

the fraud Protecting your  
advisory IT systems:  
panel a guide for SMEs

## **Disclaimer**

Whilst every effort has been made in the construction of this Guide, compliance with it does not guarantee that you and/or your business will not be a victim of fraud or criminality aimed against your business/PC systems.

The Fraud Advisory Panel and the contributors to this Guide accept no responsibility for any action taken by parties as a result of reading this Guide. Readers are strongly advised to seek and obtain the appropriate professional advice on the issues raised which affect them or their business.

the fraud **Protecting your**  
advisory **IT systems:**  
panel **a guide for SMEs**

**Acknowledgements**

The Fraud Advisory Panel would like to thank Steven Philippsohn, Chairman of the Fraud Advisory Panel Cybercrime Working Group, and the Fraud Litigation Team at Philippsohn Crawfords Berwald together with Robert Dias, Stephen Hill, and Jack Wraith for their assistance in the preparation of this publication.

# 1. Introduction

*It is estimated that the average UK business receives approximately 20 computer viruses a year and has one security breach a month<sup>1</sup>.*

Whether you are a network administrator, own your own business or just use a PC to read and send emails this Guide is for **YOU**. It is designed to provide you with information about how to protect and operate information technology in a safe and secure way.

Your IT systems, whether it is a single computer, Personal Data Assistant (PDA) or a more complex network, will be the subject of infiltration or attack from internal and external sources.

This Guide covers:

- What is protection and why it is important;
- How to protect your network/computer against attacks; and
- What to do if you become a victim of an attack.

## Information Security Management

You may not have extensive PC networks but the data you have, even on one or two computers, is valuable to you, your business and your customers and needs to be protected. Even if you do not have customers, your systems and processes can be the target for criminals who are out to steal not only your personal information (identity theft) but may also take over your IT to use it for their own purposes (spam and virus proliferation).

So what must you care about/protect?

- Data covered by the Data Protection Act.
- Financial data – either yours or your customers.
- Data that you see as important, for example personal data identifying you as a person is not covered by the Data Protection Act which affords protection for all personal data you collect, be it from your customers or your employees.

---

<sup>1</sup> Department of Trade and Industry. *Information Security Breaches Survey 2004: technical report*. April 2004.

How do you protect it?

- Make it unusable to anyone else (scramble/encrypt it).
- Make your system impregnable/difficult to penetrate (like a castle).
- Put up defences on your network (firewalls and access procedures).
- Check that only authorised users access your systems but remember that 80% of fraud is caused with inside help.

