Secure in the knowledge

Building a secure business

ACPO

National Counter Terrorism Security Office

London First

National Counter Terrorism Security Office (NaCTSO) is a police unit working to the Association of Chief Police Officers (ACPO), and provides a co-ordinating role for the police service in regard to counter-terrorism and protective security. NaCTSO is integrated within the Security Service's National Security Advice Centre (NSAC).

The unit collates and disseminates good practice and has responsibility for the management of police training in counter-terrorism protective security.

Developing and maintaining strong links with other organisations is a vital part of the unit's work, which allows for the identification of emerging needs and requirements in this area.

London First is a business membership group whose aim is to improve and promote London with the objective of ensuring that London maintains and enhances its position as a leading world city. It does this by mobilising the experience, expertise and enthusiasm of the private sector to develop practical solutions to the challenges facing London and to lobby central and London government for the investment that London needs in its infrastructure.

London First delivers its activities with the support of 300 of the capital's major businesses in key sectors such as finance, professional services, property, ICT, creative industries, hospitality and retail. Membership also includes all of London's higher education institutions as well as further education colleges and NHS hospital trusts. Its members represent 26% of London's GDP.

www.london-first.co.uk
Tel: 020 7665 1500

The Security Service is responsible for protecting the country against covertly organised threats to national security. These include terrorism, espionage and the proliferation of weapons of mass destruction. We also support the police and other law enforcement agencies in preventing and detecting serious crime. In addition we provide security advice to a range of other organisations, helping them reduce their vulnerability to the threats.

Foreword

Building a secure business is not just about supply and demand. It is about the protection and prevention measures that you can put in place against crime, the consequences of a natural disaster, electronic attack, acts of terrorism and other events that would have an impact on your business.

You can do much to reduce the vulnerabilities of your business by taking time to review your preparedness to deal with emergencies and put simple and often inexpensive security measures in place. From the basics of identifying where your business is vulnerable to making sure you have suitable IT security such as passwords and making sure your key suppliers have plans in place to continue business if they are the ones affected.

This booklet follows on from *Expecting the unexpected* and looks in more detail at how you can protect your staff and the information and assets vital to your business including how good security can give value for money.

It is a welcome initiative by the National Counter Terrorism Security Office, London First and the Security Service and helps support the Government's aim of making the UK a safe and secure place in which to live, work and do business.

The Rt Hon Hazel Blears MP
Minister of State for Policing, Security and Community Safety

1

Thinking about security

Thinking about security is good for your business

You have invested heavily in your business and you need to ensure it remains safe, secure and viable. This booklet provides guidance and information to help you improve your basic security and thereby protect your livelihood. Being better informed and better prepared also reassures your customers and suppliers that you take security seriously: it is good for you, your staff, your business and your reputation.

This booklet is primarily for small and medium-sized businesses but is relevant to businesses of all sizes. Ideally it should be read in conjunction with our previous booklet, *Expecting the unexpected*, which advises on business continuity in the event and aftermath of an emergency. By following the guidance in both booklets, you will be in the best position to prevent, manage and recover from a range of threats to your business.

2

Building a secure business

Building a secure business – how to use this booklet

Everybody in your business has a vital role in keeping it safe and secure. This booklet aims to make you aware of the threats your business may be vulnerable to, from both outside and within the business. It informs you how to physically secure your business and protect the information that your business depends upon. The booklet enables you to help yourself and includes clear visual representation, easy-to-follow step-by-step guidance, links to useful websites and a checklist at the end, to find out where your strengths and weaknesses lie.

In reality, your business is more likely to suffer from the effects of fire, burglary and fraud than from terrorism. However, terrorists, like criminals, are always looking for ways to exploit the vulnerabilities of those they wish to damage. By remaining vigilant, being security-minded and having simple security measures in place, you can help to protect your business against crime and make the work of terrorists more difficult.

3

What you need to know

What you need to know – threat, vulnerability and business impact

When thinking about the security of your business you need to consider three things: threat, vulnerability and the resulting business impact. Only when those who threaten you are able to exploit your vulnerabilities will there be an impact upon your business.

Businesses may not be able to remove a threat, but they can remove or manage their vulnerabilities. Removing vulnerabilities from within your business means that you can't be exploited by threats.

The table below illustrates a range of scenarios that could impact upon your business, depending on whether you have considered ways to limit your company's vulnerability.

THREATS can be external to your business, or can come from within	**VULNERABILITY** is a weakness that can be exploited by a threat	**BUSINESS IMPACT** is the cost resulting from a vulnerability successfully exploited by a threat
Computer virus	Do you regularly update your software virus protection?	What might happen: You lose client records and pass the software virus on to your customers. This wastes time, loses money and damages your reputation as a reliable business.
Theft of company information	Do you check your new staff records adequately?	What might happen: Commercially sensitive information is stolen and given to a competitor. This delays the launch of your products and projects.
Terrorism	Have you noticed suspicious behaviour towards a neighbour? Although the behaviour is odd, you don't want to bother the police.	What might happen: Later, a bomb explodes outside that neighbour's business. You are unhurt because you are away, but others are not so lucky.
Disruption to supply chain	Do you check whether your critical suppliers have business continuity plans in place?	What might happen: A critical supplier becomes unable to provide vital services. You lose two weeks' business as a result.

