Securing your premises

Theft, vandalism and arson are the crimes most likely to affect your business. There is no single solution. You need to identify the particular threats you face.

This briefing sets out the security measures you should consider to minimise the risks and to make your premises safer. It covers:

- Reviewing your security systems.
- Installing physical and electronic security.
- Reducing specific risks, such as IT theft.
- Contracting out your security.

1 Assessing the risk

Apart from the financial costs, crime can disrupt your business. Assess the risks your company faces and put protective measures in place. This will save time and money.

1.1 Find the **weak points** in your security.

- Is there a controlled access system in place? If not, is it practical to introduce one?
- What are the possible entry points? How easy would it be to break in at each of these points?
- If a thief gained access to the premises, what is most likely to be stolen? How secure are those items?
- How easy would it be for a thief to get away with stolen items? How long would it be before the alarm was raised and somebody arrived on the premises?
- How easy is it for somebody to start a fire?

1.2 Find out what kinds of **crime** are taking place in your area.

- Speak to police and to neighbouring businesses. For example, smashed windows or graffiti may be a problem in some areas (see box, page 3).

2 Basic precautions

2.1 Overall **responsibility** for security should be allocated to one individual who should:

- Check the premises and security systems regularly and review when appropriate.
- Check that security procedures are being followed.
- Maintain contact with police, insurers and fire services.

Contracting out some security requirements may be appropriate (see **7**), but the overall

responsibility remains yours.

2.2 Reduce the risk of thieves gaining access to your premises during **business hours**.

- Position your receptionist near the door, to keep track of who comes in and out or install an entry phone.
- Make sure visitors identify themselves and state who they are visiting. Consider issuing passes or signing visitors in and out.
- If possible, keep all other external doors locked. But check fire regulations first.

2.3 Ensure all employees understand and comply with security and safety **procedures**.

- Encourage your employees to challenge visitors ('Can I help you?') if they do not recognise them.
- Make sure safety information, such as fire drill details, is prominently displayed in your premises.
- Keep a record of key holders, and stress the importance of keeping keys secure.
- Change alarm codes on a regular basis and whenever an employee leaves.

3 Physical security

Insurance companies may insist on minimum security standards for locks, windows, and the perimeter and roof of your premises. Strengthen potential entry points.

3.1 Ensure your **locks** are effective. They should conform to British Standard 3621.

- Consider locks with registered keys, for which extra keys are only available with written confirmation from the owner.
- Label keys with a code that you can explain to employees, but which outsiders will not understand.

3.2 Make sure all **windows** are shut and locked when the premises are unoccupied.

- Repair or replace any faulty windows immediately.

3.3 **Window bars** or grilles are an effective deterrent, especially when fitted internally. If possible, protect all accessible windows.

- Consider solid steel bars set in concrete in the wall.
- Collapsible gates are also recommended, and can look better.

3.4 Protect the **perimeter** of your premises.

- Put up a wall or fence.
- Illuminate all potential entry points to the premises. But bear in mind that, in isolated areas, lighting could assist a thief in gaining entry to the building.
- Secure car park gates with a strong chain and padlock when not in use.
- Consider using barbed wire (or Hercules Cacti, a plastic product) on outside walls over eight feet high. This will discourage vandals and criminals, but it should be a last resort. Someone could injure themselves and then claim damages from you (for example, children playing).

Do not make your premises seem like a fortress. It may deter customers and potential employees.

4 Electronic security

Electronic security provides another level of protection for your business.

Intruder alarms and closed circuit TV (CCTV) can be powerful deterrents. Discuss with your insurers what measures you should consider.

4.1 Look at a wide range of alarms before making a decision. **Compare** specifications and quotes from a number of suppliers.

Consider buying an alarm system, rather than leasing one. If you lease an alarm, you are committed to using the same firm to maintain it.

- For reliability, your alarm should comply

Your insurance

A Improved **security** can save you money on insurance.

- Tell your insurance company what measures you propose, and discuss how this may affect your premium.
- Your insurers should be able to help with technical security specifications.

B Keep your **insurers** informed about any material changes to your security.

- Get your insurance company's approval for proposed security measures before buying or installing new protective measures, including new equipment.
- Most problems with insurers result from not keeping them up to date with changes to your business.

with British Standard 4737-3.0:1988.
- Make sure the company installing and maintaining your alarm is approved by the National Security Inspectorate (0845 006 3003 or www.nsi.org.uk).
- Check that your insurer will accept an alarm installed by your chosen supplier.
- Appoint a key holder to check your premises if the alarm goes off. The key holder must be able to get to the premises within 20 minutes.
- Consider installing panic buttons as part of your alarm system.

4.2 In commercial premises, audible-only alarms have limited benefit. Consider an **instant response** service by connecting to an ARC (alarm receiving centre).

- When the alarm is activated, the police are sent to your premises. A keyholder from your business must then let them in.

4.3 False alarms can be a problem.

- Many police forces now have a policy of refusing to respond if you have a history of false alarms.
- The cause of false alarms can be faulty equipment, but it is usually human error.
- Consider a system which includes alarm confirmation technology to minimise false alarms.
- Test your alarm at least twice a month.

