-to-day tasks. Many home users are taking advantage of the Internet for banking or even their weekly supermarket shopping. This can bring benefits such as increased efficiency and cost savings. However, this development also carries significant risks that need to be addressed. These include:

- **Computer viruses ('worms' or 'trojans')** are malicious computer programs which can be very destructive, causing your computer to do things like overwriting your hard drive, deleting files or even making your machine inoperable.
- **Hacking** is when your computer, network or website is 'broken into' over the Internet. This can result in incidents such as theft of data or information, disruption or 'Denial of Service', deletion or alteration of files or website defacement. These 'attacks' can be carried out by a wide variety of criminals. So-called 'script-kiddies', young amateur hackers, often carry out the attacks for kicks or to show off amongst their peers. However, attacks may be organised by criminals seeking to commit fraud or identity theft for financial gain. Hacking or 'cyber-terrorism' can also be done for political reasons by terrorist groups, agencies of foreign states or activist groups.
- **Inadequate security policies and procedures** can mean that any organisation's information and information systems are put at risk. Unauthorised access to information held on computer systems is often as a result of poor management of security controls. For example, employees may share their password or contractors may be given access to information which can leave an organisation open to theft or fraud.
- **Physical accidents or attacks** such as fire or flood can destroy an IT or telephone system. Information systems are dependent on power and often need

to be kept cool, so a power outage can mean that the systems go down.

- **Errors** in systems software or hardware design are commonplace and can cause an otherwise secure system to be vulnerable.
- **Out-of-date systems and software** can mean that information may be lost or become unavailable. Small businesses often rely on software or hardware that is out of date and does not have even the most basic security controls. If the program becomes corrupted then it may be difficult to get at the information held on their systems.

Some facts about the risks

- In the National Hi-Tech Crime Unit's 2003 survey, 83% of businesses stated that they had experienced some form of hi-tech crime. Of the 44 financial institutions surveyed, three companies had experienced a fraud worth more than £60 million.
- A study by Novell in 2004 found that one third of UK workers write their computer passwords down and 1 in 10 keep them on a post-it note on their desk.
- The Novell study also revealed that 67% of sacked UK workers would be prepared to steal information that would be useful in their next job.
- The DTI Information Security Breaches Survey 2004 of 1,000 UK companies determined that 1 in 3 large businesses had had their websites attacked by hackers in the last year.
- The MyDoom virus was at its peak in January 2004 and was making up an estimated 1 in 12 of all e-mail messages and infecting 55 million computers worldwide.
- Two thirds of UK businesses suffered an incident in the last year where they had to restore significant data from backup (e.g. systems failure or physical theft) according to the DTI Information Security Breaches Survey 2004.

Why is Government concerned with protecting *all* information systems?

Government relies on information systems to supply services to, and on behalf of, citizens. The health service, emergency services, police, the military, places of education – all rely on IT and telecommunications. We must take steps to ensure that the systems behind these services are as secure and reliable as possible.

Moreover, we live in an interconnected and interdependent society. The stability of the economy and well-being of the nation depend on more than just the continuity of public services. For example, an electronic attack on the financial sector could have knock-on effects on the overall state of the economy.

One system is dependent, to a greater or lesser extent, on other systems functioning reliably and properly. If you run a small business, you may rely on many different services to ensure that you are able to run your business as best you can. You may have made your systems as safe and secure as possible. But if a key supplier or contractor of yours has not and suffers a systems failure then you – and many other businesses besides – may not be able to meet your customers' demands. Likewise, other suppliers are dependent on the safety of your systems.

Home users are increasingly becoming a focus for hackers since they are seen as a soft target. Criminals are exploiting the Internet as a means of obtaining personal information such as credit card or bank account details. They can even go to such lengths as downloading illegal files (e.g. pornography) onto personal computers without the owner's knowledge. PCs can also be used as 'zombies' for launching attacks on other computer networks.

Government must concern itself with the availability and reliability of *all* information systems to protect the interests of the people it serves. Since information

systems are used in just about every facet of modern life, the protection of information systems must reach across the whole range of government responsibilities. Each government department should also promote information security awareness amongst their sectors regarding the risks of leaving information systems unprotected.

Who is involved?

There are a number of key government organisations involved in all aspects of protecting the UK's information systems, from combating hi-tech crime to promoting information security to business.

Central Sponsor for Information Assurance (CSIA) – Cabinet Office
www.cabinet-office.gov.uk/CSIA

Government has recognised that there is a need for a strategic and co-ordinated approach to protecting the nation's information systems. The CSIA in the Cabinet Office plays a role in pulling together all the various projects going on across government and looking at any gaps or overlaps that might need to be addressed. It works with partners across government and the private sector, as well as its international counterparts, to help maintain a reliable, secure and resilient national information infrastructure.

