

This factsheet will help you protect your business against theft involving computer systems. It covers risk, recovery, prevention, physical security and includes a case study about hardware theft.

### INTRODUCTION

The DTI's Information Security Breaches Survey 2004 found that in the case of theft and fraud involving computers, physical theft was the most commonly reported incident, with one in ten businesses having had computers stolen over the last year. Although financial fraud or theft using computer systems remains relatively rare with only 2% of companies experiencing a computer fraud in the last year, protection of information remains an important issue.

All information has value, sometimes trivial, although the list below shows some examples that are anything but:

- Medical records
- Financial transactions
- Building plans (especially if the building needs to be secure, such as a bank branch)

Value can sometimes be measured in straightforward monetary terms but there are other ways of looking at it. For example, the unauthorised disclosure of information. Loss of confidentiality could:

- Cause unnecessary personal embarrassment
- Damage a company's reputation
- Affect someone's personal safety
- Cause the loss of a commercial patent or copyright

Information is often of value to competitors, and may even be stolen to order. Such information might include:

- Customer lists
- Research and development details
- Marketing plans

- Product launches
- Staff records

This factsheet is for any business that wants to protect itself against software or hardware theft. It covers: risks, recovery, prevention, physical security and remote working.

### THEFT-RISK

It sounds obvious, but people will only steal your information if it is valuable. If information is valuable to you, it is likely that others will find it valuable too. A true understanding of risk requires risk management, but the following points should help you decide whether you need to take such a step:

- Is your company involved with the following (or similar) activities:
  - Direct marketing and/or the use of mailing lists
  - Research for example, engineering, pharmaceuticals, aerospace, IT product development
  - Patents and/or copyright
  - Intellectual Property Rights (IPR)
- Does your company handle sensitive information that could be sold (for example, to the media) or used as the basis of blackmail (such as medical or financial records)?
- Do you handle plans and itineraries? These could include:
  - Marketing plans
  - Itineraries for VIPs
  - Product launch plans

- Media programme schedules

If you answered YES to any of the above, you probably carry an increased risk of information theft.

### THEFT-RECOVERY

As with any other type of information security incident, recovery is easier when it is approached in a structured way. Some questions to be answered immediately are:

- What's been stolen?
- Is it ongoing?
- How long has this been going on?
- Who knows about it?
- Should you call the Police?
- Do you need to preserve evidence?

Action taken will depend on the scale and potential impact of the theft. For example, if the theft has affected your business to the extent that it has caused a systems failure, do you need to invoke a Business Continuity Plan? If there are legal concerns, or you suspect insider involvement, ensure that Human Resources become involved, and that you are aware of the implications.

### THEFT-PREVENTION

Prevention of information theft requires a wide range of countermeasures. Some are preventative, some detect theft attempts and others provide a means to recover. A common analogy amongst information security specialists is to view security as an onion, with each layer of the onion depicting a barrier to a would-be intruder. Using this model, the main layers would probably be:

- Physical security
- Technical controls
- People-based controls

It is essential to remember that no one single set of controls will provide a solution. In most

cases, a balance of physical, technical and people-based controls usually provides the answer.

### PHYSICAL SECURITY

Physical security is an effective but often overlooked way of keeping information safe. By preventing direct access to a paper file, or preventing access to a computer workstation, you can stop many theft attempts in their tracks.

Physical controls need not depend on a single barrier, such as a turnstile and a security guard at the front door. You can 'double-up' by providing additional security around sensitive areas, such as equipment rooms. Prevent casual access to sensitive departments such as Human Resources and, on a smaller scale, use lockable filing cabinets and safes to protect valuable items and information. Physical security is a major area for consideration, and is examined in more detail later in this document.

### TECHNICAL CONTROLS

There is a multitude of technical tools and techniques to protect information from theft. These include:

- Logical access control
- Cryptography
- Hardening of systems
- Penetration testing
- Intrusion Detection Systems (IDS)

Your choice of control tool or technique is fundamental, and should be based on risk management. There are other constraints and conditions (such as your company's technical configuration) that limit your choice, but the most important thing is to choose appropriate controls to meet the risk.

