

# WHAT YOUR BUSINESS REALLY NEEDS TO KNOW

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 your Information Security.

WHAT CAN I DO?

## 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 be able to destroy your business as rapidly as an arsonist.
- If a thief ran off with your laptop or PDA containing unprotected business-sensitive data, how would it damage your business?
- An unprotected Internet connection is like your back door unlocked!

## Purpose of this Document

- Protecting you, your business and your staff from the most common electronic threats may 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.

A survey of organisations by the National Hi-Tech Crime Unit<sup>1</sup> in 2004 [www.nhtcu.org](http://www.nhtcu.org) has revealed that:

**77%** had suffered virus attacks which cost them **£27.8m**, while **17%** had suffered financial fraud costing them **£121m**.

Back up your files regularly and maintain copies in a safe place.

## A Framework for Protection

### Basic Steps:

- Draw up a set of computer/information security policies for yourself and your staff, including notes of what to do and who to contact when problems occur and how to identify and report a possible e-crime.
- Record what your business information and technology assets are. Put a value on each in terms of what it would cost your business if it was lost or stolen.
- Back up your files regularly and maintain copies in a safe place.
- Regularly practise restoring files onto your system.
- When working remotely, ensure that you and your employees follow your security policies and that any files copied onto company systems (from any source) have been virus checked.
- Do not leave your computer in an unattended location unless access is protected by realistic passwords; avoid staff writing them down and remember to change any preset passwords on the system.

The Business Software Alliance has also estimated that one quarter of all UK companies are using pirated computer software, which may not be capable of being updated with the latest security patches.

- 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 left outside the building 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 website, make sure you understand what security it provides against unauthorised changes to it and against it allowing unauthorised access to your internal systems.
- Ensure your operating system is regularly patched.

### People:

- You, your staff and anyone else using your systems should know, understand and follow your security policies, including knowing how to identify and report a possible security incident.
- Remember to check the references of any new employees.
- 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, data and personal information.
- Cancel the access to your system for people who have left your company immediately they are terminated.

### Law:

- 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.

<sup>1</sup> Hi-Tech Crime – The Impact on UK Business

# Some of the Threats

## WHAT CAN I DO?

Threats	Action
<b>Virus and other Software Attacks</b>	<ul style="list-style-type: none"> <li>Introduce virus-checking software.</li> <li>Use a properly configured firewall between your systems and the internet.</li> <li>Do not open suspect e-mails or attachments.</li> <li>Only enable preview panes once you have removed all suspect emails.</li> </ul>
<b>Theft of Laptops or other Hardware</b>	<ul style="list-style-type: none"> <li>Maintain a list of your equipment (including serial numbers) and check your physical security.</li> <li>Control access to business premises and computer systems.</li> <li>Encrypt sensitive data.</li> <li>Password protect your hard drive and data.</li> <li>Mark your postcode on all hardware with an ultra violet pen.</li> <li>Regularly back-up essential files and store copies in a secure place, away from the premises where the computers are used.</li> </ul>
<b>Intellectual Property Theft/Copying of Information</b> – customer or prospect lists, design files, correspondence etc.	<ul style="list-style-type: none"> <li>Who has access to your systems? You should know and log usage.</li> <li>Check physical security of computers and back up files.</li> </ul>
<b>Mishandling of Personal Information</b> – unfair or illegal processing of any data which identifies, directly or indirectly, a living human being.	<ul style="list-style-type: none"> <li>Familiarise yourself with the eight data protection principles outlined in 'The Data Protection Act and You': <a href="http://www.dataprotection.gov.uk">www.dataprotection.gov.uk</a>. The site also has a section on 'frequently asked questions'.</li> </ul>
<b>Financial Fraud and Theft On-line</b> – 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"> <li>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.</li> <li>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.</li> <li>Report fraud or attempted fraud to your local Police.</li> </ul>
<b>Unauthorised E-Mail Access/Misuse</b> – sending out illegal or offensive material or placing this on a website.	<ul style="list-style-type: none"> <li>Ensure your policies are known by all employees and others with access to the systems. Ensure your policies are lawful and enforceable.</li> </ul>
<b>Unauthorised Web Access/Misuse</b> – viewing non-work material during working hours, visiting offensive or illegal websites (e.g. child abuse images).	<ul style="list-style-type: none"> <li>Ensure all employees and others are aware of your views (policies) on this, and that they are lawful and enforceable.</li> <li>Report serious incidents to local Police or the Internet Watch Foundation <a href="http://www.iwf.org.uk/">www.iwf.org.uk/</a></li> </ul>
<b>Sabotage of Data</b> – unauthorised amendment or deletion of records to disrupt the business or for other purposes, including financial gain.	<ul style="list-style-type: none"> <li>Ensure that regular back-up copies are securely stored.</li> <li>Check data regularly for changes in nature or size.</li> </ul>