Home Office www.homeoffice.gov.uk

The Home Office fulfils a number of functions in relation to information security. It is responsible for ensuring that the UK's Critical National Infrastructure (CNI) is protected as well as policing for hi-tech crime (e.g. crimes that are committed either against computers or with the support of computers or computer networks). It also deals with a wide range of crime reduction, police and anti-social behaviour initiatives which have an information security impact.

National Infrastructure Security Co-ordination Centre (NISCC) www.niscc.gov.uk

NISCC is an interdepartmental organisation set up by the Home Office in 1999 in order to minimise the risk of electronic attack against the UK's CNI. It works in partnership with the owners of the systems that support critical services in both the public and private sectors and offers a wide range of information and advice on best practice in protecting organisations' information systems. NISCC advises on how best to

protect information systems and, through investigation and work with UK and international partners, it assesses the threat of attack. It issues alerts and warnings, manages the responsible disclosure of new vulnerabilities, undertakes R&D work with partners, and promotes information sharing.

National Hi-Tech Crime Unit (NHTCU)
www.nhtcu.org

The NHTCU plays a key role in combating serious and organised hi-tech crime, both nationally and internationally. The team covers electronic crime (e-crime) prevention, reporting and investigation. Information assurance has a key role to play in ensuring that private and public organisations protect themselves from hi-tech crime and attempts to commit such crimes.

Department of Trade and Industry (DTI)
www.dti.gov.uk

The DTI aims to increase the productivity of UK businesses and encourage confidence in the use of new information and communications technologies. It has responsibility for all businesses, including small/medium enterprises (SMEs), and includes customers in the CNI. The DTI works with business to raise awareness of the importance of effective information security management and to encourage the adoption of security standards such as ISO/IEC 17799 and BS 7799. 'Foresight' is a DTI initiative which leads a project looking at future developments in IT in relation to Cyber Trust and Crime Prevention.

CESG www.cesg.gov.uk

CESG is the national technical authority for information assurance. It provides security guidance for government departments, agencies, local government and the wider public sector to help them achieve their business aims securely.

What are we doing to protect information systems?

Government has been concerned with the protection of the systems underpinning key public services for some time. In an increasingly interconnected and interdependent world we must encourage all sectors of society to take responsibility for the security of their own information systems. The nature of the work we are undertaking reflects the need to involve the public and private sectors as well as the community.

There are five key areas that our work covers:

- **combating hi-tech crime;**
- **promoting education and awareness;**
- **increasing protection;**
- **addressing training and skills for professionals;**
and
- **international co-operation.**



Combating hi-tech crime

'Hi-tech crime' or 'e-crime' covers any crime committed against or using computer systems, from hacking into an organisation's website and defacing it to online identity fraud or child abuse Internet sites. One example of this is 'phishing' which involves criminals using the Internet to deceive people into disclosing their credit card numbers, bank account details or other valuable information.

Criminals have sought to exploit the Internet as it offers a rapid and productive means of communicating as well as a good chance of anonymity. However, it is important to note that the Internet is simply a new vehicle for committing an offence; on the whole, it has merely changed the way in which many old crimes such as fraud, blackmail and the distribution of obscene and other illegal images are being committed.

Government regularly reviews all legislation to ensure that it is robust enough to criminalise offences whether they are committed on or off line. Where legislation does not adequately cover the modern means of offending, appropriate changes are made. For example, the Sexual Offences Act 2003 introduced a new grooming offence and risk of sexual harm orders, to help protect children from paedophiles who use the Internet.

In April 2001, the Home Office established the National Hi-Tech Crime Unit (NHTCU) as part of the National Crime Squad to combat national and transnational hi-tech crime within or that impacts upon the UK. As well as funding this unit, dedicated resources are also allocated to every local force in England and Wales to provide for the salaries, equipment and training of investigators in specialist units dealing with hi-tech crime investigations.

Online money scams

Scams seeking to deprive an individual of their money are not new crimes. The Internet has merely offered the perpetrators of such offences a new means of making contact with potential victims. Many online scams involve bogus online auctions, dubious work-at-home schemes and phoney credit card offers. One particular scam originates from West Africa and involves an e-mail designed to obtain the recipient's bank account details by offering to transfer large sums to them for safe keeping. It is often referred to as the 'West African advanced fee fraud' or the '419 fraud' after the relevant section of Nigeria's criminal code.

For more information on what to do to protect yourself from online fraud, go to <http://www.dti.gov.uk/ccp/scams/page3.htm#internet>

E-crime strategy

The Home Office is producing a government e-crime strategy which aims to provide a coherent, consolidated statement of the government position across departments in relation to e-crime. It provides a framework for government, law enforcement and industry action in response to e-crime, seeking to resolve current questions as well as advancing and informing the debate on longer-term issues.

The e-crime strategy will focus on issues such as the reporting of e-crime, crime reduction and prevention, legislation, the policing response, the role of business and the community in combating e-crime, and international co-operation.

