

**The Fraud
Advisory
Panel**

the fraud Cybercrime -
advisory what every SME
panel should know

Cybercrime only happens to large companies. Wake-up practical guide for SME's from the Fraud Advisory Panel

"We don't trade on-line, Cybercrime isn't a problem for us."

Cybercrime isn't something that only affects businesses who trade on-line. If you have a computer in the workplace, you could be a victim of Cybercrime.

Cybercrime isn't just about obtaining goods on-line using a stolen credit card, it can manifest itself in theft of information or disruption caused by hackers.

The aim of this guide is to highlight the risks involved, the forms those risks take, and offering practical suggestions on prevention, detection and prosecution.

Introduction

What is Cybercrime and how serious is it?

Cybercrime is a growing problem for all organisations and businesses. Indeed, it led to the formation in 2001 of the National Hi-Tech Crime Unit. Its task is to combat computer-based crime and the Unit works with law enforcement experts selected from the National Crime Squad, the National Criminal Intelligence Service, HM Customs and Excise and police forces.

Cybercrime. It may take a number of different guises and the cybercriminal's motivation may differ from simple theft of electronic money or credit card fraud to theft of information or simply disruption for the kudos, commercial or political purposes.

A report in April 2002 by the Department of Trade and Industry (DTI) found that computer hacking, cyberfraud and software bugs are costing Britain up to £10 billion a year. According to the DTI, 50% of all businesses were victims of such attacks compared with 25% in 2000 and less than 1 in 5 in 1998. The report found that attacks by hackers on firms more than tripled in the past 2 years and 4 out of 5 of the biggest companies have fallen victim to hackers, virus or fraud in 2001.

The average cost of each security lapse is £30,000. Several companies said viruses, fraud and hacking had cost them well over £500,000.

The CSI/FBI Survey of 2002 reports that in the US:

- 90% of respondents detected computer security breaches within the last twelve months compared to 85% in the previous year
- 80% acknowledged financial losses due to a breach of computer security
- 44% of respondents were willing or able to quantify such losses. This was reportedly \$455,848,000

- Most serious losses were caused by theft of proprietary information and financial fraud
- 74% of respondents reported that their internet connection was the most frequent point of attack, compared to 33% who reported that their internal network was the most frequent point of attack
- Only 34% of respondents reported such intrusions to law enforcement agencies compared to 36% in the previous year

Does your business or organisation self regulate?

Does your business:

- review the effectiveness of risk and control processes as recommended by the Turnbull guidelines
- regularly evaluate all e-business risks, including Cybercrime risks
- review at Board level the internet strategy and related risk management to reduce long term fraud liability and enable your business to effectively respond to a 'Turnbull' assessment
- review at Board level compliance with statutory requirements such as data protection and money laundering regulations
- value its data – make an assessment of the monetary value and sensitivity of the data they hold

If your business does not then it could be in danger of falling victim to a cybercriminal, falling foul of legislation and recommended business standards and being held accountable in respect of any losses that result from Cybercrime attacks.

Businesses should be:

- Cultivating a culture of Cybercrime awareness by placing emphasis on the recruitment of experts, employee training and obtaining advice
- Monitoring Cybercrime and internet news to obtain a better understanding of the threats posed by Cybercrime and to enable the business to implement new measures and best practices as they are produced
- Contributing their experience to business organisations, advisory panels and government
- Establishing better working practices for staff, such as guidelines relating to accepted internet use or guidelines to control the use of email facilities
- Considering using biometrics or other forms of security technology for the purposes of user identification
- Considering using strong encryption, digital signatures and digital identification, even on Intranets

- Investigating possibility of prosecution and loss recovery to deter further attacks
- Considering cyber insurance

To protect an organisation against Cybercrime it is important to understand what types of Cybercrime exist and how exactly a business is vulnerable. A few examples of different types of Cybercrime follow:

Examples of Cybercrime

Hackers

Hackers divide into two main groups. The internal hacker and the external hacker. The hacker may work as an individual or in highly organised gangs either of whom may attempt to gain access into a computer system in order to carry out a criminal activity. The hacker may intend to steal information or funds, to publicise a cause (more commonly known as a "hacktivist"), or to deface a website. Some hackers claim to hack software developers and other sites in order to prove that security can be violated and to highlight security flaws.

