

# A Guide to Business Crime Prevention



**NORFOLK**  
CONSTABULARY  
*Our Priority is You*



## CONTENTS

<a href="#"><u>Foreword</u></a>	3
<a href="#"><u>Introduction</u></a>	4
<a href="#"><u>Offenders profile</u></a>	6
<a href="#"><u>Offenders thought process</u></a>	7
<a href="#"><u>Situational prevention</u></a>	9
<a href="#"><u>Secure by Design Concept</u></a>	11
<a href="#"><u>Conclusion</u></a>	13
<a href="#"><u>External Security</u></a>	13
<a href="#"><u>Perimeter</u></a>	13
<a href="#"><u>Landscaping</u></a>	16
<a href="#"><u>Vandalism</u></a>	16
<a href="#"><u>Lighting</u></a>	17
<a href="#"><u>Ram raiding</u></a>	17
<a href="#"><u>Car Parks</u></a>	18
<a href="#"><u>Outbuildings</u></a>	18
<a href="#"><u>Building Security</u></a>	18
<a href="#"><u>Doors</u></a>	19
<a href="#"><u>Emergency Exits</u></a>	20
<a href="#"><u>Windows</u></a>	20
<a href="#"><u>Internal Security</u></a>	22
<a href="#"><u>Reception</u></a>	22
<a href="#"><u>Internal Doors</u></a>	22
<a href="#"><u>Property Marking</u></a>	23
<a href="#"><u>Physical Security</u></a>	23
<a href="#"><u>Computer Data</u></a>	23
<a href="#"><u>Cash Office Security</u></a>	24
<a href="#"><u>Cash in Transit</u></a>	25
<a href="#"><u>Key Security</u></a>	26
<a href="#"><u>Cash Handling Companies</u></a>	27
<a href="#"><u>Vetting staff &amp; Searches</u></a>	27
<a href="#"><u>Electronic Security</u></a>	28
<a href="#"><u>Alarms</u></a>	28
<a href="#"><u>CCTV Systems</u></a>	29
<a href="#"><u>Occupiers Liability Act 1984</u></a>	30
<a href="#"><u>Risk Analysis Program</u></a>	32
<a href="#"><u>Links</u></a>	40

## **Foreword.**

The majority of small to medium businesses in this country have little or no security in their premises. When they become a victim of crime they are often ill prepared to cope with its effects and aftermath. The incident will have an effect not only on their staff but also on their ability to service their customers and therefore on their profitability.

Often crime is committed by opportunist criminals with little or no forethought or planning. It does not take much to deter these type of criminals. The most rudimentary security precautions could make the difference between becoming a victim or not.

For many of our larger companies security is something that is decided and budgeted for at a central level without too much input from a local level. Local managers are therefore kept in the dark about security planning and systems until something is foisted upon them which often has no relevance to their situation or requirements.

This guide is intended to make owners and managers of businesses aware of the problems they may face and give them some idea of solutions that are available. Also included at the end of the Guide is a Crime Risk Survey which will highlight a particular premises weakness which the information in this guide will also help to address.

The information is not new, it is all well tried and tested by Crime Reduction Officers around the country and forms the basis of most of our work. Use the guide as a reference document to allow you to assess and update your security requirements.

Pc Pat Bailey  
Crime Reduction Officer  
Norfolk Constabulary

**[Return To Contents](#)**

## **REDUCING THE RISK OF CRIME**

### **Introduction.**

The majority of crime in this area is committed against commercial and public premises. Any losses they suffer as a result of crime would be indirectly felt by the Community in which the organisation is located.

It is a sad fact therefore that the lack of security investment and planning is endemic in the commercial and public world. I am not talking about placing guards in reception areas or calling in security from the first number in Yellow Pages. This is the approach of many organisations to a security problem, real or imaginary.

The police generally get called in after an incident when it becomes clear that the internal security functions were unable to fulfil their role effectively, firstly to investigate and secondly to advise in the form of their Crime Prevention Officer. If this advice is followed it can be a step to a more fulfilling and profitable security policy.



A number of managers continue to perpetuate the myth that security is simply a drain on the bottom line and remain unaware of the fact that proper security advice from appropriately qualified experts can actually boost their profits. In many national retail companies the security budget comes out of the Managing Directors petty cash budget, instead of adopting a full scale audit approach, much as a company would to any large tangible asset. The same applies in the public sector.

Organisations that grasp the nettle in this way find well qualified advice comes best from the outside looking in and as long as they follow up the risk analysis strategy by adopting a proper security policy the benefits permeates through the whole organisation

Far too long security meant employing an ex-policeman or army sergeant with a new uniform and guard duties which included keeping one eye on a bank of CCTV monitors, one eye on reception, ears on telephones and Walkie Talkies. The companies who have this type of security sadly are the innovators most have nothing.

## [Return To Contents](#)

If confusion wedded to ignorance pervades the world of corporate security today, at a time when the world has never been more dangerous, more needs to be done about understanding the subject and the risk. That may sound simplistic, yet managers have the sense to spend months and many thousands of pounds analysing capital investment in new tools or marketing techniques. Why not the same for security?

Clause 7 of the Health and Safety At Work Act makes clear an employers responsibility to ensure safety and well being for everything from a cut finger to canteen fist fights and protection from terrorism. This is not the same as uniformed guards acting as glorified receptionists or doorman.

The first message they should glean from Clause 7 is that security is not intangible, but one articulation of real concern for staff welfare, morale and ultimately profits. The second message is that it is a complex range of issues that need to be properly thought through.

An example of the current vogue in ill-thought security whitewash is to rush out and buy CCTV systems. A state of the art mission control of monitors looks impressive, but who benefits in the aftermath of a crime. We are surely delighted to have access to a recording of who coshed the M.D. or chief exec in his or her office. But surely the M.D. would gladly forego his moment of CCTV stardom for the price of prevention.



There are further sobering thoughts. The villain is the most security conscious player in this drama and will try to hide his true features from the camera. As if that wasn't enough of an argument against wasting cash on **ineffective** CCTV systems, 20,000 CCTV recordings were supplied to the police as evidence last year. Only one per cent were usable.

Once installed no manager appears to consider who will keep the tape heads clean, change the tapes, or with digital systems maintain the hardware or even re-align the cameras when the desks get moved around the office. Organisations who have CCTV installed should take a look at the management of these systems found in many of our town centres. Where these questions were addressed at the planning stages and as a result posed no further problems.

So security is not just a cosmetic exercise akin to putting a false alarm box on the exterior of your home. It demands the same level of risk analysis and ownership of responsibility at broad level that is applied by airline and car manufacturers developing new models.

## [Return To Contents](#)

### **The simple path to security has three elements,**

**First** appraisal of the real risks

**Second** Raising awareness from the top down, it needs a policy that is effectively communicated to all staff, backed by a clear strategy and thorough training.

**Finally** and perhaps most important it has to be effective and that means understanding how to cost requirements, how to manage needs and how to design.

Such expertise is unlikely to exist in the current management structure and cannot be found in your local police station or security guarding firm either. They can only advise and point you in the right direction.

In all of this, the old if simplistic adage, prevention is cheaper than cure holds true, so why do so many businesses treat security as an after thought.

The question what are the police doing about it? can be answered by saying we look after the streets you look after what is inside your walls. Until there is understanding of risks and what is required and proper management ownership at board level of the problems faced, the security will remain a neutered tool.



### **Offenders**

**This is our stereotypical offender,**

- 1. Usually male between 15-23 years.**
- 2. Unemployed.**
- 3. Unskilled.**
- 4. Low educational achiever.**
- 5. lives locally.**
- 6. No transport.**
- 7. Possibly drug abuser.**

## [Return To Contents](#)

## **Offender thought process.**

So what does this person think about before deciding where to break-in. The first thing is. Is there anything in there worth stealing? This decision could have been made previously and not at the time of the incident. If you bear in mind the profile the criminal is probably a local and familiar with your premises.

Another pattern of thought is. What is the social climate of the area? Do the premises here close at 5pm or are they open 24-7. Do staff park on the premises or on the street. Are there security patrols or CCTV, what type of businesses are there on the site, small independents or large nationals. Is there access control or can anyone just mingle with the staff undetected. All these are issues that the potential offender will consider when doing his risk assessment.