E-crime and business

For business, online fraud and ‘Denial of Service’ (DoS is when an information system is prevented from working properly) attacks, and the effects of viruses, worms or trojans are of growing concern. Incidents of hi-tech crime are believed to be on the increase yet many of these incidents go unreported.

When a business is broken into and their office equipment is stolen or damaged, the first thing they tend to do is call the police. However, if that same business becomes a target for a hi-tech criminal who may be out to extort money from them or wishes to wreak revenge for some reason by attacking their computer systems, then they tend not to be so keen on involving law enforcement.

There may be many reasons for this. The most significant seems to be that they are concerned that the police will march into their offices, take away all their IT software and hardware, and that they will be left with no way of carrying on the business they were trying to protect. Alternatively, they may be afraid of the embarrassment they may be caused by the event being made public.

Confidentiality Charter

The NHTCU is well aware of the concerns that industry has regarding the disruption any investigation might cause a business. In response it has developed a *Confidentiality Charter*. The Charter is designed to provide reassurance that business can report hi-tech activity and attacks without fear of causing unwelcome interference to their business.

The NHTCU has an Industry Liaison Team which is working to establish relationships with business to promote the mutual exchange of information. This relationship is vital to creating a safe and lawful digital environment for organisations to conduct their business in.

Foresight Cyber Trust and Crime Prevention (CTCP)

The CTCP project explores the underlying scientific evidence, takes technologists’ views of what might be possible and makes a leap into the future of 2018 to show some of the ways in which the UK might

evolve. It aims to identify and tackle issues which information and communications technologies might present particularly in relation to e-crime. For more information go to <http://www.foresight.gov.uk/>

Take steps to protect yourself from online scams

- Know who you are dealing with: whenever you access Internet banking, always type the bank’s address into your web browser. Never go to a website from a link in an e-mail, and if you do so inadvertently, never enter your personal details. If in doubt, contact the bank on a telephone number from a separate source.
- Keep passwords and PINs safe. If you write them down, make sure they cannot be identified by anyone else.
- Be on your guard if you receive unsolicited e-mails or calls asking you to disclose any personal details or card numbers. Keep this information secret. Be wary of disclosing any personal information to someone you don’t know. Your bank and the police would never contact you to ask you to disclose your PIN or your full password.
- Keep hold of your cash. Don’t be conned by convincing e-mails offering you the chance to make some easy money, especially if they come from outside the UK. It is much harder to trace messages from overseas and to prove that the senders are who they say they are.
- Keep your PC secure. Use up-to-date anti-virus software and a personal firewall and, if your computer uses the Microsoft Windows operating system, keep it updated from the Microsoft website. Be extra careful if using Internet cafés or any PC that is not your own and over which you have no control.
- If in doubt, a good place to get advice on how to protect your PC and yourself online is your bank’s website. Look at this regularly for guidance.
- Always check your bank statements. If you notice anything unusual on your account, contact your bank immediately.

Sources: NHTCU, APACS and the British Bankers Association (BBA)

Promoting education and awareness

Despite all the recent news coverage of computer viruses such as MyDoom in early 2004 and Sobig in summer 2003, many businesses and home users are still not taking steps to protect their information systems. Government is working with industry to promote awareness and education on a wide range of issues relating to the protection of the nation's information systems.

Information security for business

As a business, information is probably one of your most important assets. If you are denied access to the information you hold on your IT system for one day – maybe that wouldn't cause you too many problems. But what if it was for a week – or you lost that information altogether – or perhaps worse, that information was duplicated and passed on to a direct competitor?

Sadly, many businesses do not even have the most basic protection for their systems. Information security covers measures such as the installing and updating of anti-virus, patching procedures and access control of systems. Good information security practice must be adopted as an integral part of your overall business processes and can prevent your business from costly 'clean-ups' after an event. Perhaps more importantly, information security planning can add value to your business and demonstrate to your customers that you can provide a trustworthy and reliable service.

It's not all about 'firewalls'

Information security practices should reflect the needs of your business. It is vital to realise that information security is not simply about installing firewalls or anti-virus software. What is more important than the software product a business might choose to install is addressing the whole issue of information security

processes that need to be carried out – from PIN or password control and anti-virus updates, to information back-up procedures.

These may seem time-consuming tasks but, as many organisations have learned, a bit of work up front

Controlling access to information

According to the DTI Information Security Breaches Survey 2004, 1 in 5 large businesses were affected by weaknesses in access control measures to their information. This means that individuals had been allowed access to information without authorisation which could result in crimes such as fraud or extortion. Over half of all companies affected said this was their worst information security incident of the year, ahead of virus infections. This kind of security breach can cause major disruption to the business over a long period and can involve significant staff time spent on investigating and then fixing the problem (10–20 staff days on average). They also tend to be the most costly of any security incident – 15% caused more than £100,000 of legal fees, investigation costs and fines.