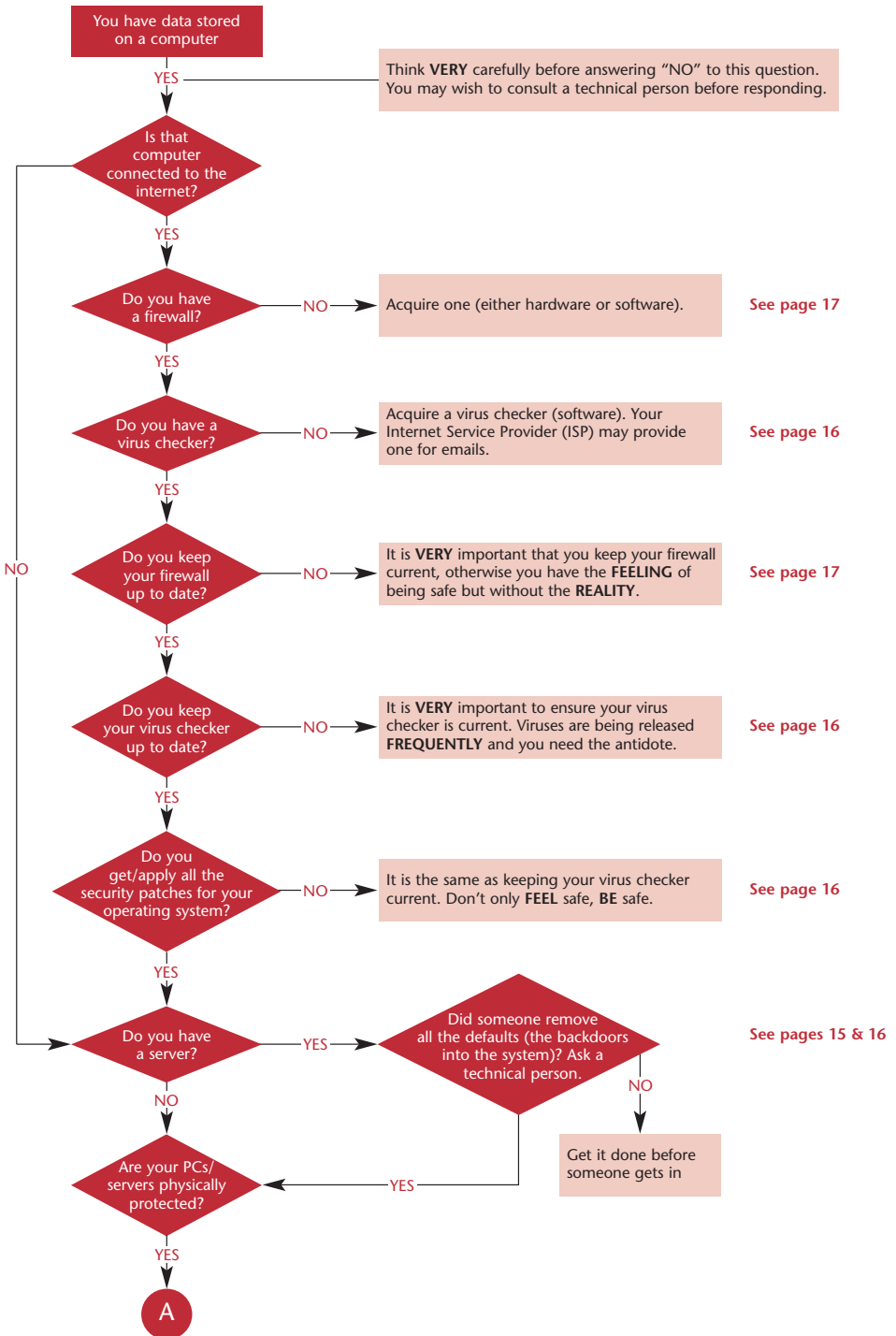
From whom do you need to protect it?

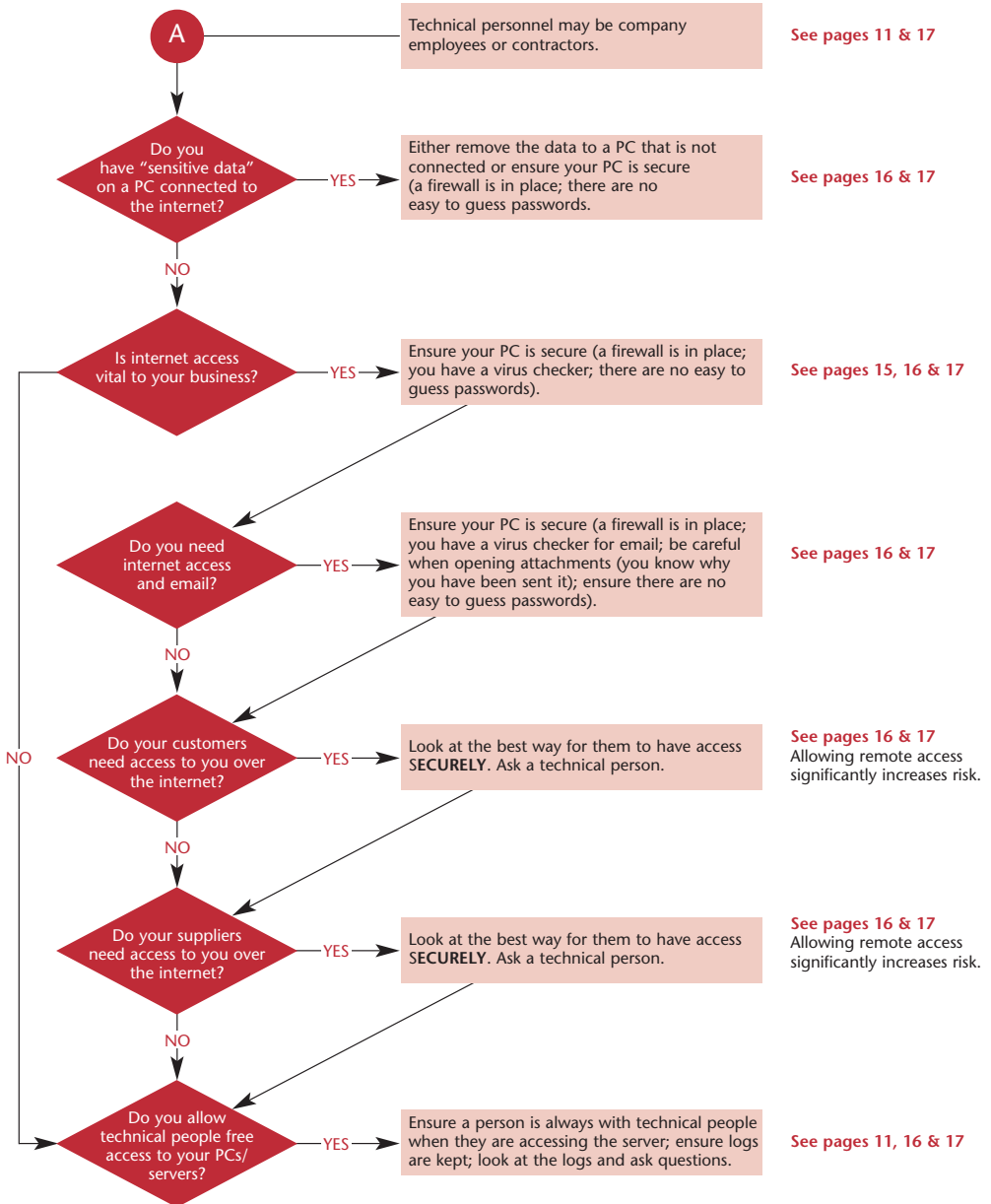
- Anyone external to the organisation who is not authorised to view or access data on the system or PC.
- Insiders who may abuse their positions and access areas for which they do not have authorisation. This may be out of curiosity, from a grudge, for money or because they are threatened. Being on the inside makes it easier for them to alter data and steal files.
- Hackers who want to manipulate your data either to steal it, for kudos (to prove they can) or so they can use the programs on your system to attack others, for example sending out spam (making emails appear to come from your machine or using your machine to bring down someone else's network).