Another factor affecting the decision process is. Are there any symbolic barriers present. It is often quite uncanny how these type of barriers can be so effective. They involve quite simple and inexpensive measures and the most common example is a building isolated from its neighbours with no fencing just an empty area round the whole building of a material that stands out from its surroundings. The criminal has to make a conscious decision to cross this area to gain access to the shell of the building.

Other examples of these sort of barriers are a line of different coloured bricks or pavement dividing the public road from a semi private close. Low fences between pavements and front gardens etc. It defines public space from semi public space, semi private and private space without physical obstacles.

The next thought is. How detectable am I? This of course depends on design and construction as well as landscaping and lighting also CCTV, alarms, manned guarding etc.

Whether the building is occupied or not is another consideration he has to make, although an opportunist thief will use the fact that, there are many people about as the cover he needs to move freely through a building, it will depend on what he has targeted to steal. Daytime thefts are usually from offices and are usually small items from staff, but burglaries out of working hours are thefts that are specifically targeted.



The final consideration he will make is whether there are any physical barriers, fences gates bars locks etc. If these are effective and obvious then they will act as a deterrent but not on their own. They have to be used in conjunction with other factors, such as design layout, landscaping etc.

## [Return To Contents](#)

### **Crime Prevention**

So how does crime prevention fit into the scheme of things. For many years Crime Prevention was the Cinderella of the service. The ethos was, catch them and lock them up. This is still a good policy but unfortunately not very cost effective. This has now been recognised by the Home Office and A.C.P.O. and as a result they produced a document called TOWARDS 2000 A Crime Prevention Strategy for the Millennium. It basically states that crime prevention is the most satisfactory way of meeting the needs of potential victims, the Police service itself, the Criminal justice system and society as a whole. The strategy has three main components; and I 'quote'.

**1) Counteraction. Which is achieved in a partly measurable way by the appreciation of knowledge and skill to anticipate, identify, then remove or reduce the cause of and opportunities for crime.**

**2) Intervention. Which is achieved to a significantly quantifiable extent by operational policing methods designed to impede, disrupt and ultimately curtail criminal activity.**

**3) Deterrence. Which is achieved to an unknown and probably unknowable, degree by the very existence of a professional police service and the day to day activities of all members working in support of an established Criminal Justice System.**

#### **These components are wholly inter-dependent:**

Deterrence is sustained both by intervention and counteraction, which are themselves mutually supportive. Thus, intervention is often facilitated by counter active measures that detect or slow down the commission of crime, whilst criminal opportunity is lessened by the risk of such intervention.

It all means that we are now using a system called intelligence led policing and people such as Crime Reduction Officers are now actively involved in the whole process. This is how it works. A pattern of crime is highlighted through crime pattern analysis using data retrieved from commuter systems. The possible offenders are highlighted and physically targeted . The crime prevention response is directed at the particular area and specific crime. Using publicity as well as situational prevention to make an impact. To date this has shown considerable results with maximum resources aimed at the problem and incurring minimum costs and wastage.

## **Situational Prevention.**

Situational crime prevention measures are those which are aimed to reduce the opportunities for specific forms of crime to be committed. Each measure, whilst it may stand alone as a preventative method, can be reliant on the others to form a total concept to prevention.

Much situational prevention falls beyond the scope of the police. For example greater inroads could be made into theft and vandalism of cars not necessarily through local police action but by improvements in vehicle design. The police can have an important part to play in tackling local problems, not so much in taking preventative action which may fall to others such as planners, housing departments, transport authorities, private businesses and even individuals, but in initiating and co-ordinating such action.

## **Target Hardening.**



This is the first and most readily recognised form of prevention through the use of locks, bolts, alarms and fences and it forms the popular image of crime prevention.

It involves the concept of effectiveness over time. In other words the greater the attraction of the target, the greater

the strength or number of barriers needed to protect it in order to deter the criminal.

## **Removal of targets.**

It is not always appropriate to harden a target. On these occasions an alternative may be to remove the target from the risk area. The problem of pre payment electricity meters in homes can be overcome by removing them and substituting alternative methods of payment. Similarly some telephone kiosks are equipped with card reading meters which removes the risk of thefts from coin boxes. At many universities students are encouraged to use MONDEX cards instead of cash, these allow them to pay for goods and services on or close to the campus without using cash. The card is topped up by the student with small cash amounts at regular intervals, this avoids the need for carrying cash and has effectively reduced muggings and burglaries on campuses. Similar strategies can be employed within a business environment.

## [Return To Contents](#)

### **Removal of the means to commit crime.**

Most crimes are committed by opportunists who will not take the risk of bringing tools to a crime. By removing what they may find on site to assist them to commit the crime you are effectively preventing it. This comes down to good house keeping. Clearing away rubble from building sites may prevent its use as materials to commit damage. Ensuring vehicles in compounds are locked away and keys are secured in proper key safes will prevent thefts. Using vandal resistant materials may prevent the application of graffiti.

### **Reducing the pay off.**

Means making the target less valuable in the hands of the criminal. Therefore it may no longer be worth him stealing it. Having the property marked in a prominent place does not effect its use to your organisation but who wants to buy a computer with your organisations logo etched into the screen or the plastic. The use of INDOSOL TRACER solutions on equipment of all types makes them a risk to the thief and the handler. It is important though to ensure that these measures are widely advertised within the organisation and externally to act as a deterrent.

### **Formal surveillance.**

The presence of uniformed police officers on the streets is a recognisable form of surveillance. Supermarkets and industrial sites have adopted the use of uniform security guards. Business watch schemes are another example where people are encouraged to take an interest in their immediate area and be vigilant. To add to this we now have many Town Centre CCTV schemes. All are overt surveillance, planned and intended and advertised for maximum deterrence. The effectiveness of these schemes deterrence factors is not in doubt but some of the practitioners are. Some of these guarding companies are less than desirable and efforts are now being made to tighten up the industry.



### **Natural Surveillance**

This is achieved by the spatial definition of an area which enables people to supervise their immediate environment whilst going about their everyday business.

### **Surveillance by Employees**

The creation of awareness of particular crime problems amongst a work force will get them involved and make them more responsible. The forming of a hospital watch or Business watch etc call it what you will but keep them regularly appraised and informed through bulletins and results.

## [Return To Contents](#)

### **Environmental Management**

This has to do with the initial design of an environment and the subsequent management of it, its known as CPTED. ( Crime Prevention Through Environmental Design) The better we handle our human and physical resources the greater our profit and lower our losses.

Frequently it is necessary to consider all situational methods and each situation should be dealt with according to its merits. This underlines the need for two further important points, those of education and training.

**These are required:-** Within Police Forces

To promote the ability to analyse problems.

To create an awareness of the situational approach.  
amongst the Public

To ensure that they are familiar with preventative measures.

To promote interest and participation and to encourage the reporting of incidents.  
within Other Agencies.

e.g. Local authorities, planning authorities and education authorities in order that they should take account of crime prevention matters when formulating their policies and planning buildings.

### **Secured by Design Concept**

Secured by design is a Police initiative which was launched in 1989, and has full backing of ACPO and the Home Office Crime Prevention Unit.

The object of "Secured by Design" is to encourage the building industry together with architects to adopt recommended crime prevention guide lines, in both house and estate design and to gain approval and to use an official logo in marketing new projects.



Where estates are concerned the object of SBD is to create a secure neighbourhood environment, which will present a less attractive target for the criminal.

The recommendations are influenced by the concept of "territoriality" and "defensible space" which is concerned with a number of ideas designed to bring the environment under the control of the resident.

## [Return To Contents](#)

Included in these, are the creation of real and symbolic barriers, which help define ownership and increase "natural surveillance" any intruder would therefore, be denied anonymity, unhindered access and easy escape routes.

### **Secured by Design Commercial**

This is the same initiative but geared towards commercial and public properties. Some of the guide-lines are:

#### **Defined Perimeters**

Either physical or psychological or a combination of both.

#### **Physical security requirements**

The maximum standard is set out in BS8220 Part 2. and Part 3. Locking systems must equal or exceed BS3621 and have at least 1000 differs. Fire doors must not have external door furniture. Laminated glass must be used in glazed doors and adjacent to any door lock. All accessible windows require locking handles and or slant restructures.

