SPECTRUM iD
Security & Identity Products

A Guide To Buildings & Property Protection

An review of risk assessment for residential, educational and business properties.

Produced by
Security & Identity Solutions Ltd

Edition 1 | SEPTEMBER 2020

International Professional Security Association

Membership body for the wider security industry.

www.ipsa.org.uk

A Guide To

Buildings & Property Protection

The aim of this eBook is to give an objective view of the varying methods that may be used to reduce risks to buildings and property.

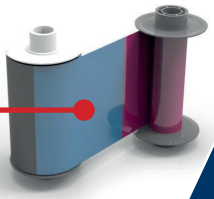
The information provided in this publication is for interest reading only. It has been drawn from experience and publications that may no longer exist. Should you find information that is out of date or incorrect, please email: *info@spectrumpositive.co.uk*

We will endeavour to update and add to all the information in following editions of this guide. A section on the use of drones and their use as a security device is already under review. If you wish to add further information please contact us. As this is a free publication, no monetary recompense will be offered.

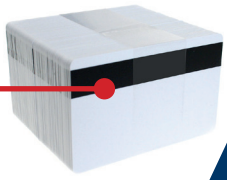
CONTENTS

Photo ID Card Printers
Single-sided
Double-sided

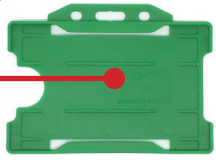
Printer Ribbons
Laminates



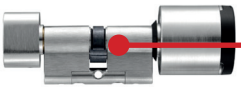
Plastic Cards
Coloured Cards
Pre-Printed



Card Accessories
Lanyards
Card Holders



Tap an image for further details or to order any of these products visit our website: spectrumid.co.uk



Security
Access Control
Bio Security

Scanners & Plotters

Staff Photo ID Card Bureau Service

SECTION 1 AN EVALUATION

This section looks at how an introduction of security measures in the planning stage of a building may be an advantage as the reality of integrated security and facilities turn new and old properties into being ‘intelligent’ buildings.

Ever since the dawn of mankind our forebears have carried out risk assessment and access control methods and one could say have used primitive CCTV by using their eyes to observe and intelligently analyse the resulting images.

Our distant relatives built their wattle and daub huts and villages on embankments, so that other individuals or groups would have to encounter difficult terrain before being able to reach the villages and possibly attack the occupants.

As the centuries passed and wooden forts replaced the wattle huts, we still had to have an understanding of the best place to build our fort and utilise the surrounding land to give the best all round view as well as allowing the best utilisation of nature and the elements for the provision of drinking water, food and wood for fires.

Time waits for no man and the technology of building with stone was developed, resulting in the many beautiful castles, cathedrals, civic buildings and other constructions that we have in Britain, and around the world.

Although the materials of our buildings were changing, the same principles still applied to new developments. We still risk assessed the area where we were going to build, to ensure that it had the required natural elements of water and wood and that the building area was not open to easy attack.

We made access into the interior of the building difficult with moats, drawbridges and the occasional dropping of boiling oil for our more persistent relatives. We maintained our CCTV-type presence with our lookouts who were placed at various vantage points around our hill forts and later with homes and castles.

As technology and time moves on, we start to formalise different ways of protecting our areas of occupation. Many of the practices that have been implemented have come from our military experience over the years and also from the police services.

Individuals with experience of the military and police services, sometimes both, have mostly provided the basis of what we now recognise as hopefully, best practice within these areas.

Eventually, we arrived in the 21st century, a time and place in which our forefathers could, and probably would, never have invisaged. With the arrival of sophisticated electronics and computers, the world has changed far beyond anyone’s comprehension and continues to do so at an alarming rate. If the 19th century was the industrial revolution, the

20th century must surely be remembered for the evolution of the motor vehicle and computing power.

It is from this point that I shall endeavour to describe and analyse our current position with a look at the future too.

Before we look at the physical side of our risk overview – our bricks and mortar part, we need to ensure that any policy that has a bearing on the security of a site, area or premises has the full backing of the company management from the boardroom down where applicable to the property.

Every tier of the workforce should be involved in implementing the security policy of the company, ensuring that the safety of the workforce is paramount and that the buildings and assets of the company are as free from risk as can hopefully be achieved under normal trading conditions.

If our premises is a new-build we may be at an advantage, as we can install into the fabric of the building many security features as part of the ongoing project. Most buildings are already existing so one has to take a good look at what may not be considered a satisfactory position from a security point of view.

Before we start any form of risk assessment, we first need to ask ourselves many questions. Why are we doing this? What does our company make, produce, sell, market or otherwise have an interest in, to make us the target of theft, burglary, or come to the attention of activists in their many forms? Do we hold high value goods or is our stock low value but easily saleable? There is a simple answer to these questions and that is that someone, somewhere, will find a market for our goods and products, no matter how peculier or seemingly useless to the general public they may be. Alternatively, are we dealing with a far more precious commodity – people?

When planning where to site our new premise, we must decide if it will be a new-build or should we lease or buy an existing building.

Our hypothetical company might have a mix of old and new buildings, fences, walls, gates, private occupancy, in fact, a bit of everything that we normally associate with an office, manufacturing facility or school on a fairly large scale.

To enable us to formulate a security plan for our site we should start by undertaking a risk assesment of the local area, as well as the site.

We should start our initial review by looking at the surrounding area for approximately a mile around our prospective site and look at the social aspects of the areas. Is the area run down, or is it well looked

after, with nice housing, good roads and general environment?

We should also see what the local crime level is and of what nature. It is also advisable to talk to other local property owners, so that you ascertain what problems they suffer and if a joint approach may help alleviate the worst of the difficulties.

Also, we should see if there is good access by road to our prospective premises for us, as the users of the premises and also for our suppliers and deliverers of our product. For example, is a motorway within easy reach of our site? Whilst good roads and other transport links are vital for us to conduct our business, they also allow any prospective villain a quick getaway should they target our premises. It's a choice of two evils.

As we normally have no control over the layout of the surrounding road interstructure, we must ensure that we take any factors, like roads heading directly to our premises, in our risk assessment, so that we take satisfactory measures to reduce potential risks. Are there stretches of pavement adjacent to our perimeter, or is there any public right of way through our premises? If so, are we able to have these rights of way redirected through a safer route, or if necessary, closed with the permission of the correct authorities?

We will start our look at the physical assets of our premises by looking at the perimeter of our site and evaluating structures like; walls, fences, tree lines, gates and other methods of access that may be used to help ensure the security of our site.

We will also be using a layered (onion skin) approach and we be working from the outside in, the exterior of the site, through the roads and landscape, to the outer skin of our buildings, being the first things to come under examination. We will examine all the further features of our site, also in a layered manner, to try to ensure that all areas are covered from a security perspective.

As buildings and companies evolve, it is important that the security measures that are in place, are constantly evaluated to take in past and recent developments.

SECTION 2 PERIMETER SECURITY

The site under assessment should have a defined perimeter, as should each development within the site. A defined perimeter may be established by the use of walls, fences, hedging or through the use of symbolic barriers. Perceived changes in surface colour, rumble strips or similar devices, or a combination of those may achieve a symbolic barrier.

Symbolic barriers can be highly effective. The objective is to clearly define *private areas* and to make an unauthorised person entering the area feel vulnerable and exposed.

The physical security of any site has three distinct aspects; the perimeter, the external protection of buildings within the perimeter and the protection of specific vulnerable or sensitive areas within buildings. In theory it might be assumed that totally effective perimeter security would obviate the need for the other two stages but in fact they are interdependent. Whilst it might be theoretically possible to render a perimeter virtually impenetrable, it is rarely possible to do so in ways that are socially acceptable and affordable. Perimeter security is then intended to define a boundary, to prevent casual intrusion and make deliberate intrusion difficult and conspicuous. Doing so, generally involves the use of gates, fences and walls. Your site's perimeter is your first line of defence, even if it is only a demarcation line. You may find it useful to study perimeters under the following areas.

Boundaries and natural obstacles

Site owners are often vague about the exact lines along which their property start. The first question must be; exactly where is your boundary? The answer to this question is of considerable importance, not only in clarifying what you are seeking to protect but also in establishing your legal right to erect obstacles or to limit, control or prevent entry along your perimeter line.

Next, do you actually want to protect *all* of your land (this is not a pointless question)? Many managers use up their security budgets by fencing in large tracts of open space that has no intrinsic value to them when they would be better employed in defining the perimeter of their essential or sensitive assets and concentrating security resources there. By all means, a simple demarcation fence and or warning signs or disclaimers can be used for outlying areas but do not waste money, energy or other resources, on an area that has no true value beyond that of undeveloped land.