You will find a wealth of information and sources within this Guide and how you use it is really down to you. You can read it cover to cover, dip into the parts that matter to you most or simply have it as a fall back when things do go wrong. What is best for you? It really depends on a number of factors and if you are unsure then try using the diagram on the next page to see how best this Guide can serve you and where to go to get advice for a particular problem.

Finally, think of your PC or network as a personal diary in which you record all of your most personal and private thoughts. You wouldn't want just anybody getting access to this, and your IT system or PC is no different. There are some basic rules you can apply which will increase the security of your data.

**Remember:** any system or process is only as strong as its weakest link and that is more likely to be a human process than a piece of hardware or software. So take a few minutes and acquaint yourself with this Guide and decide how best it can serve you and your business.





Whilst you may not have an immediate use for this Guide the information contained within may help you some time in the future.

## 2. What is System Protection?

Without appropriate network protection, there is an increased risk of becoming a victim of computer crime.

A survey by the National Hi-Tech Crime Unit (NHTCU)<sup>2</sup> estimated hi-tech crime cost UK businesses £2.45bn in 2004. 89% of those interviewed experienced at least one incident of computer-related crime in 2004.

What is system protection? Quite simply it is processes you put in place with a PC or system that acts as a buffer between your stored data and the outside world. This buffer (firewall) can be applied at varying degrees of strength and would normally be configured to meet the exposure risk you place on data stored on your system/PC. For example, if you had very sensitive data then it makes sense that the security you would apply would be the most robust. It would not only stop illegal and unauthorised access to the system/PC but would also provide secure access to the actual data which in itself may be encrypted or scrambled. If, however, all you had stored was information already available to the public, then what you would be doing would be stopping your PC or system being used by unauthorised users and access to the data would attract a lower level of security.

### Example 1

In October 2004, it was reported that a hacker accessed the network at University of California at Berkeley. There he gained access to 1.4 million social security numbers of California residents that were held there for research purposes.

**Source: Reuters, 20 October 2004**

### Example 2

In March 2005, it was reported that US data broker ChoicePoint had inadvertently released files on 145,000 US consumers to thieves posing as ChoicePoint customers. The news led to the company's share price dropping by more than 20% and shareholders commencing legal action against the company and its directors to recover their losses.

**Source: *The Financial Times*, 9 March 2005; *Computerworld*, 7 March 2005**

---

<sup>2</sup> National Hi-Tech Crime Unit. 'E-crime costing British business billions: survey discovers £2.4 billion loss', press release, 5 April 2005.