In January 2002 hackers cut off the website to the World Economic Forum through a denial of service attack, disrupting a conference held for world political and economic leaders. The previous year, the hackers broke into the site and stole details of 27,000 delegates attending the conference by attacking the website. The DTI report of April 2002 reveals that key UK Government Departments face an average of 84 hacking attempts a week.

Web sabotage is a major cause of concern for police. Hackers access genuine web sites and alter their appearance, change information or set up a replica website using false information. A recent example of web sabotage involved the Red Cross website. The Red Cross website was cloned by hackers following the events of September 11th and for 36 hours, all donations made to the Red Cross were diverted to a cyber fraudster.

Internal hackers do not have to penetrate the system from the outside. It is therefore far easier for an internal hacker to cause damage. PriceWaterhouseCoopers reported in June 2001 that 60% of frauds were committed internally. It has also been reported that up to 75% of thefts and frauds have been committed by an insider.

E-Theft

It was reported in early 2001 that an employee of an oil company managed to steal \$473,541 through E-theft. She transferred funds from the company to her husband's business in two electronic transactions over an 11- month period.

The fraud took so long to uncover because of the procedures adopted by the company. The broker handling accounts never received a list of authorised accounts to which he could transfer funds and because duties in the company were segregated, the left hand didn't know what the right hand was doing!

In January 2002 it was reported by Evans Data that 27% of US and Canadian banks suffered a hack attempt during 2001.

Netspionage

Netspionage is where confidential information is stolen by hackers, to sell to a competitor or for the use of individuals' business exploits. Espionage was originally limited to governments, but with the information age, the rise of corporate espionage has been rapid.

In March 2001 it was reported that an unidentified hacker escaped with the system codes for satellite and missile guidance systems. The theft was not even discovered until three days after it had happened. It was widely suspected that the information was to be used for the purposes of industrial espionage.

According to recent surveys, world-wide losses suffered through misappropriation of computerised intellectual property cost copyright owners close to \$20 billion last year.

Canal Plus is suing NDS for \$3 billion for allegedly sabotaging its business. It is alleged that NDS obtained the security code on the Canal Plus smart card which enabled viewers a choice of different channels. Whilst many companies engage in reverse engineering to examine their competitors' products, Canal Plus claims that NDS published the security code on the internet, where it was picked up by international counterfeiters. In turn, it is alleged that the counterfeiters produced fake smart cards which allowed users to watch subscription channels free. Canal Plus says this was a deliberate plan to sabotage the business in which it was a market leader. The allegations have been denied.

In a report by the CBI in August 2001, 6% of UK respondents reported that they had suffered from netspionage and quantifiable losses were £151 million as compared to £66 million in the same report last year.

Domain Name Renewal Scams

A recent scam to emerge is the domain name renewal scam. This has been a concern in both the USA and Europe. A victim will commonly receive an email from a sender who is purportedly a Domain Name Registrar. The registrar offers you an opportunity to upgrade your website address with the new suffix ".info". The email will include a link to allow you to read more information about the upgrade, however when you enter the link the program functions as if you had agreed to transfer your domain name. The domain name is then transferred to their company as registrar who claim that you requested the transfer.

Telecom Fraud

Telecom fraud is a less well-known method of committing e-theft. This method is estimated to net organised gangs of fraudsters £40bn a year. One method used is "Phreaking" which is the equivalent of hacking on computer networks. A company's telephone exchange is penetrated using a computer programme which permits the calls to be resold to other users. Usually a cheap telephone company is set up offering international calls at a very low cost. In one case this type of fraud cost a business £750,000 in extra telephone calls.

A different type of telecom fraud is known as premium rate fraud. Businesses are particularly susceptible to this kind of fraud which involves an employee ringing a premium rate number at night and leaving the telephone off the hook. The employee's accomplice has set up the premium rate number and charges the company for the cost of the telephone call.

Identity / Credit Card Fraud

Online retail has made the life of the credit card fraudster far easier due to the degree of anonymity permitted. There are a number of methods of obtaining credit card details, from the low tech methods of bin raiding to the high tech methods of cloning, skimming and obtaining the details by hacking in to websites.

The fraudster then carries out online purchases using the credit card details and requesting that the goods are sent to a different address to the genuine card holder. The credit card holder eventually discovers that a number of purchases have been made on their card fraudulently. The credit card company generally reimburses the credit card holders account but the retailer usually foots the bill due to the terms and conditions of the contract they have with credit card companies. This is commonly known as a charge back.

