A GUIDE TO BUSINESS SECURITY

GREATER MANCHESTER POLICE

Crime can be managed like any other aspect of business and controlled through business strategies.

It is not just luck that one business suffers crime and another enjoys a safe environment. It is not just luck that some businesses collapse due to the impact of crime.

Whereas no one guide can be totally applicable to every individual business and organisation, it is intended that this guide will give you ideas to interpret and apply in your own personal business environment.

This booklet generally outlines measures that could be taken to reasonably reduce the opportunity of crime. The recommendations are based on current best practice.

Any crime risk assessment should be based on crime trends and patterns, which dictate reasonable, practical and cost-effective measures, that can be incorporated to reduce the risk of crime. There can never be any guarantee that crime will be effectively reduced.

It is strongly recommended that other statutory organisations are consulted, eg Health & Safety, Local Authority Planning requirements, Fire prevention, etc.

The guidance on law contained is not meant to be an accurate statement of the law, but to offer guidance only. You would not be able to rely on it to provide a defence to any criminal charge or civil claim.

BUSINESS CRIME TEAM, GMP

CONTENTS

CONTENTS

RISK MANAGEMENT

Over recent years many businesses have been concerned only with Loss Prevention and not Crime Prevention; as long as insurance covered the loss then only basic preventive measures were taken. To their cost, these organisations discovered that it was impossible to mitigate all the losses from crime with insurance.

Managers have to determine and assess the risk of crime to their organisation and then consider, if necessary, strategies to either prevent the potential loss or reduce it to a controllable, manageable level.

The actual *"loss"* that has to be managed, from a manager's perspective, is anything that may erode the profit or core functions of the organisation.

What are your risks?

There are many security infringements that could have sufficient impact on an organisation to upset a potential financial gain.

Although a major disaster such as a fire is often perceived as the only catastrophe that would seriously threaten the business, even minor *"insignificant"* issues in isolation or cumulatively, can have far reaching implications.

Risks have to be continually assessed. A change of location, change of employee, or even the purchase of new computer equipment can be just a few of the considerations that could effect your risk assessment.

The actuality of crime is not the only consideration. The fear of crime can effect both public and employees, creating a hostile environment.

All employees have to identify the risks that a business may suffer - anything from financial loss to core functions of that individual organisation, in the present or future. After all, it is everyone's responsibility to ensure the success of your business.

How often do they happen?

Many organisations are unaware if they suffer from crime because employees are not encouraged to identify security infringements *(actual and potential)* and management systems do not always exist to measure the effect of crime.

A security register / diary should always be maintained. If details of incidents are recorded, including every associated cost, then these can always be analysed at a later date to discover trends and identify the most effective preventive action.

Although commercial burglaries may be rife in a particular area, most businesses only become aware of a high crime risk when it happens to them. Regrettably, it is only then when most organisations consider crime prevention.

The likelihood of a second or subsequent attack on the same premises within a short time is very high.

The criminals' motivation for the attack will probably remain *(eg new computers will be quickly installed)* and the offenders know there is a low risk of getting caught because they have already succeeded once. In addition, many organisations do not respond quickly to an attack - often the security will only be improved long after the stock has been replaced.

How serious is the event?

Even relatively minor crime incidents can have a major impact on a business.

An example could be a computer stolen in a burglary. In most cases, it is not the actual computer that is of concern *(the Primary Costs),* nor the repair costs to the building or the lack of work achieved whilst a replacement is sought *(the Secondary Costs).* It is the suspicion that others now have possession of confidential business information and also the fear that clients may discover that confidential information has been removed. It would be exceedingly difficult to mitigate any losses against these *"Repercussion Costs"* by insurance, as the effects cannot be quantified.

Repercussion Costs are often the most damaging to a business. Financial loss and employee satisfaction are all destroyed through crime.

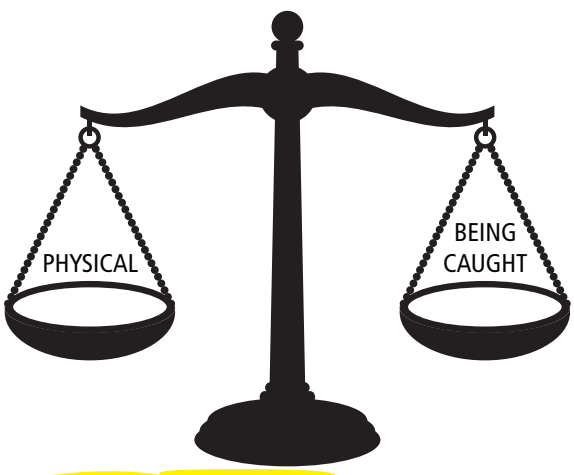
If the chance of a particular crime occurring is very low, and the cost of security measures is very high, then it would be more cost effective to mitigate the loss by insurance rather than meet the high preventive costs. That having been said, the subsequent high premiums, secondary losses and associated inconveniences still have to be considered, as improved security costs may not then be as significant.

Managers therefore need constantly to assess, monitor and evaluate their results *(both achieved and proposed).*

Finding solutions

Detailed throughout this booklet are numerous ideas for managers to interpret for their own situation.

It should be stressed, however, that no one individual measure will prevent crime. Each security measure is part of a system to have an impact by either deterring, preventing or minimising the loss.



This is achieved by creating a balanced prevention strategy in which the thief is delayed trying to overcome physical devices whilst in immediate danger of being caught.

This can be illustrated in the example where one business is protected only by barred windows, locked doors and computers secured to the floor. A burglar could enter the building and spend several hours negotiating the security devices undisturbed.

In other business premises the computers are protected by CCTV cameras, extensive alarm

systems and the natural surveillance afforded by passing traffic. A burglar may simply force his way into the building in a *"smash & grab"* style, and escape before any person could react to the incident.

The solution is to incorporate physical security devices that delay a burglar from committing a *"smash & grab"* offence, but also to install security devices which notify everybody that the building is under attack.

This balance prevention strategy means that they will either give up or be caught *(most thieves will not remain longer than 3 minutes after the alarm has activated).*

WHY ME?

One of the most effective strategies in trying to prevent burglary is to ask yourself the question *"Why would a burglar want to break into my premises?".*

Listed below are a few simple tips to deter a burglar from choosing your business, in addition to the many others throughout the booklet.

Signs

Some businesses unnecessarily advertise to a thief by placing nameboards and signs outside the premises. Examples include warehouses erecting external signs like *"...Computer Chips Ltd"* or *"...Sportswear Ltd".* If there are no benefits to advertising to the public what is inside your property, then don't advertise to a burglar!

Questionnaires

Criminal intelligence now indicates that professional criminals may be targeting businesses from trade information publications. Always be aware of disclosing confidential information, especially about computer systems, hardware, software, and details of senior IT personnel. This information would clearly benefit a prospective thief.

Working Late?

Burglars don't want to be disturbed by workers in the premises. You could trick thieves into thinking you are working late, or that you have staff cover 24 hours a day, by leaving selected lights on around the premises.

These may be controlled by switching devices made primarily for domestic use.

Flat Above?

Many small offices and shops could benefit from making people think that there is an occupied flat incorporated in or above the property.

This tends to be particularly relevant to small shops where they can easily make an upstairs storeroom look like a flat by fitting curtains and timer lights. Even a false door bell push outside labelled *"Flat 1"* can be a deterrent.

Nothing to Steal

If a thief did not want to steal anything from your property, then the level of security would not need to be as extensive.