## Examples of Possible System Attacks

There are a number of ways in which a system can come under attack from both internal and external sources. External attacks can be from the basic to the very sophisticated. In essence the attacker is gaining access to your system/PC by exploiting weaknesses in your security software or by engaging inside help to illegally connect to it. The following table describes both internal and external risks.

### INTERNAL RISKS

#### Management and employees

According to the KPMG Fraud Barometer<sup>3</sup>, theft by management and employees accounted for a third of all significant fraud cases in 2004. These frauds cost their companies about £106m.

In the context of system protection, management and employees can pose a particular threat because they have regular and legitimate access to the computer system. They often, therefore, have a detailed knowledge of the security systems and passwords, people's attitude to passwords and may even know some people's passwords.

Management and employees can take advantage of their position in a number of ways. They may access and sell confidential information or they may sell passwords and their knowledge of the security systems. Alternatively, they may install software that captures the keystrokes of users (to learn their passwords), that triggers a security breach at a certain point such as a date or a computer event (called a 'Trojan' after the wooden horse given to the Trojans by the Greeks) or that is a virus.

### EXTERNAL RISKS

#### Viruses, bots and other malware

It has been reported that 40% of the world's large companies had their IT structure compromised by computer viruses and worms in the first six months of 2004<sup>4</sup>. Viruses damage computer systems in many ways. They may pick up all email addresses (for use with spam). They may delete data. They may make a 'backdoor' into the computer so that their controllers can use your machine at a later date or they may just slow down servers and other key computers.

---

<sup>3</sup> KPMG, Forensic and Litigation Services. 'Phantom fraudsters haunt UK businesses', press release. 26 January 2005.

<sup>4</sup> *The Financial Times*, reporting Symantec. 20 September 2004.

Some viruses turn infected computers into bots – computers which can be used remotely by third parties to send spam or launch denial of service attacks. According to Symantec, during the first six months of 2004, the average number of monitored bots rose from less than 2,000 to more than 30,000 per day<sup>5</sup>. It has been reported that the majority of attacks on the unwary asking for personal data (known as phishing) comes from just five remotely controlled networks.

---

### **Hacking**

Hacking is a constant threat to IT systems. Hackers spend their time trying to break into systems or just trying to break the security of an application. They may do it for criminal purposes or just to prove they can and therefore improve their standing in the hacking community. The damage caused by hackers depends on the motive of the hacker. Some hackers deface websites to make political statements; others hack to gain access to personal and confidential information.

---

### **Extortion and (distributed) denial of service attacks**

Failure to protect a computer system can leave an individual or business vulnerable to extortion. Criminals using other computers that they control, cause a flood of messages to a system so that it cannot handle all the messages. This overload means that genuine work cannot be done. If you rely on the internet for your business...your business stops. You may then get a phone call asking for money to stop the criminals attacking you.

---

### **The dangers of unprotected wireless networks**

The signals between computers in wireless networks can be intercepted using radio monitoring and broadcast equipment. If the wireless network is not protected, anybody with the appropriate equipment may be able to gain access to your network. The setting up of a secure wireless Local Area Network (LAN) requires knowledge of the security issues and technical expertise.

#### **Example 3**

A [recent] study shows an unpatched machine lasts about 20 minutes on the internet without getting infected by something.

**Source: News@UofT [www.news.utoronto.ca], 27 September 2004**

---

<sup>5</sup> Symantec. 'Symantec internet security threat report identifies more attacks now targeting e-commerce, web applications', press release. 20 September 2004.

#### Example 4

In October 2004, it was reported that one website was allegedly threatened with a child pornography smear campaign unless it paid £4,800. The criminals threatened to hack into the business's network and send emails containing child pornography from the company's computers.

**Source:** *The Financial Times*, 26 October 2004

#### Example 5

In March 2005, it was reported that thieves attempted to steal £220m from the British branch of Sumitomo Bank. If the theft had been successful, it would have easily been the largest theft from a bank in British history. The National Hi-Tech Crime Unit (NHTCU) had been investigating the attempted theft since October 2004 and one man has been arrested in Israel.

It is believed that the thieves installed 'keystroke loggers' on the bank's computers. The keystroke logger was then used to record all information typed into Sumitomo's computers. Once information such as passwords and security codes had been collected, the thieves would have been able to steal money out of Sumitomo's accounts. It is not believed that the Bank suffered any losses.