In March 2002 APACS reported that credit card fraud in the UK had cost £400 million. Card not present fraud which is carried out over the telephone or internet rose by 94% in 2000 and is one of the fastest growing types of fraud in the UK. Credit card fraud has been estimated to reach £600 million per year in the UK by 2005.

Reasons to act

In the past, companies have failed to deal with Cybercrime due to lack of awareness or because of the stigma associated with being seen as a victim of fraud or Cybercrime of this nature. There have also been few requirements that companies do take proactive steps to prevent this type of fraud. This approach is no longer acceptable and businesses must now act to ensure that they are adequately protected from and take action in respect of Cybercrime. Taking adequate steps to improve an organisations risk management in terms of Cybercrime is no longer simply desirable, it is imperative.

Businesses are now under pressure from a number of different pieces of legislation and guidelines to get their approach to Cybercrime right.

- The Turnbull Guidelines
- Data Protection Act 1998
- The Human Rights Act 1998
- Liability as an accessory
- Liability of directors

Turnbull Guidelines

Whilst the provisions of the Turnbull Guidelines are only requirements for publicly listed companies, they are increasingly being viewed as the benchmark on good corporate governance for all listed UK companies and the standard by which they may be judged.

Provision D2 of the Turnbull Guidelines states that: "The board should maintain a sound system of internal control to safeguard shareholders' investment and the company's assets."

Provision D.2.1 states that: "The directors should, at least annually, conduct a review of the effectiveness of the group's system of internal control and should report to all shareholders that they have done so. The review should cover all controls including financial, operational and compliance controls and risk management."

Provision D.2.2 states that: "Companies which do not have an internal audit function should periodically review the need for one."

Data Protection

Anyone who stores information about another person, be it for a commercial or other purpose, has a duty to maintain that data in accordance with the principles of Data Protection. This means that as well as the requirement that the data stored is accurate and not stored for a period of time longer than necessary, the data must be kept secure.

This will require businesses to take steps to ensure that their computer systems and operational functions comply. The DTI provides a business standard benchmark for businesses and organisations attempting to comply with the Data Protection Act and other IT security issues called BS7799 (now adopted as ISO 17799). This is a common sense security standard which every business should benchmark themselves against (even if they do not go for full accreditation).

Human Rights

The right to privacy and family life are rights enshrined under the Human Rights Act 1998. Whenever a company or organisation stores information it must do so with these principles in mind and take adequate steps to ensure that their organisation implements the correct controls and processes to ensure that data is secure as possible and that in the event a company does suffer a Cybercrime attack the Human Rights principles are infringed to as lesser an extent as possible.

Liability of Directors

Directors may, under the Turnbull Guidelines, find themselves in breach of duty to the company and consequently the shareholders for failing to carry out the correct risk management procedures and controls in respect of Cybercrime.

Directors owe the company a number of fiduciary duties due to the position they hold within the company including a duty of good faith and duty to act with due diligence. They also owe duties of professional competence depending upon the terms of a director's service contract. If a director breaches the duties owed to the company he may face personal liability as against the company.

In the event that a company loses a substantial amount of money to a cybercriminal it may be unable or not commercially viable for a company to pursue the fraudster.

In that case a company may be obliged to look to the director responsible for the implementation of risk management for redress. If the director has failed to act with due care in respect of a foreseeable risk, this may result in the company seeking to establish that the director was liable for breach of duty of care and to recover damages from that director.

Liability of Accessories

It is important to appreciate that the person who has committed the fraud may not be the only person against whom a remedy can be obtained. There may be other people involved in committing the crime and therefore equally accountable.

For example, in the case of cyber laundering, a firm may become liable by virtue of the principle of constructive trusteeship depending on whether they were at any point in receipt of laundered funds.

It is as a result of the principle of liability of accessories that mean that banks and others used as a conduit by money launderers may find themselves in a difficult situation to avoid becoming secondary victims.

Many countries and, notably, the European Union are looking to the registration authorities to verify the identity of e-traders by issuing digital certificates. There therefore may be scope for a claim against a registration authority (RA) that issues a certificate to a launderer.

Lawyers and accountants who have been involved in setting up any scheme may also be legitimate compensation targets.