Before planning expensive man-made perimeter obstacles, consider

those that nature has already provided. As an obvious example; a facility located on a cliff edge may have little or no requirement for a fence on the cliff side. Keep in mind though, that many apparently natural *obstacles* are friends more to the intruder than the defender. For instance, the tree line which conceals, or the river which lulls you into thinking that nobody will swim it. The basic principle of a perimeter fence or wall is that to bypass it, you can go over, under, through or around it.

Landscaping

It is important that landscaping is complementary to the other security features of the development and does not obtrude on the natural surveillance of the site so that any unauthorised person remains clearly visible. For example, trees when fully grown should not mask lighting columns or obstruct the view of doorways or windows which may be points of entry. The judicious use of prickly shrubs and thorn hedges will help ensure that callers use only the designated routes around the site.

Walls

Walls may be constructed from a number of materials, traditionally erected from stone or brick, cast concrete structures are also used. Walls that are erected or adapted to have a security usage, should ideally be a minimum of eight feet high and be substantially built.

We have used anti-bandit mesh as a security measure in partitions in banks. This can also be fixed to the face of the inner skin of blockwork which will give a higher level of security. Any long runs of wall will require additional support by the use of buttresses at approximately four metre distances along any stretch.

The structures should have a base thickness which is wider than the top of the wall and be of a tapered construction with the top of the work being a minimum of, or equivalent to nine inches (225mm) of brickwork and the material should be set in cement or an equivalent bonding material. Additional security features may also be added to the top of the wall, such as barbed wire, razor wire or other devices. The local council planning department should be consulted before any fixture is permanently added to a wall, as it might contravene planning or health and safety regulations and may be considered by the planning department as a danger to the public. Decorative areas on any wall should not if possible allow toe and grip holds which might allow a person

to scale the wall by using the patterns or the texturess as a climbing aid.

Many wall styles and heights could be used to blend into the architecture and the surrounding environment. The important factor is that all structures should be well-maintained and kept clear of trees and rubbish that could be used as a climbing aid to scale walls.

Any wall or fence should have at least a six-foot clear area on either side to provide clear vision.

Fencing

There are many different types of fencing, all with different degrees of effectiveness within a secure environment. We shall overview the subject from possibly the least applicable for a secure environment, through to what may be considered, fairly state-of-the-art fencing, incorporating electronics and other features. Fencing comes in different grades and heights and in some circumstances, planning permission may be required before its installation. It is advisable to check with your local council planning department before ordering.

Chain link fencing

This is normally plastic or galvanised-coated thin wire, easy to cut and pulled out from posts and it easily collects debris and rubbish blown in the wind. The bottom of the wire is sometimes encased in a concrete ridge to assist stability but is prone to rusting if the protective coating is old or damaged. The mesh is normally supported on concrete or angled iron posts, normally at a height of six feet with angled extensions that may carry barbed wire or tape which is often used to give additional height.

Timber fencing

This tends to have high maintenance costs, is frequently stolen but can impede visibility from outside.

Quick-thorn hedges

May be used initially in conjunction with other forms of fencing, which may be removed once the hedge has matured. Low maintenance costs.

Tree lines

Any use of trees to protect the perimeter of a site is a false judgement. The area may look secure from a distance but as any youngster will tell you, not only are trees good fun to climb, they also provide easy access

to a site by the use of climbing. The use of a rope as a swing can also be used as a method of gaining access to a premises. Any tree line should still be fenced and any branches that extend over the fence line into the adjoining property which are substancial enough to support someone's weight, should be lopped back to the outside of the fence line, to a minimum length if practicable.

Weld-mesh/Expanded metal

This is difficult to scale without aids, effective against all but the most determined intruders and available in a range of gauges and strengths. It may be considered unattractive in appearance although the planting of low shrubs can soften the look.

Steel palisade

A very substantial but costly barrier. It may be used effectively along vulnerable stretches of boundary, partically in places where unauthorised vehicles are known to be driven onto the site. Rather than consider it for the perimeter of sites (a reduced cost option) which has proved effective, one could provide these fences closer to the building and therefore close off concealed areas or irregular building perimeters.

Steel palisading is normally constructed by using vertically fixed steel rods, or sheet steel sections, which have been pre-formed into the required shape. The sections are welded or riveted onto horizontal bars, which are supported by steel posts.

Each vertical strip may be split at the top and each bar sharpened and turned out to provide a deterrent to climbing. The posts and fencing strips may be galvanised or plastic coated and possibly embedded in a concrete ridge for added stability. The sections are available in varying heights and section thicknesses. Normally erected on site, the finished fence is difficult to breach and provides very few, if any, holds for climbing. As with all types of fencing, it has both advantages as well as disadvantages. The advantages include, moderate to low maintenance, swift erection, difficulty to breach, difficulty to climb, allowing outside vision and have possibly a more acceptable nature than other types of fencing. Its disadvantages are, high initial costs and a tendancy to collect wind-blown rubbish and vegetation.

Barbed wire and razor wires may be used as a deterrent. If the use of such methods is contemplated, care should be taken in its use with regard to the Highways Act 1980, Section 164.

Planning authorities should be consulted for their view on the use of such deterrents, especially if the wires are intended to be used along the side of any section of highway or pavement.

Where fencing is used to protect a high security environment, the physical presence of the fence line is often not, in itself, sufficient and a number of additional methods may be implemented to add more protection to the perimeter line.

The use of electronics to add an extra level of security at this point may be implemented by alarming the fence line. This may be achieved in a number of ways, such as; geophonic sensors, continuous wiring, proximity detectors etc.

Infra-Red Beams. A beam of infra-red light is projected across an opening and any movement or disturbance of the beam will create an open circuit state within the receiver and thus, alarm the system. Infra-red is suitable for outdoor environments. as it is not affected adversely by fog or rain.

Geophones – a device which picks up vibrations transmitted by a person's footfall, may be incorporated into the fence line, although wind-blown vibration may also cause an alarm state.

Fibre optic detectors consist of a fine fibre optic tube through which light is passed to a receiver. Any interruption in the passage of the light, such as a breakage, will result in the receiver activating an alarm state.

Continuous wiring may be threaded along a fence line. The wire, in a constant state of tension, with an electric current passing along its path, should there be an interference with the current, possibly by voltage drop or other means, will activate the receiver and create an alarm state.

Alarm states may be registered in many ways – bells, gongs and sirens have all been used in the past and in some situations, still present the best method of warning that an alarm state has been activated.

Central monitoring stations receive alarm calls by telephone, autodiallers, radio signalling and British Telecom Red Alert. These are methods that have been adapted for the notification of alarm states. Although many of these technologies are still in use and look likely to be used for some time to come, we now have the advent of more advanced computing and mobile phone technologies. These mean that the alarm state is often now brought up on a manager's computer, mobile phone or Personal Digital Assistants (PDAs) as well as the more traditional methods.

Any gates fitted within the secure line must have an equivalent security value as the wall or fence that they are part of. If the gate is of a lesser value in security terms, it compromises the complete security of the site.

A gate should be of a material that is able to withstand a high level of abuse as they often undergo stresses, not only in it's normal operation, but also from being swung on and often struck by vehicles. A gate should maintain many of the values of the main wall or fence as in the same height and difficulty in passing – either by going over or under, or even through any spaces in the bars, if of that type.

As the gates become larger and the weight goes up, it brings with it the additional problems of ensuring that adequately sized hinges are used to support the gate. Hinges should be fixed in such a way that the gates are not able to be lifted from the hinge pins. A large gate may require a support wheel on the front inside face of the gate to provide a better closing action.

From a security point of view, single gates are better than a pair of gates. Paired gates are normally used on main entrances. From an architectural point of view, they often look better than a single gate. If the gates are large they may be opened hydraulically, with the operating system buried in the ground, or they may be opened automatically by the use of a magnetic field system. The top meeting edge between pairs of gates is often the weakest point and if the gates are levered at this point, they might buckle and ruin the fundamental structure of the gate. The use of a vehicle and chain has the potential to destroy the security value of any gate. Should the gates be attacked and pulled from this point, with such great forces acting on the gate, it has little hope of escaping without damage. If the gates have to protect a large opening, sliding gates are possibly the best option. When they are opened, there should be sufficient space for the retracted gate to slide safely and securely within the protection on the wall or fence line. Single gates that are not used on a regular basis should be padlocked shut with a good quality short bar padlock, which if possible, should be protected by a steel box welded to the gate into which the padlock sits, thus protecting the lock from physical attack. Should a single gate lead onto a section of the site that is relatively unused, such as a picnic area, the gate and the lock should be part of a regular security patrol route. The practice of locking gates with a chain is not good security practice as it allows for easy attack with a tool such as a boltcutter. Also, a strong bar could be inserted into the links of the chain to provide a point to apply a twisting

and levering action and applying strain on any lock that is being used to completing the loop.