You can reduce a thief's desire to steal property by permanently marking it in an obvious position *(see the identifiable property section).*

Do not underestimate the importance of keeping valuables out of sight. A computer and printer near a window is nothing more than an advertisement to a thief.

Similarly, cash tills in closed retail premises should be kept open to show that all the money has been removed.

Rubbish

Rubbish can provide a ready source of ammunition for arson attacks.

Even if the fire is not malicious, careless litter and rubbish can easily cause accidental fires.

Your rubbish can also provide a thief with valuable information - not just information which is subject to Data Protection or even confidential lient information, but the waste boxes will inform a burglar that you have new computers and printers.

Carefully consider where all rubbish is stored. If a locked *"out-house"* type store cannot be arranged, consider a lockable bin or skip.

Alternatively lock and chain waste bins, especially wheeled skips, to a strategically placed post away from the building. If the bins were set on fire, the damage would be minimal.

Graffiti

Neglect is infectious. All Graffiti should be removed as soon as possible, thus eventually deterring vandals.

A variety of surface treatments are available which will make any graffiti easier to remove. It is often cost effective to prepare the more vulnerable areas of walls and fences from any future damage.

OUTSIDE: FIRST LINE OF DEFENCE

Making thieves feel exposed when they approach your property can help. People passing by your unoccupied property should be suspicious of an intruder before he attempts actually to enter the building.

Similarly, restricting vehicles from being driven right up to the closed building will greatly assist in minimising your loss. What criminal would want to make several journeys, carrying the stock all the way to a car parked some considerable distance away?

Restricting vehicles from approaching the closed premises also assists in preventing ram-raid type offences.

Although not everyone can control the immediate environment surrounding their business premises, it is still worthwhile considering these points. Staff from other neighbouring properties may also wish to assist in a crime prevention project that would benefit you all, eg a shop's location may not make it possible to restrict vehicles from approaching at night, but staff from several shops could organise security bollards to benefit them all and ensure pedestrians are safer.

Bollards - Standard PAS68:2010

To restrict vehicles approaching your property consider bollards.

If they have to be removable, consider all the different types on the market. There is little point in installing one that would break if a vehicle drove into it.

Raised concrete flower beds make an aesthetic alternative to bollards, as do ditches and even ponds in the right situation.

Fences - Standard LPS 1175

Thorny low hedges and low fencing *(or transparent high fences)* will increase security, as will outside lighting.

Most burglars break into buildings from the back. Good rear fences or hedges, coupled with a lockable side gate will help. The side gates are best positioned level with the front of the building so that they can be seen.

When choosing the type of fence you should consider the view neighbours or the public have of the front and rear of your property. A high fence may be difficult to climb over but can stop people casually observing your business. A low fence is easy to climb over but enables everybody to see a burglar.

Higher security fencing does not have to look oppressive. A galvanised palisade fence can be painted in colours suitable to the local environment.

A weld-mesh fence is similar to a chain-link type, but far more secure. Whilst being too small to obtain a foothold, the many small holes make the fence appear transparent. It is difficult and time consuming for potential intruders to cut the sections.

Barbed Wire

Barbed wire may be used to defend your property, but the law puts certain restrictions on its use. Section 164 Highways Act 1980, says that where on land adjoining a highway there is a fence made with barbed wire in or on it and the wire is a nuisance to the highway, a notice may be issued by the Local Authority for the nuisance to be removed.

Being a nuisance means that it is likely to cause injury to people or animals using the highway.

In practice, most Local Authority Highways Departments usually consider that barbed wire lower than eight feet from the ground could be a nuisance to highway users.

The term *"Barbed Wire"* means anything with spikes or jagged projections so would also include razor wire and the wooden carpet gripper strips which have nails sticking up through the wood.

If the barbed wire is not adjoining the highway and an injury results, you could still be faced with a claim for damages under the Occupier Liability Acts. Occupiers of premises have a duty of care, to people entering or using their premises. This duty even extends to trespassers, although it is not as extensive as it is to people lawfully using or visiting the premises. So a burglar, who could not be aware that barbed wire was on top of a fence and injured himself on it, could have a claim against you despite the fact that he was a trespasser.

If you wish to have some sort of barbed wire protecting your property, it may be a good idea to check with your insurance company that they would cover you in the event of a person claiming for an injury caused.

An important consideration is also people innocently hurting themselves on your barbed wire, eg a police officer checking an alarm activation or a young child trying to retrieve a football. This sort of injury could result in unwelcome media attention and thereby harming an established company's reputation.

Electric Fencing

Electric fencing is not as unrealistic as may be first thought. There are now companies offering this product as a cost effective, viable option. Naturally, the electric fence has to be installed to defined specifications.

A specialist installation company could assist with further enquiries.

Lighting

External lighting must be provided to all areas of the site in accordance with BS 5489. The spread of lighting should be evenly distributed with no areas of shadowing or pooling. Levels should be sufficient to support any CCTV systems in operation in the area.

Fittings should produce *'white'* light, as opposed to yellow/orange light. Metal halide *(or bulbs with a comparable output)* should be used, as these offer superior colour rendition over alternatives such as high and low pressure sodium bulbs.

Lighting fixtures must not be positioned to provide climbing aids over boundary treatments. Dusk 'til dawn lights, operated by photoelectric cell/daylight sensor, should be installed to all external doors.

PHYSICAL SECURITY

Check Insurance

Most insurance companies now insist on a specified level of physical security, detailed in your policy. Check the small print and if in doubt, write to your broker before it is too late. Some insurance companies will even offer a discount to secure premises or security surveys to ensure you obtain appropriate advice.

Doorsets

External doors must be compliant with and certified to BS PAS 24:2012, WCL2, or LPS 1175 SR2.

Any sliding doors should be tested and certified to ENV 1627-30 *(WK2+)*. If circumstances could prevent this, please consult with Design for Security.

Any revolving doors should be tested and certified to ENV 1627-30 *(WK2+).* If circumstances could prevent this, please consult with Design for Security.

External escape-only doors *(as with external doors in general)* should be certified to BS PAS 24:2012, or LPS 1175 SR2. It is crucial that the door ironmongery is permitted for use on these doors under the security certification of the product.

Letterboxes within doors must be located a minimum of 400mm away from internal handle and locking hardware.

Garage or sectional overhead doors must be tested and certified to LPS 1175 SR2. If circumstances could prevent this, please consult with Design for Security.

Doors to individual offices and store rooms should have 44mm solid core doors, 3 hinges, with a mortised sash lock to BS3621/8621 to allow the rooms to be secured when not in use.

Mortise Locks

If you have wooden external doors to your property, you are advised to fit a mortise dead lock that needs a key to open it from either side of the door. If you choose one that conforms to British Standards *(BS3621)* or has at least 5 levers, this should be acceptable.

To disperse the force on a door when someone tries to kick it down, many people fit two mortise locks, widely spaced.

Check the door is thick enough to accept the locks and keep its strength, although it may be better to approach a qualified locksmith for advice.

Bolts

Mortise bolts tend to be more secure than the tower bolts, which are embedded into the door and frame. With a mortise bolt one key fits all. When it is rotated in the keyhole it makes a bolt shoot out of the door itself into the door frame.

They are most effective when two are placed on a door, one near to the top and one near to the bottom.

The key can be used only on the inside of the door, put them on doors that you do not leave by.

Door Drop- Bars

Security devices can be specially made.