#### **Landscaping**

This must be complementary to other security features of the development and should not obtrude on the natural surveillance. Trees when fully grown should not mask lighting fixtures or cameras.

#### **Lighting**

This is an important aspect of SBD the main requirement is adequate lighting of the whole site but with higher levels for vulnerable areas.

#### **Telephone Lines**

These should enter the building underground to protect the integrity of any external connected alarms or CCTV monitoring systems.

#### **Car Parking**

This must be subject to good natural surveillance from the building and has to be illuminated at night an alternative is secure garaging.

These and other principles can be adapted to all types of building and property but as mentioned at the beginning it is often best to seek outside help to look at the problem e.g. a Police Architectural Liaison Officer or Crime Prevention Officer and then adopt all or some of the recommendations to your sites.

## [Return To Contents](#)

### **CONCLUSIONS**

The days when crime prevention consisted of some "old put out to grass PC" coming round to tell you to cancel your newspapers when you went on holiday are long gone. It has now become a speciality in its own right and has become more one of community safety working in partnership with local authorities and other agencies. Whilst further specialist will evolve to deal with crime prevention in other fields such as I.T, ART LOSS, TERRORISM etc. The expertise is available for you to use now. What we don't know personally we can get access to via the Home Office Crime Prevention Unit and other agencies in our force HQ.

Crime prevention does not generate profits but it prevents loss, this is sometimes hard in this financial climate to reconcile to chief executives or MD's. The disruption to an organisation that a minor theft can cause if it hits the right target has to be good enough reason to look at your security.

Please do not hesitate to contact your local Crime Prevention Officer if you want advice. If they do not know the answer they know someone who does.

## **External Security**

### **PERIMETER PROTECTION**

No fencing can be guaranteed to be impregnable but it can deter criminals or provide critical delay time and assist interception of intending intruders by internal security or police.

There is a multiple choice of fencing available and careful consideration should be given to what type you should use for your premises. Factors to take into considerations are. Environment, location, level of security, what type of risk you are trying to protect against, finance available.



Steel palisade, welded mesh, expanded metal, chain link, bow topped fencing or even good quality hit & miss timber fences may be used in those areas not classified as "Ultra High Risk".

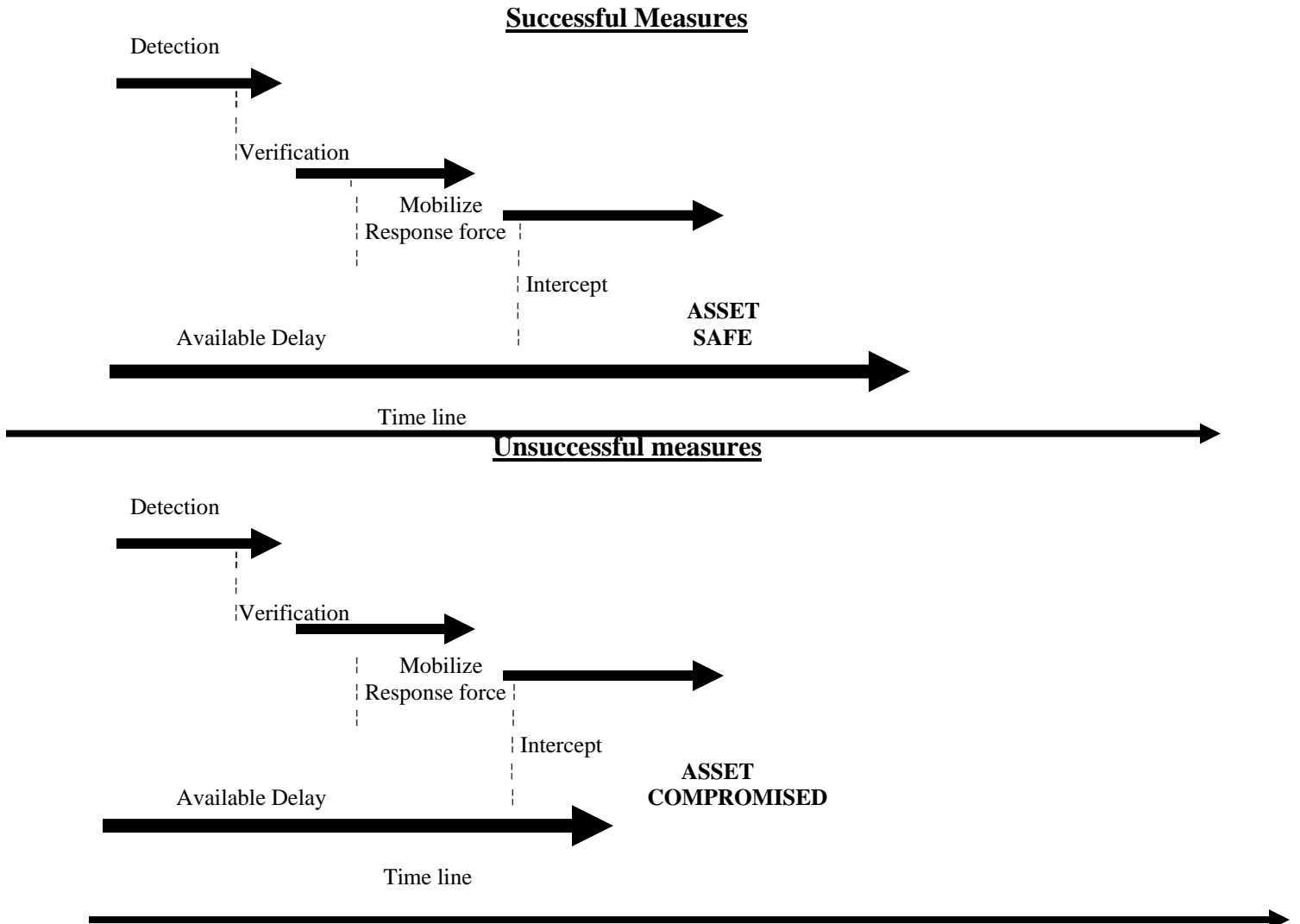
To raise the level of security on basic fencing they can be topped with barbed wire, razor barbed tape or revolving spikes to discourage climbers.

Where a higher degree of security is required. Patented high security fencing systems with alarm sensors and surveillance equipment can be used to make entry difficult, noisy and time consuming as well as detectable.

[Return To](#)

**Contents**

**The aim of your perimeter fencing in High Security situations is as follows.**



Advice on high security fencing can be obtained from The **Police Scientific Development Branch**. Sandridge, St Albans, Hertfordshire. AL4 9HQ. Tel 01727 865051

Ornamental fences can incorporate high security characteristics for projects that are highly visible in urban areas.

British Standard Specification 1722 (Parts 1-14 ) covers a variety of fencing systems. The majority of which would serve as good fencing systems as long as the project was properly planned and costed.

## [Return To Contents](#)

Even the best quality fence can deteriorate or be subject to damage. It is therefore imperative that regular checks are carried out to ensure that the fence is in good repair and still maintains its security integrity.

Good perimeter security is often compromised by bad housekeeping such as storing equipment such as boxes, containers and vehicles next to the fence,. Very often the perimeter of a site becomes the dumping ground for obsolete equipment. Avoid having trees or other climbable structures such as lighting poles next to fencing as this provides a step up either into or out of your site.



What ever type of fencing you install it has to be commensurate to the risk but in nearly all cases the fencing needs to provide natural surveillance. This is a Secure by Design concept that is well proven to work. The offender likes to be obscured from view and anonymous. By opening him up to view you will deter him from using that particular entry point as it will make him feel vulnerable and threatened. In some circumstances a well lit property surrounded by a large clear open space with no physical boundary could be just as effective as one surrounded by high fencing.

Gates are an important part of your perimeter protection and should be to the same physical standard and height as your fencing. They should be fitted so that there is no possible access underneath and be impossible to lift of their hinges. They should be secured with a welded locking plate and high quality close shackle padlock.

In larger sites consider electrically operated gates either sliding or swing type. Where you have staffed access points, retractable road blockers could be used in conjunction with raising barriers.