**Source:** *The Financial Times*, 17 March 2005

### Who Should You Protect Your System Against?

- People (hackers) who want to see if they can break in and how far they can get just for the fun of it. It's the same as mountain climbers climbing mountains – they do it because they are there to be climbed! To quote a hacker 'systems and PCs are there to be broken into – that is what they are there for!'
- People who want to break in to steal important information either for personal gain or to sell on to others. This could be your customer list or the customers' financial details.
- People who call and ask for information (known as social engineering – duping staff to release details unsuspectingly). **Remember:** this does not have to be sophisticated; it could be as easy as someone calling you and using a false identity or simply just asking for information. People can be very trusting when someone says they are from a financial institution and are checking on a client. Giving away information in this way is just as damaging as someone hacking in. In fact it may be worse, as there is likely to be no record of the call.

- People who want to use your system to send spam to millions of email addresses, or worse, use your systems/PCs to proliferate viruses to other PC users. 40% plus of all spam is now sent via compromised PCs<sup>6</sup>.
- People who want to bring down a site by bombarding it with messages. This is known as a (distributed) denial of service (DDoS) attack and it can take a number of forms. It is important to protect your system so that it cannot be used in this way.
- People sending you emails with virus attachments which when opened invade your system/PC.
- People who have access on the inside. **Remember:** it is far easier to hack into a system where you already know a lot about the security (or lack of it).
- Former employees whose usercode and password still work after they have left. It is important to delete usercodes and passwords either before someone is about to leave or immediately after they have left, particularly if the employee has been dismissed on disciplinary grounds.
- Contractors and third-party companies' staff who have access to systems, have usercodes and passwords and understand the security system.

This is not to say that your systems/PC is vulnerable to all the threats outlined above. The majority of people are law abiding and honourable. However, you should still ensure that your security measures are robust enough to make it very difficult for any unauthorised person to access your sensitive information. You may trust your neighbours but you still lock your house when you leave it. Think of security software as the key to lock down your systems/PC in much the same way.

### Example 6

It has recently been reported that a Californian man was convicted of distributing spam by hacking into unprotected wireless networks. The hacker drove through Venice, California with a scanner searching for unprotected networks, which he then used to send unsolicited emails.

**Source: ZDNet UK [www.zdnet.co.uk], 8 September 2004**

---

<sup>6</sup> Sophos. 'The 'dirty dozen' 2004: Sophos reveals the top spamming country', press release. 24 December 2004.

### 3. Security and Risk Management

All organisations face risk in one form or another on a daily basis and in order to mitigate risk it is essential to have a security policy in place. This does not have to be some highly developed document and the following points aim to give a basic outline on which any risk and security assessment should and could be made.

#### Risk Management

Any plan needs to take into consideration the following questions:

- What could happen? – Think of where the threats or actions are likely to come from.
- How bad could it be? – What would the consequences of the threat or action be to your business?
- How often will it happen? – The frequency or exposure to a risk will differ based on a number of factors.

When reviewing the answers to the above questions, management need to critically question their answers for accuracy because it is from these that the security policy will flow.

#### Security Policy

A security policy allows an organisation or business to manage the risks and has three key components:

- **Confidentiality:** ensuring information/data is accessible only to authorised individuals.
- **Availability:** ensuring authorised users have access to information/data when required.

An **appropriate** security policy will protect information from both internal and external risks.

#### Reviewing Policy and Procedures

In order to effectively review policy and procedures in terms of risk it is necessary to have a regular program to review internet, email and access policies. Such a review will have the advantage of reducing the risks to systems and PCs as well as the liability for failure to comply with current standards and legislation.

The importance of developing or reviewing risk management and internal controls was recognised in a recent Department of Trade and Industry (DTI) study<sup>7</sup> where the following key findings were identified:

- 74% of UK businesses had suffered at least one security breach.
- Two thirds had suffered a malicious security incident (such as a virus, unauthorised access, misuse of systems, fraud and theft).
- Only 1 in five UK businesses had a disaster recovery plan.
- Nearly one quarter of businesses indicated that they believed better backup and contingency plans could have prevented their worst security incident.

**Remember:** risk management simply involves the identification of the boundaries within which protection is to be provided. The business and internet environments are so vast and diverse that it is necessary to draw a boundary between what is within the organisation and what is outside. It will help in this process if you identify potential threats and vulnerabilities. In particular you should have a clear understanding of:

- The backing up of data. If you copy your essential data onto another device (floppy/CD ROM) then if your original data is corrupted or damaged you have a copy to fall back on. Essential data should be regularly backed up in this way.
- Anti-virus systems.
- Firewalls (physical and logical).
- Blocking access to your system as opposed to filtering access to your system.
- Access controls (ensuring the right people get to the right systems and data).
- Physical controls.
- Wireless local area networks.
- Staff selection and training.