A metal girder can be dropped into a horizontal bracket on either side of the door - on the inside, of course. Although it is not normally necessary, this bar can be secured in position with padlocks. It could even be hinged so that anyone could move the heavy bar out of the way.

Fire Doors

Contrary to popular belief, it is usually permissible to fit additional locks to external fire doors. However, when the property is occupied a fire door must be capable of being opened in one quick and easy action. Your life may depend on it!

It is usually acceptable to fit extra locks on fire doors as long as you have an established system to ensure the extra locks are taken off when the first person enters the building and not replaced until the last person leaves.

To ensure that an additionally secured door is always safe, it is possible to secure the door with an electro-magnetic lock which pulls the door into the frame. These aren't as unusual as they sound. They are quickly becoming a very common locking device used with most combination or card swipe mechanisms. The lock is linked into the fire alarm system so that when the fire alarm activates the power to the door is cut off and the door may be opened. If required, a separate push switch can be fitted near the door to allow easy access or egress.

It must be stressed that your personnel safety is more important than the safety of tangible assets. If you are in any doubt that you may be compromising the safety of your staff in the event of fire, obtain advice from your local fire officer.

Some fire doors may benefit from having a separate alarm fitted. Staff misuse of fire doors would then be discouraged.

Gated Doors

To improve the security of an external door, a metal gate could be fitted externally over the door. Similar to a traditional side gate from a house, the gate could offer some of the benefits of a roller shutter.

Roller Shutters

Shutters must be tested and certified to LPS 1175 SR2 *(or SR1 if perforated laths are required),* and installed in accordance with manufacturer's instructions. Dependent on the individual criminal risk to your premises, it may be appropriate to fit metal security shutters.

The consequences of fitting shutters should be explored from every aspect before a decision is made. For example, shutters may be prohibited by local authority planning requirements; they may restrict prospective sales to *"window shoppers"*; they may restrict the public from actually seeing a burglar in the premises; oppressive shutters may, if everyone fitted them, curb legitimate use of the area due to a perceived fear of crime - especially if they become a target for graffiti.

A shutter on the inside of a display window can be more effective than one placed on the outside, due to the fact that the breaking of the glass would activate the alarm before the shutter is forced. However, if it is the window itself that has to be protected from damage *(eg a furriers from attack by animal welfare groups)* then the type of shutter, and its placement, would need to be reconsidered.

Carefully consider the type of locking mechanism fitted. Most shutters would benefit from additional padlocks fitted along the bottom of the shutter, about every 6 to 10 feet.

All shutters should have an alarm contact fitted so that the alarm is activated at the first moment a burglar tries to gain entry.

Windows

Windows must be compliant with and certified to BS PAS 24:2012 or BS 7950.

Ground floor and easily accessible opening windows *(escape requirements permitting)* must be key-lockable, and have fixed/lockable opening restrictors *(not releasable from the outside)* limited to 100mm.

Window Locks

To obtain the correct type of lock for a wooden framed window, try to choose the sort which does not involve any of the window catches. The type of lock that pulls the window into the frame with a key are normally stronger. They may even stop a person forcing the window open or leaning through a smaller window to undo it.

If the opening section of the window is quite large, fit two window locks. Window locks can be supplied and fitted by a locksmith, but most types can be fitted by anybody who can use a screwdriver.

Self-locking window locks are a little more expensive than other types, but may be more convenient to use on windows which are frequently opened and closed *(canteen or lavatory windows etc).*

Louvre windows on the ground floor should generally be avoided. If you cannot replace a louvre window, consult a glazing firm who may be able to secure each pane of glass in each frame with strong adhesive.

Bars

Remember that windows of upper floors are vulnerable to a climbing burglar and one who brings ladders.

Bars should be to standard LPS 1175. There is now a wide range of commercially produced *"bar"* systems designed to protect a window. They range from simple steel bars like something from a prison cell, to subtle folding systems in a variety of colours and finishes which only become obvious when in use. Some businesses have non-oppressive designs fabricated especially for them, incorporating their company logo or name.

Some systems may be folded out of the way, or even removed, when not in use, although this may become a chore that doesn't always get done.

Such protection does not have to be oppressive - they can even be painted white or made a feature *(most cathedrals used ornate designs to successfully protect windows).*

Double Glazing Standards

If choosing double glazed windows, it may be preferable to check to see that it is not just the handle that stops a window from opening. Many windows use a number of bolts coming out of the opening frame into the fixed frame, operated when the handle is turned. You should need a key to unlock the window.

Whether your window unit is glazed from the inside or outside you should be satisfied that the glass cannot be removed without it being broken. A good glazier familiar with UPVC frames should be able to secure existing externally beaded frames.

Fitting extra locks to UPVC or aluminium framed doors is usually beyond the DIY amateur. If the door does not lock along its full length, consult a glazier or locksmith for advice, or ask them if they can do the job.

It is advisable to check with the company which installed the double glazing before fitting any additional locks to windows or doors. Unauthorised fitting may invalidate the guarantee.

Glass

Glazing to a height of 2400mm *(or if otherwise accessible)* must incorporate at least one pane of laminated glass rated as P4A under EN 356. The remaining pane in a double glazed unit may be toughened glass.

Laminated glass is preferable to toughened glass, for security and safety. When broken, toughened glass breaks into many small pieces over the entire pane of glass. Laminated glass will break as normal glass, but will hold in place in the window, slowing down a burglar from entering, or stopping a child from cutting him or herself. The thicker panes of laminate glass are often called *"unbreakable".*

Georgian wired glass is not a security glass - it is designed for fire resistance.

Polycarbonate, a *"plastic"* type of glazing material, is unbreakable during normal use. However, the disadvantages are that most types can be easily scratched and usually discolour with age.

Specialist contractors can fit a security film to most types of existing glazing. Apart from affording protection from burglars and bomb blasts, these can often pay for themselves through energy efficiency.

Doors – Internal Commercial

Secure rooms: doors should be certified to BS PAS 24:2012, WCL2, or LPS 1175 SR2.

Locking internal doors while you are away from the business can sometimes stop a burglar from going further into the property, but in other instances the locking of an internal door can result in a lot more damage if the door is smashed down.

Keys

As with exterior doors consider the strength of the wood in the door and how well the door frame is secured before fitting any lock or bolt.

Don't leave spare keys for your windows and doors about the building. All keys that have to be used during the normal working day should be retained in a secure cabinet designed for that purpose.

There should be strict control of who borrows keys, a trusted employee allocating only that specific key.

It may be appropriate for your business to use only security keys - keys which can be copied only by a designated locksmith under proper authorisation.

Never leave keys in the door locks. This makes it easy for a burglar to unlock them and remove larger items from your property.

Walls & Roofs

Although it is often not very cost effective to replace roofs or walls, weak sections, especially in some modern industrial units, may need additional protection. Walls can be made more secure by cladding internally.

Roofs can be made more secure by incorporating deep eaves. Guttering should be recessed or flush faced. Attempts to gain access to roof voids by removing a few tiles can be prevented by fixing expanded metal to the topside of rafters. In some cases it may be possible to protect the roof void by fixing coiled barbed tapes within that space. Bolt all ceiling hatches from below.

In addition, give consideration to extending your Burglar Alarm into the roof void and internal wall areas.

Post Boxes

Letter boxes give easy access for the both the determined arsonist and the prankster to fire a building.

Specially constructed post boxes are available which are separate from the building. Some now have heat sensors and fire extinguishers incorporated.

Safes

If you wish to protect items of high value, check with your insurance company first to see if they recommend any particular type of safe.