It is sometimes not economically viable to replace the existing perimeter defences such as walls or fences but they can be enhanced by the use of protective toppings such as rotating cacti, wall spikes, razor wire or barbed wire. Advice should be sought from the local police Crime Reduction Officer regarding the Occupiers Liability Act and the Highways Act in respect of the above forms of protection.

In isolated rural areas an alternative form of perimeter protection could take the form of ditching and banking. Bearing in mind that in these type of locations the offenders will almost always have to use vehicles to take away the goods, by denying them vehicle access close to the target you will make it extremely hard for them to commit the offence.

## [Return To Contents](#)

In many cases the perimeter forms part of the actual building leaving little room for extra defences. CCTV could prove a valuable tool, enabling staff to monitor entrances and other vulnerable areas from a central point.

## **LANDSCAPING**

Planting should be kept to a low level. (1Metre in height) and any trees should be pruned so that the lowest branches do not fall below 2.4 meters from the ground to allow for site lines and to prevent climbing . This will ensure maximum opportunities for natural surveillance of buildings. This is especially important next to buildings as it will also remove hiding places and screens for the intruder. Young trees should not be planted too close to a building where in maturity, they could provide a climbing aid.

If planting is considered then use spiteful plants such as Roses, Berberis, Pyracantha etc. These plants can be judiciously placed to provide perimeter protection to a site or to vulnerable parts of a building, such as around ground floor windows.

## **VANDALISM**

Any criminal damage to the buildings or within the site should be quickly repaired. Failure to do so will encourage further damage. (This is known as the broken window syndrome). Neglect is infectious. Temporary buildings and temporary repairs give the impression of slack housekeeping and say to the criminal that this is an easy target. Any repairs should be to a high standard and be effective. There are many good security screens and doors on the market for blocking up void buildings



Empty buildings must be properly secured against entry and the immediate are kept well maintained so that it does not appear abandoned.

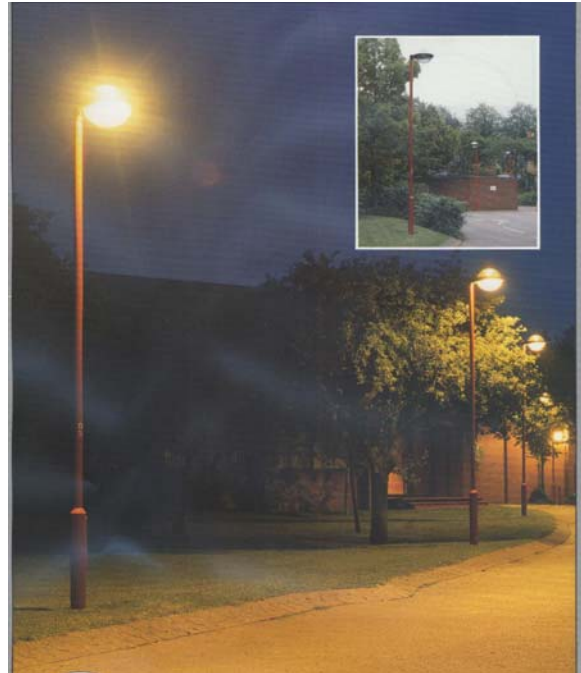
Wheelie bins and rubbish skips should be stored well away from buildings and wheelie bins should be secured in place so they cannot be moved. They should be sited in highly visible and well lit areas. They are a ready target for vandals and arsonists and the high sides of the container act as a chimney sucking flames up to heights of 30 ft or more making roof

lines vulnerable to the fire. They are also attractive to the totters who come looking for scrap metal etc. once attracted to your premises they can then check out the rest of the site for other items to steal.

## [Return To Contents](#)

### **LIGHTING**

Commercial premises usually fall victim to crime during the hours of darkness, so it follows that lighting is an important factor in prevention. There is a variety of lighting available to the commercial sector. The most efficient systems are High-Pressure Sodium Vapour lights (SOVN) These should be activated with Photo Electric cell. This will ensure that the lighting comes on when the ambient lighting levels drop below a certain level. For medium size premises the traditional Halogen security lights can be just as effective. Again they should be connected to a Photo Electric Cell. For the smaller premises bulk head lights fitted with low energy bulbs can also be effective as long as there are enough fittings to light up all the areas deemed necessary. (The shell of the building). Good lighting is of benefit in reducing the fear of crime for your staff and visitors. It can also deter the intruder and aid in surveillance of your property, and assist in the recognition of your visitors.



### **RAM RAIDING**

This is still a problem in most areas of the country and needs to be addressed especially if your premises contain the high value bulk items that may be attractive to the ram raider. An effective deterrent to ram raiding is a physical barrier placed some distance in front of the wall or windows of your building, such as a row of bollards or heavy planters containing flowers. The latter can also help make your building look more attractive. You may also consider installing rising barriers in front of vulnerable doors.



## [Return To Contents](#)



### **CAR PARKS**

Car parking is not only a security issue but also an emotive issue that can affect staff moral especially if space is limited and taken up by senior management, where ever possible arrangement should be made to provide parking for all, even if this has to be out sourced. Car parking areas should be well lit, even when the building is unoccupied. This is particularly important when small numbers of people are required to work late or out of core working hours and may need to cross the car park to reach

their cars unaccompanied. It is important to ensure the car park can be observed from the building and is not obscured by landscaping or temporary constructions.

### **OUTBUILDINGS**

Out buildings such as plant rooms and bin storage areas should be sited in such a position so as not to obscure vulnerable parts of the building and so they do not provide easy access to the roof or upper floors. They should be secure and locked using adequate locks and bolts.

If they are to be used to store hazardous or dangerous waste then guidance as to the storage should be sought from the Health and Safety Executive and extra provisions should be considered regarding security.

### **BUILDING SECURITY**

The walls of some buildings may be of steel frame construction with weak building panels and therefore be vulnerable to attack. In risk areas this type of construction can be improved by lining the walls with welded mesh panels.

Roofs can also be vulnerable area and it is worth assessing the risk of entry through the roof . Consider using anti-climb deterrents such as spiked collars around external pipes or anti climb topping such as Viper spikes or roller spikes.

## [Return To Contents](#)



Any roof lights should be of polycarbonate variety which can be secured in place with non return screws.

## **DOORS**

There are many different types used in commercial buildings these days and it would be impossible to cover the security of all types here. Doors should generally be set flush with the outside wall and not in a recess or porch that will provide cover for anyone attempting to force an entry. Recesses also provide places for youths to hang out when your premises are closed and this attracts damage and graffiti.

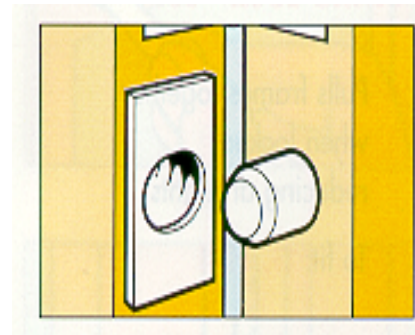
Doors and locks should be compatible its no use spending money on good quality locks if the doors in which you are going to fit them are of poor quality or of the wrong sort. Ensure you get advice from an expert such as a carpenter or you local Crime prevention Officer before proceeding in changing doors and locks. All door locks should meet BS3621 specifications as a minimum standard. Your insurance could be affected if this is not the case.

Doorframes must be securely fastened to the surrounding wall. Frames must be substantial enough both to carry the door weight and to allow good fixings for the hardware. If there is any doubt about the suitability of the frame it should be changed.

Door sets should meet PAS 24 standards.

Poor quality hinges will cause failure very quickly. If a door is to operate effectively for a long time install ball hinges.

As an additional security measure it is recommended that hinge bolts are fitted. This will prevent the door being removed if the hinges are attacked or if force is applied.



Door closers are an essential item of door furniture in

commercial premises. You would be well advised to look for the best available. A good door closer must be fire-resistant and have the following easily set independent controls which should not need readjusting.

### [Return To Contents](#)

**General closing speed** – controls door from open position to last few degrees of closing.

**Latching speed** – controls speed for last few degrees.

**Back check** – controls the last few degrees of opening to prevent door being thrown back against adjoining walls causing damage to the wall, hardware and frame. Spring power adjustments allows you to choose the strength you require.