Part of the risk management process should consider the environment. Information might be safe when manipulated and stored on an

in-house local network but it could become vulnerable when stored on a laptop used by a manager who often works from home.

### PEOPLE BASED CONTROLS

The most common people-based controls are:

- Education & Awareness.
- Contracts, including Non-Disclosure Agreements (NDAs).

There is no stronger control than an informed, attentive and motivated employee. They are able to spot anomalies and other odd events much better than automated systems. Contracts and Non-Disclosure Agreements are powerful preventative controls, as they make it clear to any employee or contractor what is and is not permitted. They can also be used retrospectively in the event of an incident as part of the recovery process.

### PHYSICAL SECURITY

One of the simplest but most effective means of protecting your information assets is to use physical controls. These range from the obvious, such as locking sensitive papers away in a drawer at the end of each working day, to more complex solutions such as integrating door access control systems with Closed Circuit Television Cameras (CCTV).

Methods used will depend on budget, the size and type of business, and the sensitivity of information. The following sections provide broad guidance on physical controls. Some may not be applicable to your organisation, but all are worth considering:

- Risk analysis
- Physical access control cards/tokens
- Security perimeter
- Secure areas
- Local environment and location
- Doors and windows

- Delivery areas.
- Storage and supplies

### RISK ANALYSIS

It is worthwhile performing a risk analysis exercise to understand the risks and requirements relating to physical security. This should help to decide the appropriate controls required.

### PHYSICAL ACCESS CONTROL CARDS/TOKENS

- If you use access control cards, all permanent staff and contractors should be issued with one. The card should remain the property of the company and be revocable at any time.
- Entry cards should only be used by the person to whom they are issued, and should not be given to anyone else, even temporarily.
- If you have front desk security staff, all badge holders should produce their ID or access token on request.
- Review of access control rights on a regular basis, across all areas of the company, is essential.

### SECURITY PERIMETER

It can be worth establishing a defined security perimeter around the company's premises. This perimeter should incorporate several layers, with consideration given to the following controls:

- External walls that form part of the perimeter should be of solid construction.
- External doors that form part of the perimeter should be protected against unauthorised access attempts.
- The doors should slam shut and be alarmed.
- The perimeter should incorporate barriers extending from floor to ceiling.
- Unauthorised recording, photography or filming must be prohibited within the perimeter.

- All building entrances likely to be used by outsiders (visitors, delivery people) should be manned.

### SECURE AREAS

- There are areas within the security perimeter that may require additional controls. These areas are known as secure areas. Examples include:
  - Computer rooms
  - Network and communications equipment rooms/cabinets
  - Human Resources areas
  - Areas handling concentrations of sensitive information e.g. medical records stores
- Only authorised personnel should be permitted to enter secure areas, and visitors to them should be supervised.
- It is sensible to record the entry and departure of visitors to secure areas (for example, identities, dates, times), and visitors should be permitted access only for defined and authorised purposes.
- All personnel within secure areas should wear visible identification, and staff should be encouraged to query unescorted strangers in secure areas.
- As control lists tend to become out of date quite quickly, access rights to secure areas should be reviewed on a regular basis.

### Local environment & location

- Many companies have limited choice when it comes to location. However, if possible, bear the following points in mind when deciding location and office organisation (data centres, computer rooms, etc):
  - Fire
  - Flood
  - Explosion

- Civil unrest
- Other forms of natural or man-made disaster
- The location exercise should also take account of:
  - Health and safety regulations
  - Threats from neighbouring premises (for example, a company making volatile chemicals)

### Doors and windows

- Lock your doors and windows when they're not in use
- Consider installing intruder detection systems. If you do so, test them periodically

### Delivery areas

- If possible, isolate delivery and loading areas from main office work areas and information handling facilities. Access to holding and delivery areas should be restricted only to those who need it.
- Holding areas should enable items to be loaded or unloaded without access being gained to other parts of the building. External doors should be secured when doors giving access to other parts of the building are open.
- Deliveries to a holding area should be registered on entry to the site and inspected for hazards before movement to their point of use.