What you need to think about:

- Who should have access to what information within your company?
- Regularly review your systems for individual user access rights
- Consider using an automated system for access to information if you have many users accessing many different systems.
- Passwords may not be enough. There are means of user authentication such as tokens, smartcards or even biometrics.

Source: DTI Information Security Breaches Survey 2004

Who's using your Internet connection and why?

A medium-sized company had provided staff with Internet browsing access for some time but the access was shared amongst employees with one username and password per group. This meant that the business had no way of tracking Internet usage to particular users. They became concerned about the lack of monitoring and eventually installed a system whereby users within the company would gain Internet access by simply logging on to their own computer. By law, the company had to notify staff that the system was in place and that their usage would be monitored.

Over a number of days they spotted a significant amount of accesses to an Eastern European 'brides for western men' website. The action was traced to a contractor who was questioned about the activity. It became clear that he was running the business as a sideline and accessing the site to maintain it.

Apart from costing the company a great deal of time and money in terms of his contracted time being spent on this work and not the company's, there was also a question mark over the legality of the site.

What you should do:

- Make sure that Internet access can be traced back to the user – if someone is accessing illegal sites, you need to find out about it and deal with it promptly. Otherwise, you could be legally liable.
- Publish a policy on what is acceptable and what is not in terms of Internet access.
- Avoid using the same username and password for a number of users.

For more information go to <http://www.dti.gov.uk/bestpractice/technology/security.htm>

can save a lot of trouble and cost after the event. After all, there are added benefits from making your business more secure. Your customers will have more trust and confidence in your business if they know that you have made your information systems as secure and reliable as possible.

Web-savvy customers want reassurance that your systems are safe and they are increasingly likely to demand proof. As international standards for information security become more widespread, you may be asked to demonstrate the dependability of your information security arrangements.

The DTI promotes the benefits of good information security practice and provides objective information and advice for businesses on how best to protect your business. You can find this information at http://www.dti.gov.uk/industries/information_security

Warning and alerting systems

It is difficult to establish with any accuracy the actual cost of computer virus and worm attacks. But what is certain is that these attacks are currently increasing in frequency and in sophistication. The recent Sasser worm caused significant problems for major services such as airlines and the coastguard. Early warning is vital to counteract the effects of such attacks and to enable organisations to put appropriate measures in place.

Warning and alerting systems are an important tool in combating electronic attack. NISCC operates the UK Government's Computer Emergency Response Team (CERT) called UNIRAS which issues technical alerts and briefings. To assist in response, NISCC undertakes research into computer network vulnerabilities and alerts stakeholders as necessary.

Information sharing

NISCC promotes a number of information sharing groups. These groups gain quick information on new problems so that advice on ways to manage them can be implemented in time to prevent damage. Organisations can protect their identity and reputation by telling NISCC about a new attack method or vulnerability and allowing this information to be passed on to others in an anonymised form together with advice on what to do.

NISCC has also developed an initiative called WARPs (Warning, Advice and Reporting Points). These enable communities with similar interests to link together and share information in a secure and trusted online environment. They can give early warning of electronic attack, threats and vulnerabilities which can be tailored for the communities' particular requirements. London Connects (see next page) has been running a WARP for London boroughs, and Kent has recently set up a similar system. Other WARPs in business communities and amongst further public sector bodies are being planned.

WARPs (Warning, Advice and Reporting Points)

Local government services are increasingly being delivered over the Internet. This provides citizens with a convenient method of interacting with local government, whether for finding out about local childcare services or paying council tax. In order to bolster uptake of online government services, it is essential that the systems supporting them are as resilient as possible. Warning and advice systems provide a valuable service in alerting organisations to possible vulnerabilities and giving information and advice on dealing with threats such as computer viruses and worms.

The London Connects WARP (LCWARP) provides London boroughs with a secure and trusted warning and alerting system for all forms of electronic attack. The service gives information bulletins about cyber-threats, good practice advice and incident reporting. The information is co-ordinated and managed from a central point and can be tailored to the needs of the local government community.

The LCWARP was introduced as a pilot scheme with funding from the CSIA in the Cabinet Office. The Office of the Deputy Prime Minister is now providing further funding to explore the establishment of local authority WARP services on a national basis.

NISCC has developed a freely available WARP Toolbox to make it easy to establish further WARPs. For more information on WARPs go to <http://www.niscc.gov.uk>

Promoting safe use of IT for children

The Department for Education and Skills (DfES) and the British Educational Communications and Technology Agency (BECTA) promote acceptable and safe use of information and communications technology (ICT) for schools. This combines knowledge of the needs of education with an understanding of the power of technology. Information and advice on the safe use of the Internet and ICT are available on the Superhighway Safety website (<http://safety.ngfl.gov.uk/schools>) and the ICT Advice website. BECTA has also recently launched the Internet Proficiency Scheme to help teachers educate children on staying safe online.