STOP AND THINK Things happen. Although the likelihood of a terrorist attack affecting your business is low, its impact could be devastating. Do not be fooled into thinking that simply because things do not happen often, they never happen. You need to consider worst-case scenarios in your security planning, however unlikely they may seem (you can find out more about worst-case scenarios in *Expecting the unexpected*).

Simply doing business may expose you to threats and may create vulnerabilities.

Ask yourself the following questions:

- Where within *my* business are my vulnerabilities? List them.
- Do my vulnerabilities result from others (customers, suppliers, neighbours)? If so, how?
- How often are identified threats likely to exploit the vulnerabilities within my business?
- What will be the likely impact on my business for one day, one week and one month?

It is not always possible to remove the threats to your business but you can do something to reduce or remove your vulnerabilities. You have a number of options open to you.

What are my options?

STOP AND THINK Even if you are insured, you should behave as if you were uninsured!

What are my options?

Having understood that your business is vulnerable to security threats, you have three choices in deciding how to deal with them:

1. Put security measures in place to remove or reduce vulnerabilities.
Although you can't remove all security threats to your business, you can remove or reduce your vulnerabilities. You are probably already managing some of your business's vulnerabilities (by protecting your products and maintaining your customer base, for example), but every business needs to think more carefully about the risks from crime and terrorism.

2. Transfer some or all of the vulnerability (insurance).
Transferring some of the vulnerability by insurance provides some financial recompense, but it cannot replace lost information and will never fully recover your lost business and reputation. It is best to consider insurance for some vulnerabilities in conjunction with good security measures for others.

3. Do nothing.
Doing nothing will leave your business dangerously exposed and it is likely that sooner rather than later an exploited vulnerability will bring your business to a halt or seriously disrupt it.

DID YOU KNOW?

Terrorism and insurance

Insurance can:

- spread the losses of an individual firm amongst many policyholders so that no one business need suffer a loss and risk business failure;
- provide peace of mind for the insured, shareholders, customers and suppliers;
- help you to focus on investing in your business rather than keeping back reserves for emergencies; and
- offer coverage for buildings and contents against physical loss or damage by an act of terrorism, and also against business interruption.

Where can I obtain terrorism insurance?

- There is a global terrorism insurance market, which can be accessed by your insurance broker.
- A government-backed scheme called Pool Re supports products that can be obtained by the property insurer who, in the case of a loss, would be reinsured by the scheme.

You should:

- shop around and be aware of what insurance is available;
- read the wording of the policy carefully and discuss it with your broker;
- understand what is covered and what isn't. Be aware of any gaps in cover; and
- ask your broker if you have any doubts.

What about those gaps? You need to ensure that:

- you have a structured security process that you stick to;
- where possible you use physical protection, for example blast-resistant glazing or films; and
- you remain vigilant and report anything that you consider to be suspicious.

Your insurer will expect you to have taken reasonable steps to protect your business.