Some safes appear cheap to purchase, but are very difficult to fit. Discussing your needs with a qualified locksmith will help.

Smoke Generating Units *(Standard EN 50131-8)*

Systems are now available that fill an area with thick smoke in seconds when an intruder is detected, making it impossible to see for more than a half a metre.

These systems are designed to keep an intruder out of a building rather than trap a burglar inside.

This type of security device is constantly being improved. There are now several *"types"* of smoke making it possible to install these devices in most environments without it damaging your property or stock.

Fire

Further advice can be obtained from the manufacturers, or approved alarm companies.

With all this security some people worry about escaping from a fire. Good security is designed to stop burglars getting in, not people getting out. Burglars want to operate quietly without being seen, whereas if there was a fire you want everybody to see and hear you.

Fire prevention may be a requirement in law, although it is obviously within everyone's interest to make sure they are safe. If in any doubt whatsoever, always take expert advice.

Remember to be safe as well as secure.

Permission?

Remember that whenever considering the use of any external protection, consideration should be given to any Local Authority planning permission requirements.

Your local Planning Department will offer advice before costly mistakes are made.

ALARMS

Burglars don't like to draw attention to themselves. The sound of an alarm will cause most burglars to grab what they can quickly before making their escape, without exploring the rest of the building.

Choosing the correct alarm system can be quite difficult due to the variety of features available.

Which Type of System?

In a nutshell, there are two types of alarm system: Type A and Type B.

Both types of alarm system should have an automatic cut-off so that the noise does not continue for more than 20 minutes.

· Type A (Remote Signalling) Alarms

A monitored alarm system, also known as a *"remote signalling"* system or *"Police Call"*, is similar to a Type B system, but is monitored by a private central station 24hrs a day.

On activation the alarm system automatically informs an approved monitoring station somewhere in the country, who will notify the police on a dedicated line. You can give a password or code number to stop a false alarm.

Unlike monitored alarms at domestic properties, systems at commercial premises cannot make any audible sound at the scene for 10 minutes. This allows time for the police to attend and apprehend the intruders.

This type of alarm system is particularly suitable for isolated buildings away from residents, or where you do not wish to rely on the assistance of neighbours.

Discuss with the alarm company the various ways in which the alarm system can be protected from attack by a burglar *(eg if the phone wires are cut, will the alarm still activate?).* Enquire about the additional annual charge for the monitoring.

· Type B (Audible Only) Alarms

If a thief sets off the alarm, or you press a personal attack button, it will ring instantly outside whether in commercial or domestic property. This system then relies on someone hearing the noise as it does not signal to a monitoring station or the police.

You are advised to leave key-holder details with your local police. The key-holder may be any person you trust.

The cost of this type of alarm system should be for the installation only, although some customers prefer to take out a service and maintenance contract.

DIY *"Bells Only"* systems are currently available, but make sure that the system you are considering conforms to BS6707. If you are considering fitting an alarm yourself, you should be fully competent in working with electricity. You should also ensure someone else is totally familiar with the system for the occasions when you are not opening or closing the premises yourself.

Most people prefer to choose an alarm company recognised by their insurance company.

Which Alarm Company?

· Type A (Remote Signalling) Alarms

Police will only attend remote signalling alarms installed by alarm companies whose business is subject to inspection by a recognised Independent Inspectorate organisation. Currently, these Inspectorates are:

NACOSS *(National Approval Council for Security Systems)* Tel. 01628 637512

SSAIB *(Security Systems and Alarm Inspection Board)* Tel. 0191 296 3242

AISC *(Alarm Inspectorate Security Council)* Tel. 01704 500 897

IAI *(Independent Alarm Inspectorate)* Tel. 07000 780 831 or 01706 210 999

Integrity 2000. Tel. 01277 262 000

These organisations publish lists of authorised alarm fitting companies.

· Type B (Audible Only) Alarms

The police do not recommend individual alarm companies *(or even "recognised" companies).* Of course, most of the companies that install Type A alarms also install Type B alarms.

What Should I Ask?

Discuss with your alarm company the various ways in which the alarm can be protected from attack by a burglar. Consider a battery backup/pulse line monitoring for the alarm to ensure it continues to function even if the alarm wires are cut. Be aware of signs of tampering. Door contacts have previously been removed/re-positioned or altered to prevent the alarm system being set.

We will only attend alarms installed by companies approved by the two main regulatory bodies: National Security Inspectorate *(NSI)* and the Security Systems and Alarm Inspection Board *(SSAIB).*

The following organisations publish lists of authorised alarm fitting companies in your local area; NSI *(National Security Inspectorates)* Tel. 01628 637 512 www.nsi.org.uk

SSAIB *(Security Systems and Alarm Inspection Board).* Tel. 0191 296 3242
www.ssaib.org

Personal Attack Buttons

· Type A (Remote Signalling) Alarms

Personal attack buttons should not be used as an easy way to summon the police, unless you are unable to get to the phone without putting yourself in danger. A "999" call is always preferable, both to you and the police.

· Type B (Audible Only) Alarms

The only purpose of a personal attack button in a Type B alarm system would be to make a noise, thus attracting attention, and scare the attacker away.

In many situations the noise would scare away shoplifters, attackers, rowdy customers, etc. However, in some situations it could make an attacker more annoyed.

The only answer is to have good staff training. All staff should know under what circumstances it would be preferable to press the button, why they are actually pressing it and what happens when they press it. See the section on Robbery.

Designing the System

Remember to try and achieve an alarm system that will activate at the first stage of entry into your building, not just when someone has actually entered a room. This could be achieved by having alarm contacts fixed to roller shutters, break-glass detectors over windows or, at the very least, detectors in the reception and corridors, etc. The installing alarm company can advise you in this respect.

Passive infra-red detectors (alarm sensors fitted in the corner of rooms) have a red light that illuminates when the sensor detects someone, regardless of whether the alarm system is switched on or not. It has been found that some intruders will plan their route through a building so that they will not activate the alarm. The alarm engineer can easily disable the light without affecting the sensor's main function.

Generally...

Consider an installation contract carefully before you sign, checking all details. Check such things as whether you own or rent the system, the maintenance contract, the cost and whether it could be easily operated by all your appropriate employees.

An alarm system should cause no mess to the decor, since the wiring will be concealed.

All alarm calls should be treated as genuine by neighbours and they should be encouraged to call the police if they see something suspicious, whether the alarm is monitored or not.

Remember that the employees who may be opening or closing the premises need to be fully conversant with the system. False calls will result in the alarm response being withdrawn by the police, which may affect your insurance cover.

Try to avoid false alarm calls. False calls can cause a loss of credibility with neighbours, who may stop taking any notice of your alarm.

CCTV

CCTV can prove an effective tool in reducing crime. Camera positioning, lighting and quality setting are all key considerations for ensuring the images produced are clear and of sufficient quality to allow the successful identification of the culprits.

N.B. The requirement to register a CCTV system with the Information Commissioners Office *(Data Protection)* and the requirement to keep records of its use does not apply to any residential property or any business premise with a CCTV system that has less than 4 cameras. The size of image that your cameras capture determines its use in an investigation.

This is a RECOGNITION size image, the image may be useful for the investigation in terms of showing clothing worn by offender and actions taken by them etc but would not be likely to be accepted in court as evidence of identity.

This is an IDENTIFICATION size image; it shows the offenders actions in more detail and is of a size that would be accepted as proof of identification in court.

