

The Risk of Computer Crime to Small & Medium-sized Enterprises

What Your Business Really Needs to Know

Introduction

More businesses and customers are using computers and the Internet than ever before, but so too are more criminals. This document gives basic advice on the minimum requirement for protecting your computer and the information you keep on it. This process is called 'Information Security'.

What is Computer Crime?

- Criminal actions accomplished through the use of computer systems, especially with intent to defraud, destroy, or make unauthorised use of computer system resources.

Risk of Computer Crime to Your Business

- If you or your employees use a computer - even one not connected to the Internet - a criminal could destroy your business as easily and rapidly as an arsonist.
- If a thief ran off with your laptop or PDA containing your business-sensitive data, how would it damage your business?
- An unprotected Internet connection is like an open door to your shop!
- How would you stop hackers vandalising your system or website?
- How easily could criminals pretend that they're you and hijack your customers.
- Think: **Reputation – Credibility – Public Embarrassment – Loss of Revenue**

Purpose of this Document

- Protecting you, your business and your staff from the most common electronic threats need cost no more than you spend on locks and alarms for your shop or office. This document aims to point you in the right direction to get the basic help and information you need to ensure that inaction does not cost you dear. If in doubt seek expert advice.

A survey of organisations by the National Hi-Tech Crime Unit¹ www.nhtcu.org has revealed that 77% had experienced theft of laptops, 67% had suffered virus attacks, and 40% had seen theft of other hardware (for example, desk-top computers).

The Business Software Alliance has also estimated that one quarter of all UK companies are using pirated computer software.

The BCC ICT survey of 2002 showed that 60% of SMEs have been victims of computer-related crime and 75% are worried about the security of doing business online.

¹ Hi-Tech Crime – The Impact on UK Business

What Can I Do? – A Framework for Protection

Basic Steps:

- Draw up and publish a set of computer/information security policies, including notes of what to do and who to contact when problems occur, and how to identify and report a possible computer-enabled crime. Ensure that your staff receive regular training on those policies.
- List the equipment and files requiring protection, identify any risks to which they may be exposed, and set out in a plan how you should react if these risks were realised.
- Think in terms of how confidential the information needs to be, how to assure the integrity of the information, and how to ensure that it is available only to those who need to have access.
- Back up your files regularly and maintain copies in a safe place, in another building or off-site.
- Regularly practise restoring files onto your system from your backups to check they work.
- When working away from the office, ensure that you and your employees follow your security policies and that any files copied onto company systems have been virus checked.
- Do not leave your computer unattended unless absolutely necessary and then only if access is protected by a password (ideally a random string of at least 9 alphanumeric characters); change all preset administrator and user passwords 'on delivery'; thereafter regularly change passwords (ideally every three months); remind staff not to write down passwords.
- Look at the default settings on your computer operating system and switch off any accesses that you do not want.
- Install a virus checker and firewall, look at the default settings, set them to block what you do not want and update regularly (at least daily) BEFORE looking at your e-mails.
- Do not leave evidence of recently purchased equipment for thieves to see (for example, packing cases and boxes left outside for disposal).
- Do not use e-mail "out-of-office" routines if the premises will be unattended while you are away.
- Check if your Internet Service Provider provides filtering services. If so, consider using them to reduce spam and inappropriate access (although this may give problems with "false positives" - e.g. blocking access to web-sites with Essex in the address or the text of this document).
- If you run a web site, make sure you understand what security it provides against both unauthorised changes and unauthorised access to your internal systems.
- Regularly check security advice from your operating system and software suppliers and ensure your system is patched to protect against new weaknesses.
- Check to see if your business insurance covers 'cybercrime'.

People:

- You, your staff and anyone else using your systems should know, understand and follow your security policies, including how to identify and report a possible security incident.
- Make sure staff policies and procedures include guidance and standards for email, internet and computer use.
- Remember to check the references of any new employees, contractors and temporary staff.
- Check the accreditations/references of any consultants and advisors who have access to your systems, including maintenance contractors and Internet Service Providers (ISPs.)
- Beware of attempts to obtain information regarding your system, its data, and personal details.
- Cancel the access to your system for people who have left your company, cancel their passwords, and change passwords to shared services and material to which they had access. For staff about to be dismissed, cancel access before a notice is served to prevent the risk of subsequent malicious activity.

Law:

- Do you have a process in place to prove who carried out an electronic transaction. This is called 'non-repudiation' and is fundamental to e-business.
- Remember that the law exists to protect you. Contact your local Citizens Advice Bureau, Chamber of Commerce or the Law Society for local solicitors with relevant expertise if you need legal help.