Should a sliding bolt be used to secure the gates. often the padlock passes through a hole in the end of the sliding bolt. This often leaves the padlock bar accessible to attack from bolt cutter or levering. A possible method may be to have the entry hole for the lock secured on the inside of the gate, behind a steel plate where the padlock might be afforded some level of protection.

Professional guidance has advised that, “Whilst gates should be locked to prevent unauthorised access by pedestrians & motor vehicles whilst the premises are unoccupied, it is recommended that the fire brigade should be consulted on the locking mechanism. This is another reason for use of a padlock as the fire brigade require access in an emergency, they are able to cut the lock. They may otherwise resort to knocking the gates down. It may also be advisable to consult the local police to seek their view in respect of their patrolling officers.” Gates, as with fencing, should have additional security added by the use of similar electronics to that used within the fence line.

Pedestrian access/egress

If people require to use our site, we now need to look at how we control allowed access to pedestrians and vehicular transport. Firstly, we need to look at; ways of distinguishing staff from non-staff, pedestrian and vehicle traffic and also the control of trade and or, building-maintenance vehicles.

We also need to look briefly at the number of technologies which we are able to use to control site access, looking at pedestrian access first. Any one of the following methods may be used, depending on the traffic volume and the time scale that individuals will have in entering the site.

We could exercise no controls at all. This is not a recommended action as it breeches health and safety regulations and does not allow for a headcount in cases of fire or other emergencies. Alternatively, a pass could be shown to a security officer upon entering and collected and signed for at the gate-house of the site.

A gate or turnstile could be opened by use of an electronic device such as a card with a magnetic code written into its stripe. A proximity card or tag, where electronics built into the card recognise the signal frequencies the master electronics send out could also be used. The number of passes on entry and exit can be collated by a computer to

have an accurate headcount of the number of individuals who have passed through the controls at any given time. Some systems may also record which control points are in use, the date, time, passcode and other relevant information deemed a requirement by management. The systems are normally devised to stop individuals trying to cheat the control by *tailgating*, i.e., two persons entering or exiting in one operation of the control point.

The way people may access or egress the site should be devised so that everyone has to pass the control point. Any passes held by staff should be distinguishable from non-staff passes and any expiry dates on both types of passes should be legible and checked frequently.

Vehicle access/egress

All vehicles entering the site should either have a staff car pass, a visitor pass, or a contractor pass. Whilst staff passes may run for quite a period of time, visitor and contractor passes should be for a maximum of a week for contractors and daily for visitors.

Should there be more than one individual in a vehicle, they should all be required to hold individual passes in addition to the pass issued for the vehicle. Vehicle passes should not be transferable between vehicles.

It will depend on where the control point is situated within the main site as to where the vehicle occupants will be required to show their passes. Methods of controlling the entry and exit of vehicles often require a removable physical barrier to block vehicle progress. It will very much depend upon the level of security required as to the chosen method used and the higher level of technology used will reflect in the installation and running costs of the whole system but the more sophisticated the system, the more can be expected of it as a site management tool.

The more usual of the entry and exit systems are:

Lifting pole – hand or motor operated. These are relatively weak and require sufficient headroom.

Slewing pole – hand or motor operated, requiring the swing arc to be clear of obstructions – weak.

One way plates – metal plates set into the ground which will pivot when pressure is applied by a vehicle's wheel. Only allows access in one direction.

Rising step barriers – undoubtably the best of the barriers, set flush into the road surface. When operated, the barrier rises to form a solid barrier in front of vehicles. They may rise to two feet in height and models are available that will resist entry by large vehicles. This system has varying methods of control.

Power operated gates – double gates, sliding gates and occasionally a portcullis-style gate are all available. The methods of operating vary from the simple hand operation, to the use of movement sensor and CCTV. Other methods include; magnetic loop, keypad, radio tag, swipe card, proximity card amd mifare/chip card entry systems. As biometrics become more widely used, they will perhaps take over from some of the more traditional methods of identification, or at least compliment them in providing a system which gives increased management data.

Standard gate types – operated by hand in the normal manner. Whatever method is chosen will be selected as to the level of security required. All systems should have regular checks for damage and operational efficiency and have a good standard of maintainence applied to them.

Security Services For
Now and in the Future

WE SUPPLY

Corporate Hospitality	Hospitality	CCTV Operatives
Traffic Management	Stewards	Event Stewards & SIA
Night-watch	SIA Licenced Officers	Signage
Patrol		Response

Custom made Requirements & Plans | **Fully Insured & Protected**

CONTACT COMET SECURITY GROUP LTD 24/7

Get in touch for a **FREE** No obligation consultation.

01495 740194 / 07566 854256

security@cometsecuritygroup.co.uk

www.cometsecuritygroup.com

Unit 9/10 Waterside Court, Albany Street, Newport, NP20 5NT

SECTION 4

THE GROUNDS

Although we do not have the ability to influence the layout of the roads around our site we can apply influence on the immediate road infrastructure within our site. The use of any roads that are not used for a useful purpose should be restricted by a barrier. Roads which lead up to your site should be clearly signposted so that visitors do not have to drive around private areas of the site in a bid to find reception or visitor parking.

Staff parking should also be well signposted. The parking of staff vehicles should, if possible, be separate from visitor parking and all vehicles should be at a sufficient distance from the building to prevent stock or other articles being stolen from a vehicle's rear door or open window without security observation.

"Most every commercial premises includes the provision of a car park but vehicle security is often overlooked. This is despite the fact that theft of and from vehicles, accounts for a large proportion of recorded crime.

"It is vital that the vehicle owners or staff should oversee car parking. Failing this the area is fairly inaccessible to intruders. When planning surface car parking it should always be within the natural surveillance of the surrounding buildings. Parking spaces should be arranged in straight rows to prevent the creation of blind spots, and well illuminated at night with no pools of darkness.

"Underground and multi-story car parks should be designed with bright reflective finishes and a high degree of lighting, which should illuminate both the bays and the driveways.

"Staircases should be well light, to minimise the incidence of assault. There should be no uncontrolled access from the underground car parks into buildings. Gates or barriers are essential at entrances and exits. CCTV is now often used in car parks to observe any cases of damage, theft, or other events such as joy -riding after the car parking areas are vacated".

Lighting

"Lighting is a proven deterrent to crime but is often a neglected in commercial developments. Even with the smallest projects, lighting should always be provided to illuminate vulnerable areas, contributing to the protection of property and the personal safety of individuals.

"The objective with larger developments should be to provide an agreed level of illumination consistently over the whole site with

vulnerable areas subject to special attention. It is not sufficient to rely on street lighting for security, as this will be designed for traffic management and road safety. The rear of buildings will often be in darkness. Lighting is a complex subject and the guidance of a specialist in the field of security lighting should be sought to give correct impartial advice".

Bollards and curtilage

If it is possible to have a raised curtilage around the building it may be an advisable method of preventing vehicles being driven into the walls of the building. Any gaps in the curtilage should be kept too narrow for a vehicle to gain access to the outer-skin of the building, except in the case of loading bays with double or shutter doors.

If curtilage cannot be of such a height to prevent a vehicle gaining access, the use of bollards set into the ground may be considered at the front of buildings. Bollards, which are able to be raised from being flush with the road surface and operated, either by hand or magnetic loop or radio frequency tag, are available and may provide a solution to the protection of vulnerable areas, such as double doors, from forced entry by ramming. Steps up to the front entrance of a building may also be useful in this scenario, although consideration should be given to those aspects of Health & Safety and the routes used by persons who have to evacuate a building in the case of an emergencies, such as fire or explosions.

Another very important consideration is that safe access or egress must be provided for individuals who suffer from any disabilities. Their needs are paramount by law.

Also, with the regeneration of many parts of our towns and cities, it may be prudent, as with so many other areas, to consult local council planning to ensure that they have no objections to your plans but also to ensure that the installations planned will compliment the work and appearance of adjacent street furniture.

SECTION 5

BUILDING EXTERIOR

The outer skin of a building may be made from many different materials depending on the age of the building, the envisaged use of the building and the environment within which the building operates. Through the ages, the building materials that have mostly been used have been wood and stone, with many early houses being made from timber, wattle and a mud infill as in many old black & white timbered houses to the cut stone that was used in the construction on our many impressive municipal buildings and churches.