The Parents Online campaign (<http://parentsonline.gov.uk/safety>) run by the DfES aims to raise awareness amongst parents of how to help children to go online safely. The campaign provides online learning kits in age-related categories and encourages parents to organise Internet safety events and workshops offering advice and support to local communities.



Increasing protection

Government must ensure that its systems meet internationally recognised security standards as well as requirements for legislation such as the Data Protection Act. If key public information systems are to be adequately protected, Government must work with industry to ensure they are able to supply the necessary products to provide the right level of protection.

Information security products

The CSIA in the Cabinet Office is working with software suppliers to ensure that there is a range of assured products that meet the information security needs of the whole marketplace. The CSIA is also exploring opportunities for working with industry to influence future product development.

The Cabinet Office sponsors a technical capability programme at CESG to promote the development and use of risk management capabilities and the use of assured information security products. This programme will form the basis for research and development of products that are required to protect key UK Government systems and related services.

GIPSI (General Information Assurance Products and Services Initiative) is led by the CSIA and brings together representatives from central and local government, industry, commerce and academia. The group works on defining and promoting UK pan-governmental requirements for information assurance products as well as establishing the means to ensure that those requirements are met.

The Office of Government Commerce, CESG and the CSIA in conjunction with information assurance (IA) product vendors are also establishing CIPGOG (Civil IA Products and Services Co-operation Group). The

group aims to serve the requirements of those working in information assurance across the UK public sector.

Making government systems more secure

Government needs to ensure that the systems underpinning key public services are made as secure and resilient as possible. Government systems from the military and health to education authorities all need to be adequately protected. As more and more government services go online, it is vital that we ensure that the public has trust and confidence in those services. Public sector organisations must create policies and processes to minimise risks to their information and the systems in which it is handled.

There is a requirement that all central government departments must meet internationally recognised information and security management standards (e.g. ISO/IEC 17799 and BS 7799) for their systems. The Cabinet Office has produced an *e-Government Interoperability Framework* (e-GIF) which defines the technical policies and specifications governing information flows across government and the public sector. Public sector bodies must be vigilant in monitoring and auditing the systems holding their information. The CSIA has produced and maintains *security framework documents* which provide key guidance for both central and local government on providing secure online services.

Telecommunications resilience

The CSIA works with other government departments in maintaining emergency telecommunications planning and business continuity plans. The CSIA, in conjunction with industry, addresses the vulnerabilities of public sector and commercial telecommunications systems as well as those of the financial and banking sector.

Privacy, data processing and data sharing

The public sector is responsible for the collection and provision of an enormous amount of data which it deals with on a daily basis. Some of this information is of an extremely sensitive and personal nature and needs to be treated with the utmost respect and confidentiality. Patient health records, social service details, tax returns – all are held on information systems. Private sector organisations also handle personal data on behalf of citizens and must adhere to legislation governing the protection of that information.

Information systems must protect the information they handle by making the correct information available when necessary and only for use by those people who are authorised to have access to it. The Data Protection Act (DPA) lays down the principles for the processing of personal data. Sharing of data is covered not only by the DPA, but also the Human Rights Act as well as common law confidentiality. The Department for Constitutional Affairs has published guidance on *Data Sharing in the Public Sector* and will be publishing a public service guarantee on data handling. For more information go to the Department for Constitutional Affairs website (<http://www.dca.gov.uk>).

Government Secure Intranet

Central government depends on the Government Secure Intranet (GSI) for its telecommunications and e-mail services and Internet access. The GSI has been running since 1997 but has recently been revamped to increase the range of services provided and it now includes scope for local government and other government agencies to join, creating a wider reaching, more secure and joined-up government service.

It's not just a matter for the IT department

It is often the case that responsibility for the security of government department information systems rests in the hands of the IT department who do not necessarily have the power to enforce adequate processes. Public sector bodies have to acknowledge their dependence on information and communications systems and place overall responsibility for the risks they face at the appropriate level within the organisation. They must recognise the fact that any lapse or weakness in security can have a direct impact on the reputation and value of the organisation as a whole.

The Cabinet Office has required that central government departments must appoint a Senior Information Risk Owner, at board level, who will take responsibility for ensuring that the information security procedures within their department are managed appropriately. The CSIA will work with departments to develop a framework for assessing information assurance standards in departments based on the security controls of BS 7799 and procurement through the Office of Government Commerce Gateway process.

Local government

More and more local government services are becoming available online. People will go to their local authority website to do anything from paying their council tax to filling out forms for their children's school admission. Citizens have a right to expect that any information they give to local government is treated with due care and respect for privacy.

The Office of the Deputy Prime Minister (ODPM) is actively encouraging local government to meet national information security standard requirements. Local authorities are also obliged to comply with the BS 7799 security standard by 2005 as part of their Implementing Electronic Government (IEG) requirements.