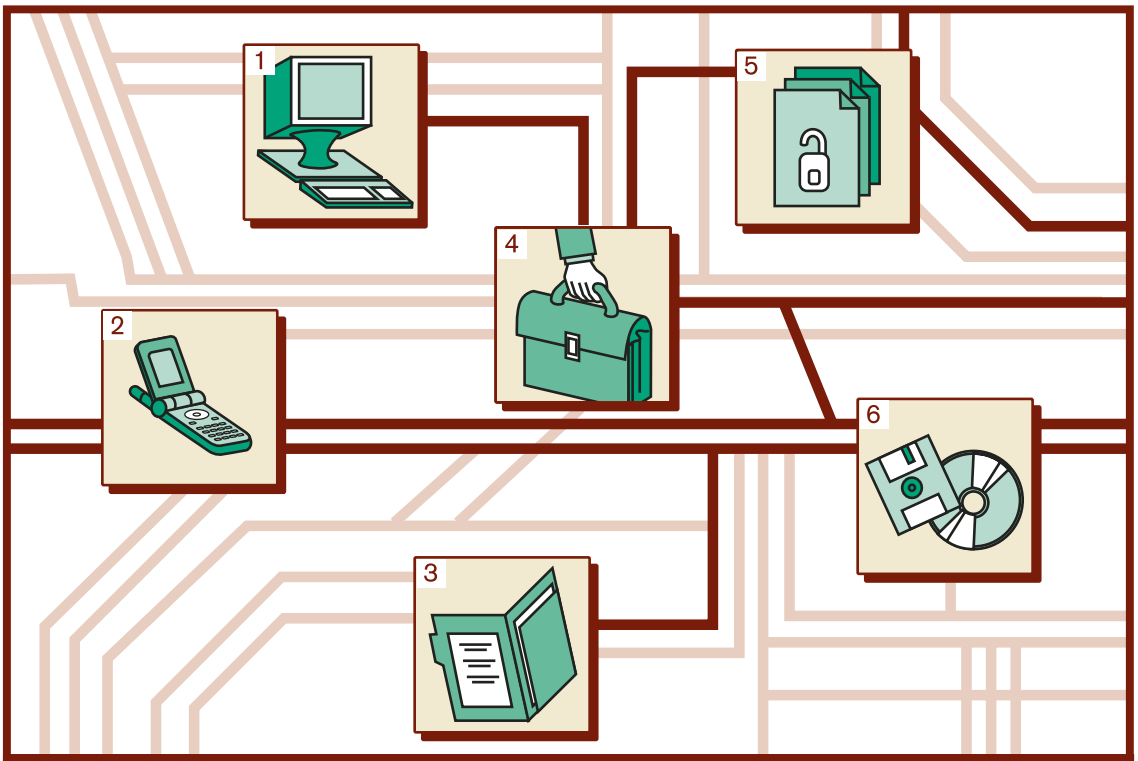
5

Information is the key

Information is the key – protect it!

Information is vital for any business and you will need to think about how you can protect it from theft and misuse. Hackers and viruses can paralyse your business and destroy its reputation. Therefore you need to handle information securely.

Where are the information vulnerabilities in your business?



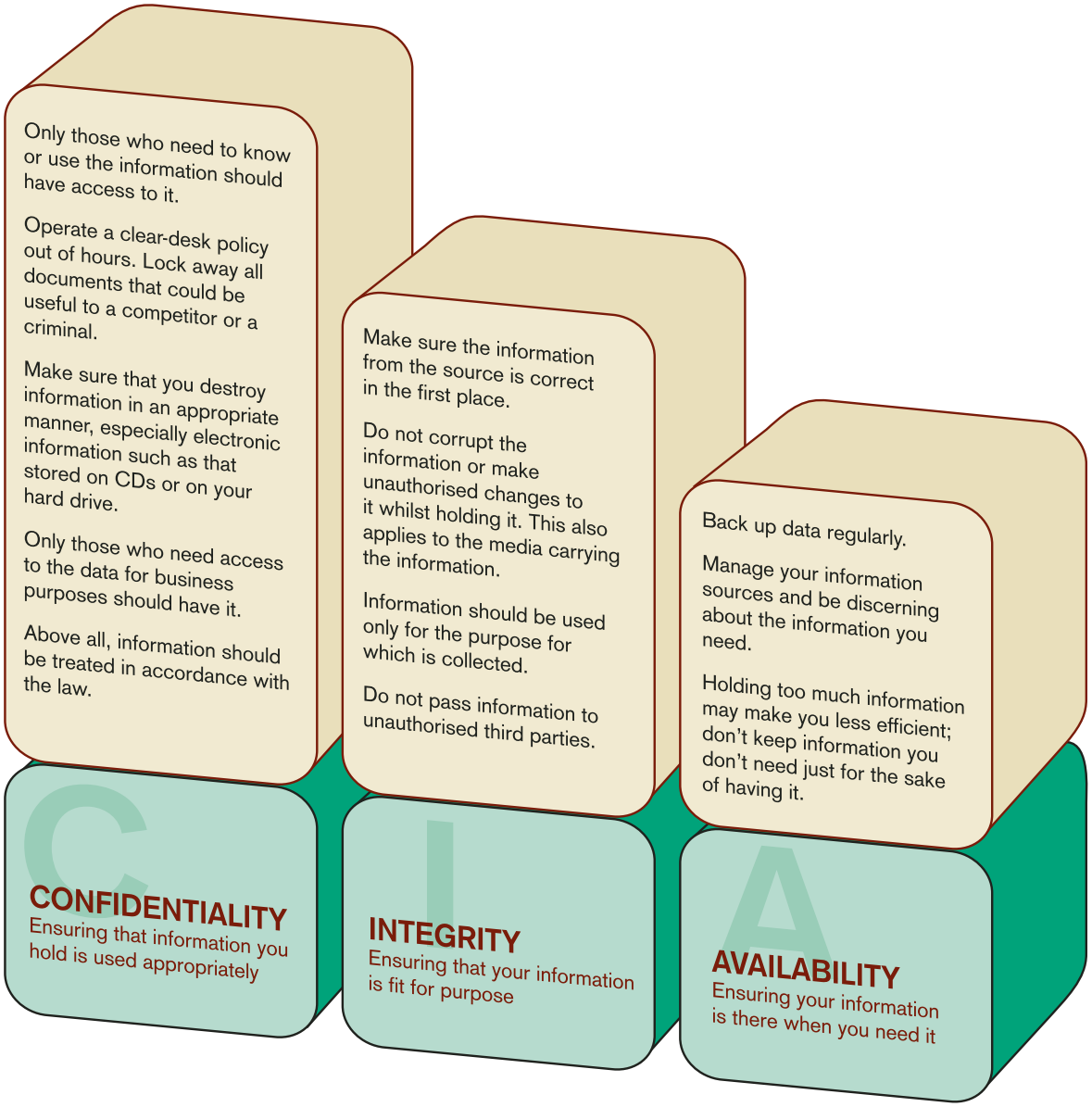
1. Data transmissions
2. E-mail and mobile phone indiscretion
3. Careless storage of information
4. Physically moving files
5. Insecure electronic files
6. Data copying

STOP AND THINK Do you know what your legal responsibilities are in relation to the holding and use of information under the Data Protection Act? If not, then visit the Information Commissioner's website at **www.dataprotection.gov.uk**

Getting it right!