The materials and mixes of materials that have been used over the years has moved and progressed rapidly over time and the use of iron, steel and sometimes plastics, have all brought the construction of homes and factories into the twenty-first century. The one common component of the everyday building we all use is the humble brick as it comes in many shapes, colours and hardnesses. It, along with concrete block, is the main material used in the construction of most forms of building today. As it is durable, strong and takes a great deal of stress if the building is constructed correctly, we must not forget the use of poured concrete, as that method of building, in conjunction with steel bracing rods, provides extremely strong wall structures. Although not always nice to look at, the outer surfaces can be covered or treated, to give a more visually appealing appearance.

We are able to construct a box which, from a security point of view is good, nothing and no-one is able to get in or out of. Unfortunately, the solid box is of no real use to anyone!

If we use brick as the main component of our building construction so that the building has only single brick walls around the structure, it will be able to bear a certain amount of weight in a direct downward direction. However, it is not able to withstand attack from the side by any form of striking, as in a blow from a sledgehammer and the wall will disintegrate under a constant attack from such methods. The use of concrete blocks for the inner walls of our building, built in such a manner that steel or plastic ties are used to connect the inner and outer walls, gives greater stability to both walls. A gap of approximately four inches (100mm) between the brickwork that is used for the outer face of our building and the concrete block interior walls, is also needed. It is a requirement that this cavity, which is part of the damp-proofing, exists, as it is also used to house the polystyrene sheet that performs as an insulator for the building. If a high-security value is a requirement to be implemented in the construction of the build, the cavity may also be

used to accommodate steel mesh to prevent access through the walls should the outer skin of the wall be breached by some method.

When we consider the type of concrete block to be used in our structure, there are many and varied types, depending on the requirement of our build, which may be used that vary from the very heavy block, for strength, to very light blocks with thermal qualities. For our security values to be preserved, the use of heavy, strong block is recommended for all outer wall construction with the lighter block only used for interior work. Once our building shell has been completed, we will hopefully have a design that is both aesthetically pleasing and structurally strong. We now look to further this by adding windows, doors and the other details that are required to make our buildings work.

From our early stone-based buildings up to today's steel, brick and block structures, the need for windows and doors to be made sufficiently strong remains the same. Although windows, by their very nature, are the weakest point in most buildings, by implementing good practices, maintaining good quality structures and locking mechanism's the risk can be minimised.

Moving on to other aspects of our building, we need to look at methods of transferring rainwater to prevent pooling and water ingress to our property and the potential security problems that may possibly be compromised.

The use of drainpipes and guttering to remove and divert rainwater can cause difficulties, especially on older structures where they tend to be made from cast iron. Where individuals utilise the pipework to gain access to a property or rooftop, the application of anti-climb paints can deter individuals from using this type of drainpipe as a climbing aid. On some new-builds the drainpipes are sometimes built within the structure of the buildings, thus avoiding this problem. Most new buildings that use external water drainage use plastic pipes for the drainage. Using this type of pipe for climbing can be a problem as it is sometimes possible to build a weakness into the pipe structure so that if any weight or force is applied, the pipe joint will fail and the pipework collapse. This approach to the potential problem of drainpipe climbing may not hold up in court under current Health and Safety law, should someone be injured.

Roofs

A considerable amount of costly damage is caused to roofs by children who are playing as opposed to trying to commit a crime.

Problems are often exasperated by many roofs being easily accessible, often due to adjacent canopies, bin compounds or other building features. These features should be eliminated at the design stage in new buildings and existing problems should be addressed by moving or modifying any features that afford easy *staircase* access to the roof.

If possible flat roofs should not be used within your structure, although in practice, this is a virtual impossibility as many existing structures have flat roofs as part of their integral build structure.

Another problem that may arise at roof level is that of skylights – a common target for intruders. By their very nature of being difficult to reach internally without scaffolding or mechanical lifting structure, skylights are very often ignored by the occupants and deteriorate over the years. With the skylight being partly out in the elements, the use of double-skin polycarbonates in place of glass and the maintenance of their frameworks and locking mechanisms will assist in maintaining security values. The use of internal steel grills should also be considered when looking to enhance the security value of any skylights.

The raised edgings that have been used on many older properties that have flat roofs also provides a convenient hiding place for people to seek cover, out of sight of others on the ground, to enable them to cut and destroy areas of the roof surface to gain entry to the interior of the building. Measures should be taken to restrict access to any roof areas to authorised personnel, not only from a security perspective but also from a Health & Safety point of view.

The use of lead in waterproofing and guidance of rainwater has attracted many criminals over the years to steal it from roofs, as many a churchwarden will testify! Modern alternatives should be used when at all possible, not only in new buildings but also on older properties where possible as long as that change does not degraded the property or its look.

The material used in the construction of roofs is expensive and expanses of tile, welsh slate and other coverings, have in the past been stolen by the brazen thieves who look and act just like bonafide building contractors. Not so much stealing from under your nose but from over your head.

Moving around the exterior of your building, if you have parapets that may allow access to upper floor windows, either from a flat roof or adjoining building, it may be prudent to have the opinion of an architect

about fixing a barrier that protrudes out from the building, possibly on the corners which will prevent the parapet being walked and access to upper story windows gained.

Windows

As there are numerous styles of windows in use, to deal with each type and style individually, would be laborious and time-consuming. Today's use of PVC in the construction of window frames allows for all manner of previous technical problems to be overcome by allowing windows to open in a number of directions. Some swing, others tilt-turn and there are many other combinations of opening but the same basic security rules apply to them all.

You should ensure that they are of sound construction and that locking devices work and provide the security level that you seek. Many the newer windows, like their door counterparts, have multiple locking points and it may only be cost that is the factor between a secure product and one that just looks attractive but is an inefficient security product.

Windows that are hidden from general view at mid-building and ground levels will benefit from having security grills. They should be internally fitted and of a good quality, not only in construction but also in anchorage points and proper security fastenings that are not able to be removed with out the proper tools or complete destruction. Discuss with your insurance company and fire officer before barring windows.

As many buildings utilise windows for ventilation and in regulating the ambient temperature, staff should be made aware of the associated risks of not keeping good security in mind by leaving windows and doors unchecked throughout the working day. Their own personal belongings as well as the company's are at risk from casual intruders. If a window must be left open, try to maintain visual observation of it and the nearby locality so that security in that area of the environment is a normal activity to everyone. Needless to say, someone should have the responsibility to ensure that all windows are secured at the end of the working day.

Doors

All exterior doors should be built to a high standard, even doors that are not in public view. Where doors are required to look good to project the status of a building and any or all companies resident within a building,

they also should be constructed to a high, secure standard as well as appearance.

Doors within a building do not generally require being of a high security standard other than doors to computer suites and other secure environments, locations of safe for instance. There is a school of thought that believes that locking of interior doors is not useful because intruders will resort to damaging locked doors to gain access, even if there is no apparent value in the immediate location.

Possibly, best practice is to lock and target hard with alarms, CCTV etc., areas of risk and leave other areas under the control of the normal alarm activation systems. Again, ensure that staff lock all relevant doors upon vacation of the building – *lock it, not lose it*.

HOUSEHOLD SECURITY

Elements of the following section are equally relevant to domestic and business premises that we are looking to protect.

Every day we are constantly presented with reports in the media (TV, radio, newspapers etc.) of premises being burgled, cars stolen, bags snatched, people being assaulted etc.

Most crime is committed against property by unprofessional opportunists, a large proportion of whom are male adolescents who stop offending when they mature. The peak age for offending is 15 and the risk of crime varies greatly depending upon who you are and where you live.

Whatever type of home you live in, business premises you occupy and wherever you live, a burglary can be one of the most disturbing experiences of your life. Some people are so upset by the experience that they move away. There is however, a great deal that an individual can do to help protect their own and their employer's property.

Firstly, we need to know how the law interprets burglary for us to have an understanding of the measures that we may use to reduce the risk of us falling victim to it.

The Theft Act 1968, Section 9

1. The offence of burglary is committed by a person who enters a building or part of a building, as a trespasser with the intent to:
    a) steal anything therein,
    b) inflict grevious bodily harm on any person therein,
    c) do unlawful damage to the building or anything therein.
2. Having entered the building or part of a building as a trespasser:
    a) steals or attempts to steal anything therein,
    b) inflicts or attempts to inflict grievous bodily harm on any
    b) person therein.

That is only a small section of the full act.

Are YOU inviting crime? Put yourself in the burglar's shoes. How attractive is your home or premises? Take a look around from a perspective of a burglar – are there easy ways for them to gain access?

Is your home or premises hidden from view by trees or hedges? Is it well lit? Do you have poorly-maintained gates or fences.

Wall and hedges on your boundary should not be so high as to provide concealment for intruders. If the burglars are able to spend time in concealment, the more time they will have to attempt to enter your property.

Do not make life easy for them

How do we go about making the burglar's life difficult? "Why bother, it always happens to someone else?" "This is a nice area, no problems here."