Therefore, depending on the particular nature of your business, there are a multitude of different ways in which a business can incur liability for the Cybercrimes of a fraudster.

The key to avoid the money laundering liability is to "Know your customer". Firms should take action in support of Anti-Money Laundering measures in order to:

- comply with legal requirements
- protect their corporate reputation

Evidence of identity & beneficial ownership should be sought and a higher level of due diligence undertaken where there are:

- numbered or alternative accounts
- high risk countries involved
- offshore jurisdictions
- high risk activities
- public officials involved

Reviewing Policy and Procedure

Many firms will carry out financial controls, audits and assessments. The Turnbull report places greater emphasis on the need for assessment of risk and operational controls. This means that senior management are required to review the procedures applied to risk management and control on an annual basis and decide which areas are lacking in such controls. Essentially they will have to start carrying out an internal audit of operational risk. The business benefit of this is that it can be stated on your annual accounts and could lead to greater trust by your customers and therefore increased business or market share.

In order to effectively review policy and procedure in terms of operational risk management, companies should be reviewing at Board level, their internet strategy and the related risk management issues. In particular it is advisable that companies and organisations appoint one director to oversee the area where business strategy warrants this level of supervision, attaching responsibility for operational risk in relation to Cybercrime to this individual or their department. This has the advantage of reducing the risk of criminal and civil prosecution of directors or the company for failure to comply with current standards and regulations and may well reduce long-term fraud losses. It may also reduce the chances that the company is rendered liable for receiving laundered or fraudulently obtained funds under the doctrine of constructive liability. However the fight against Cybercrime must be fought on all company levels. It is necessary to establish policy and procedure which applies to everybody in the business.

Cybercrime Policy Statement

A policy statement and settled working practices should be published by the Board to ensure that every employee knows the standard required of them and the company stance in relation to Cybercrime. Such a statement needs to be explained to every employee and should ideally be included in contracts of employment, supply and outsourcing agreements.

The policy statement should make clear the action that the company will take in the event that an act of Cybercrime is detected. The statement should clearly express the company's policy towards Cybercrime and it's determination to deter fraud generally.

- The company should make clear that it will investigate and report to their local police or other appropriate authority any suspected acts of Cybercrime
- The company will assist the police in their investigations and prosecution of a cyber criminal if appropriate
- The company will take civil action where possible and recover assets which have been stolen or pursue a cyber criminal for damages
- The company expects employees to report any incidence of Cybercrime of which they are aware and clarify that each employee, irrespective of their level of seniority, has a responsibility for reporting Cybercrime
- Internally perpetrated Cybercrime will be treated as seriously as a Cybercrime perpetrated by an organisation outsider
- The procedure which should be followed in the event that a Cybercrime occurs

The DTI report says the increase in Cybercrime is partly because companies give employees access to their web and their own work e-mail addresses. It may also be of merit to include guidelines and company policy statements in relation to employee internet and e-mail use in their employment contracts. For example, highlighting the danger of opening emails with attachments from unknown sources, or listing sites which are prohibited from use, explaining company policy in relation to internet and software piracy (another common form of Cybercrime).

Managing the Prevention, Detection and Response to Prosecution of Cybercrime

Cybercrime management should be dealt with throughout the organisation and the importance of employee awareness should be emphasised at all levels.

Cybercrime needs to be treated as a business risk and an organisation therefore needs to carry out a risk management assessment procedure to ensure that the steps taken to prevent Cybercrime are effective in relation to the practices peculiar to that organisation. Anti-Cybercrime procedures should be tailored to match the type of business in which an organisation is involved. For example, an e-tailer is more likely to be concerned with establishing the identity of the individual attempting to carry out a 'Card Not Present' transaction to make an online purchase as this type of business is more prone to the risk of identity theft and credit card fraud. The fraudster is more likely to be an outsider. A business to business company which trades on-line may be more concerned with establishing procedures and controls which reduce the risk of e-procurement fraud and may wish to employ fraud detection methods such as data mining or require procedures for the making of e-tenders. In the case of e-procurement fraud the fraud is far more likely to be perpetrated by an insider and as such the methods of detecting the fraud need to reflect this fact.