Local crime prevention

A Arrange to meet your local **crime prevention officer** and seek advice on security measures.

B Meet your **permanent beat officer** — or the liaison officers for self-help schemes, like your local office watch, pub watch or club watch.

- Ask them about other businesses or organisations in the area which could affect your security.

C If appropriate, establish **key contacts** with the police. If you are particularly at risk, officers may check your premises regularly during the night.

D Ask your local police station, crime prevention or community support department to add your details to their email or sms list to receive local **community news** and broadcasts relevant to your business.

Make sure regular maintenance is carried out by a competent NSI-approved alarm company.

4.4 Consider installing **CCTV**.

- CCTV is widely used as a deterrent to criminals and can also discourage employee theft.
- It allows one person to monitor multiple areas, including remote sites. This is especially useful for security guards.
- CCTV can be cost effective for monitoring remote sites. It can be used to call a Security Guarding Company or the police for instant response with visual and audio verification from a remote manned centre. If it is not monitored, it is only useful after the event.
- Your employees may not like the idea of being watched. Explain why you are introducing CCTV and clear up any objections before it is installed.
- Ensure suitable signage is installed to comply with the Data Protection Act. Guidance is available from the Information Commissioner (08456 30 60 60 or www.ico.gov.uk).

5 Preventing IT theft

IT theft often has serious consequences for businesses. The loss of computers can be extremely costly and disruptive.

5.1 There are many ways to secure your **physical** IT assets, including a wide range of security products.

- Site your IT equipment away from the most visible and accessible places. Consider putting key equipment, such as your network server, in a locked room or a security cage.
- Mark your equipment in a permanent and visible way.
- Use steel cables to anchor your equipment to furniture or the floor. Use special security screws that will prevent any intruder gaining quick access to the components inside your computers.
- Fit computer alarms which detect tampering.
- Theft of laptop computers is common, so lock them away when not in use.

Read guidance on securing your IT equipment on the Department for Business, Enterprise & Regulatory Reform website (http://www.berr.gov.uk/sectors/infosec/index.html).

5.2 Secure the **data** on your computers.

- Back up files regularly. Check that your back-up system is working properly, by re-installing and checking files.
- Keep copies of back-ups off-site.
- Use passwords to prevent unauthorised access to computer files.
- Use anti-virus software.
  Set up procedures to screen all incoming material – and insist they are used.

BS 7799-3:2006 is the recognised international standard for IT security. While mainly directed at larger businesses, smaller businesses may find its provisions a useful starting point.

6 The threat of arson

6.1 Do not allow **combustible material** to accumulate in or near your premises.

- Arsonists could use it to attack the building.

6.2 Lock away hazardous and **flammable materials**.

- Control access to vulnerable areas, such as warehouses.

6.3 Make sure you have the necessary **precautions** in place to alert people in case of fire and to limit any damage.

- Fit fire alarms and smoke detectors to detect fires early. They should conform to British Standard 5839-6:2004.
- Ensure there are enough fire extinguishers, of the right types and in the right places.

  Recent changes to fire regulations mean businesses are now responsible for fire risk assessments.

7 Additional security

If your business faces particular risks, you may need to consider additional security measures.

7.1 Contract out your security to a **security company**. The services a good company can offer usually include:

- Auditing current security arrangements and suggesting improvements.
- Specifying and fitting any new security systems required.
- Providing periodic (eg twice per night) or full-time inspection of your premises outside business hours.

7.2 A security company can provide a security **guard** to protect your premises.

- Make sure the guard comes from a firm registered with the British Security Industry Association (0845 389 3889 or www.bsia.co.uk) or the International Professional Security Association (020 8832 7417 or www.ipsa.org.uk). The guarding service should conform to British Standard 7499:2002. Or, look out for firms with the Security Industry Authority (SIA) Approved Contractor Scheme accreditation mark.
- Make sure the security guard holds a SIA licence. It is illegal not to hold one – without it, insurance claims could be invalid.
- The security company should screen and interview each guard as thoroughly as you would check a new employee. The screening should conform to British Standard 7858:2006.
- Discuss the security orders for the guard, including hours, duties and equipment with the supervisor responsible for your site.

Integration of security is the key to success. For example, using CCTV and guards together will provide maximum protection.

8 Mitigating any loss

Review your security systems regularly.

8.1 **Anticipate** possible losses.

- Maintain a detailed inventory of your assets. Send a copy to your insurer.
- Devise a disaster recovery plan to cover the whole range of possible situations.
- Take pictures of your assets and store off-site on a CD or DVD.

8.2 Act **quickly** after the event.

- Involve the police and your insurance company immediately.
- Secure any broken points of entry.
- Review and upgrade your security systems.

8.3 You are most at risk immediately **after a break-in** or a theft.

- The criminals know the layout of the premises and that you will quickly replace the stolen items.

Published by BHP Information Solutions Ltd, Althorp House, 4-6 Althorp Road, London SW17 7ED
Tel: 020 8672 6844, www.bhpinfosolutions.co.uk