Question why burgleries are not so common in a 'not so nice' area. Nothing worth pinching maybe, or there's the chance of getting a very serious beating if the local mafia find out.

Let us have a look at some of the obvious things that we all know and realise should, or could, have been done but is a 'tomorrow' job. Burglars don't do jobs tomorrow, they do them now when the opportunity presents itself.

Make sure that gates and perimeter walls and fences are in good condition and have the facility to be locked, especially if they are at the rear of a premises, where regular access is not required.

Sheds should have secure windows and doors. Screw windows shut if not in use. Doors should have good locks, or a quality padlock with hasp and staple. There may only be junk in the shed but if a bar or screwdriver from the shed helps facilitate entry into the main premises, a cheap lock and fittings will be a false economy. The rear door to the house and buildings are often the poorer of the doors with most expenditure being on the front door whitch is in full public view. Doors of equal quality need to be on all entrances to the premises, where it is architecturally suited, preferably of UPVC construction with a five-leaver locking deadlock mechanism as the minimum requirement. Similarly, windows should have locks on them and we all should endeavour to have a routine of checking that they are secured before we go to bed or leave the premises.

Burglars work a 24-hour shift. They do not only work nights! A large number of breakins and walk-ins are done throughout the day when we are a little less alert to the possibility. How many times have you heard people say, "I was only out a few minutes," " I only picked up the kids from school," "I was asleep in the chair?"

Opportunists love it all when we leave doors and windows unlocked during the day. We should not have a fortress mentality but on the other hand, should not give it to them on a plate. *If you are not using it, lock it.*

There are currently a number of security lights on the market and every area where possible should be given adequate light. Again, you should look at this from an intruder's point of view. They do not wish to be seen and a good lighting set-up is a worthwhile investment.

Alternatively, you should consider areas that you should not illuminate, such as places which are not visible either to yourself or the public, where lighting will help an intruder have better visibility to gain entry. A critical look at your premises can often bring home a few disturbing facts.

A properly fitted burglar alarm should be installed where possible. If you have pets, have an animal-friendly area within your security zone so that your pets can move freely around the area but if within the home, without setting off the alarm.

Modern CCTV systems are now affordable to the general public. Consider installing IP cameras that work via an app on your mobile phone.

Do not forget to alarm your garage. Surely it must be only the British who keep the kids' bikes and various junk in the garage but leave 20 thousand pound's worth of car on the drive or road! Again, thieves will enter the garage first to gain use that nice set of ladders leaning against the wall. Then, in through an upper window of the house, away with the car keys and eventually your nice car with most of the things that you once owned on the back seat.

Please don't look at this article as all doom and gloom. Spend ten minutes in a burglar's shoes and look at your property and possessions from his viewpoint. If you are able to see a world of opportunity for yourself, do something about it before someone else takes the time to do it for you. You are also able to have a professional assessment of crime reduction risks conducted by contacting your local crime prevention officer.

Finally, lock it up and support your local neighboughhood watch scheme.

SECTION 7

ACCESS CONTROL

As previously stated, all civilizations have used varying forms of access control, be it a log across a chasm or a drawbridge to a castle. Even down to our basic door, which if properly secured by a suitable locking mechanism, acts as a quite reliable form of access control, although this is not what we think of when we use the term *access control* in regard to today's systems.

Today's modern access control systems are able to offer unforeseen advances in technology, that even thirty years ago would not have been imagined by a professional security manager of the time, let alone the general public. Even today, not many people outside the security industry have a good idea of what technologies are available, or what in terms of management data, may be realised by the use of computer software. There are many different types of access control varying from the basic aforementioned door, to doors which have their own built-in electronics which, coupled with computerization, are able to recognise and read different types of code, be they in the form of a key with build in electronic circuits, magnetic swipe cards (hi-lo co-magnetic fields) proximity cards, digital push button systems, infra-red ray systems, or smart-phone apps. All these systems may be combined, either in different combinations and with or without CCTV imagery, as the risk element increases. All technologies have a role to play and are able to provide a security level expedient with regard to the perceived risk. Future control systems may also incorporate RDF transmission technologies as this technology is rapidly spreading from the logistics industry into many other areas.

Whilst we as daily users, normally only expect, on a basic level, that the chosen form of access control does what we expect of it, that is, to allow us in or out of the premises or office and not allow in unauthorised personnel. As the control of calculated risk is expected of most modern systems, they normally offer many other features. One of those features is zoning of areas, only allowing individuals with the correct credentials, be it password or electronically generated code, into specific areas of the building. This may also be linked into the company's IT system, where again, computers can be operated only at a given level and the opening of files, or linking into other networked computers, is restricted. It may operate a head-count, so that the number of people within a building or any given zone, may be controlled to comply with the relevant building fire precautions. A range of other bespoke features may be added, if required.

The initial aim of many intruders is to enter a building and move through as quietly as possible so as not to create any outside interest in their activities. This is mostly achieved when premises are empty and probably between the periods of 7pm-5am and at weekends and holiday periods when the staff have vacated the building. Although this is not always the case as people may often wander into large public buildings, enter rooms and areas that are not open to public or staff without authorisation, all such rooms should be protected by being zone-protected with the alarm activation being silently triggered and monitored at the security point, be it on site, or distant to the main site area.

Early alarm systems were quite basic and often consisted of little more than a bell and some form of trigger device. Most were easily overcome by tampering with the bell itself or cutting the wire joining the trigger and the bell.

Technologies have advanced rapidly over the years, especially with the advances in the design and use of the microchip, either on its own, or as part of a conventional computer system operating sophisticated alarm and fire detection systems.

Modern alarm systems allow the design engineer many ways of detecting an alarm state and also a number of responses to the activation of the alarm. The avoidance of false alarms is important as the police will not attend the alarm activation in a premises if the system has an history of false alarms.

When installing an alarm system, guidance should be sought from the local police as to their policy on alarm malfunction. During a prescribed period, three or more false alarm activations may render the property to have police response withdrawn.

All proposed new systems should be to the BS EN 50131 series of standards. Many companies have their alarm systems routed through an alarm receiving centre where any activations can be checked and recorded independently, before any response is required. This response may be by a mobile security officer or the police, depending on how the alarm state is categorised.

The responder will often check for more than one source of activity such as movement and sound to try to find out if intruders are still present. The initial activity may be sensed by varying technologies, although several different technologies may make up the whole system, depending on the requirements to be met at each individual site. A site survey should be carried out to determine what the system is required

to achieve before the brief is passed to the system engineer. It may be prudent to remember that an over-elaborate system can be as useless as an under-designed one and that price might not always be the correct determining factor regarding the purchase of any new system.

The cost of an independent consultant could be money well-spent in the long term. All of the following may be used in the design of such a system.

Magnetic contacts on door and windows most are flush-fitting and activate by the door or window opening and breaking the pull of the magnetic part of the switch which holds a reed switch in place, thereby activating the alarm.

Foil on glass (an old technique) activated when the very thin foil is damaged due to the breaking of a glass panel.

Vibration glass break detector. This device uses an amplifier and a piezo-electric detector. The alarm condition is generated when the characteristics of breaking glass are detected.

A beam interruption device which consists of a transmitter and a recovery unit. Infra-red light is transmitted between the two devices and an alarm state is activated when the beam is interrupted.

PIRs (Passive Infra-Red detectors) detect changes in the infra-red activity within an area which differ from normal, such as a heating radiator.

Ultrasonic movement detectors use ultrasonic energy of a fixed frequency to protect your area. Should the partner transducer detect an altered frequency state from the norm, it will activate an alarm state.

Microwave detectors work on a similar principle to ultrasonic – very often dual technologies, such as passive infa-red with ultrasonic or passive infra-red with microwave, are used in mixed combinations to achieve maximum cover in different situations.

Once an alarm state has been activated, it may possibly be verified by one or more of the following:

- **Digital communicators,** send a coded message to a monitoring station
- **BT Red Care,** where telephone line provide monitored signals to a receiving station
- **Dedicated direct lines** to a 24-hour monitoring station
- **CCTV** with **motion detection** may also send alerts directly sent to a monitoring station in the event of alarm activation.

With the most up-to-date systems using the internet, alarm status may be

received and checked from virtually anywhere in the world using the Data over Internet Protocols. Computers, phones or Personal Digital Assistants (PDAs) all may be programmed or dedicated to the monitoring of specific alarm states.