The information gathered during this exercise will prove useful when controls are being designed, in the sense that they will point to all the areas in which there are dangers threatening the confidentiality, integrity and availability of data.

Any risk management review/assessment should be approached as follows:

- Identify the areas within the business that are most vulnerable to cyber-attack.
- Establish the controls that are already in place to address these risks.

---

<sup>7</sup> Department of Trade and Industry. *Information Security Breaches Survey 2004: technical report*. April 2004.

- Identify any further controls that may assist in reducing the risk.
- Monitor pre-existing controls to ensure they have been implemented effectively.
- Assess the controls to account for any changes or developments made in the operation of the organisation.
- Ensure that procedures and controls are workable and supported by a sufficient level of resources.
- Establish a regular review procedure.

## **Requirements for Businesses Accepting Card Payments – Payment Card Industry (PCI) Compliance**

Businesses that accept payment cards (be they debit or credit cards) for any form of purchase at point of sale or over the internet or telephone, must comply with the aligned security standards set out in the PCI rules. Any business which stores, transmits, or processes credit card transactions must comply with this standard; otherwise they could become liable in the event of a security breach.

Communications about PCI compliance will come from your acquiring/processing bank, whom you should contact with any questions.

If you think you might be affected by PCI you can also find out more information from the following card scheme websites:

- [www.visaeu.com](http://www.visaeu.com)
- [www.mastercardmerchant.com](http://www.mastercardmerchant.com)

## **Frameworks for Security (BS ISO/IEC 17799)**

The British Standard for Information Security Management (BS ISO/IEC 17799) provides the framework necessary to create a secure system and draws on the experience of a group of professional information security practitioners. The framework has been developed to provide a systematic approach to identifying and combating the risks to an organisation's information asset – data. Assurance is attained through controls that management creates and maintains within the organisation. The key factors to this process are:

- Define security policy.
- Define the scope of the information security management system.
- Undertake a risk assessment of the system/process.
- Manage the risk(s).

- Select control of objectives and controls to be implemented.
- Prepare statement of applicability.
- Enforce policy, standards and procedures.

The degree of assurance required is attained through controls that management create and maintain within the organisation. The standard identifies 10 key controls for the implementation of a successful information (data) security program:

- Information security policy.
- Security organisation.
- Asset classification and control.
- Personnel security.
- Physical and environmental security.
- Computer and network security.
- System access control.
- Systems development.
- Business continuity planning.
- Compliance.

Businesses have a legal obligation to protect personal information entrusted to them. The Data Protection Act 1998 legislates for the various processes data must go through from initial recording to final destruction when it is no longer relevant. Providing a good management security framework and by following a comprehensive structure with defined policies and procedures, an organisation can be assured that its information security is implemented successfully and efficiently. More details are available at:

- [www.iso.org](http://www.iso.org)
- [www.bsi-global.com](http://www.bsi-global.com)

#### **Simple tips for network protection**

1. Ensure that anti-virus software is kept up to date.
2. Apply security patches for standard software.
3. Appoint a designated person or board to oversee risk management.
4. Introduce appropriate information security policies and enforce them.

## 4. Types of System Protection

Organisations that do not implement adequate system protection can leave themselves vulnerable to attack. Key issues to be considered when implementing system protection measures are:

- What information held by your business is commercially or business sensitive and needs to be kept from others?
- What information or hardware is business-critical so that if it is unavailable for any time the business or business processes suffer?

Effective system protection requires a combination of hardware, software, people and policies. Having educated users, good policies and keeping security updates current will also assist an organisation to keep ahead of the game.

Organisations should also consider the information behind their networks and protect that information. This can include PDAs and wireless networks. Remote workers may also have copies of sensitive information on their home computers.

### Information Security Policy

Introduce an information security policy which is strictly enforced. This policy should be clear and concise. It is essential that all employees (including third-party staff) are made aware of the policy and the reasons for it. It should be emphasised that the policy is strictly enforced. This will go some way to stop problems entering the system.