Information and advice on implementing electronic government can be found on the ODPM website at <http://www.localgov.gov.uk>

Protecting local government online services

Luton Borough Council receives more than 20,000 e-mails a day. It has collected over £1.25 million in e-Payments since April 2003, when the service first started. Add to this the fact that the number of attempted electronic attacks is in the hundreds and sometimes thousands **per day** and they have a very good reason for ensuring that their IT systems are adequately protected.

Adherence to the disciplines of security standards (BS 7799) means that not only do you ensure that the right information security products are active but that you constantly test and retest your ability to react and respond to electronic attacks. This also means that you must ensure that key staff are adequately trained to deal with events and that a continuous campaign to inform users of basic housekeeping procedures (e.g. password policy) is maintained and reviewed.

But what about the cost of putting these IT security systems and procedures in place? Luton is confident that a bit of investment up front can save a lot of expense in putting things right after the event.

“If you add the cost of staff sitting around twiddling their thumbs while their computer system is down to the cash-flow implications if monetary transactions are halted – you will quickly realise that the losses you incur can far outweigh the cost of combating the attacks in the first place.”

C E Kadwill, ICT Manager and Acting Head of Service, Luton Information Management Services



Addressing training and skills for professionals

It is important that those individuals involved in the protection of the nation's information systems are given the appropriate level of training and that their skills are developed as and when necessary.

Government is addressing the training and development needs of those responsible for ensuring that government information systems are secure. It will look at the training needs of those who are tasked with assessing and advising on the risk management of the systems (e.g. accreditors) as well as any developmental requirements for those appointed as responsible owners for the risk to government information systems.

Government is reviewing the current provision of training with the aim of identifying necessary steps to improve the effectiveness of education, training and development for personnel responsible for the protection of information systems in organisations across the public sector.

Government and industry are working together to address standards for professionals involved in information security to ensure that individuals within the profession meet agreed requirements.



Developing international co-operation

The term 'global village' is becoming more of a reality every day. The Web has brought the world together in ways that could never have been imagined only decades ago. The Internet does not recognise international borders or differences in domestic laws. We must find ways of working with other countries to ensure co-operation in dealing with international threats and security issues whilst at the same time facilitating international commerce.

Various organisations within the UK Government work closely with a vast number of international organisations in order to ensure that the UK's national information infrastructure is protected.

The Home Office, DTI, NISCC and Cabinet Office have strong links with their international counterparts to exchange information and best practice to mutual benefit. The relationship with United States government organisations such as the Department of Homeland Security and its National Cyber-Security Division is important, not least because of the influence the US Government has over the US IT industry.

The European Information Security Agency (ENISA) was established in March 2004 and the UK Government is working with UK industry to ensure that it is involved in the activities and projects which the agency initiates.

The UK Government works within NATO to influence policy and standards to do with information security and assurance as well as participating in the NATO emergency planning forum. We also continue to participate in G8, Organisation for Economic Co-operation and Development (OECD) and UN initiatives in order to ensure that UK assets are protected from risks arising from poor information security activities in other countries, maximise UK influence on the international agenda, and improve our expertise in the field through involvement with other leading nations.

OECD guidelines for the security of information systems and networks

The OECD has developed guidelines which promote the need for a greater awareness and understanding of security issues. They focus on the need to develop a 'culture of security' in the development of information systems and networks, and the adoption of new ways of thinking and behaving when using and interacting within information systems and networks.

International hi-tech crime

International co-operation is essential to be able to effectively investigate and combat hi-tech crime. Co-operation is most easy where different legislative systems have common offences which allow for the investigation and prosecution of an offence regardless of the country it may have been committed in or wherever the evidence of an offence may be located. The Council of Europe Cybercrime Convention, signed in November 2001, aims to provide for common definitions and minimum standards for offences concerning a variety of computer and computer-enabled crimes. It also seeks to provide for investigative methods appropriate for the collection of electronic evidence and to define measures to ensure effective international co-operation.

The NHTCU has close working relationships with a range of foreign law enforcement agencies and through an established network of contacts is able to facilitate investigative responses in those regions. On occasions when it is not possible to arrest and convict through criminal proceedings, the NHTCU will seek to lawfully dismantle the infrastructure of the organised crime group involved so that they no longer pose a threat to UK interests.

What you can do to make your information systems more secure

Large organisations

Most large organisations are very aware of how vital it is to protect information systems. Chief Information Security Officers advise their boards and Chief Executive Officers (CEOs) on what measures need to be implemented and oversee the implementation and maintenance of their information security measures. Company boards and CEOs are increasingly aware, through pressure from legislation and regulation, that their corporate governance responsibilities must include co-ordination of the risks to their information systems.

Government, large organisations and SMEs must all work to ensure that the information security market meets changing needs and developments. Each sector plays a vital role in driving market forces to ensure that the providers of information security products are kept on their toes. Businesses must demand more secure products from suppliers, thereby influencing the development of these products so that they meet their needs. Smaller organisations can benefit from this as well as the knowledge and R&D resources that government and large organisations can provide.