Managing information safely and securely means that the *right* information reaches the *right* people at the *right* time. Getting this right makes you more efficient and reassures others that information they provide will be kept securely by you. It will also make it more difficult for those who wish to steal or interfere with your information to do so.

There are three building blocks that support better information security and smarter working practices for your business: Confidentiality, Integrity and Availability (CIA).


Only those who need to know or use the information should have access to it.
Operate a clear-desk policy out of hours. Lock away all documents that could be useful to a competitor or a criminal.
Make sure that you destroy information in an appropriate manner, especially electronic information such as that stored on CDs or on your hard drive.
Only those who need access to the data for business purposes should have it.
Above all, information should be treated in accordance with the law.
C
CONFIDENTIALITY
Ensuring that information you hold is used appropriately
Make sure the information from the source is correct in the first place.
Do not corrupt the information or make unauthorised changes to it whilst holding it. This also applies to the media carrying the information.
Information should be used only for the purpose for which is collected.
Do not pass information to unauthorised third parties.
I
INTEGRITY
Ensuring that your information is fit for purpose
Back up data regularly.
Manage your information sources and be discerning about the information you need.
Holding too much information may make you less efficient; don't keep information you don't need just for the sake of having it.
A
AVAILABILITY
Ensuring your information is there when you need it

STOP AND THINK Good security measures need not make doing business more difficult.

Making your information secure

To help you improve your information security, consider the points below and apply them to your business.

People

1. **Ensure you can identify everyone with access to the information.**
   On an IT system, this may mean getting people to take password security seriously, or implementing some other form of user authentication. In a small office you might know everyone by sight, but in a larger office some form of ID would be appropriate. If you cannot clearly and accurately identify the people accessing your information, you cannot guarantee its safety.

2. **Provide continuous employee training for information security.**
   If you have the policies, systems and procedures, but employees are not aware of them, they simply will not work. Staff need to know what system is in place and why, to ensure that information remains secure.

Protection

3. **Develop, follow and test appropriate back-up and recovery procedures for critical information.**
   Although these procedures need to take data deletion and retention policies into account, ensuring that you can recover critical data that has been corrupted and deleted, particularly within IT systems, is a separate and vital issue. Restoring critical systems after a crime or disaster is vital for the continuity of the business. Additionally you should make sure that critical business information is copied and held elsewhere in a secure location as part of your business continuity plan (BCP). (See *Expecting the unexpected*.)

4. **Establish a strong perimeter defence for your information.**
   A small business may simply need to ensure that its paperwork is securely filed away and all office doors and windows are locked at the end of the day. A large company may need to implement a swipe card access control system or ensure that the IT system is adequately guarded by firewalls. All of these measures provide perimeter security that will help keep your information safe.

5. **Ensure that your IT safeguards cover the current threats.**
   Firewalls, anti-virus software, anti-spyware… IT safeguards cover a wide range of possibilities. The key to successful IT protection is to ensure that your security systems are constantly updated against the latest threats – new computer viruses are released daily. For more information, visit **www.itsafe.gov.uk**

STOP AND THINK Are there things you can do now at little or no cost? Consider tightening up on existing security or encouraging staff to be more security-minded.

Practices

6. Assess the information you use in your business environment.

Understanding the information in your business is essential to ensuring that your key business information is preserved. Backing up IT systems is meaningless if your key information is kept in handwritten folders on desks and the IT system is just used for personal e-mails and browsing the internet.

7. Employ the principle of least privilege.

This is an important principle that is often overlooked. When implementing any form of security or safety precaution, permit someone the minimum level of access to allow them to do their job. This does not imply lack of trust; it is simply a good principle that helps to prevent accidents and avoids complications, particularly as a business grows in size.

Think of a balcony – people might jump off it deliberately, but it is very unlikely. You put up a safety rail to prevent accidents, not because you do not trust people. The same applies to information security.

8. Develop effective data retention and deletion policies.

There are legal requirements for both the retention and deletion of much of the information a company holds, regardless of the size of the business. Ensuring that you have an adequate strategy in place to meet these obligations is very important.

9. Regularly review your information links with other companies.

Sometimes customers or suppliers regularly provide and receive information through established channels, which may become inappropriate if a business relationship changes. Accepting or providing information based on a previous relationship can bypass your information security safeguards. For example, if another company pulls out of an alliance, you may need to cancel their access to a corporate extranet, or remove them from confidential mailing lists.