Risk management of the threat of Cybercrime should be approached as follows:

- The company should identify the areas within the business which are most vulnerable to cyber attack
- Establish the controls that they already have in place to address these risks
- Identify any further controls which may assist in reducing the risk
- Monitor pre-existing controls to ensure they are being 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

Whistle-blowing Policy

All organisations should establish a culture of Cybercrime awareness and part of doing so is to ensure that employees know that whistle-blowing is a necessary part of the fight to prevent Cybercrime.

Employees should have available to them a simple procedure for reporting any suspicion that Cybercrime is taking place. This may include an internal email address to send details to or a hot line to enable them to report their complaint quickly and if the employee wishes to do so, anonymously.

It should also be made possible for the employee to report to management in different departments or management with no direct responsibility for that employee, given that the employee may fear that their direct manager is somehow implicated in an act of cyber fraud.

It should be made clear to employees that all reports will be treated as confidential. Where such reports are made in good faith, they are made in good faith, the employee would normally be protected under the Public Interest Disclosure Act 1998 (PIDA).

This is particularly relevant to incidences of Cybercrime where as discussed earlier, a good proportion of the problem arises from the unlawful conduct of insiders and employees. The objective of the PIDA is to ensure that employees can inform their employers of wrongdoing within a company without fear of repercussions, to allow problems to be identified and resolved in as little time as possible. The repercussions referred to cover different types of detriment that an employee may suffer having made such a disclosure, including denial of a promotion, training opportunities or facilities which the employee would have been offered had it not been for the disclosure.

The employee is protected by PIDA if he makes a qualifying disclosure of information which he reasonably believes (and the employee can show that he reasonably believes) tends to show that one of the following offences or breaches have, are being or will be committed, irrespective of whether the employee is later shown to have been incorrect:

- A criminal offence
- A breach of a legal obligation
- A danger to the health and safety of any person
- Environmental damage
- Intentional concealing of information which demonstrates that any of the above have occurred

The disclosure is protected if the employee makes the qualifying disclosure to his employer either by company procedures authorised by the employer or directly to the employer or by making the disclosure to another person whom the worker reasonably believes to be solely or mainly responsible for the relevant failure.

The employee must also make the disclosure in good faith. If the employer wishes to make the disclosure to a prescribed body or person then he is protected if he makes the qualifying disclosure in good faith, he reasonably believes that any allegation or information is substantially true and reasonably believes that the matter falls within the remit of the prescribed person or body. For example if the information relates to a fraud the employee might reasonably think the Serious Fraud Office would be the correct body to make the report to or in the case of an offence relating to the environment, that the Environment Agency was the correct body.

Where a company does not have the resources to set up a whistle-blowing mechanism internally, it is possible to outsource this service. For serious cases of cyber fraud, it is possible to report the offence to the National High Tech Crime Unit.

What to do when Cybercrime is detected

It is necessary to maintain a procedure for dealing with any report of cyberfraud. The procedure to be implemented will vary depending on the size of the business and the scale and seriousness of the Cybercrime being investigated.

A firm may wish to appoint one person as responsible for investigating the Cybercrime. They will in turn be responsible for researching the best methods of investigating a specific type of Cybercrime.

This individual may also be given responsibility for assessing the in-house skills available for investigating Cybercrime. For example whether the firm has anyone with the computer science skills to enable electronic evidence to be detected and preserved. It will also be necessary for that person to establish contacts with specialist lawyers and investigators.

Damage mitigation is another issue which must be addressed by the firm. It should be decided how it is possible to stop a particular Cybercrime from happening again and whether improved techniques of risk management are necessary.

It must be considered how the firm intends to secure and gather the evidence without alerting the criminal. The firm must address the question of how does the firm intend to deal with a suspect and whether, if so, when should the firm contact the relevant authorities including the National High Tech Crime Unit?

As with all frauds, it must be considered when it is appropriate to inform the public that a Cybercrime has occurred, bearing in mind the damage that such an announcement can have on a business compared to the value of the crime itself.

If an organisation does intend to prosecute a Cybercrime it must bear in mind the following:

- Speed
- Strategy
- Surprise

Money is transferable by one e-mail, telephone call or fax. It is therefore vital that not only is any investigation/analysis conducted in utmost secrecy but action is taken before the fraudster has an inkling that he is being investigated.

At the very earliest opportunity, an analysis should be carried out to assess:-

- a) whether there has been any fraud
- b) the extent of the fraud
- c) whether it is viable to try and recover the losses sustained

To do this it may be necessary to examine computer server logs and individuals' computers. Consult Appendix A before taking any action, otherwise vital evidence needed for civil recovery or criminal action, may be destroyed.