The closure arm is a prime target for vandals. Select a unit which will resist attack.

**Letterboxes** - Besides meeting Post Office requirements letter boxes should have a spring on the flap and a cage on the inside so that no one can get at the locks and bolts. The cage should have no bottom to prevent mail from being grabbed from outside.

To reduce the risk of arson several products are now available such as steel boxes and flame resistant bags.

## **EMERGENCY EXITS**

Emergency exits are commonly used by intruders to gain access to a building. Ideally, these doors and frames should be protected with wrap round galvanised steel sheet fitted using clutch head screws to resist jemmying and drilling. The door furniture should meet fire service requirements. Using proprietary fire escape door furniture is the best solution ensuring that the equipment provides multi point locking.

These doors and the door furniture should be regularly serviced to ensure that they function properly and also that they do actually secure the door when closed.

To prevent misuse by staff a stand alone alarm should be fitted to the doors to indicate when they are opened as it is common practise in many companies for staff to use the fire exits as short cuts to other parts of the premises or to use them as a place to stand for a quick smoke. The danger then is that the doors will not be closed properly and an intruder will have ease of access to the building.

Before any alterations are considered to your fire escape routes your local Fire safety Officer should be consulted. Any unauthorised change may result in contravention of a Fire Certificate.

## **WINDOWS**

Windows are probably the weakest point of any building. Ground floor windows being particularly vulnerable. It is therefore advisable to reduce the number of opening panes to the minimum and those that cannot be replaced should be fitted with window locks.

Laminated glass should be installed as it is an effective burglary deterrent. It is simply two layers of glass sandwiched together by a strong flexible layer called polyvinyl butyral (PVB).

### [Return To Contents](#)

It can be up rated until you have eight ply laminated glass which will withstand the impact of a rocket propelled grenade.

Laminated glass may craze at the point of impact but will remain in one piece because of the resistant (PVB) interlayer holding it together, continuing to protect your assets against theft or looting and the weather. It should be fitted in all ground floor windows and in doors and glass panels next to doors.

Shatter resistant safety film is the most effective and economic method of converting existing ordinary glass into Safety Glass and conforms to British Standard Code of Practice BS6262. This is particularly useful if you are taking over a building from other tenants who may not have improved the security of the glazing.

Window safety films are made from a tough clear polyester film to which a pressure sensitive acrylic adhesive is added and remains optically clear when bonded to glass. It will protect against terrorism, vandalism, accidental damage and the risk of injury from flying glass shards. It must be professionally installed.

These films also reduce ultra-violet light, the main cause of fading, and are available with a protective abrasive-resistant coating with a choice of coloured, reflective and opaque film to provide privacy and solar heat and glare control.



Working on the principle that opportunity makes the thief. If the object of their desire is hidden from view there is less chance that they will target your premises. Therefore blinds should be considered on all ground floor windows. A low cost, but effective solution being metal Venetian blinds as they are noisy and provide an entanglement for anyone trying to get through them, and hence a deterrent. There are more robust blinds available some are even bomb proof and should be considered for high risk areas. They are unobtrusive during the day but provide an impenetrable steel barrier when closed out of working hours.

Steel grills should also be considered for vulnerable downstairs windows. Again these are unobtrusive during the day but once closed they provide an effective barrier to the thief.

## [Return To Contents](#)

# Internal Security

## RECEPTION AREA

The reception area is usually the first line of defence in any business during working hours. It is imperative that this area is staffed continually during working hours. Firstly it creates a good image of the company and can be a showcase of products and services. Secondly it provides the first line of security. Thirdly it provides a point of contact for staff and visitors and allows vetting of visitors.



The reception area should be clearly signed and be near to the first entry point to the premises. It can be a security point at the perimeter entrance or alternatively it could be the foyer of the building secured from the rest of the premises. It should be the hub of the company's security system. Incorporating, visitor recording, using a badge system, CCTV monitoring in smaller companies, telephone exchange and Health & Safety control centre.

Access to the remainder of the premises via reception should be controlled either with an electrically or mechanically access control lock, or if the reception is at the main gate of a larger premises by a barrier or gate system. Visitor parking should be close to reception so that the car park can be overlooked and to avoid visitors wandering about the premises looking for a point of contact. Good signage is also important as it directs your visitors to the place you want them to go it avoids confusion and prevents the excuse of "I didn't know where to go" being used by walk in thieves who are challenged.

## INTERNAL DOORS

As a general rule internal doors should be closed out of core working hours as a fire precaution. They should not necessarily be locked. Burglars can cause a great deal of damage to doors and frames just to find out if a room has anything in it worth stealing. The exception of course, are rooms where you do have items of high value or equipment that is vital to the operation of the business such as computer servers and data storage. These rooms should in fact be specially secured and the doors should be of a much higher standard and kept locked and alarmed.

## [Return To Contents](#)

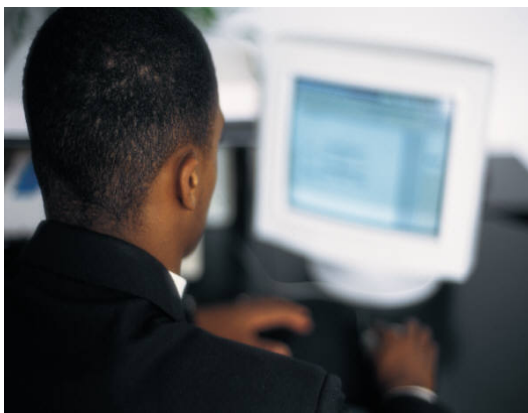
### PROPERTY MARKING

Despite all the security measure that you take, your property might still be at risk from theft, either from an outside or internal source. It is strongly recommended that you mark your property. There are numerous ways to do this the simplest form is to mark the items with a UV marking pen and stick on a label to say that the property is marked. Etching or engraving are another method that can be done in house and is more visible and permanent. There are a number of other proprietary methods that are available such as using a dot matrix template and etching paste etc. Your local crime prevention officer will be able to advise you as to what is available.



### PHYSICAL SECURITY

Valuable office equipment such as computers, Laser printers, copiers and fax machines should be secured to the work surface to prevent easy removal. There is a large selection of equipment available to enable this sort of equipment to be secured ranging from simple lockable clamps, steel cables to lockable steel cabinets and work stations. The equipment can also be alarmed using internal alarms which activate by movement to sophisticated electronic tagging which can activate alarms when taken beyond a specified point. The locating of this type of equipment is also important, Expensive photo copiers kept in the foyer next to a glass front door because no other suitable space can be found. Computers located next to windows so they could be stolen without the thief actually having to enter buildings. Lap tops left on workstation docking ports when unattended. These are all house keeping issues that need to be addressed.



### COMPUTER DATA

The security of computer data in small to medium companies is an issue that raises concerns and should be guarded against. The loss of your own data could prove a major set

back to the running of your business but the theft of a customer's data that you were storing or using for a project could leave you liable to damages and could be disastrous for your business. There are two main ways that you could lose the data through crime.

### [Return To Contents](#)

The first way is that the data could be stolen or lost electronically. It is therefore imperative that you ensure that you have an up to date and effective firewall built into your system and that you also have an effective virus detector running which is regularly updated. These can be bought from most computer dealers who can advise you on the type of program your equipment should be running.

All terminals should be password protected and the passwords changed frequently to prevent unauthorised access. Staff responsible for making up passwords should avoid the use of common names and numbers. Some of the most common passwords are "secret" and "password".

There should also be a staff computer protocol which everyone is familiar with and complies to. This refers to bringing in outside programs or taking home data to use on unprotected systems. It involves the limitations that you put on staff using the internet for their own use etc.

The second way that data can be stolen is through physical theft. If the thief steals the computer the data goes with it. Data should always be backed up preferably on a daily basis and the backed up discs or tapes stored securely in a fire and thief resistant safe. Equipment can be replaced the next day the data cannot and not having it available could ruin your business.

Confidential papers should be locked away in a desk or cabinet. Your company may not be involved in highly secret work or techniques but the information could be of use to a rival or could become damaging to you if it was stolen or used by a disgruntled employee. Employ a clear desks policy, where whenever an office is left unattended the desk is cleared and everything locked away. This includes stationary. You would be surprised how much the constant replacement of office stationary cost over a year.