### Physical Security

A typical network or even a single PC connected via broadband to the internet is made up of hardware (such as routers, servers and hubs) and software. Consider the hardware – where is it located, how secure does it need to be? Allowing easy physical access to network equipment and servers can be dangerous. It is best to restrict physical access by using key, key pad or biometrics. Other options include cameras, security cards, security guard(s) or housing the equipment in a cage, depending upon the level of security required.

### Logical Security

Logical security takes several forms:

- **Authentication of users:** this may be as simple as assigning usercodes and passwords for people onsite and may include dialling back to a known telephone number, biometrics or a key fob for remote workers. The rules for the creation of

passwords should be laid down in the security policy document and the rules and reasons explained. Do not permit easy passwords or the writing of passwords on yellow sticky notes.

- **Security patches:** ensure that security patches are applied speedily. It should be part of the designated staff member's role to check for security problems and patches and to apply them. Security patches are additional software which update any newly discovered security weakness in a product and are issued by product developers from time to time to ensure their product is as secure as possible in all operating conditions.
- **Remove defaults:** ensure that standard, default usercodes and passwords are removed from the system together with other well-known usercodes and passwords.

## Application Security

Application security can take a number of forms, including:

- **Intrusion detection systems:** these look at patterns of usage and use databases of known data to try to determine if unauthorised access is being attempted. They will stop access to systems that they determine to be unauthorised. The purpose of these systems is to try to stop the problem before it occurs.
- **Anti-virus software:** this is one of the most common forms of protection. It will detect known viruses and will stop them running, such as viruses attached to emails. **However, this software MUST be kept up to date for it to be effective.**
- **Anti-spyware/adware tools:** these tools are designed to prevent some types of software being downloaded on to your PC. Such software is not strictly a virus but is normally designed to record your shopping or surfing habits as well as presenting special adverts via pop-up windows and banners on your desk top. Ad-Aware and Spybot search and destroy this particular type of software.
- **Filtering systems:** these restrict access for users. They can work on words, parts of words, picture content (including colour) or website address.
- **Software updates:** a designated employee should ensure that security patches are always applied in a timely manner to all software. There are packages that can be run to check systems to ensure that all known patches have been applied.
- **Encryption:** data can be encrypted either on the disk (so that if someone accesses the data it will be useless) or across the network. There are standard systems that will ensure that communication between a user and the server is scrambled so that if anyone listens in they will be unable to understand what is being passed. The length of the key used determines how difficult the code will be to break.

- **Internal traffic monitoring system:** these systems are now readily available. They are inexpensive and provide a means to monitor unofficial/unauthorised usage of the network (both internal and internet use) without the need for a highly-skilled system administrator. These systems provide an assurance that the firewall and anti-virus software are working properly. They can limit access to sensitive information to those who need it, and can identify misuse of business servers by outsiders exploiting lax internal security.

## Firewalls

Firewalls can be either software or hardware. Firewalls are designed to provide security between the internet and your system or PC and only allow authorised access to your PCs and servers in your system. They can stop different types of access, such as access to, or from, certain sites (filtering), and can range from simple systems with simple rules to highly sophisticated systems. They are often combined with anti-virus software to provide a level of security to prevent unauthorised access and risk. Care must be taken in loading a firewall on to your system and there is a need to ensure that the provider of such software is a 'trusted' source especially when the application is being downloaded from the internet. More information on firewalls can be obtained at:

- [www.wisegeek.com](http://www.wisegeek.com)

## Employment Screening and Monitoring

Experience and research has shown that, unfortunately, the majority of fraud is carried out by, or through, people within a business or organisation. It is estimated that about 70% of all CVs are deceptive. Confirmation of the integrity and good intentions of employees and business partners is therefore critical prior to allowing them into positions of trust.

There are many ways in which attacks can be facilitated against companies from internal means. These include:

- Direct theft of intellectual property.
- Passing on business information, for personal gain or out of fear, to competitors.
- Passing customer details to third parties in order that attacks may be facilitated against that organisation. This is where there may be an employee of a financial institution passing customer account details to organised criminals.

### **Lessons that can be learnt are:**

- The role of HR and staff vetting. Ensure you really do know who you are employing. Are their references correct? Does their identity stand up to scrutiny?
- How good are systems for identifying whether there has been an internal attack?
- What whistle-blowing policies are in place?
- Where an organisation has an investigative branch, how do they investigate? Consider a proactive approach to investigation.
- Are there policies and procedures in place for internal controls? Are staff aware of the risks of becoming embroiled in crime?