Third party disclosure as to assets and whereabouts

The English courts provide invaluable assistance to a victim in that in certain circumstances they grant orders which enable the victim, without notice to the fraudster, to discover :-

the extent of the fraud

who is responsible and

who was involved in the commission of the fraud and therefore could be liable as well

The court would for example grant orders against 3rd parties who have been unwittingly involved in the fraud, whether such fraud has been committed electronically or in the physical world. For instance, the court will require disclosure of relevant information by an Internet Service Provider or a bank through whom for instance money stolen from the victim has passed.

Such orders for disclosure can be combined with what is called a "gagging" order which prevents the party giving disclosure from notifying the fraudster. Breach of such an order will amount to a contempt of court which is punishable by prison.

Once the extent of the fraud has been assessed, decisions need to be taken as to whether it is commercially sensible (and whether there is an obligation) to pursue the fraudster and if so, to what extent. No victim, however large or small, should fail to assess the significance of publicity, given the fact that it has been the victim of fraud which is often caused by inadequate security measures or lack of judgement.

Recruitment, Training and Personnel Policies

The majority of financial crime is perpetrated by insiders and employees. Cybercrime is no different. It is therefore essential for organisations to take appropriate steps to ensure their computer and physical security is adequate. Personnel should be carefully vetted. References should be checked and this includes temporary and contract staff. The procedure for vetting and checking should become more stringent when employees are promoted to positions of greater responsibility and the greater the amount of personal, financial or sensitive data to which the employee is privy.

Employers should consider multi-level security, including biometric finger printing employees and implementing similar security procedures of this nature to ensure that employees are only permitted access to an appropriate level according to their role or seniority. Access level should be reviewed on a frequent basis.

Employees who leave a firm (for any reason) should immediately be removed from the security clearance lists and any access to an organisation's database should be removed. Security lists should regularly be reviewed to ensure that those who do have access should have access and whether access is necessary to the level which is permitted.

Employers should consider the use of monitoring emails and communications in order to prevent fraud and other forms of Cybercrime, where it is warranted, but should inform employees in general that this is likely to occur.

Collaboration with Government Agencies and Professional Advisory Bodies

Organisations should consider collaborating with governmental and professional advisory organisations to report how they manage information security and Cybercrime threats and work with suppliers and users to co-ordinate information on incidents. This will assist businesses in plugging the knowledge and information gaps, assessing where risk management procedures are lacking and where a business' vulnerabilities lie.

In connection with this, organisations may find it of great assistance to collaborate with government and industry advisory bodies to produce educational materials on the nature of Cybercrime, why it has posed a problem for their particular business and how they have obtained information and guidance on the subject.

Ultimately, reviewing existing and producing further guidance on basic information security requirements and good risk management practice to combat Cybercrime could be used to produce a Superhighway Code. This would ideally take into account BS7799, organisations established by the Information Systems Audit and Information Control Association and also the work of the IT Governance Institute in the USA.

The aim is to eventually raise general awareness among industry, accountancy and the legal professions of the law relating to Cybercrime and its effective precaution.

Compliance

No procedure or control is effective unless properly implemented throughout an organisation. Regular checks must be undertaken in order to ensure that all necessary controls are being adequately implemented by employees at all levels, short cuts are not used in such a way as to dilute the controls effectiveness and that controls remain effective in the light of changes in the law or in the development of the organisation's business.

Disclaimer

Whilst every effort has been made in the construction of this Guide, compliance with it does not guarantee that your business will not be a victim of fraud. Each business should take appropriate independent advice on the management of fraud risk.

The Fraud Advisory Panel and the contributors to the Guide accept no responsibility for any action taken by parties as a result of reading the Guide. Readers should obtain the appropriate professional advice on the issues raised.

Appendix A

Do's and Don'ts for computer based information

Computer evidence or data is fundamentally different from, say, paper evidence. Just the act of turning on a computer can change a whole series of dates and times and invalidate its use in a court or tribunal. Therefore, a few basic principles need to be followed when dealing with potentially valuable computer evidence.