Information contained in documents, plans, drawings or visual aids, should be protected by:

- Shredding or burning of notes or spoiled paper.
- Numbering of copies and recording to whom copies are issued against signatures.
- Not using temporary staff on sensitive type work.

### **CASH OFFICE SECURITY**

The security of a cash office is of equal importance to that of a bank.

Physical protection and alarm protection should be afforded to the staff and the cash holding in this area.

Safe routes should be planned within the building between the cash office and the entrance to facilitate the movement of cash.

### [Return To Contents](#)

The cash office should be sited in a part of the building which is inaccessible to the public and concealed from their view.

When cash is on site or is being handled, the office should be locked and no access to other personnel should be permitted.

Cash awaiting transportation should be deposited in a locked safe of suitable quality.

All staff should be trained in security procedures and in actions to be taken in the event of attack. Alarm systems should be tested regularly.

Doors of cash offices should be fitted so they open outwards and not into the room.

The doors should be of a solid wooden construction at least 44mm thick, fitted with a door chain and viewer and ideally should be sheathed with a steel plate which overlaps the frame. Morticed hinge bolts should also be fitted for added strength.

There should be at least two 5 lever morticed locks to BS 3621 these should be fitted 33cm down from the top of the door and 33 cm up from the bottom of the door this dissipates any pressure that may be exerted against the door.

Ensure good key security and limit the number of people who can have access to the cash office, only allow staff who have been vetted and have been with you for some time to deal with the cash. The fewer people who know your procedures the more secure they will be.

Consider a counter cache at the till points so that the amount of cash kept in the tills is at a minimum to reduce the loss in case of a till snatch.

Written instructions should be issued to staff as to their duties especially in cases of attack and also to staff outside the cash office environment as to actions to take in the event that the alarms are activate The systems and procedures should be tested on a weekly basis.

Minimum overnight cash storage should be the rule.

### **CASH IN TRANSIT**

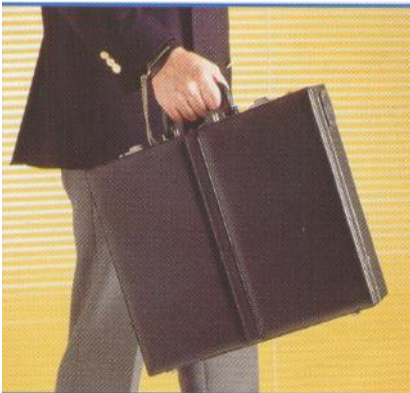
Movement of cash to and from banks and other premises should be governed by a number of basic rules:

1. Cash should be banked as often as possible. Not allowed to accumulate on the premises.

2. Because of their vulnerability juniors, the elderly, the infirmed or new staff should not be employed for this task.
3. The messenger should preferably go by vehicle with a second person as driver.

### [Return To Contents](#)

4. Accompanied pedestrian messengers should face oncoming traffic to prevent an ambush by a following vehicle.
5. A special waistcoat or alarm bag should be used, the first and last hundred yards are the most likely to attack especially the point of entry to the bank or office.
6. If a vehicle is used it should be varied. Do not use taxis.
7. Where large sums are involved the receptacle should be anchored to the floor of the vehicle.
8. In all cases sufficient escort should be provided.
9. Drivers should view with suspicion any accidents, unexplained traffic or other distractions or following vehicles when carrying cash.
10. Always keep doors and windows locked.
11. Night safe facilities are useful, especially for weekends. Money should not be exposed until the night safe door is open.
12. Routes should be varied at each cash run. S



Cash Transit Case



Case Activated on Attack



Vehicle Security Box

### **KEY SECURITY**

Key security should be kept simple, problems arise when this is not the case because control is lost and security becomes compromised.

Keys to the premises should be issued only to nominated key holders. These should be kept to a bare minimum. All other keys should be kept in a key safe. This should be a steel cabinet securely bolted to the wall. It should be lockable and have numbered or coloured hooks inside to allow for quick visual checks.



Only the nominated key holders should have access to the key safe.  
All keys should be signed out and in by the person nominated to control the keys such as a receptionist.

### **[Return To Contents](#)**

For special secure areas within the building such as data centres or laboratories it is advisable to use locks which require codes or magnetic cards to obtain entry. This will ensure that only authorised persons have access. The codes should be changed frequently to avoid compromise.

An alternative to keys which easily become compromised is electronic access control systems. These are becoming more and more sophisticated and easier to run. They start with simple electronic swipe card systems or proximity keys which will open doors to authorised persons only and progress to highly integrated systems using biometrics that not only control access but record movement through out the complex as well as monitor CCTV, fire alarms, Staff booking on and off, for pay role purposes. Heating, lighting, computer access, in fact every facet of your business can be interconnected into a management control package.

### **CASH HANDLING COMPANIES.**

Where large sums of cash are regularly moved the services of a cash handling company should be considered, to reduce the risk to your staff. These companies will not only deliver or collect money from the bank but can also provide a number of other services such as data collection and storage.

Instructions to these companies should be very specific as to date time and place the pick up or drop is to take place and this should be by way of a written contract to prevent any ambiguity as to performance or argument in the event of an insurance claim.

There should be a way of verifying the authenticity of the collector using a code word to ensure that they have not been compromised and a verification system with the company's despatch department.

### **STAFF VETTING & SEARCHES.**

As part of your internal security measures the option to randomly stop and search staff should be written into their contract of employment. It is not only important that staff are aware and agree to this happening but it must be carried out on a regular basis.

One major national retailer operates a random self selection process where staff on leaving the premises blindly select a card which either says "pass", "Bag search", "personal search" or vehicle search. This is carried out routinely and ensures that no one is above scrutiny. This in itself is a good deterrent to staff theft.

All staff applying for work should provide verifiable references which should be followed up. In positions of high risk or in highly sensitive areas Criminal Record Bureau checks should be carried out as a matter of course before a position is offered to the applicant.

It is important that line managers have a good knowledge of their staff and their private lives. This does not mean you check up on them, but keeping an ear to the ground to keep abreast of changes in personal circumstances which could affect their performance, reliability or trustfulness is good management practice and shows leadership skills.

## [Return To Contents](#)

### ELECTRONIC SECURITY

#### ALARMS

No modern business what ever its size should be without a functioning alarm system. A properly installed alarm system will help to protect your premises in a number of ways. It will act as a deterrent in most cases of opportunist crime. A potential opportunist offender will think twice before attacking an alarmed premises. Secondly an alarm can reduce the impact of a determined attack as it will reduce the time the offender can stay in the premises before he is likely to be caught as he will not know what the response will be or the time it will take for it to get there. It can also act as a management tool to check up on staff working hours as the time an alarm is set or un-set is recorded within the system enabling management to confirm lone workers time in and out etc.

Such system should comply to the new BS EN 50131 standard. The requirements from A.C.P.O. ( Association of Chief Police Officers) for alarm system requiring a police response are.

1. The system should meet BS EN 50131 standard.
2. Be installed by an installer who is a member of either NACOSS or SSAIB these are installers organisations which provide accreditation to their members and who are expected to comply to the standards set by them and which are acceptable to the Home Office and ACPO.
3. The system should work in the following way, either by:-
  - Sequential activation. Of the internal sensors
  - Audio confirmation of intruders movement.
  - CCTV confirmation of intruders.
4. The key holder must be within 20 minutes travelling time from the premises.

The majority of these systems are installed using BT Red Care as their alarm carrier. The system and the equipment associated with this ensures fewer false activations and has a self testing and monitoring capability.

Once the basic system is installed it can be expanded and integrated with many other security programs such as external long range PIR (Passive Infra Red) sensor to cover large outside areas. Lighting. Fence monitoring. CCTV. Smoke Screen. Access control. Staff monitoring. Fire alarms.

## [Return To Contents](#) **CCTV SYSTEMS**

Closed Circuit Television is now cheap enough to be well within the reach of even small businesses. Systems can be bought outright or rented. The benefits are many and its deterrent effect well documented. It should be remembered that CCTV is not a substitute manned security no camera has ever detained a person. CCTV is just another tool in a co-ordinated security system and it should dovetail in with the other measures you have in place. I do not intend to be specific on equipment because the technology is moving so fast that what ever I write will be overtaken.