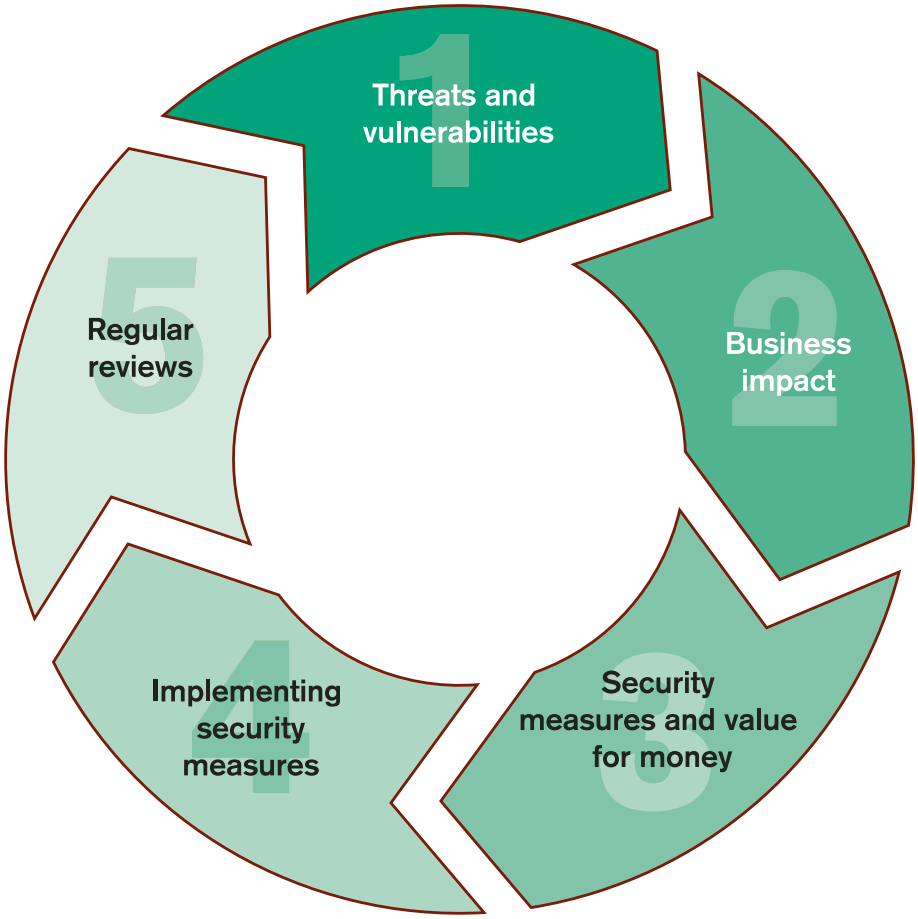
10. Continually revise, update and test the procedures, policies and systems you have implemented.

Information security is not implemented just once – it is a process. If you have successfully worked through all of the previous nine points it is time to begin again at point one!

Making your business secure

Making your business secure

In order to make the most of your efforts to protect your business, follow the steps outlined below. This process will help you achieve the most cost-effective protection for your business, and allow you to identify vulnerabilities that might be exploited by terrorists and other criminals.



Step One
Threats and vulnerabilities

Threats

Threats come in many guises and spending some time thinking about the types of threat your business faces will help you make better choices when protecting it.

To start the process:

- Contact other businesses in your neighbourhood, and trade associations that represent your business interests. Can they give you advice tailored to the risks facing your line of business?

- Set up a Warning, Advice and Reporting Point (WARP). These small-scale communication networks keep you up to date with the threats to your IT system. Visit the website – **www.warp.gov.uk** – for more information.

- Make use of public information about threats from crime and terrorism. The following websites are a good starting point:
  www.crimereduction.gov.uk
  www.businesslink.gov.uk
  www.homeoffice.gov.uk
  www.mi5.gov.uk

DID YOU KNOW? Warning, Advice and Reporting Points (WARPs) are part of the National Infrastructure Security Co-ordination Centre's (NISCC) information sharing strategy. They have proved to be effective in improving information security between businesses and other groups. You can set up a WARP with local businesses in your neighbourhood or with businesses similar to your own. All the information you need to set up a WARP can be found at **www.niscc.gov.uk** The site will also answer any queries you may have about the WARP system.

NISCC
NATIONAL INFRASTRUCTURE SECURITY CO-ORDINATION CENTRE

WARP
Warning, Advice and Reporting Point

- Keep up to date with current affairs in relation to terrorism. Attacks by terrorists in other countries can help you to understand better the risks your business might face.

- Become an active learner. When you next see or read a news report on a crime or act of terrorism, ask yourself: 'What could I have done to help prevent that event or reduce the impact of that event on my business?'

- Remember to visit the Security Service website at **www.mi5.gov.uk** for more information on the threats from terrorism. Other useful websites are **www.ukresilience.gov.uk** and **www.homeoffice.gov.uk/terrorism**

Vulnerabilities

No one knows your business as well as you. You are the expert in what you do and how you do it. Understanding the 'how' will help you identify vulnerabilities within your business:

- Complete the 10-minute checklist starting on page 38 and see where your security vulnerabilities lie.

- Ask your staff to identify vulnerable areas of the business. They may have valuable ideas to contribute from another perspective.