### Storage & supplies

- Hazardous or combustible material should be stored securely at a safe distance from normal premises. Computer supplies (such as stationery) should be stored away from computer rooms until needed.

### Physical security and remote working

- Home offices, mobile devices, broadband and wireless connections have provided

opportunities for increased productivity and convenience for many companies.

However, the shift from traditional office-based working has introduced risks that are not always obvious, and dealing with these risks requires a planned approach. Remote working requires you to carry out the same information security duties as an IT department in an office situation. You are responsible for backing up your information, keeping these backups safe, keeping your equipment and software up to date, and making sure people cannot read, overhear or steal your information.

### WORKING AWAY FROM THE OFFICE

When you work in an office it is easy to take security for granted - for example, the availability of security guards and having trusted colleagues and a secure building that is locked out of hours. When you work outside of the office, security risks change and it is vital that you adapt your procedures accordingly. For example, in an office environment, you tend to know your colleagues. Also, people are less likely to steal your mobile telephone or PDA. In a public situation (e.g. travelling on a train), you cannot be sure of the integrity of people close by.

Similarly, it is very unlikely that you would employ the same level of physical security at home as in an office. For example, most people do not have facilities for disposing of sensitive papers securely, or have items such as lockable filing cabinets, safes, etc.

When you work away from the office, always consider:

- Physical security how secure is your hotel room, your car, your briefcase, etc?
- Proximity are you being overlooked? Could someone be eavesdropping?
- Virus management do your mobile devices have appropriate anti-virus software installed?

Is this up to date?

- Backups is your data backed up regularly? How much information would be lost if your mobile device was mislaid, stolen or damaged?

### Minimising the risks associated with remote working

Most security risks associated with working away from the office relate to travel and the home, as summarised in the guidelines below.

#### Travel

- Never leave equipment unattended in a public place.
- Avoid leaving equipment in your car. If you must do so, make sure that it is not visible.
- Most hotels provide safes, either in rooms or at reception. Use these to store valuable equipment and information when not in use.
- Avoid displaying any sensitive information on your laptop screen in a public place you never know who may be looking over your shoulder!
- When using public access to the Internet (for example, Internet cafes), remember that computers can store information that has been entered. As a rule, do not use such places if you are handling sensitive information.

#### At home

- Have your home checked by your local Crime Prevention Officer. Their advice can help to improve the general security of your home, and help to protect work information at the same time.
- Ensure that valuable equipment is covered by an appropriate insurance policy.
- Check that your laptop or workstation has adequate virus protection software installed.

Keep this up to date and, if necessary, download security patches from trusted sources (for example, Microsoft).

- Backup your data on a regular basis. Keep all backups safe and secure, preferably away from your usual place of work.
- Use a shredder to destroy sensitive papers if they are no longer required. A 'cross shredder' is best as it is virtually impossible to reconstruct papers that have been cross-shredded.
- Destroy CDs that contain sensitive information when it is no longer required.
- Purchase a fireproof safe for storing valuable or sensitive papers, discs and CDs.
- Ensure that valuable equipment is locked away when it is not in use for a long period of time.

### Insurance

- If you are running a business from home, remember that your general household insurance is unlikely to cover expensive business equipment or your liability if someone is hurt whilst visiting your business.
- Another area which may not be covered is loss of income if your home is damaged to the extent that you cannot work there. Speak to your insurers to clarify your position. Many insurance companies offer specific policies for home businesses, which can be cheaper than standard business insurance.
- If you (or your staff) take office equipment off site (e.g. laptop computers) make sure that it is suitably insured. Many policies will be invalidated if equipment is damaged or lost outside of the insured premises.