Some of the key locations for positioning of cameras are:

Counters/Tills, access/egress points, any cash in transit routes, routes to safes or areas where cash is housed or counted, and any vulnerable or high risk areas.

External CCTV cameras capable of capturing images of potential getaway vehicles or providing further information about offenders and the direction of their travel can be of value.

In terms of robbery, a camera at the point of exit positioned inwards to achieve clear head and shoulder images should be considered essential in order to obtain images of evidential value in court. Criminals will quite often try to hide their identity by wearing, masks, caps or hoods. However, many remove facial coverings on exiting the premises to fit in with the street scene. The access/egress point to the premises is often the only opportunity to obtain a clear facial image.

Cameras which are vulnerable to damage should be protected from attack either by relocation to a higher level and using a bigger lens to achieve the view required, or through the fitting of a vandal resistant housing.

Storage

Home office recommend storage of CCTV data for 28 days.

Local Authority licensing departments may have specific on the storage of CCTV data, so checks will need to be made if you are a licensed premises. If there is a violent incident it may be that there is a late reporting of the incident and it is important therefore that images are

not lost. CCTV can assist in recording valuable information on images captured by offenders during the period running up to a robbery or burglary when the premises were being checked out.

Smaller scale premises may consider clear images recorded for 7 days may need the requirements of the business and financial restrictions. A minimum of 7 days recording is suggested, however systems should be in place to ensure images can be downloaded promptly to ensure recordings are not lost.

Your system should be set up to record with the Highest frame rate & Lowest compression rate that your memory permits for the number of days you wish to record.

Quality

Where a CCTV system is in place staff must be trained in how to download images. CCTV systems *(and lighting that support them)* should be regularly maintained to ensure continuous quality of image and retention.

Regular checks are recommended to ensure the system is working effectively i.e. correct date and time, images recording clearly etc.

Colour systems are advised wherever possible to gather detailed descriptions.

CCTV lighting compatibility

During daylight hours colour cameras can capture good quality images. However, during the hours of darkness cameras can struggle to capture anything meaningful due to the lack of light. Black and white cameras work better at night and can be enhanced with appropriate lighting. Infrared lighting used as an integral part of the camera, will provide a clear image. Consider fitting cameras that automatically switch from colour to black and white at night. Systems should not be accepted unless they can capture good quality images in the provided lighting conditions.

Signage

Signage must be displayed in the customer area advising that CCTV is in operation, it should state the purpose and provide a name and phone number where images can be obtained. Pictorial signage is preferred *(non English speakers).*

Additional considerations

A monitor would provide staff with the opportunity of checking for suspicious people or vehicles, loitering and banned/excluded persons to enable staff to refuse entry.

Screens where visitors can see themselves entering the building can prove effective as a preventive measure. Monitors *(except comfort monitors)* should not be in a position viewable by the public.

The requirements of a CCTV system can vary from site to site, depending on variables such as the purpose of the system, the physical layout of the site, and the available budget to name a few. A useful manual in planning for a CCTV system is the:
Home Office Operational Requirements Manual, which can be downloaded here:
http://www.designforsecurity.org/uploads/files/CCTVRequirements.pdf

SECURITY GUARDS

Although security guards posses no special powers of arrest different from any other member of the public, they can range from someone simply taken off the street and given only a flat cap, to highly trained professionals from established organisations.

A security guard used in the correct environment may not only assist in reducing crime, but can also reduce the fear of crime by reassuring the public and employees.

Security staff can be hired from various manned guarding businesses, or employed directly by the company as with any other member of staff.

Contract Guarding Companies

THE POLICE DO NOT RECOMMEND OR ENDORSE ANY INDIVIDUAL SECURITY COMPANY.

Suggested questions which could be used when enquiring about obtaining such services include:-

- How long has the company been trading?
- What kind of liability and indemnity insurance does the company have?
- Does the company issue written contracts?
- What is the company's vetting procedure for employing staff?
- Do the company's guards have terms of employment?
  (maximum working hours per week, maximum 5 shifts per week)
- What type of uniform does the company use and do they produce identity cards?
- Are staff trained and to what qualifications?
- Will the company sub-contract to a lesser security company?
- Does the company operate a control room or how are staff controlled supervised in work situations?
- Does the company work to an Industry Code of Practice *(BS7499 & BS7598)*
- Has the company independent certification to verify this?
- Can they supply references from companies similar to yourself?

Security Guard Employees

Consideration should be given to a replacement when a guard is ill or on holiday.

Careful consideration should also be given to the consequences from any unlawful arrest. The employers of the security guard may be liable to pay any damages under the principle of *"vicarious liability".*

Dependent on the circumstances, it is possible that the most damaging consequence of any civil action for wrongful arrest may be the publicity and ensuing damage to the company name that such an incident could attract.

IDENTIFIABLE PROPERTY

If your computer was stolen, would you know its make, model and serial number? If you could find the receipt, you will probably be able to find out the make and model. Unless, however, you've made a special effort to write the serial number down, your computer would be no different from the millions of others stolen all over the country.

If the serial number of a stolen item was known, it could then be circulated throughout the country as stolen, in a similar way to a registration number of a stolen car.

Not only are your chances remote of getting unidentifiable possessions returned, but also without being able to prove an item was stolen it can be very difficult to substantiate a charge against a suspect. Arresting offenders isn't difficult. Getting evidence is!

Don't just restrict your list to highly expensive items like computers and their peripherals. Telephones and other electrical goods are just as desirable to a thief.

About the Immobilise.com system

Immobilise is the world's largest FREE register of possession ownership details and together with its sister sites the Police's NMPR (www.thenmpr.com) and CheckMEND (www.checkmend.com), forms a very effective tool in helping to reduce crime and repatriate recovered personal property to its rightful owners.

Immobilise can be used by members of the public and businesses to register their valued possessions or company assets, and exclusive to Immobilise all account holders registered items and ownership details are viewable on the Police national property database the NMPR (www.thenmpr.com).

This online checking service is used by all UK Police forces to trace owners of lost and stolen property. In addition Immobilise is checked daily by a huge range of recovery agencies and lost property offices.

As a direct result of Immobilise there are over 250 cases a week where property is returned or information collected that assists the Police in investigating criminal activity involving stolen goods.

Immobilise is also the only ownership registration service supported by all UK Police forces, the Greater London Authority, and the Mobile Phone Industry.

Ultra-Violet Marking

Available in all good stationers, security shops, etc., are ultra-violet marker pens for about £1.00.
These felt-tip type pens are designed for writing on your property, including audio/visual equipment, in an ink that is invisible to the eye under normal light.

All Police Stations in the country have portable lights that clearly illuminate the writing on such possessions.

By printing your postcode followed by the street number, or the first three letters of your property's name, it is possible to trace an owner from anywhere in the country.

Just a few tips, though. Always mark your items underneath as the postcode can be slightly visible on non-porous surfaces, and try to renew every twelve months. Don't worry about an impending move. Simply postcode your items again. Then the police only have to make two or three phone calls to make to trace an owner instead of two or three thousand.

Branded!

Although secretly marking possessions may be ideal for certain articles, it would be far better to make this identification obvious to a thief, thus deterring the theft in the first place!

There are a variety of systems available, from elaborate branding irons which will emboss your company name or postcode into the surface, to a kit which includes a pre-arranged stencil and acidic paste for neatly marking any surface. Systems don't have to be expensive. Some schools simply make a thin cardboard stencil of their postcode and spray all equipment with a paint which will *"eat"* into the surface *(car bumper paint is ideal for most plastics).* Try it on a sample first!