IS YOUR BUSINESS IN NEED OF

PRINT

PRODUCTS WE OFFER:

Flyers • Leaflets • Business Cards • Posters • Stickers • Banners
Menus • Booklets • Letterheads • NCR Pads • Sticker • Signs
Compliment Slips • Pop Up Banners • & more

Vinyl / Embroidered Printed Workwear

ADVERTISE YOUR BUSINESS

Covering over **48,000** Homes in Pontypool, Cwmbran & Newport

IF IT'S PRINTED, GIVE US A CALL

01495 760592

email: sales@thegolocal.co.uk web: www.thegolocal.co.uk

location: 132 Osborne Road, Pontypool, NP4 6LT

GO LOCAL
MAGAZINE & PRINT LTD

CCTV has evolved over the years, from systems which sometimes gave poor recording and image visualisation through to today's digital systems which, if set up correctly, should give near perfect image definition.

The different situations and fields in which cameras have been used, have grown immensely. Areas which would not have been suitable for any form of monitoring, be it from heat, moisture, cold or the time that a person would be exposed to the elements, or in dangerous arena such as a war zones or near riot situations have changed.

Mini cameras are used in steel making, sometimes fixed in furnace hoppers where they check on the colour of the molten metal. Eventually the heat destroys the camera.

Public space CCTV monitors town centres, shopping precinct areas, shop and pub interiors, the list of its current uses is nearly endless. Innovative uses, such as monitoring gambling tables, shop tills and checkout tills in supermarkets, make the CCTV camera a very useful surveillance tool in the business and commercial communities. The health and safety of the workforce has also been aided by the use of CCTV, where the camera is able to monitor production processes without having people to be physically near to a potentially dangerous process.

Other health and safety uses arrive from the ability of the cameras to track a person, possibly a security officer conducting a checking routine, ensuring their safety is monitored. Its use for observing the interiors and exteriors of a building or site perimeter for the prevention of loss and fire hazards, are paramount to its use within the security sector.

Today's cameras have a wide scope, with operating mechanisms allowing pan tilt and zoom (PTZ) and 360° turning ability – a distinct advantage over a fixed camera although all systems have their own uses.

With the correct lenses, software applications such as number plate and facial recognition is available to search databases for matches to individuals or vehicle registration plates. This latter method is having success in assisting the police to apprehend criminals who travel the country, when it is installed on motorways and other major routes. Vehicle-mounted systems also provide data at sporting events for crowd control and assisting in identification of known, problematic individuals.

Specialist companies provide one-off systems to do specific tasks. For instance, one company offers a system which uses a special carrier allowing the camera to ascend and descend lampposts under its own power and monitors its target for whatever time is required. After, it can

be demounted and located at a different point, should the requirement for more observation be needed. This system replaces the requirement for an hydraulic lift (cherry picker).

Some police forces use a system which is able to send real-time pictures to a PDA hand-held computer. Now people can have the technology as part of their crime prevention strategy with small CCTV systems available for the home and small business as well as the larger companies. The spread of the technology is insatiable, which brings with it the little-known and often less-understood, observance of the data protection act and its requirement to ensure that the medium on which the images are recorded, is kept secure and that images are not allowed into the public domain.

The control of the storage medium is also vital where the evidence of the recording may be used in a court of law. Should there be any concern about the validity of the material, it will not be used as part of the presented evidence for either party concerned.

CCTV is another field in which the internet is playing a big part. Now with the ability of CCTV images to be viewed from the internet, it has maked the flexibility of the system more and more versatile. As Voice over the Internet (VoiP) becomes more widely available, perhaps the speech of transgressors will be heard over the internet system as opposed to now, through a microphone-enabled CCTV system.

The flexibility of CCTV in all its varying formats, remains its best feature and new uses of the technology will develop as it combines with the technologies of the past, present and undoubtedly, the future.

SECTION 10

SECURITY LIGHTING

Most cases of arson, theft and vandalism occur when premises are unoccupied and when intruders have the time to penetrate defence systems. Given time, any defence system can be penetrated. In darkness, an intruder might find it easy to work undetected for many hours to achieve his objective.

Intruders often feel that they are exposed to a greatly increased risk of detection when they are saturated in light. This feeling is more intense when the intruders cannot tell if they are also under observation. Even when the lighting itself is an insufficient deterrent, its mere presence is likely to increase apprehension, restricting the time of a break-in to a minimum and thus, reducing the extent of any loss.

Without the presence of effective security lighting, the police or others responding to an intruder alert are hampered. Intruders may hide in the shadows, observing the investigators and take the opportunity to escape, or to attack those responding to the alert. In dark areas, investigators need to carry torches and be aware that their presence and movements may be obvious to criminals hiding in the shadows.

Security lighting is normally directed upon buildings and the surrounding grounds so that intruders can be observed by police patrols or others, outside the premises. Conversely, where there are people inside the premises, there is an advantage in casting some light from the building towards its boundary. The intruders are then faced with the daunting prospect of walking towards the glare produced by powerful lights without being able to see what lies beyond them and whether or not they are also being observed from within the building. In all cases, great care must be taken to avoid nuisance to neighbours or a glare hazard to drivers of passing vehicles. Security lighting which deters intruders can be a cost-effective form of defence. For maximum effectiveness, security lighting should be used in conjunction with other security measures, including intruder alarms. However, there are instances where security lighting is not useful. In premises which are not overlooked by houses or passers by, generally out of town sites, security lighting makes it easier for an intruder to gain entry by illuminating the building for them. In these cases, other forms of security would be more appropriate. Security lighting should only be used if there is a probability of intruders being observed.

Designing a security lighting system has, in recent times, become a very specialised subject. This is due to technical developments in lighting and greater crime prevention awareness. Both of these developments

have been driven by the rising cost of energy and crime. In concept, a security lighting installation should be based upon the technical and psychological factors that serve to both deter and detect intruders. To be effective, a security lighting installation should be designed by a suitably qualified person. This is even more important where CCTV is to be used in conjunction with a lighting system. One of the many issues that should be addressed by the system designer, is the affect of colour rendering.

Colour rendering is a measure of how accurately the colour of surfaces appear when illuminated by the lamp type, when compared with their appearance under a standard light source, e.g. daylight. Thus, good colour rendering means giving an appearance approximating daylight conditions. Colour rendering is not important for purely security applications but may aid identification of suspects and vehicles. Where black and white CCTV is employed, colour rendering is unlikely to be an important consideration. For colour CCTV, it is likely to be critical to the overall performance overall of the system.

Reputable manufacturers of security lighting systems provide a design support service and provide comprehensive product information. Easy-to-use guidance charts are available, showing how to achieve a given light level using different lamp types, at various spacing and mounting heights. A rough guide to suitable levels of illumination is 5 lux on building facades and car parks and 3 lux on the surrounding areas.

A full brief should be given to the designer for any new system so that major changes do not have to be done should additional security (CCTV) and possibly infra-red lighting be added at a later date.

INFRA-RED

What is infra-red? For the purposes of CCTV, it is light which the human eye cannot see but which mono cameras can. Sometimes called black light, it lies approximately between 700nm and 1,000nm (1 micron). Infra-red illumination is essential in the 24-hour digital world. Without infra-red, dark night-time scenes may remain dark to CCTV cameras, pictures may suffer from shadows, signal noise and loss of focus. Infra-red has the ability to allow the cameras to work at their maximum potential, irrespective of the level of light.

Key factors to take into account when choosing an infra-red lamp include the required viewing distance and scene and the sensitivity of the camera lens. Please note that most modern CCTV cameras have infra-red built in.

Cameras with smoked glass domes may lose up to 70% of available light – this should be taken into consideration when planning for lighting levels with normal or infra-red lighting. If possible, clear domes should be used to maximise light and may possibly require less lighting to be provided artificially.

Often a CCTV end-user will require covert or semi-covert illumination for their CCTV installations. A number of filters are available to provide this option. The filters are offered at 730nm, 830nm and 930nm. Generally speaking, a 730nm filter will have a glow similar to that of a traffic light, an 830nm filter will give off a dull red glow, only just visible to the human eye and a 930nm filter will appear totally covert to the human eye. No glow is visible.

When retro-fitting, or planning a new CCTV installation, lighting and infra-red illumination should be given as much importance in the overall plan, as what type and where, the cameras are installed.

The matching of any proposed system will require sound information and expertise, to ensure that any given system has the ability to perform to its maximum potential and allow for cost-benefit savings, achieved by using systems which match the requirement of the need, cost and benefits.

By the very nature of any home or business, materials, paperwork and money are accumulated from cash sales, float money, wages and petty cash. That is besides other information that should be secured and not left on view, on desks or placed in unlocked cupboards and desk drawers. Possibly the best solution for day-to-day working, where information is required to be kept on site for periods, is the investment in a safe.

Like all things, safes come in many and varied sizes and prices, so some thought should be applied to the buying process before we purchase our safe. In today's world, the old safe from Uncle Joe's butcher's shop that he ran in 1930, is not good enough, even if it lasted out the war.