Do:

- Fully assess the situation before taking any action
- Isolate the computer so that it cannot be tampered with
- Record where the computer is based and all who had access to it
- Consider securing all relevant logs (e.g. building access logs, server logs, Internet logs etc.) and any CCTV footage, at the earliest opportunity
- Call in IT security staff or external consultants as appropriate

Then ask the relevant expert to:

- Disconnect the relevant computers from your network
- Restrict remote access
- Take an "image" copy of the computer

Don't:

- Alert any of the potential suspects
- Call in your own IT support staff (they often change evidence inadvertently)
- Turn on the computer if it is switched off
- Turn off the computer if it is turned on
- Move the computer if it is switched on
- Make a copy of the computer
- Examine electronic logs without first ensuring that they are preserved elsewhere

The Fraud Advisory Panel

For a printed version of this document, please send a cheque for £3 made payable to Fraud Advisory Panel. For information about the Fraud Advisory Panel, please contact Helen Fay by email at

Helen.Fay@icaew.co.uk

or write to

The Fraud Advisory Panel
Chartered Accountants' Hall
PO Box 433
Moorgate Place
London
EC2P 2BJ

Useful Links

Serious Fraud Office
Tel No: 020 7239 7272
www.sfo.gov.uk

Companies House
Tel No: 0870 333 3636
www.companieshouse.co.uk

City of London Police Fraud Squad
Tel No: 020 7601 2222
www.cityoflondon.police.uk/level1/crime/fraud_main.html

National Audit Office
Tel No: 020 7798 7000
www.nao.gov.uk

Metropolitan Police Fraud Squad
(for high value fraud over £750,000)
Tel No: 020 7230 1212
www.met.police.uk/so/so6.htm

Institute of Chartered Accountants in
England & Wales
Tel No: 020 7920 8100
www.icaew.co.uk

National Criminal Intelligence Service
(NCIS)
Tel No: 020 7238 8431
www.ncis.co.uk

Law Society
Tel No: 020 7242 1222
www.lawsociety.org.uk

Financial Services Authority
Tel No: 020 7676 1000
www.fsa.gov.uk

Home Office
Tel No: 020 7273 4000
www.homeoffice.gov.uk

Confederation of British Industry
Tel No: 020 7395 8195
www.cbi.org.uk

Public Concern at Work
Tel No: 020 7404 6609
www.pcaw.demon.co.uk

Small Business Service
Tel No: 0114 259 7788
www.businesslink.org

Crimestoppers
Tel No: 0800 555 111
www.crimestoppers-uk.org

Inland Revenue
www.inlandrevenue.gov.uk

Health & Safety Executive
www.hse.gov.uk

HM Customs & Excise
www.hmce.gov.uk

UK Online for Business
www.onlineforbusiness.gov.uk

Trading Standards
www.tradingstandards.gov.uk

Data Protection Commissioner
www.dataprotection.gov.uk

Department of Trade & Industry
Tel No: 020 7215 5000
Information Security Group Policy
Tel No: 020 7215 1962
www.dti.gov.uk

National Hi-Tech Crime Unit
PO Box 10101
E14 9NF
Tel No: 0870 2410549
www.ncs.police.uk/nhtuc

www.fraud.org.uk

Cybercrime Working Group

Steven Philippsohn (Chairman)	Philippsohn, Crawford, Berwald
Paul Barnes	Nottingham Business School
Monica Bond	Bond Associates
Allie Burgess	CIFAS
Simon Carman	CGU Guarantee Society
Paul Friedman	Baker & Mckenzie
Malcolm Gardner	Malcolm Gardner Associates
Elaine Hardy	Hardy Associates
Frank Heinrich-Jones	PLC Consultancy Services
Ian Henderson	Haymarket Management Services Ltd
Miles Hewitt-Boorman	Chantrey Vellacott DFK
John MacGowan	Advisory Forum for Retail Credit Card Transactions (AFRECT)
Sarah Markham	AIG Europe (UK) Limited, Crime Department
Tony Neate	National High Tech Crime Unit
Terence Palfrey	Crown Prosecution Service
David Rowe-Francis	Carney Solicitor
John Ryder	Royal & Sun Alliance
Pamela Taylor	Confederation of British Industry
Ian Taylorson	Constant & Constant
Alan Wilkie	Law Commission
Euan Williamson	PLC Consultancy Services
Mark Witchell	Royal & Sun Alliance
Keith Woolland	Financial Services Authority
Peter Yapp	Control Risks Group
Helen Fay	Fraud Advisory Panel