Photographs

For small items which obviously cannot easily be postcoded with an ultra-violet pen, a picture is worth a thousand words!

Photographing all items against a ruler is better than any detailed description, making it easier to make comparisons with found items.

If you have a video camera with a *"Macro"* lens *(for close-up filming)*, then video record all your possessions.

Not Wanted!

If items are suitably marked so that the true owner is permanently visible, then most criminals would not want to steal them. This has the benefit of reducing the security needed to protect a building.

Forensic Coded Solutions: Liquid

Becoming very popular in recent years is a system of painting a special forensically coded solution over items from large TVs to small computer chips. This solution is visible only under ultra-violet light.

Each batch of the painting solution is made specifically for just one customer and the code of the paint recorded at the Home Office forensic science laboratory. In the event of the property being stolen and recovered by the police, a tiny paint sample is removed for examination. From this swab it is possible to trace the true owner.

Forensic Coded Solutions: Spray

It is now possible to install sprinkler devices in buildings so that if an intruder were to activate the alarm, a forensically coded solution would be sprayed over both the intruder and whatever property he is stealing.

The solution is similar to the paint described above in that it is only visible under ultra-violet light. Warning signs placed around the building are important if a criminal is to be deterred.

Further advice can be obtained from the manufacturers or approved alarm companies.

Asset Records

It is imperative to maintain accurate records of all the company's tangible assets, including make, model, serial number, whether identifiable or post coded and the physical location within the company.

If a stolen item were returned to your business, it would be necessary for you to state whether that item had been sold, thrown away or stolen.

In the case of computers, the asset record should contain details of authorised operating systems and software installed. This, amongst other reasons, enables a speedy recovery after any incident.

COMPUTER SECURITY

Computers are very attractive to a thief.

The theft of a computer can have far reaching implications for a business. It's not just the replacement of the hardware that is the key issue, nor the interruption to the business until it is replaced. It is the fact that any person could have your data and use it for their own commercial advantage.

The Targets

The main targets are:-

· The File Server

The heart of your network is very costly to purchase and often critical to a core business function. It is therefore worth taking extra precautions to protect this one item of equipment.

· The Personal Computer

There are many examples of thieves not stealing the entire unit, but simply stealing the valuable components within *(RAM, SIMMs, processors, hard drives).* It is suspected that staff theft is also responsible for the loss of certain components, especially memory chips *("Chip Dipping").*

· The Laptop

A very portable and valuable piece of property, easily identified by a thief when carried in a public place. Hide its designer case in a plastic carrier bag. The handles can be carried together quite easily. If you have a long walk from a car park to the office, consider dropping your laptop off at reception or returning in your car to collect it on your way home.
Be vigilant in the vicinity of airports and railway stations.

Obviously, these points are also for personal safety reasons.

· The Peripherals

Computer accessories *(especially colour and laser printers)* may not be as critical to your business as a computer, but they are very attractive to a thief. The sight of a desirable printer in the reception area or through an office window may attract unwelcome attention.

Physical Solutions

Always ensure keys are removed from lockable computer cases. There are a number of extra security devices that can physically restrain the computer.

Briefly, these include:-

· Cable Ties

A cheap, low security restraint which attaches the equipment to either furniture, the wall or floor *(a minimum of 8mm diameter cable is recommended).* In general, these do not protect the computer's components, but they do deter the casual removal of an item whilst you are distracted.

· Security Screws

The replacement of existing computer cabinet screws will go some way to preventing *"downgrades"* of memory by employees, but the chip thief may still simply smash a way into the processor unit.

· Lock down Plates

Generally, locking the base of the computer to the desk is more secure than using cable devices. It must be stressed, however, that this device tends only to be effective when used as part of a general security package, eg to slow down a thief whilst an alarm is ringing.

This type of device tends not to protect the internal computer components.

· Entrapment Devices

These surround the whole computer processor unit, allowing it to be bolted down.

Some devices rely on self-adhesive plates to adhere to the desk, but they are only as good as the laminate on the desk.

Models are also available for securing laptops in vehicles or on a desk. Authorised removal is easy with a key.

The security standard LPS 1214 is applicable to entrapment devices tested by the Loss Prevention Council.

· Security Cabinets

These are basically lockable steel safes that house the processor unit, again bolted down for maximum protection.

This device probably offers the most secure environment and is therefore ideal for file servers and critical personal computers.

Computer Alarms

There are a number of electronic devices that can be installed around, or in, the computer:-

· Loop Alarms

These effectively connect the computer to either *"a stand alone"* alarm or an existing alarm system.

· Movement Sensors

Detecting movement of the computer, the alarm activates only when a unit is unplugged. A common type fits into the expansion slot within the computer and contains various devices to detect movement.

It is always wise to check with your supplier that fitting a device will not invalidate any warranty.

· Proximity Alarms

These work on the principle that the alarm sounds when a computer is moved out of a protected area. They tend to be similar to a clothing store tagging system.

Whilst this type of alarm may be effective for detecting someone tampering with or stealing a computer during office hours, their effectiveness outside working hours is questionable.

· Network Monitoring

Where a network exists, it is possible to monitor all the connected computers. However, the systems must be monitored at all times so that a person knows when to respond to an attack

· Data Security

Use a disk lock to prevent unauthorised copying or importing of data which may contain a virus. Make regular back-ups to minimise potential loss in case the worst scenario happens and ensure the back-ups are stored off site *(at least 500 metres is preferred).*

Remember that even if data is not destroyed in a disaster, access could be denied to all staff for as long as several weeks *(as has been the case in recent bombings).* Ensure that you comply with BS 10012:2009 *(British Standard 10012:2009).*

· Data Security Software

There are various companies that can provide 'data recovery' services. BS 1002 is a legal standard created to maintain the privacy of all sensitive personal information held by companies. It outlines how and when you may or may not use data and gives guidance on communicating with customers about their information.

ACCESS CONTROL

Some criminals won't go to the trouble of breaking into your business premises, if they can just walk straight in.

Bogus callers come in many shapes and sizes. They could be men or women, dressed in overalls or suits.

Not having correct access control not only compromises the security of tangible business assets, but it could also:

- have the potential for making staff prone to violent attacks;
- place staff possessions at risk from theft: How often are jackets left on a chair in an office with a wallet in the pocket?;
- increase the opportunity for persons to hide on the premises until the building is closed; and
- increase the opportunity for terrorist attack.

External Entrance

It is good practice to limit the number of outside access / egress points to as few as possible *(see Fire Doors in the Physical Security section).* This would limit the areas to be controlled, thereby reducing the cost.

Reception Areas

In most situations the reception area will need to be staffed, either by a receptionist, concierge or security guard. However, consideration should be given to when the person tasked with security in this reception cannot be present for any reason from a refreshment break to holiday periods.

Whereas personal identity cards may be necessary for employees, no one receptionist could possibly check the identity of every employee entering a large building. They cannot be informed of every lost card, personnel suspensions and dismissals, etc.

It is therefore preferred practice to have a physical device to control access *(a turnstile, self-closing door, etc)* overseen by a member of staff *(to prohibit by-passing the barrier).*

There are many manufacturers supplying aesthetic physical controls. Turnstiles, glass screens and doors have become discreet, non-oppressive in design, without compromising their function of access control.

Control Devices

In situations where there are few users requiring infrequent access, a key controlled lock is cost effective. But for situations with more staff and frequent use, other solutions are available:-

· Coded Lock

A coded door lock can be mechanical or electrical. These require a pre- determined code *(letters or numbers)* to be pressed before the door becomes unlocked.