### CASE STUDY - HARDWARE THEFT

#### The Organisation

A national testing, training and research centre for specialist technology used in the sub-sea industry based in northern Scotland.

### What Happened

A thief broke into the research centre via a damaged fence and stole mobile telephones, cash and a laptop computer belonging to a subcontractor. The theft took place whilst staff were busy performing a test. Up to five years' worth of work was stored on the laptop hard disc. Although the device was valued at a few hundred pounds, the software was worth as much as £15,000. This was low compared to the value of the research information the device contained. It also stored thousands of e-mails, source documents, web pages and other data. Although there was a backup of the data, it was incomplete and stored on many CDs. The cost of rebuilding the information would run into hundreds of thousands of pounds.

### Impact

There were immediate direct costs involved in rebuilding the data, as well as immediate losses when the subcontractor was unable to operate effectively. The subcontractor would probably have suffered unquantifiable harm to its reputation, which would affect future contractual negotiations.

### Lessons

- Back up your data. Never rely on a single store of information.
- If your data stores are large, prioritise what is essential and make sure it is backed up in a structured manner that makes rebuilding priority systems and applications as quick and easy as possible.
- Physical security is an effective tool in preserving information. Make sure you maintain a secure perimeter if your systems and processes handle valuable information.

**Checklist risk**

- Is your company involved with the following (or similar) activities:
- Direct marketing and/or the use of mailing lists.
- Research for example, engineering, pharmaceuticals, aerospace, IT product development.
- Patents and/or copyright.
- Intellectual Property Rights (IPR).
- Does your company handle sensitive information that could be sold (for example, to the media) or used as the basis of blackmail (such as medical or financial records)?
- Do you handle plans and itineraries? These could include:
  - Marketing plans .
  - Itineraries for VIPs.
  - Product launch plans.
  - Media programme schedules.

If you answered YES to any of the above, you probably carry an increased risk of information theft.

**Recovery**

If you are the victim of information theft, consider the following questions immediately:

- What's been stolen?
- Is it ongoing?
- How long has this been going on?
- Who knows about it?
- Should you call the Police?
- Do you need to preserve evidence?

**Prevention**

The following basic steps can be taken quickly to reduce the likelihood of information theft:

- Make sure you know the sensitivity of your company information - consider performing a formal risk analysis.

- Make sure your people know what's at risk. If they routinely handle sensitive information, make sure they know how it should be handled and what the consequences for disclosure are.
- Establish appropriate physical security controls.
- Use logical access control whenever possible; make sure people understand any password rules and that each individual has their own ID.
- If sensitive computer information is likely to be carried outside your company premises, consider using cryptography as a means of protecting it.
- Think about encrypting your company's laptop hard discs.
- Harden your computer systems using the appropriate technical builds.
- Consider performing (perhaps using a third party) a penetration test to highlight your strengths and weaknesses.
- Consider installing an Intrusion Detection System.

**Physical security**

The following controls are common-sense suggestions that should enhance the protection of your information assets:

- Establish a 'clear-desk' policy. Sensitive material left on a desk could be asking for trouble.
- Establish a 'clear-screen' policy. Workstations should not be left logged on when not in use.
- Consider using padlocks, passwords or equivalent controls to protect workstations and laptop computers.
- If you have an internal mail point, it should be protected, as should unattended fax machines.
- Consider locking photocopiers outside normal working hours.

- If you print sensitive or classified information, clear it from the printer immediately.
- Information, software, equipment or items belonging to the company should not be taken off-site without formal approval. Equipment should be logged out when removed from the premises and logged back in when returned.

#### GENERAL BUSINESS ADVICE

For more information on achieving best practice in your business contact your local Business Link advisor by visiting the website at <http://www.businesslink.gov.uk> or calling 0845 600 9 006.

Published by the Department of Trade and Industry. <http://www.dti.gov.uk> © Crown Copyright