Our starting point, as in most things, should be to decide what we are intending to store within the safe. Once that is ascertained, we need to consider what we may require to store in the safe, even for a short period, that may have a monetary value, over and above our normal monetary-valued holding.

That figure should be a starting point for our decision on the type of safe to acquire, as that figure will be one of the initial considerations which will affect all other issues. Things to consider are:

Cash rating: this is the figure that an insurance company will offer overnight cover on. You should check with your insurers to ascertain their requirements.

Fire Resistance: usually measured by the number of minutes that a safe or cabinet has been tested and its contents exposed to fire. The longer the period in minutes, the greater the fire resistance. This rating is normally obtained by measuring the internal temperature of a safe whilst being exposed to temperatures around 1,000°C in a furnace. The critical temperature before paper chars, is about 177°C. Computer media cabinets however are tested to maintain internal temperatures of approximately 52°C, which is the maximum temperature most media manufacturers recommend.

Safes and cabinets should be anchored in position and the appropriate manufacturer's instructions should be followed. You may find that the insurance company will not pay out on an incident if the safe has not been fitted either by an appropriate engineer or at least to the manufacturer's standards.

Consult your insurer for advice on installation and cash ratings before losing more money than you intend to store in the save, by buying the wrong one in undue haste.

SECTION 13

VEHICLE SECURITY

Most businesses can't operate without one or more vehicles, be it a company car, van or lorry up to a forty-two ton gross LGV vehicle. Vehicles in all their variables are often overlooked when we undertake a security survey, as they are not always parked in the same area, are mostly being used off-site and may be away from the vehicle's base during a normal working day for the majority of the day or even working week. Some vehicles may only return to base when it is due its maintenance period or for other legal requirement. The cost of a vehicle, even without considering any tools, equipment or goods that it may carry is considerable and should the vehicle be stolen or damaged, it may cause major disruption to any sized business which requires transport to carry out its daily routine.

Ideally, any staff member who has a requirement for a company vehicle should have a vehicle dedicated to them for their own use. Other staff members who may use company pool vehicles, should have to sign a log with the relevant details of any specified vehicle's usage. Details that a log should require are: driver, destination, vehicle registration, mileage, fuel usage, time out, return time, driver signature, any damage to vehicle and any defects which may affect the road worthiness of the vehicle.

Before a driver is allowed to use any vehicle, they should have their driving licence checked to ensure that they hold a valid licence to drive the class of vehicle that they may be required to use. This should be repeated at least every six months to ensure that there has not been any change in driver status – a driving ban, for instance. Also, they should be medically fit to operate such a vehicle and they understand the company's policy on the usage of its vehicles. It would be pertinent for the company to hold on record, photo id of all the staff who hold entitlement to drive, or operate any company, vehicle. Many companies are now looking for their staff that operates company vehicles to undertake an advanced driver course through a recognised body such as the RAC or other specialist companies who run advanced driver training. This not only pays from the point of reducing accidents and vehicle damage but also it is a requirement of many insurance companies, especially those who insure fleet vehicles. It should be ensured that all vehicles are kept in a road-legal manner and that the taxation, insurance and MOT, or plating of all vehicles, is catered for as by the requirements of road transport law.

All company vehicles should carry the name and address of the

company as part of its livery and if the vehicle is used to carry anything of a hazardous nature, that should also be displayed in a prominent position on the vehicle. All operators of the vehicle should have received adequate training in the carrying of hazardous materials whatever its nature, if handling it is part of their working day.

All companies should ensure that its vehicles receive at least the minimum recommended levels of maintenance and that those that operate within the security industry should be paid special attention to. The maintenance of vehicle reliability is a major factor in being able to deliver the required level of service.

Security companies who offer dog patrol services should have their vehicles fitted with a suitable cage for the purpose of not only restraining any animals carried but also to protect the animals themselves from any equipment and food vessels which may move around the cargo area of the vehicle. The operation of any vehicle brings with it responsibilities, not only for the driver of the vehicle but also for the company. Vehicles, by their inherent nature,can create security and health and safety issues which must be carefully controlled and not be allowed to go unchecked.

Vehicles of all types are the target of thieves, as their monetary value is high and they can be easily sold on or dismantled for their parts. With many vehicles being stolen to order by criminal gangs, all vehicles are at risk if precautions are not taken as a matter of daily routine.

Although we all think that we do what seems to be the obvious, how many times have we all paid for petrol at a garage and then realised that we have left the vehicle keys in the ignition or our wallet or computer etc. in full-view on the vehicle seat.

Many people have not been lucky and have had their vehicles stolen and sometimes the unfortunate victims have had their vehicles used as a weapon against themselves and been driven into and severely injured or killed by the impact. Although we all presume that this only happens to someone else, it is happening more frequently within the working environment and as the cost of vehicles and their loads increase, it appears to becoming a very common crime.

We should all endeavour to see that the security of our vehicles is catered for at all times. The only way of achieving that is by ensuring that we routinely lock our vehicles and check all doors on the vehicle to ensure that they are secured. On LGV vehicles that use tail lifts, the power lead should be stored in the vehicle's cab when not required, as any potential thief could connect the lead, lower the tail lift and if not

secured by a lock, open the rear shutter or door of the vehicle. Is the vehicle left stationary for a period of time? Various anti-theft devices are available, depending on the type of vehicle, ranging from audible alarms to fifth-wheel locks for articulated vehicles as well as devices which prevent the air from being built up in the brake release tanks on heavy goods vehicles. The air which when built up to the correct pressure releases the braking mechanism. CCTV and biometric readers are also used in the higher risk environments.

If possible, all vehicles should be stored within the confines of the building or suitably erected compound and all keys for the vehicles should be stored within a key safe, not left on the office desk.

Within the commercial sector, many vehicles use a variety of seals to ensure the safety of their cargo. These depend on the type of goods carried. They range from plastic seals with a serial number, to electronic seals which generate a random number, through to bolt-type seals normally used within the shipping cargo sector. Despite all the technology available thieves still operate with some success in many areas of transport. The police, through their stolen vehicle desk and operations directed at this type of crime, are also achieving successes in many parts of the country. At the end of the day, we all have to operate due diligence in the operation of our own and the company's vehicles and not allow ourselves to become lax where security is concerned. "It may be a long walk back home."

SECTION 14 SUMMARY

We have looked at the overviews and some of the hardware that may be used in certain situations to achieve the aim of providing a risk reduction in a given area and help to control loss, guard against fire and flood and help in the provision of a safer home and working environment for all concerned.

With a little crystal ball gazing we might imagine all sorts of scenarios where we may wish to achieve better results from our efforts and hopefully achieve a 98% non-incident record. Will 100% be achievable?

Even without the acquisition of some futuristic new technology, we are able to achieve steps in the direction of future security systems, not only by utilising different mixes of readily available products and systems but also including into our mix; technologies that are aligned to security but not always associated with the field, other than in possibly a few specialist circumstances. Before we start to consider how we may achieve the technical side of things, it is worth re-iterating that no amount of electronics, however clever, can dispense with individuals who are able to put into place the basic criterias of intellect, good management practices and the motivation of staff at all levels, to treat the workplace as if it were their own.

One such technology that might come more into the security field is the Radio Frequency Identification (RFID) system. This is currently used in the logistics industry and as the technology spreads is overtaking bar coding as a means of identifying products and the monitoring their path in the journey from manufacturer to the consigner prior to the distribution to the consumer, if the product is suitable.

Many major companies purchase products and basic materials from around the globe. Goods may pass over a number of continents before arriving at their destination port.

A number of the world's major companies ship and transport goods over the same route for many years and require a constant travel audit for them to be sure that any given product will reach its destination at the correct time and also the correct point within a destination, be it a shipping port, warehouse or other such area. In today's time-conscious world, the use of just-in-time purchasing systems mean that the arrival of the goods into their warehouses, is critical to the continuity of the business.

From a logistics point of view, a management review may dictate a route for any given product to take. When the product is boxed, a RFID

tag is fixed to the box and that tag is then read by readers that have been installed at various locations throughout the product's journey. Obviously, a vast amount of expenditure is involved in setting up such a system to provide an audit trail of such dimensions, especially throughout several countries, but as the growth of international companies continue, the use of this type of audit trail will become common to us.

This is the basis of how the technology works on a large scale – to assist us within a more modest security operation. Possibly, RFID badges which are already available and sometimes used at conferences, have delegate's interests fed into the software programme and when two delegates pass each other at a conference, the badges flash, indicating that they have a common interest within a particular buying process. Where it is envisaged this to be of use within a security scenario, is a building such as a hospital, factory or any other place where the control of access to specific areas is vital and the observation and control of people who stray from the public or staff routes, are required to be monitored.