These systems tend to be effective only in limited use situations not demanding too much pedestrian traffic.

With any lock where all the users share the same code, there will always be potential problems associated with people leaving. Every legitimate user then has to be informed of the new code.

It is not uncommon for the code in a large business to be well know by everyone, employees, paper-boy, window cleaner, office cleaners, etc.

Consecutive or repetitive numbers should be avoided. Codes should be regularly changed.

· Card Swipes

Systems in which a personal identity card is used electronically to afford entry to a building are becoming very affordable and a cost effective option for a business.

The action of using the card swipe can be used to control a variety of security procedures, from simple door locking mechanisms to turnstiles and alarm system control.

The systems available range from the simple to the elaborate. An inexpensive type uses pairs of cards. One is issued to the employee and the other is retained by the employer. The act of swiping the employer's card through the doors for which that particular employee is permitted automatically authorises that employee entry.

More advanced systems are computer controlled and can be used for interrogating the system for a variety of reasons *(eg time keeping).*

In a situation where a greater level of security is needed, a coded lock and card swipe system are relatively common.

Many systems now have had incorporated into them an *"anti pass-out"* facility, which means that whilst the employee is recorded as being in the building their card cannot be passed to someone else for them to also gain entry.

· Advanced systems

As technology has increased rapidly over recent years, so has the number of systems for controlling access.

Automatic authorisation systems that read people's eyes, scan fingerprints, read identification badges from a distance *(proximity readers)* are no longer confined to science fiction.

If a higher level of access control is considered necessary, then the specialist manufacturers can assist.

Visitors

There may be a requirement under various laws *(Health & Safety, Fire, etc)* for your business to record every person visiting the premises, in addition to the common sense need for security and fire safety reasons.

All visitors' details should be recorded and verified, before issuing a visitors' badge which should be easily identifiable from employees' identity badges. On leaving, visitors should surrender their badges and be booked off site.

Visitors should be escorted throughout the building, especially when leaving, rather than be left to wander on their own. This also applies to delivery workers, service repair visitors, etc

Internal Access

Visitors and employees should be excluded from certain designated areas inside the premises. These designated areas *(eg computer rooms, data storage areas, wages department, stock rooms, etc)* may be identified because of the risk from sabotage *(a disgruntled employee),* casual and determined staff theft, or sneak- in type offenders.

STAFF THEFT

Unaccounted losses, often called *"shrinkage",* accounts for an unnecessary amount of lost profit opportunity.

In the retail environment this is often blamed on customer theft - shoplifting. However, an increasing number of studies are revealing that an appreciable cause of shrinkage is due to staff theft.

It is therefore relevant to all business environments to consider the issues of staff theft. It is insufficient to simply ask yourself, *"Do I have a problem?".* It is more appropriate to ask, *"Do I know if I have a problem?".*

Reasons why some businesses ignore the problem may include:

Lack of data *(eg stock control cannot indicate problems until the annual stock-take).*

It is easier to tackle other problems *(eg it is often easier to blame it on a recent burglary or on shoplifters).*

It is not seen as good for morale amongst staff.

It could reflect badly on the company *(eg a bank with dishonest employees could cause adverse publicity)* or it may reflect badly on an individual manager's ability.

Vulnerable Business?

Ask yourself:

- How easy is it to steal from this business? Can staff simply walk away with items? Are they given unrestricted access?
- How acceptable is it to steal? Is it simply seen as a staff *"perk"* and the attitude *"I do enough for them"* prevails?
- What is the punishment? Is the punishment for theft clearly defined? Is theft perceived as a dismissable offence?.

Profiles of Staff Theft

Address the issues of:

- How do staff steal?
- How many staff steal?
- What do staff steal?
- Why do staff steal?
- Which staff steal?
- Where do they steal from?
- Do staff ever get caught?
- What stops staff theft?

Prevention

The most effective prevention strategy for your business depends very much on your own individual circumstances.

On examination of businesses where staff theft has been a problem, certain organisational similarities included:-

- Large amounts of cash & stock;
- Minimal supervision or staff responsible for asset control;
- Minimal record keeping;
- Lax in account reconciliation;
- Documents were not serially numbered and checked.

Generally, you may wish to consider:-

- Improving staff selection procedures *(eg integrity testing, etc);*
- Define the company policy;
- Define employment contracts;
- Develop internal controls *(eg stop check staff leaving, etc).*
- Regular stock checks involving staff.

In conclusion

This very extensive subject has only been dealt with very briefly. It is important, however, that the subject is not ignored. Staff theft should be measured and managed like any other business issue.

ROBBERY

Robbery is a lot more than just theft. In every case of robbery a person has been the victim of violence, or the threat of it, and had to suffer the associated tremendous psychological trauma.

There is no exact formula to prevent the offence, but generally the more security precautions a business has, the safer it is.

You must take into account the many variables which will be found; numbers and dispositions of employees, locations of premises, interior lay-out, cash holding, etc. In the office environment a major consideration will also be access control *(see separate section).*

Although the following tips are more suited to shop premises, there will be many points applicable to office situations, especially those dealing with money or other valuable goods.

Objectives

- Prevent the crime from happening
- Secure the safety of employees and customers
- Reduce the monetary loss
- Effect the arrest of offenders

Section 1 - Before the Hold-Up

- The General Design, ie wide counters, etc.
  - Shield around till
  - Cashier / till can be seen by other staff
  - Personal attack alarm button out of sight
- Low aisles, to see customers around the shop
- People on street should be able to see in *(no posters in window)*
- Staff should have facilities to observe the street from within premises *(description of vehicles before & after)*
- Larger shops. Tills away from each other, but within view
- Employee in rear of shop, able to observe, call police, etc.
- If staff left alone, other staff in rear *(not to leave shop during dinner hour, etc.)*
- Personal Attack button and door bell to other staff upstairs, or code name for less serious incidents - and all staff know!
- No access to / from rear private part of shop *(cheap combination lock, key, or even buzzer on door if access is not from behind counter)*
- CCTV Cameras covering tills and customers at tills, not just at stock for shoplifting *(see CCTV section)*
- Small shop. Consider dummy CCTV, with LED *(red light)*
- CCTV or not, advertise with stickers, especially on the till and door
- If alone in shop building, can you ring the police without leaving shop floor?
- Personal Attack Alarm. Is it a Monitored alarm or just an audible bell? *(Staff should know what would happen)*
- Test alarm by prior appointment with police
- Look out for people surveying the shop, even from a vehicle
- Look out for suspicious cars and vans outside the business
- Keep a pen and paper by till *(suspicious reg. nos., descriptions)*
- Don't keep too much money in till *(why keep £20 notes in till?)*
- Consider secure cabinet / safe under till with *"post-box"* facility for larger & excessive amount of notes
- If till locks, use it when you walk away
- Consider putting till key on *"expanding string"* affixed to each member of staff's belt

- Consider lone member of staff being joined by extra member of staff at closing times, especially when leaving shop to close the shutter, bring advertising board in, going to night safe, etc.
- Lock shop door before removing drawer from till / cash box
- Count money in rear out of sight
- Locking up. Don't leave alone or park in dark car park
- Survey street before unlocking door to leave / open up
- Unlocking. Consider asking a neighbouring shop to call the police if you don't give them the *"thumbs up"* after unlocking and checking the property.
- Avoid fixed and regular routines *(trips to night safe, etc)*
- Don't park regularly in a dark car parking spot - don't put shop name on parking space
- If money kept in safe, still consider above if you carry shop keys.
- Consider cash collection company
- Check security requirements needed on insurance policy
- Talk about Robbery amongst staff *(even rehearse a scenario)* and have ready a PLAN

Section 2 - During the Hold-Up

Extreme caution should be exercised at this stage. There are three types of robbers.