What Can I Do? – Some of the Threats

Threats	Action
Virus and other Software Attacks	<ul style="list-style-type: none"> • Introduce virus checking software and managed firewalls (updated daily). • Do not open suspect e-mails or attachments. • Only enable preview panes once you have removed all suspect emails. • Check the privacy settings (cookies and active code like Java) in your web browser.
Theft of Laptops or other Hardware	<ul style="list-style-type: none"> • Maintain a list of your equipment (including serial numbers) and check your physical security. • Control access to business premises and computer systems. • Encrypt sensitive data. • Password protect your hard drive and data. • Mark your postcode on all hardware with an ultra violet pen. • Regularly back-up essential files and store copies in a secure place, ideally in another building.
Intellectual Property Theft/ Copying of Information - customer or prospect lists, design files, correspondence etc.	<ul style="list-style-type: none"> • Who has access to your systems? You should know and log usage. • Check physical security of computers and back up files. • Consider shredding any sensitive documents; putting them in the bin (even in piece) means someone can find, take them, and reassemble them.
Mishandling of Personal Information – unfair or illegal processing of any data that identifies, directly or indirectly, a living human being.	<ul style="list-style-type: none"> • Familiarise yourself with the eight data protection principles outlined in 'The Data Protection Act and You': www.dataprotection.gov.uk. The site also has a section on "frequently asked questions". • Register your business with the Information Commissioner.
Financial Fraud and Theft On-line – use of false or stolen credit card information to buy goods from you or to buy goods in your name, advance fee fraud.	<ul style="list-style-type: none"> • Make sure you understand the risks associated with different types of "card not present" transaction, including goods not being received by the cardholder or sending goods other than to the address of the cardholder. • Validate new customers and suppliers using published information (e.g. address or phone number) and obtain an on-line credit status report and electronic identity check. • Report fraud or attempted fraud to your local Police.
Unauthorised E-Mail Access/Misuse – sending out illegal or offensive material.	<ul style="list-style-type: none"> • Ensure your policies are known by all employees and others with access to the systems.

<p>Unauthorised Web Access/Misuse – placing illegal or offensive material on a website, viewing non-work material during working hours, visiting illegal or offensive websites (e.g. child abuse images).</p>	<ul style="list-style-type: none"> • Ensure your policies are known by all employees and others with access to the systems. • Report serious incidents to local Police or the Internet Watch Foundation http://www.iwf.org.uk/.
<p>Sabotage of Data – unauthorised amendment or deletion of records to disrupt the business or for other purposes, including financial gain.</p>	<ul style="list-style-type: none"> • Ensure that regular back-up copies are securely stored, ideally in another building or off-site. • Check data regularly for unexpected changes in nature or size.
<p>Identity Theft – impersonation of individuals & “Developed Identities” (fictitious identities). Don't be a victim of ID fraud http://www.cardwatch.org.uk/</p>	<ul style="list-style-type: none"> • Do not provide personal information without validating the identity of the organisation making the request. • Does the identity exist? Is it really them? Use identity authentication and credit status checking services to help.
<p>Spoofing attacks/Passing Off – impersonation of business</p>	<ul style="list-style-type: none"> • Forward email to sender's ISP for action and have your filters adjusted to block unwanted email.
<p>Telecommunications Eavesdropping</p>	<ul style="list-style-type: none"> • Use SSL* on computer lines but remember that careless talk costs jobs! Who was in earshot when you told your secretary the password over the mobile phone on the train?
<p>Denial of Service Attack – attempt by attackers to prevent legitimate users of a service from accessing or using that service, including “flooding” a network with mass e-mail and disrupting connections between machines.</p>	<ul style="list-style-type: none"> • Contact your ISP if you think you have been attacked. If you cannot get through it may be that you are one of many, try alternative routes.
<p>Active Wire Tapping – unauthorised interception, modification and relaying of data over an electronic network.</p>	<ul style="list-style-type: none"> • Use SSL* or other encryption when logging on.

*SSL is an acronym for Secure Sockets Layer, a protocol used for authenticating and encrypting web traffic

Table : Actions
Compiled with the assistance of the National Hi-Tech Crime Unit

Reporting Computer Crime

Any crime, including computer crime can be reported to your local police station, Information about crimes can be passed to the Police by calling **Crimestoppers on 0800 555 111**. A full list of all regional police services is available at www.police.uk.

The table below shows other non-police organisations that also exist to help identify and put a stop to computer crime, or which can provide practical advice on your business' electronic security.

Organisation	Category of Advice
Association for Payment Clearing Systems (APACS)	Credit/Debit card fraud and identity protection www.cardwatch.org.uk
British Chambers of Commerce	Information on e-security and digital signatures www.britishchambers.org.uk
Business Software Alliance	Software theft and counterfeiting www.bsa.org
Department of Trade and Industry	Guidance on securing systems at www.ukonlineforbusiness.gov.uk
e.centre	Security of electronic messaging in supply chain www.e-centre.org.uk
Federation Against Software Theft	Guidance on software licensing www.fastcorporateservices.com
Information Commissioner	Mishandling of personal information www.dataprotection.gov.uk
Institute for Communications Arbitration and Forensics	Best practice in defining evidential trails to detect e-crime www.theicaf.com
Internet Service Provider	Illegal sites, denial of internet service attacks, sabotage of internet networks
Internet Watch Foundation	Child abuse images www.iwf.org.uk
The National Computing Centre	Practical applications of standards for information systems security and risk management www.ncc.org.uk
Telecommunications UK Fraud Forum (TUFF)	Useful advice on checking credit applications www.tuff.co.uk
Telecoms Provider	Denial of telephone service attacks, sabotage of telephone networks