Systems are now very flexible and are now able to transmit images in various formats. Although hardwired systems are preferable, it is now possible to install radio controlled systems that can transmit over great distances or to use ISDN or ADSL transmission to send you signals to the monitoring point.

Systems can be fitted with alarms so that cameras can remain dormant until activation occurs. The operator is then able to carry out other tasks without the need to sit in front of banks of monitors.

The system can be interfaced with your own systems including alarms. Each system can be adapted to fit in with your needs and working practices. Technology is moving ahead so fast that by the time you have read this any thing that I may have said will have been superseded

What is however vital is that you plan and resource the purchasing of a system in exactly the same way as you would any major capital investment. The Home Office Website can help by linking through to the **Police Scientific Development Branch Document 17/94. CCTV Operational Requirements Manual**. This can guide you through the whole process and will ensure that the system you buy is suitable for the task.

[Return To Contents](#)

## **OCCUPIERS LIABILITY ACT 1984**

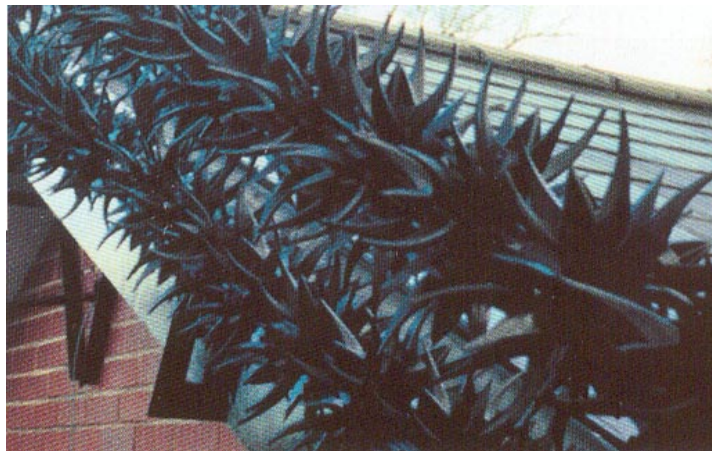
The Occupiers Liability Act 1984 has implications for those occupiers of premises who may wish to implement preventive measures intended to deter intruders from unlawfully entering their premises. It is a miss understood Act from which people often draw the wrong conclusions as to what they can and cannot do to protect their property.

Below is the legal opinion as provided by the Home Office Legal Advisers Branch.

The Occupiers Liability Act 1984 is intended to fix the duties which an occupier of premises owes to persons, other than visitors, who come onto his premises. Generally speaking a visitor is someone who has the occupier's permission, whether expressed or implied, to be on the premises.

The duties owed to visitors are regulated by the Occupiers Liability Act 1957. Following the passing of the 1957 Act doubts arose as to the extent of the duty owed by an occupier to persons who did not have permission to come onto his premises, in other words trespassers, who might be expected to be found there. The 1984 Act is intended to put an end to these doubts by placing the occupier's duty to such persons on a statutory basis.

The Act has a clear application to intruders who, because they do not have the occupier's permission, cannot be said to be visitors. Section 1(3) has the effect that an occupier owes a duty to intruders in relation to risks of which he is aware, and against which he may reasonably be expected to offer some protection. Sub section (4) provides that it is his duty to take **reasonable steps** to ensure that the intruder does not suffer injury; but sub section(3) provides that **his duty may be discharged by taking reasonable steps to give warning of the danger or discourage persons from incurring the risk.**



## [Return To Contents](#)

1. Thief resistant devices are clearly contemplated by Section 1(1) (a), whether they take the form of devices which may be said to be part of the state of the premises or come into existence as a result of things done or omitted to be done on the premises.
2. The terms “visitors” does not include an intruder, but the act is drafted so as to impose duties in relation to people who are and consequently applies to intruders.
3. Section 1(5) provides the duty may in an appropriate case be discharged by taking such steps as are **reasonable** to give warning of the danger. This does not mean that an occupier is automatically absolved by putting up a warning notice, only that a warning notice may, depending on the circumstances, be sufficient to discharge his duty.
4. So far as crime prevention is generally concerned, it seems to me that the effect of the Act is that an occupier will be liable for injuries sustained by an intruder because of the thief resistant devices, **whose existence is not reasonably apparent to the intruder**. For example, a device which gave an intruder an electric shock would probably make the occupier liable, if no warning were given. I think the same must apply to razor wire which, as I understand it, is very dangerous material. Things like barbed wire and broken glass are much more obvious risks and I think the duty to warn intruders against them is much less strong. However, I should have thought that, in terms of crime prevention, it was always advisable to warn potential intruders of the risks they would run in trying to enter premises without permission. If this is done in all cases where devices are installed, which may cause injury to intruders, the likelihood is that the occupiers concerned will have discharged their duty pursuant to section 1(5) of the 1984 Act.

## [Return To Contents](#)

# **RISK ANALYSIS PROGRAMME**

## **1. INTRODUCTION**

- 1.1 It is a recognised fact that crime, to varying degrees, intrudes on most business trading today.

Although there have been successes in reducing the amount of recorded crime across the U.K, it still continues to rise in some areas. Even where it has fallen, there is no comfort in that fact if yours is one of the companies unlucky enough to be targeted.

- 1.2 So what can be done? You have taken a first step by contacting your local Police. This guide has been produced with one main objective in mind, to raise awareness.
- 1.3 When you receive this risk analysis programme, we would ask that you follow it through and complete it as honestly as possible. By simply being asked specific questions you may find that you already have your own solutions to hand.
- 1.4 Companies are in business to secure a profit. Crime Prevention measures will not show an obvious return on any investment. It will not, in the short term, serve to improve efficiency, widen your product range or improve your market potential. In the long term however, it may effect all of these important areas.

## **2. ASSESSING THE RISK**

- 2.1 Use the questionnaire provided to assess the risk to your company in terms of criminal attack. Simply go through each section, omitting those areas not relevant, to formulate a picture of the strengths and weaknesses associated with your premises.
- 2.2 To assist, you may wish to draw up a 'Security Register'.

This should contain a copy of the questionnaire, details of any security already in situ, guards, alarm systems etc., and also a plan of your premises. By using a plan you can identify each profile of your building, number each door and be able to carry out regular checks, endorsing any problems in the register.

- 2.3 A senior member of management within the company should be given the role of 'Security Liaison'. The register should be completed each week and submitted for him or her to check and endorse.

### Return To Contents

- 2.4 Any member of staff could be given the duty of checking the premises, usually on the Monday morning, where the business closes at the weekend, or any time considered appropriate.
- 2.5 This serves to include all staff in the checking procedures and gives them a sense of 'ownership' with regard to the company's security.
- 2.6 Incidents can be picked up earlier and anything out of the ordinary quickly identified.
- 2.7 Where companies have external compounds or grounds, everything should be designated its own area, pallets, skips, stock etc., and every effort made to keep the outward impression of the company, one of efficiency and effectiveness.
- 2.8 Details of broken windows or damaged fencing etc., should be acted upon quickly, as failing to do so generally leads to further incidence of damage.
- 2.9 Where appropriate, details of alarm activation's should be kept in the register with an account of why any such activation's occurred.
- 2.10 Key holders to the company should be kept up to date in the register.
- 2.11 Any other appropriate information relevant to the security of your premises should be listed.

### 3. CONCLUSION

- 3.1 Much of the information in this guide will be common practice within your company. It may be, however, that a number of files are kept appertaining to security and that more than one person has overall responsibility for security in general. By following this simple guide it should be possible to integrate security into the general management of the business.
- 3.2 You may fee that by following the advice contained in this programme, you now have no need to invite a Crime Prevention Officer to your premises. **We would point out however that one would always be available to offer unbiased advice, free of charge, should you require further assistance.** It would help the CPO if you could complete the questionnaire prior to his visit.

3.3 The implementation of measures contained within the survey may also serve to improve Health and Safety conditions for your staff—a major concern in the commercial environment today.

3.4 Finally, it must be stressed that, as with all security advice, the total diminution of crime can never be guaranteed.