If all out of bounds areas had RFID receptors fitted and all visitor control badges utilised RFID technology, all visiting persons would be issued with a unique code, programmed into their badge or other device. Should that badge then alarm within a non-public area, security may either covertly view the situation or send an officer to ascertain why that person was in the prohibited area. Obviously, provision must be made to insure that the badge or tag is not disregarded or deliberately left on a shelf, or something of that nature. Many other systems may tell security that an alarm has been activated within a specific area but they do not have the capability to track an individual throughout their passage within a building.

A system such as this may be used overtly to track an individual possibly on a guard patrol, should there be any concerns of the health and safety within the environment. The technology has been used to check on children in a leisure park where they are allowed to roam freely without parental supervision, a check being kept on the whereabouts of each child through the use of RFID technology.

As more building design engineers over the last 20 years have adopted designing out crime principles, some now think about security and are starting to build the fundamentals into their new buildings from the start. With fire detection and alarm systems being installed with CCTV into the fabric of a building, it makes it more efficient to

have all the systems controlled from a single integrated point within the site. Access control systems situated at entrance and access points also provide management data on how many individuals are on a given site at any particular time so that health and safety and fire regulations may be complied with. All data should be backed up, with it also being duplicated into storage systems, either within a separate building on-site or at some other location off-site, as should any disaster recovery plans and other related information.

All this design planning, procedures and use of specific knowledge of the security industry is good as it hopefully should allow us to achieve our aims of a crime, loss and hazard-free environment. Wonderful stuff for the security consultant and designer to look and admire their achievements within these black arts. What about the people who work within the environment that has been created? Are today's managers and workers able to exist comfortably within this environment or will they find ways to circumvent all our efforts, proping fire doors open with extinguishers, for instance? Tomorrow's workers who are growing up within the current digital revolution may find that their lives are governed by their PDA handhelds as much as today's train commuters are by their endlessly-chattering laptops on the way to work.

From locking one's hand-held into its cradle in the car in the morning and keying in one's unique identification number, the PDA gives our manager the benefits of an all-in-one support system. At the touch of a key, it will supply information on temperature, vehicle speed and global positioning. It will also function as a route finder, informing us of the most advantageous route to a given destination. It may also, if you ask it, act as a speed camera monitor and advise you of the correct speed limit for your current road.

On arriving at the office foyer, you point your PDA at the receiver on the access control system to register your arrival, place your finger on the biometric reader so the database can check that it's really you and not someone else with your PDA. The software in the access control, if required, can switch on the lighting and heating within your office and also bring up a message on your computer of any electronic mail that you may be require to read. Access to areas not recognised by the PDA will be barred as the software informs other security hardware of our presence, similar to the CCTV monitoring our passage throughout the establishment.

When the building is vacated, our manager then reverses the entry process so that the management control database is up-to-date.

With building and energy costs rising, efficient use of all buildings is paramount. Heating and lighting constantly on in an unoccupied office, represents a loss for a company in today's business world. Adaptable systems which integrate security, access control and fire detection, all have the ability to be controlled by the computer network of a building. Tomorrow's security manager will require to be a specialist in many disciplines if they are to cater for the demands of tomorrow's security challenges.

BIBLIOGRAPHY

The books, manuals, magazines and articles used in the preparation of this document are:

Security & Guidance Manual. International Professional Security Association

Building Security by Management & Design. Thorn Security

Integrating Security into Intelligent Buildings. Security XML

The Security of Buildings. Graham Underwood

Police Architectural Liaison Manual of Guidance

A Guide to Security Surveys. Bill Wyllie

Web page. Sanderson Security

Nightime Handbook. Derwent e-information

Information from Security Lighting - Crime Prevention in Schools/ Architects & Buildings Branch. Department of Further Education

Police Architectural Liasion Manual of Guidance

No article or section from any of the reading has been used verbatim.

- NEXT EDITION - JANUARY 2021

To advertise in the next eBook

To Order Your Advertisement

Your company's advertisement in the next edition of this eBook is only a few clicks away! Firstly, choose which shape and size you wish to order from the illustrations alongside. Then, by clicking on the link below you will be taken to our webpage where there are a few simple instructions to follow.
Order now: *www.spectrumid.co.uk/ebook*

Advertising Specifications

Sizes

There are five sizes of advertisement for this publication, each of which is shown with their dimensions. Advertisements should be saved to the dimensions shown and NOT include bleeds or trim marks.

File formats

Advertisements should be saved in RGB colour mode as JPEGs or PNGs. PDFs cannot be accepted as exact conversion cannot be guaranteed.

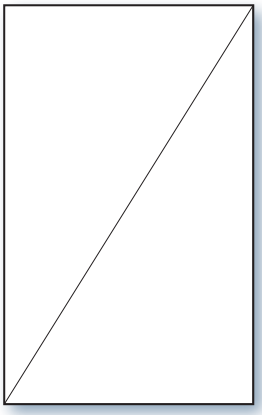
Design considerations

All typography, logos and important illustrative details should be at least 5mm from the edges of the design as there are no gutters between advertisements. Any advertisement that requires white borders should have the borders saved within the file provided and not added to the dimensions shown here.

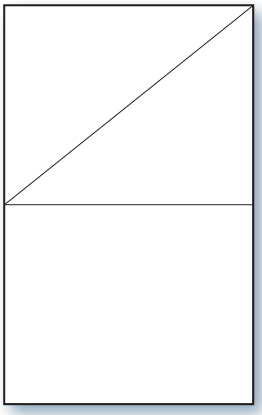
The publisher accepts no responsibility under The Consumer Rights Act 2015 or the Consumer Protection from Unfair Trading Regulations 2008 for any product or service, bought or commissioned, as a result of an advertisement published in this document. All responsibilty for defective goods or services, or unfair, misleading and/or aggressive commercial practices rest with the advertiser themselves. These may include: displaying a quality mark without authorisation, falsely claiming to be a signatory to a code of conduct and falsely stating that a product will be available for a very limited time in order to obtain an immediate decision.

Help with your design

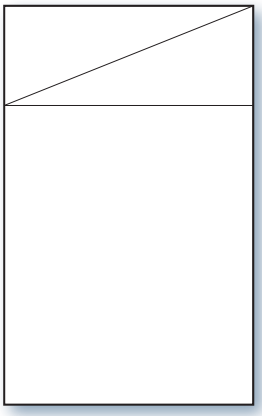
This eBook has been by db Designs who can offer help in the creation of your advertisement.
Please contact: *david@dbdesignstudio.co.uk*



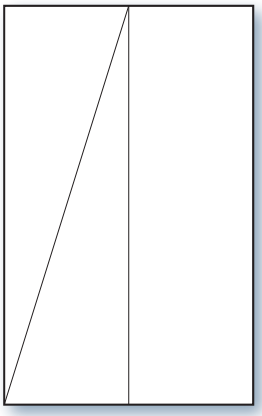
FULL PAGE (£100.00)
258mm (Height)
161mm (Width)



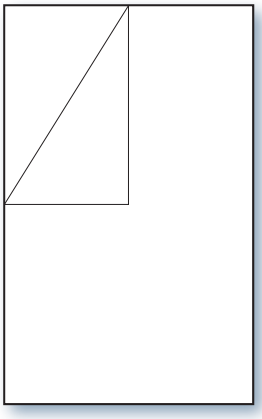
HALF PAGE (£50.00)
(Horizontal)
129mm (Height)
161mm (Width)



QUARTER PAGE (£25.00)
(Horizontal)
64.5mm (Height)
161mm (Width)



HALF PAGE (£50.00)
(Vertical)
258mm (Height)
80.5mm (Width)



QUARTER PAGE (£25.00)
(Vertical)
129mm (Height)
80.5mm (Width)

Multiple advertisements booked at the same time are eligible for a 10% discount.

Further discounts are available for orders over 5 booked at the same time. Contact: *sales@spectrumid.co.uk* for more details.

IDENTIFY
YOURSELF WITH THE
BRAND
YOU REPRESENT

PERSONALISATION OF **"ACCESS CONTROL CARDS"** NOW AVAILABLE.

- **Plastic Cards**
- **Card Printers**
- **IP Cameras**
- **Security Hardware**
- **Biometrics**
- **Access Control**
- **EWA Airkey Smart Locks**

Contact Dennis on:

01495 757 153 / 07802 664 267

sales@spectrumid.co.uk
www.spectrumid.co.uk

SPECTRUM POSITIVE

A Guide To Buildings & Property Protection
is written, produced and the sole property of
Dennis Ricketts HonFIPSA at Security & Identity Ltd
trading as Spectrum iD.