Government is keen to promote relationships with large organisations and projects that seek to improve private sector information assurance and security. Government works closely with a number of different initiatives, from those involved in promoting best practice and awareness to training and development for professionals and forums for addressing the latest technological developments (some of these organisations are listed in the 'Useful links' section).

Large organisations, which may have state-of-the-art information security products and stringent security policy procedures, should not be complacent. Technological changes will constantly alter the way information security should be handled. For example, the use of PDAs (palm-top computers) and wireless networks is now fairly commonplace yet they are often not given adequate security controls. Information risk assessment and management must be an ongoing part of the organisation's core business practices.

Regulation and legislation

It is not only common sense to address the information security needs of your business, there are also legal and regulatory requirements to consider. In the UK, there are laws governing the use and retention of information on individuals as well as the systems which handle that information. These include the Data Protection Act, Regulation of Investigatory Powers Act (RIPA) and the Computer Misuse Act.

The Turnbull Report provides regulations covering organisations' internal control procedures and risk management. Additionally, there are a number of EU directives governing issues such as privacy and the use of electronic signatures. There are also international regulations which affect many UK organisations. The new Basel II Accord, governing risk for financial service organisations, is currently being developed and is due to be released in mid 2004.

The Sarbanes-Oxley Act in the US has brought significant legislative changes to financial practice and corporate governance regulation. It was introduced in 2002 in the aftermath of a spate of high profile cases of corporate fraud and aims to enhance corporate accountability; it is pertinent to UK companies or their subsidiaries that are quoted on the New York Stock Exchange. Security is a particular theme in the Act including adherence to the international information security standard ISO/IEC 17799.

SMEs (small/medium enterprises)

Good protection online means better business. More and more businesses are going online and customers want to know that their interests are in safe hands. By making your business more secure, you are advertising the fact that your organisation is safe and trustworthy to deal with.

Protecting your information systems does not have to be expensive. The size of your organisation will probably indicate the level of protection you need. Every business should consider their information security procedures and assure themselves that they have the appropriate level of security for their needs.

The same advice applies whether you are a voluntary organisation, charity or community organisation. You will need to ensure that you protect your information

systems and the information they carry to preserve your interests and those of your customers or donors.

You can find information on how to protect your business at:

http://www.dti.gov.uk/industries/information_security

Small enterprises need to protect themselves

A 2004 survey by Network Associates of small firms in Europe revealed that many are not adopting simple techniques to protect themselves from the threat of viruses and malicious hacking. The research found that virus outbreaks can take a company out of action for days and cost an average of €5,000 (£3,300) to put right. For small businesses this can be a significant amount.

Although 40% of those businesses questioned had suffered a virus attack in the last year, and a quarter of companies admitted infecting partners and customers, 45% still said that information security was a low priority.

Source: Network Associates, research carried out in winter 2003 involving 500 small businesses of fewer than 20 employees in the UK, Italy, Spain, France, Netherlands and Germany.

Basic advice for SMEs

- Always back up the information on your system. This should be done regularly and the copies stored away from the business premises.
- If you are connected to the Internet, you should ensure that every computer in your system is protected with regularly updated anti-virus software.
- If you are using Broadband or ADSL, you should use a firewall. Most operating systems contain firewall capabilities, but you can buy more advanced software and hardware firewalls either online or from your software provider.
- Passwords help prevent unauthorised access to your computer network. They can also restrict access to certain sensitive material.
- Make sure everyone in your organisation is aware of basic information security steps such as never opening unsolicited e-mails and updating anti-virus software.

Business Link (<http://businesslink.gov.uk>) gives advice and information on securing your IT systems.



Home IT users

Do you have virus protection on your computer?
Do you update it regularly?

As home computer users we are becoming increasingly aware of the threat of computer viruses and worms. We read about them in the papers and, unfortunately, many PC and home business IT users have suffered the consequences of the various viruses that have spread across the Internet.

Many of these virus attacks can often be easily prevented. Anti-virus software can be downloaded on the Internet and there are a range of software options which can suit the needs of your particular home computer use. If you have a family, you may wish to consider combining the benefits of anti-virus with other measures such as filtering devices, which can help block content such as pornography from entering your system.

However, it is important to remember that you will not gain adequate protection by simply installing software. New viruses are developed all the time and it is essential to practise good security habits to help protect yourself and your family from these and other threats. Remembering to update your anti-virus

software and backing up any important information are basic home security steps.

Home IT users are often afraid that they will not be able to understand information security jargon or procedures, or they simply feel they don't have the time to go through with it. Protecting your information systems doesn't have to be complicated, time-consuming or expensive. Besides, many home users have found out that it can take up much more of their time and money to put their computer right after they have been hit by a virus.

You can find more information online at <http://www.ukresilience.info/protecting.htm> or your Internet Service Provider (ISP) or software provider should be able to give you information/advice.