- Speak to other businesses in your neighbourhood, or businesses similar to your own, in order to learn from their experiences in dealing with their vulnerabilities.

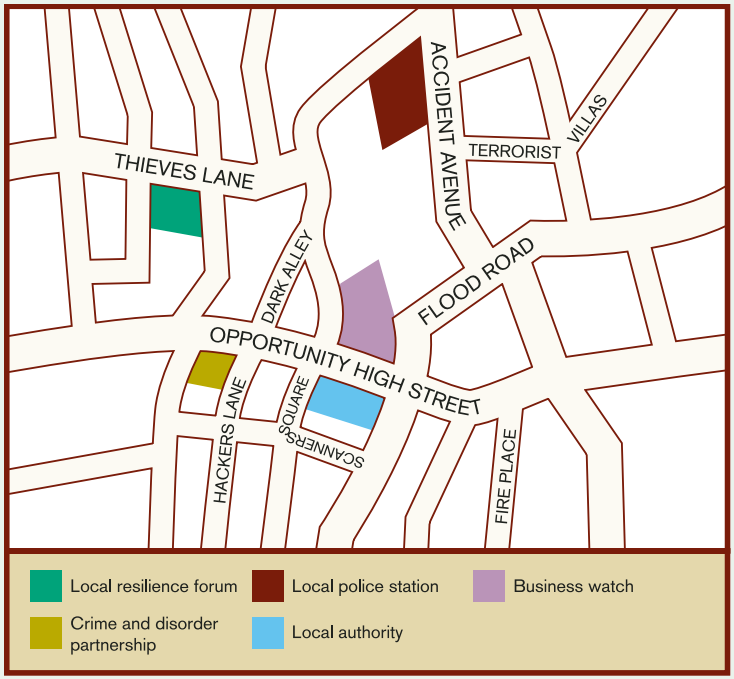
- Contact your local authority and the police. What are the crime problems in your area? Find out about your local Crime and Disorder Strategy – what solutions does it provide to prevent crime against businesses?

Networks work!

Developing a local network of contacts, talking to others and sensibly sharing information can be a useful way to help identify both threats to and vulnerabilities of your business.

Starting within your own neighbourhood:

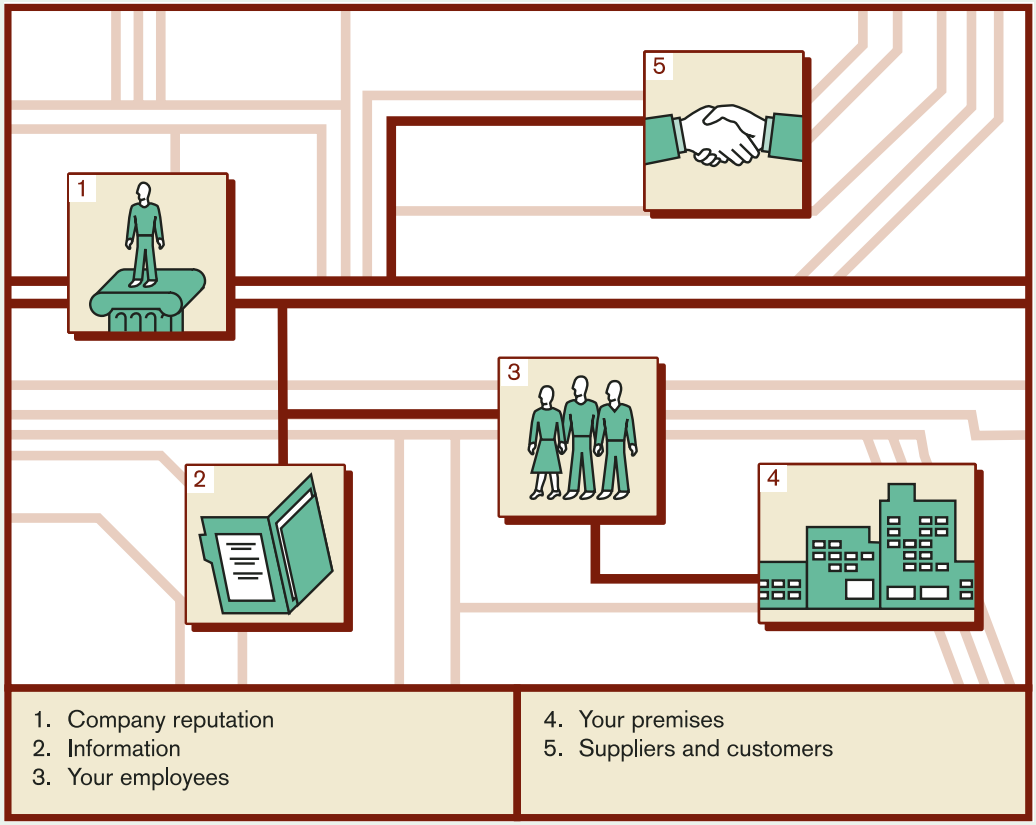
- Do you talk to your neighbours? Do you know what they do?
- Do you know whether there's a local business organisation that can represent your interests?
- Do you know your local police or community support officer?
- Are there large businesses in your area that can help you and your neighbours improve the security of your neighbourhood?
- Is your neighbourhood part of a Business Improvement District (BID)? (A BID is a partnership arrangement through which local authorities and the business community can take forward schemes which benefit the local community.)