[Return To Contents](#)

**COMMERCIAL SECURITY**

**RISK ANALYSIS QUESTIONNAIRE**

**REF. NO:**

**DATE:**

**NAME OF COMPANY:**

**ADDRESS:**

**INTRODUCTION**

This questionnaire is designed to help you to assess the risks from damage, loss and injury to your premises. It is intended to highlight any areas where action is required. If the answer to any question is 'No', then remedial action should be considered. Where the question does not apply show 'N/A'.

(Note:- This form may be photocopied if further copies required).

<b>PART ONE</b>	<b>YES</b>	<b>NO</b>	<b><u>N/A</u></b>
<b>MANAGEMENT INFORMATION AND PRACTICE</b>			
1. Are the existing systems capable of identifying the total cost of vandalism, arson, burglary and theft?			
2. Do recording systems allow distinctions to be made between the cost of criminal damage and the cost of accidental or careless damage or wear and tear?			
3. Is there a specific budget each year, or a rolling programme, for crime and vandal prevention measures, separate from any general repair fund?			
4. Has any money been allocated specifically for the prevention of crime and vandalism during the next five years?			
5. Has there been any expenditure on crime or fire prevention measures?			
6. Are any acts of vandalism recorded and reported immediately upon discovery?			
7. Is there a central alarm responding point in the establishment known to staff?			

8.	I damage quickly made good to discourage further similar damage?			
9.	Is criminal damage automatically reported to the Police?			
10.	Are details recorded of the nature, time, place and cost of theft and vandalism?			
<a href="#">Return To Contents</a>				
11.	Have you sought to identify any areas, which are particularly vulnerable to vandalism or forced entry?			
<b>PART TWO LIAISON</b>		<b>YES</b>	<b>NO</b>	<b><u>N/A</u></b>
1.	Have you considered forming or bring part of a business watch scheme?			
2.	Has guidance been sought on security and damage control from: <ul style="list-style-type: none"> <li>The insurance industry?</li> <li>The security industry?</li> </ul>			
3.	Has a risk evaluation survey of the premises been undertaken and its recommendations implemented?			
4.	Are you in contact with other businesses in the area to exchange information about security matters?			
<b>PART THREE TRAINING</b>				
1.	Are staff warned to note suspicious activities?			
2.	Are staff warned to notify management when strangers are seen on the premises?			
3.	Are staff and employees trained in security awareness?			
<b>PART FOUR CONTINGENCY PLANNING</b>				
1.	Is there an establishment procedure for Police to contact key holders promptly in the event of damage occurring?			
2.	Is there a contingency plan to minimise disruption of normal activities after a serious incident?			
3.	Are duplicate records and back-up copies of computer files kept in a separate location?			

4. Do your staff know their role in an emergency?			
<a href="#">Return To Contents</a>			
<b>PART FIVE SECURITY OF BUILDINGS</b>			
1. Are the premises in good repair?			
2. Is the boundary of the premises clearly defined?			
3. Has consideration been given to protecting or eliminating recessed doorways, concealed yards, shrubs, planted areas and similar features which can give cover to intruders?			
4. Are the main buildings free from examples of flimsy construction, such as low-level glazing or lightweight panelling?			
	<b>YES</b>	<b>NO</b>	<b><u>N/A</u></b>
5. Are all entrance doors locked and windows and skylights secured when the premises are not in use?			
6. Have steps been taken to restrict easy access to the roof from parts such as lower, adjacent structures, compounds, walls, down pipes?			
7. Are tools and ladders locked securely away?			
8. Has an intruder alarm system been installed?			
9. Does the intruder alarm automatically notify the Police?			
10. Is the alarm system set and unset solely by designated persons who are trained for the task?			
11. Is the alarm system regularly maintained and inspected?			
12. Are materials, which could be used as missiles to commit damage removed from around the property?			

[Return To Contents](#)

**PART SIX**  
**KEYS AND LOCKING UP**

1.	Is there a proper system to control the issue of keys?		
2.	Is there an established procedure for locking up?		
3.	Are rooms such as toilets checked to ensure that there is no one concealed in the building when it is locked up?		
2.	Are buildings designed to prevent ready access except through normal entrances?		
3.	Are visitors encouraged to use the main door and is this clearly signposted?		
4.	Is it possible to monitor the arrival and departure of visitors?		
		<b>YES</b>	<b>NO</b>
			<b><u>N/A</u></b>
5.	Are visitors asked for identification?		
6.	Are visitors asked to sign in and out?		
7.	Are visitors escorted to their destination?		
8.	Are members of the public prevented from entering unauthorised parts of the building?		
9.	Do staff challenge strangers who they see in the building?		
<b>PART EIGHT</b>			
<b>SECURITY OUTSIDE OF WORKING HOURS</b>			
1.	Are special arrangements made for surveillance during vulnerable times such as holidays?		
2.	Are the premises checked by: <ul style="list-style-type: none"> <li>• Business Watch Schemes?</li> <li>• Security Firms?</li> </ul>		

3.	Are the premises well lit when not in use?		
4.	Is external security lighting provided?		
<a href="#">Return To Contents</a>			
5.	Is there natural surveillance from surrounding buildings or passing members of the public?		
6.	Is the caretaker on site?		
7.	Is the caretaker readily accessible?		
8.	Can the caretaker quickly contact the security company, Police and Fire Service?		
9.	Is the timing of cleaning arrangements designed to facilitate supervision?		
<b>PART NINE</b>			
<b>THEFT</b>			
1.	Are there secure storerooms or containers for securing attractive items such as audio-visual equipment, computers and videos?		
2.	If secure workstations are not available, are valuable items always placed in secure storage when not in use?		
3.	Are rooms containing other attractive equipment – offices workshop and storerooms kept locked when not in use?		
4.	Are staff and employees advised on the need to safeguard personal property?		
		<b>YES</b>	<b>NO</b>
			<b><u>N/A</u></b>
5.	Are secure worktop fittings provided for attractive portable equipment		
6.	Are cash holdings kept to a minimum?		
7.	Is cash counted out of sight?		
8.	Is money removed from the premises overnight?		
9.	Is equipment marked so as to identify the owner and are signs displayed to this effect to deter thieves?		
10.	Is a safe installed for storage of cash or other items of value?		
11.	If installed, is the safe of an adequate standard for the risk?		

<a href="#">Return To Contents</a>			
<b>PART TEN SPECIAL RISK - CONTRACTORS</b>			
1.	Is a named person designated to ensure that statutory controls are properly applied and that the appropriate extra security, safety and fire precautions are taken when contractors are working on the premises?		
2.	Are pre-contract meetings held between interested parties to identify on-site risks and procedures necessary during the work, including the raising of alarms?		
<b>PART ELEVEN PERSONAL SAFETY</b>			
1.	Have adequate arrangements been made for the personal safety of staff and employees who work in isolated areas?		
2.	Have guidelines been developed for staff to deal with members of the public exhibiting disturbing behaviour?		
<b>PART TWELVE ATTRACTIVE TARGETS</b>			
1.	Have special arrangements been made to protect items of particular interest to thieves, such as food stocks, shop supplies, tools and solvents?		
<b>PART THIRTEEN VEHICLES</b>			
1.	Are vehicles garaged, particularly during the hours of darkness, as a precaution against vandalism and theft?		

## LINKS

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

Data Protection Commissioner

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

Home Office Crime Reduction Site

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

Norfolk Constabulary

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

Trace recovery of stolen art work

[www.dantec.ltd.uk](http://www.dantec.ltd.uk)

Property Marking equipment

[www.top-tec.co.uk](http://www.top-tec.co.uk)

Computer Security

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

Computer Security

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

CCTV Equipment

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

ID badges

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

ID Badges

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

Alarms

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

Fence Toppings

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

Fencing and Cages

[www.jacksons-fencing.co.uk](http://www.jacksons-fencing.co.uk)

Fencing

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

Electronic Perimeter Security

[www.bekaert.com/twil](http://www.bekaert.com/twil)

Fencing

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

Cash Handling Products

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

Anti Ram raiding

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

Security Screens

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

Electronic Intruder Monitoring

[www.redcare.bt.com](http://www.redcare.bt.com)

Alarm Carrier

[Return To Contents](#)