• The Amateur

This type is new and inexperienced, prone to violence because he is nervous.

• The Professional

The committed robber is organised and ruthless, prone to violence in order to achieve his objective.

• The Unstable

This type is usually unpredictable in his actions, which may, for example, be due to a drug withdrawal.

They are all dangerous!

Remember that no person gets paid enough to get injured *(or worse)* in order to protect money.

Make sure you've done the points in Section 1, it's too late during the attack!

- Press the personal attack alarm button only if it's safe to do so.
- Obey the robber's instructions.
- Avoid sudden or jerky movements. Control all movements
- Try to keep calm. Don't increase his adrenaline
- If ordered to fill a bag with money, *"stuff"* money in to fill it up quicker
- Give him small denominations first *(£5.00 notes or even £1.00 coins)* and hold back bigger notes
- Don't volunteer extra money *(a lot do!)*
- Ignore your under counter safe / strong box, unless he tells you to open it
- Concentrate on his description *(you can practice on regular customers and test each other)*
- Note his methods. Every detail aids detection
- If possible look for accomplices / vehicles outside
- If already out of danger *(second member of staff)* then it is important to stay out of trouble, out of the way

Section 3 - After the Hold-Up

Every member of staff should perform specially allotted tasks, detailed below, systematically and quickly.

It is not sufficient just to bring the recommendations to the notice of staff. Constantly remind them and rehearse what each member of staff should do.

- Speed is vital
- When safe to do so, look outside for vehicle leaving, etc
- Telephone the police and be guided by the operator
- Give description of thieves & cars, and means of escape / direction
- Lock up the shop, and ONLY let the police in
- Don't touch where the robber touched
- Don't try to determine the loss at once if it means touching anything
- Preserve anything left behind *(a note, etc)*
- Keep customers involved in the crime on the premises *(if they're adamant about leaving, get their names & addresses)*
- Write down time & details of events. You'll soon forget the smaller points
- Don't discuss what's happened / descriptions, until police have attended
- You can lose your cool now!

GUIDANCE - Websites, resources and references

HSE Work related violence topic: http://www.hse.gov.uk/violence/index.htm

RIDDOR Reporting: http://www.riddor.gov.uk

Information and guidelines: http://www.hse.gov.uk/pubns/hse31.pdf

DTI Employment Regulations 2003: http://www.dti.gov.uk/er/equality/eeragsa.htm

Part Time Workers Regulations 2000: http://www.dti.gov.uk/er/ptime.htm

Working Time Regulations http://www.dti.gov.uk/er/worktimeregs/wtr.htm

(amended 2003)

ACAS Equality Direct website: http://www.equalitydirect.org.uk

Advice and guidance for business managers Helpline: 0845 600 3444 on all equality issues

The Suzy Lamplugh Trust: http://www.suzylamplugh.org/home/index.shtml

The leading authority on personal safety offers advice, publications, training and research.

Telephone: 020 8392 1839

Victim Support: http://www.victimsupport-gm.co.uk/index.html

Union of Shop, Distributive and Allied Workers,

USDAW, 'Freedom from Fear' campaign:
http://www.usdaw.org.uk/campaigns/freedomfromfear/

British Retail Consortium (BRC): http://www.brc.org.uk/

Workplace violence video and training programme 2003

Association of Convenience Stores: http://www.thelocalshop.com

References:

Tackling violence and abuse at work, an employer's guide, fact sheet 9 (2003), London Chamber of Commerce and industry in conjunction with Corporation of London.

Occupational health helpline; 020 7203 1871

Upson, A. (2004), Violence at Work: Findings from the 2002/2003 British Crime Survey, Home Office

Rogers, K.A.; Chappell, D. (2003), Preventing and responding to violence at work. International Labour office

Violence at Work, a guide for employers, (2002), HSE. INDG69(rev) 4/02.

Violence at Work. Facts 24 (2002), European Agency for Safety and Health at Work.

BUSINESS WATCH SCHEMES

An enthusiastic Business Watch scheme will reduce crime

Protecting your business with locks, bolts and bars is fine, but you will enjoy greater security and peace of mind if everyone around you is working with you. Employees and residents in a business community possess a very specialised knowledge of their neighbourhood that even the proverbial *"Village Bobby"* would take years to achieve. A police officer might not recognise someone in your property as a stranger, but an employee or neighbour would.

By letting the police know of anything suspicious you see or hear, you are helping to reduce the opportunities for crime to occur. Even going to the trouble of letting a stranger who is wandering about your area know you're keeping an eye on him helps tremendously.

This is what Business Watch Schemes are all about

Business Watch schemes are about mutual support, being a partnership against criminal behaviour that undermines local business.

Some workers think they should not ring the police when they see something suspicious going on at a neighbouring business as they don't want people to think they're being nosey, intrusive or interfering in other people's concerns.

In Business Watch the participants all agree that they want each other to be vigilant as far as crime is concerned. If you have the phone number of the building next door and you ring up a contact there to check that a suspicious van removing items from the yard is okay, who wouldn't be grateful?

Some schemes have collectively purchased radios so that they can quickly pass on information about suspicious persons, shoplifters, crime trends, etc. Others find it preferable to have a telephone system or text where one person calls another.

Regular informal meetings between partners and the police help establish methods of targeting resources to reduce crime by sharing information.

If you want to start a scheme or find out if one exists in your area, contact your Local Intergrated Policing Team on 101.

THE WAY FORWARD...

Designing out crime

The police have always recognised that the environment around a building, the construction materials used and internal layouts can all influence criminal behaviour.

The police can assist and advise on *"designing out crime"* whilst a building is still at the planning stage.

Design for Security Team (DFS) at police headquarters will provide advice and information for you to incorporate into new or refurbished properties.

Design for Security is a design-led crime prevention consultancy based within Greater Manchester Police. The practice specialises in design-led crime prevention in the built environment.

They are a small team of professionals with backgrounds in planning, surveying, design and the development industry, and are accredited by the National Police Improvement Agency (NPIA) to deliver crime prevention, and 'designing out crime' advice. Everyone is entitled to live in a well-designed, safe environment where the quality of life for individuals and communities is not undermined by crime or the fear of crime.

What they do

They work with local authorities, housing associations, architects, landscape architects, planning consultants and developers to support the production of designs that address crime and security issues and minimise future opportunities for offenders.

They bring an added perspective to a design team, one that:

- Understands the competing considerations and trade-offs involved in design decision-making
- Ensures balanced advice and intelligence-led solutions that relate to a development's context
- Supports innovation and creative thinking

In Conclusion

Detailed throughout this booklet are numerous ideas for managers to interpret for their own situation. Each security measure is one part of a system that either deters, prevents or minimises the loss.

Remember the importance of creating a balanced prevention strategy in which the thief is delayed trying to overcome physical devices *(locks, bolts, bars, etc)* whilst in immediate danger of being caught *(alarms, surveillance, CCTV, etc).*

This balanced prevention strategy means that a burglar will either give up or be caught, thus minimising the business loss and increasing the profit or service.

Crime prevention will then save money.


GREATER MANCHESTER
E II R
POLICE