Threats	Action
<b>Identity Theft</b> – impersonation of individuals & 'Developed Identities' (fictitious identities).  <b>Don't be a victim of ID fraud</b> <a href="http://www.cardwatch.org.uk/">www.cardwatch.org.uk/</a>	<ul style="list-style-type: none"> <li>Do not provide personal information without validating the identity of the organisation making the request.</li> <li>Security measures must be taken to ensure that your business records can not be stolen for use in identity theft.</li> <li>Does the identity exist? Is it really them? Use identity authentication and credit status checking services to help.</li> </ul>
<b>Spoofing attacks/Passing Off</b> – impersonation of business.	<ul style="list-style-type: none"> <li>Forward email to sender's ISP for action and have your filters adjusted to block unwanted email.</li> </ul>
<b>Denial of Service Attack</b> – 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.	<ul style="list-style-type: none"> <li>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.</li> </ul>

## 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](http://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)	<ul style="list-style-type: none"> <li>Credit/Debit card fraud and identity protection <a href="http://www.cardwatch.org.uk">www.cardwatch.org.uk</a></li> </ul>
British Chambers of Commerce	<ul style="list-style-type: none"> <li>Information on e-security and digital signatures <a href="http://www.chamberonline.co.uk">www.chamberonline.co.uk</a></li> </ul>
Business Software Alliance	<ul style="list-style-type: none"> <li>Software theft and counterfeiting <a href="http://www.bsa.org">www.bsa.org</a></li> </ul>
Department of Trade and Industry	<ul style="list-style-type: none"> <li>Guidance on securing systems at <a href="http://www.ukonlineforbusiness.gov.uk">www.ukonlineforbusiness.gov.uk</a></li> </ul>
e.centre	<ul style="list-style-type: none"> <li>Security of electronic messaging in supply chain <a href="http://www.e-centre.org.uk">www.e-centre.org.uk</a></li> </ul>
Information Commissioner	<ul style="list-style-type: none"> <li>Mishandling of personal information <a href="http://www.informationcommissioner.gov.uk">www.informationcommissioner.gov.uk</a></li> </ul>
Institute for Communications Arbitration and Forensics	<ul style="list-style-type: none"> <li>Best practice in defining evidential trails to detect e-crime <a href="http://www.theicaf.com">www.theicaf.com</a></li> </ul>
Internet Service Provider	<ul style="list-style-type: none"> <li>Illegal sites, Denial of internet service attacks, sabotage of internet networks</li> </ul>
Internet Watch Foundation	<ul style="list-style-type: none"> <li>Child abuse images <a href="http://www.iwf.org.uk">www.iwf.org.uk</a></li> </ul>
Telecommunications UK Fraud Forum (TUFF)	<ul style="list-style-type: none"> <li>Useful advice on checking credit applications <a href="http://www.tuff.co.uk">www.tuff.co.uk</a></li> </ul>
Telecoms Provider	<ul style="list-style-type: none"> <li>Denial of telephone service attacks, sabotage of telephone networks</li> </ul>