Basic checklist for home IT users

- If you are connected to the Internet you should install anti-virus software.
- Update your anti-virus software regularly.
- Never open an unsolicited e-mail with an attachment.
- Consider whether you need filtering devices to control e-mail contacts or block unwanted content.
- Consider whether or not you need a firewall on your computer – especially if you are using your home computer for business.

For more information consult your software provider or Internet Service Provider.

Conclusion

Information systems are now an integral part of the way most of our society lives and works. Developments in information and communications technology (ICT) continue to increase at an incredible pace and ICT product shelf life is shortening. Computer viruses are a current risk to our information systems – but they may disappear and the future may hold other threats. It is vital that Government and industry work closely together to ensure that the right range of services and technologies are available for all, to combat these risks as they develop.

In an ever-changing technological society, it is essential that we work together in partnership to ensure that all our interests are protected to mutual benefit. Both Government and industry must ensure that good information security practice is firmly embedded in the business processes of their organisations. Responsibility for risks facing each organisation's information systems must be clearly acknowledged and defined.

Ensuring the confidentiality, integrity and availability of your information systems, whether delivering public services or business, means that more people will continue to use those systems. Ultimately, assuring that information systems are protected and managed appropriately helps to foster and maintain trust and confidence in both Government and business.

Glossary

Assured products – IT products which have been approved by Government as having a recognised level of security efficiency.

BS 7799, ISO/IEC 17799 – A set of best practice rules and methods for information security management defined by the British Standards Institution and the International Standards Organisation.

Critical National Infrastructure (CNI) – the most important elements of the nation's infrastructure involving vital systems and services, such as communications and utilities.

Denial of Service (DoS) attack – where a target system becomes overloaded by messages sent to it and it collapses.

Firewall – a piece of hardware or software designed to limit access between your computer and the Internet.

Information assurance – the confidence that information systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users.

Information systems – information technology or telecommunications systems, services and networks.

Malware – general term used to describe any sort of malicious software such as viruses, worms, trojans, etc.

Phishing – involves criminals using the Internet to deceive people into disclosing their credit card numbers, bank account details or other valuable information.

Trojan – a program designed to allow it unauthorised access to the computer systems it infects. Trojans may also be used in order to exploit a computer system to send unsolicited e-mails.

Virus – a computer program designed to run on one computer (often with undesirable effects such as deleting files or sending unsolicited e-mails) and send copies to as many other computers as possible.

Worm – an independent computer program that replicates from machine to machine across network connections, often clogging information systems as it spreads.

Useful links

- SAINT (<http://www.uksaint.org>) brings together industry leaders and government to exchange information and best practice.
- tScheme (<http://www.tscheme.org>) is an industry-led self-regulatory scheme, which aims to provide a level of assurance to individuals and companies using or relying upon e-business transactions.
- IAAC (the Information Assurance Advisory Council) (<http://www.iaac.org.uk>) brings together corporate leaders, public policy makers, law enforcement and the research community to address the challenges of information infrastructure protection.
- The British Computer Society (<http://www.bcs.org/bcs>), an industry body for IT professionals, plays an important role in establishing standards and training needs for information security professionals.
- The National Computing Centre (<http://www.ncc.co.uk>), a membership and research organisation for IT professionals, is playing a key role in promoting information security best practice and guidance.
- Parents Online (<http://www.parentsonline.gov.uk/safety/>) gives advice and support for parents on the safe use of the Internet and other technologies.
- The Home Office (<http://www.thinkuknow.co.uk/home.htm>) gives advice and support for parents and children on the safe and effective use of the Internet.
- The DTI (<http://www.dti.gov.uk/bestpractice/technology/security.htm>) provides advice for businesses on protecting their information.
- Business Link (<http://www.businesslink.gov.uk/>) provides advice for businesses on implementing and managing information security.
- Superhighway Safety (<http://safety.ngfl.gov.uk/schools>) has information for schools and teachers on the safe use of ICT.
- Crimestoppers – (<http://www.crimestoppers-uk.org>) or call 0800 555 111.
- UK Government CERT (<http://www.niscc.gov.uk>) is the UK Government's Computer Emergency Response Team, part of NISCC.

CSIA
Cabinet Office
Stockley House
130 Wilton Road
London SW1V 1LQ

Tel: 020 7276 3115
Fax: 020 7276 5096
e-mail: csia@cabinet-office.x.gsi.gov.uk
Website: <http://www.cabinet-office.gov.uk/CSIA>

© Crown copyright 2004

The text in this document may be reproduced free of charge in any format or media without requiring specific permission. This is subject to the material not being used in a derogatory manner or in a misleading context. The source of the material must be acknowledged as Crown copyright and the title of the document must be included when being reproduced as part of another publication or service.

The material used in this publication is constituted from 75% post consumer waste and 25% virgin fibre.

Ref: 262949/0604/D40