Step Two
Business impact

Having identified the likely risks, you will need to consider what damage they can inflict on your business. This is likely to occur in one or more of the following areas, or it may affect your relationship with a third party, for example a supplier.

It is likely that the critical assets you have identified for your business continuity plan (BCP) are the same as the ones you will need to keep safe.



1. Company reputation
2. Information
3. Your employees
4. Your premises
5. Suppliers and customers

STOP AND THINK Reading our other publication, *Expecting the unexpected*, will enable you to identify critical areas within your business. Remember we are talking about elements that are critical, not desirable. For example, staff will always be critical to the running of your business. You can download *Expecting the unexpected* from the Security Service website:

www.mi5.gov.uk

Protecting your business through good security is just as important as the recovery from a security failure; every business seeks to operate without disruption. Make sure your security procedures complement your business continuity plans by:

- ensuring security supports the efficient day-to-day running of your business. If this is done well it won't make business more difficult;
- making sure your security priorities protect the critical parts of your business; and
- involving whoever has responsibility for security in the development and reviews of your business continuity plans.

Step Three
Security measures and value for money

The most effective way to keep your business safe is to have in place a number of different control measures, which when taken together are known as defence in depth. These may include physical measures (locks, alarms) and management processes (such as checking references of potential employees and managing visitors). Defence in depth allows you to respond flexibly to new threats. The 10-minute checklist starting on page 38 will help you identify areas for improved security.

Security adds up

Having identified your threats and vulnerabilities and their potential impact on your business, you will need to consider the cost-effectiveness of your security measures.

Remember that assets destroyed or stolen are costs you will have to bear, in terms of both replacing the asset itself and of any lost business. You need to ask the question: 'Could I carry on business as usual when this asset has been lost or compromised?' If the answer is no then you need to protect it. Prevention is always better than cure and it will save you money – invest to save.

If you plan protection for the worst-case scenario then you are likely to be able to cope with most security risks.

Cost of security measure > Value of asset at risk

Is security alone the best option?
(See 'What are my options?' p12, point 2.)

Cost of security measure < Value of asset at risk

Implement and review security measures.

Cost of security measure = Value of asset at risk

Implement and review security measures.

STOP AND THINK It may be difficult to put a price tag on some assets at risk, such as your customer database or company reputation. But their loss could seriously affect your ability to carry on business. Do not assume that just because something is difficult to price, you should not protect it. Instead, work out how much its loss would disrupt your business, and in turn, how much the disruption would cost.

STOP AND THINK

1. Your spending on a security measure should not drastically exceed the value of the asset you are protecting.
2. You should protect those assets within your business that you have determined are the most valuable. The loss of these assets may have the greatest negative impact upon your business.

Step Four
Implementing security measures

Having identified what threats and vulnerabilities may affect your business, you can now put measures in place.

The checklist starting on page 38 covers the main areas of basic security. You might well be surprised to find that you are already security-minded and that with only a little more effort you can further improve the security of your business.

Successful security measures require:

- the support of management;
- staff awareness of the measures and their role in making them work. A written policy helps to achieve this as long as all staff are aware of its existence and contents; and
- someone within your business to take responsibility for security, and report to management.

STOP AND THINK Continue to test your security plans to ensure they meet the needs of your business.

Step Five
Regular reviews

It is important to review all your security measures regularly to ensure that they continue to support the needs of your business. Things change, new threats and vulnerabilities become apparent and effective security should reflect this.

In particular, review the effectiveness of your security:

- after a security incident within your business;
- after a security incident in your neighbourhood;
- after a change in your business practices; and
- when information is received about threats.

7

Checklist

THE 10-MINUTE CHECKLIST

Below is a checklist to help you to identify the areas where you may be vulnerable. It is not designed to cover all aspects of security, but it will identify some common vulnerabilities. Answer all of the questions.

The colour-coded boxes will help you to identify your business strengths and weaknesses.

Visitor access to your building

	Yes	No	Don't know
Are visitors allowed entry to your building by appointment only?	☐	☐	☐
Do they have to report to a reception area before entry?	☐	☐	☐
Are visitors asked for proof of ID?	☐	☐	☐
Are they provided with visitors' badges?	☐	☐	☐
Are all visitors asked to sign in when they enter the building?	☐	☐	☐
Are visitors' badges designed to look different from staff badges?	☐	☐	☐
Are all visitors' badges collected from visitors when they leave the building?	☐	☐	☐
Does a member of staff accompany visitors at all times while in the building?	☐	☐	☐
Are the visitors' badges cross-checked against those issued?	☐	☐	☐
Do your staff wear ID badges at all times when in the building?	☐	☐	☐