## 5. What to Do if You Become a Victim

There are a number of warning signs that may indicate that your system is being attacked. These include:

- System slows down for no apparent reason (this '**may be**' an indication that the virus or Trojan is using your PC's power leaving little or nothing for you).
- System becomes unresponsive to your commands.
- Your anti-virus program informs you that it has detected a virus.

Even if you are careful to avoid a computer virus, you may still be unlucky. If you are a victim and damage is done to your data you may consider taking legal action to seek recompense, if the person who sent you the virus can be identified. It is important that once you suspect or detect such an attack you do not panic and in the process destroy important evidence you may need later to follow through with a prosecution. If you decide this is a possible course of action then take professional advice when the problem is detected so as not to accidentally destroy valuable data which might make prosecution more difficult to pursue. However, if this is not a course you want to consider, then providing you have installed an anti-virus program, you should be able to follow the instructions to remove the virus from your system.

### Legal Recourse

Many attacks on computer systems are illegal under the Computer Misuse Act 1990:

- **Section 1:** makes hacking a criminal offence, irrespective of whether any harm is intended. Hacking out of curiosity or for the challenge of breaking through a security system is covered if the hacker is aware that his access is unauthorised. The intent does not need to be directed at any particular type of program or data.
- **Section 3:** is aimed at people who introduce worms and viruses to computer systems. If the physical condition of the computer is impaired, whether intentionally or recklessly, an offence under the Criminal Damage Act 1971 may also have been committed. Section 3 covers non-tangible damage which is now (by section 3(6)) expressly excluded from the Criminal Damage Act.

The victims of cybercrime should always consider using civil proceedings as a method of recovering stolen assets. It is possible to use court orders to trace stolen assets through different bank accounts and even into assets purchased using the money. If the criminals can be identified it may also be possible to freeze their worldwide assets and require them to disclose details of any further assets.

## Useful Links

### **Fraud Advisory Panel**

[www.fraudadvisorypanel.org](http://www.fraudadvisorypanel.org)

### **Bank Safe Online**

[www.banksafeonline.org.uk](http://www.banksafeonline.org.uk)

### **CIFAS – the UK'S Fraud Prevention Service**

[www.cifas.org.uk](http://www.cifas.org.uk)

### **City of London Police**

[www.cityoflondon.police.uk](http://www.cityoflondon.police.uk)

### **Crimestoppers**

[www.crimestoppers.co.uk](http://www.crimestoppers.co.uk)

### **Department of Trade and Industry**

[www.dti.gov.uk](http://www.dti.gov.uk)

### **Financial Services Authority**

[www.fsa.gov.uk](http://www.fsa.gov.uk)

### **Federation of Small Businesses**

[www.fsb.org.uk](http://www.fsb.org.uk)

### **HM Treasury**

[www.hm-treasury.gov.uk](http://www.hm-treasury.gov.uk)

### **Home Office**

[www.homeoffice.gov.uk](http://www.homeoffice.gov.uk)

### **IT Governance**

[www.itgovernance.co.uk](http://www.itgovernance.co.uk)

### **Metropolitan Police Service**

[www.met.police.uk](http://www.met.police.uk)

### **Microsoft**

[www.microsoft.com/security/protect](http://www.microsoft.com/security/protect)

### **National Hi-Tech Crime Unit**

[www.nhtcu.org](http://www.nhtcu.org)

### **National Criminal Intelligence Service**

[www.ncis.gov.uk](http://www.ncis.gov.uk)

### **Office of Fair Trading**

[www.of.t.gov.uk](http://www.of.t.gov.uk)

### **Scam Busters**

[www.scambusters.org](http://www.scambusters.org)

### **Stay Safe Online**

[www.staysafeonline.info](http://www.staysafeonline.info)

### **Websites Dealing with Credit Card Schemes**

[www.visaeu.com](http://www.visaeu.com)

[www.mastercardmerchant.com](http://www.mastercardmerchant.com)

**For more information on the Fraud Advisory Panel please contact:**

**Fraud Advisory Panel**

Chartered Accountants' Hall, PO Box 433, Moorgate Place, London, EC2P 2BJ

Tel: 020 7920 8721

Fax: 020 7920 8536

Email: [info@fraudadvisorypanel.org](mailto:info@fraudadvisorypanel.org)

**Or visit:**

[www.fraudadvisorypanel.org](http://www.fraudadvisorypanel.org)

Registered Charity No. 1108863

September 2005