Physical security of your building

	Yes	No	Don't know
Building security			
Are there good quality locks on all doors and windows at ground level?	☐	☐	☐
Are there good quality locks on each accessible door and window above ground level?	☐	☐	☐
Can internal doors be locked when left unattended for long periods?	☐	☐	☐
Are all fire doors alarmed?	☐	☐	☐
Do you nominate members of staff to check that all doors and windows are closed and locked at the end of the business day?	☐	☐	☐
If you have a burglar alarm are your staff familiar with the procedures for switching it on and off? (In order to reduce false alarms)	☐	☐	☐
Do you maintain good visibility around the perimeter of your building? e.g cutting back overgrown planting.	☐	☐	☐
Do you have adequate lighting around your building during the hours of darkness?	☐	☐	☐

CCTV

	Yes	No	Don't know
Do you have your CCTV cameras regularly maintained?	☐	☐	☐
Do the CCTV cameras cover the entrances and exits to your building?	☐	☐	☐
Do you have CCTV cameras covering critical areas in your business, such as server rooms or cash offices?	☐	☐	☐
Do you store the CCTV images in accordance with the evidential needs of the police?	☐	☐	☐
Could you positively identify an individual from the recorded images on your CCTV system?	☐	☐	☐

Information security

	Yes	No	Don't know
Do you lock away all business documents at the close of the business day?	☐	☐	☐
Do you have a clear-desk policy out of business hours?	☐	☐	☐
Do you close down all computers at the close of the business day?	☐	☐	☐
Are all your computers password protected?	☐	☐	☐
Do you have computer firewall and antivirus software on your computer?	☐	☐	☐
Do you regularly update this protection?	☐	☐	☐
Do you employ the principle of least privilege?	☐	☐	☐
Do you back up business critical information regularly?	☐	☐	☐

Personnel security checking

It is important to prove the identity of potential new staff. You should see original documents and not photocopies and, where possible, check the information, explaining any gaps. During recruitment do you require:

	Yes	No	Don't know
Full name?	☐	☐	☐
Current address and any previous addresses in last five years?	☐	☐	☐
Date of birth?	☐	☐	☐
National Insurance number?	☐	☐	☐
Full details of references (names, addresses and contact details)?	☐	☐	☐
Full details of previous employers, including dates of employment?	☐	☐	☐
Proof of relevant educational and professional qualifications?	☐	☐	☐
Proof of permission to work in the UK for non-British or non-European Economic Area (EEA) nationals?	☐	☐	☐

Proof of identity is vitally important and the following documents can assist you in verifying their identity.

	Yes	No	Don't know
British Citizens			
Do you ask for:			
Full (current) 10-year passport?	☐	☐	☐
Or two of the following:			
British driving licence (ideally the photo licence)?	☐	☐	☐
P45?	☐	☐	☐
Birth Certificate – issued within six weeks of birth?	☐	☐	☐
Credit card – with three statements and proof of signature?	☐	☐	☐
Cheque book and bank card – with three statements and proof of signature?	☐	☐	☐
Proof of residence – council tax, gas, electric, water or telephone bill?	☐	☐	☐
Other EEA nationals			
Do you ask for:			
Full EEA passport?	☐	☐	☐
Or			
National Identity Card?	☐	☐	☐
Other nationals			
Do you ask for:			
Full passport AND A Home Office document confirming the individual's UK immigration status and permission to work in the UK?	☐	☐	☐

Communication

	Yes	No	Don't know
Do you have a security policy or other documentation showing how security procedures should operate within your business?	☐	☐	☐
Is this documentation regularly reviewed and if necessary updated?	☐	☐	☐
Do you have a senior manager who takes responsibility for security within your business?	☐	☐	☐
Do you regularly meet with staff and discuss security issues?	☐	☐	☐
Do you encourage staff to raise their concerns about security?	☐	☐	☐
Are you a member of a local Business Watch or a similarly constituted group?	☐	☐	☐
Do you know your local community police officer or community support officer?	☐	☐	☐
Do you speak with neighbouring businesses on issues of security and crime that might affect you all?	☐	☐	☐
Do you remind your staff to be vigilant when travelling to and from work, and to report anything suspicious to the relevant authorities or police?	☐	☐	☐

What do your results show?

Having completed the checklist, you need to give further attention to the questions that you have answered ‘no’ or ‘don’t know’ to.

If you answered ‘don’t know’ to a question, find out more about that particular issue to reassure yourself that this vulnerability is being addressed or needs to be addressed. If you answered ‘no’ to any question then you need to address that particular vulnerability as soon as possible.

Where you have answered ‘yes’ to a question, remember to regularly review your security needs to make sure that your security measures are fit for purpose.

With thanks to the following London First members for their knowledge and expertise:

Addison Lee
Anglo Irish Bank UK
Barclays Bank PLC
Berwin Leighton Paisner
DTZ
Ernst & Young
Hilton Group plc
J Sainsbury plc
KPMG
MWB Business Exchange
Prudential plc
Shell
Tesco plc
UBS

Thanks are also extended to:
Willis
Continuity Forum (www.continuityforum.org)
Business Continuity Institute (www.thebci.org)

Produced by the National Counter Terrorism Security Office (NaCTSO)