



Physical Security - General Advice for Business



www.bcrc-uk.org

Selecting your Supplier

Businesses often rush into purchasing new security measures after becoming a victim of crime. When a crime has occurred it is tempting to rush into action. It is far better and more effective to take your time and ensure you seek appropriate advice so that the security measures appropriate to the particular business and its vulnerabilities are selected. Many businesses waste money on inappropriate measures. It is vital to carefully identify what needs to be achieved and how this will impact on the rest of your business.

Allocating a specific budget and devising a rolling programme of measures to improve security is the best way to address any issues.

Selecting your Security Measures

It is important that you seek professional advice when it comes to choosing what security measures to put in place. Many businesses fail to seek advice whilst overlooking things that make the business vulnerable to crime.

The Business Crime Reduction Centre (BCRC) will visit your premises and carry out a free and complete security audit of your business producing a free and impartial report highlighting all areas of weakness. BCRC will look at all aspects of your business including:

- Environment
- Perimeter
- External areas
- Internal areas
- Ensuring the correct staff policies are in place
- ICT equipment and network security

Whilst the BCRC will recommend areas of security that need to be addressed, they will always remain impartial. The BCRC cannot recommend companies and will never point you towards a particular supplier. Visit www.bcrc-uk.org or call 0114 275 1343 for more information.

Things to look for in a Supplier

- How long has the company been trading?
- Can it provide an ongoing service?
- Is it a member of a recognised industry body or association?
- What is the level of training and qualifications of the staff?
- Can the company carry out all of the work or will they have to sub-contract it?
- Does the company specialise in any particular field?
- Is it adequately covered by insurance?
- Can it provide references or testimonials from satisfied customers?

Choosing a suitable supplier is extremely important. The right supplier will ensure that the security being put in place is fit-for-purpose. Installing CCTV or an alarm is great but if they are positioned wrong or not set up correctly, they could be an expensive waste of money.

Visit www.nsi.org.uk for a complete list of national approved security suppliers.

Drawing up Accurate Guidelines

Having drawn up a shortlist of companies, contact them and tell them the exact nature of your problems. Let them provide their expert advice on how to solve them. There are often several options that could meet your needs, so make sure your short listed companies explain the advantages and disadvantages of each option clearly in a detailed specification.

Equipment Quality

Always confirm the quality of the equipment to be installed. Poor-quality equipment can be cheaper, but can also carry longer-term costs, being prone to breakdown and needing more frequent servicing. Conversely more expensive products and services may include more than you actually need.

Written Guarantees of Provision

Always get a specification, written in layman's terms, of precisely what the supplier is agreeing to provide. Examples might include how many cameras are to be supplied, how many guards will be employed and what hours they will work, and the costs.

Talk to at least three companies, set out the specifications and quotes before making an informed choice.

Security Consultancy

Large companies should consider using specialist security consultants. A BCRC Business Adviser or local Crime Reduction Officer will be able to give you advice of a more general (rather than technical) nature.

Security Measures

External Environment

Business premises do not have to look like fortresses. Good design, landscaping and lighting, along with careful management and appropriate use of security technology can help to create a good impression whilst generating safety and security for your building, staff and visitors.

No perimeter protection can be guaranteed as impregnable, but it can delay or deter intruders and make it easier to intercept them.

You can minimise the quantity of goods that can be stolen by restricting vehicle access.

For instance if you can reduce the amount of space in front of roller shutters or large entrances, you can reduce the impact of a ram-raid. Ensuring that vehicles cannot build up speed to hit an entrance head-on may reduce the threat of being a victim of such a crime.

Surveillance

There is a tendency for businesses to build high barriers to keep potential criminals out and make valuables harder to see from the outside. However, the same barriers can provide a protective screen for intruders, allowing them to carry out their activities and escape without being seen.

The area around the outside of the premises should offer good surveillance to detect intruders, ensure staff and visitor safety, and allow fire and other emergencies to be detected early. This can be achieved in two ways:

- Natural surveillance by people on-site, passing by or in nearby buildings
- Formal surveillance by security patrols or electronic surveillance - CCTV, movement detectors, etc

If opting for CCTV, the business needs to make sure they choose a suitable supplier and ensure the system they choose covers the areas needed.

CCTV is most effective if it is being monitored. Monitoring can be done by an external company who will alert the key-holder or police. It can also be done in-house over an internet connection.

Boundaries

A perimeter fence or wall is a defining boundary of your premises and should restrict entry to a limited number of places - it should always be under your control.

Fencing

There is a variety of fencing systems on the market. The height of the fence should be appropriate to the risk and site geography. In general, the minimum acceptable height for industrial estates is 2.4 metres - these will require planning permission.

A mesh construction that allows natural surveillance can be used internally and externally. It should have a mesh small enough to prevent finger or toe holds.

Welded mesh, expanded metal or steel palisades are the best choices for fencing material. Chain link is no more than a boundary marker and is unsuitable for any degree of security.

A range of toppings, from barbed wire to revolving spikes, is available. The business must consider their legal position to ensure they adhere to the proper health and safety laws.

Large-scale and/or isolated premises can consider electric fencing. This might seem an extreme form of protection, but it can be an effective deterrent even to the most determined criminals. Such forms of security should only be used to address identified risks, and appropriate technical and legal advice must be obtained before installing them. Electric fencing may also be appropriate for high security applications.

For high-security requirements, alarm sensors and other surveillance technology can be included. Fences can be linked to alarm monitoring and CCTV systems that allow a small number of security staff to observe large areas of perimeter fencing and arrange for an appropriate response, even if they are off-site. Such measures can also be linked to speakers through which a remote security officer can address and deter an intruder.

These systems can dramatically cut crime when fitted. They should comply with British and European standard BSEN60335.

Building Security

Every building differs in its location, construction and contents, and the crime risk varies accordingly. The best time to address the security of a building is during its design, when your local Architectural Liaison Officer (ALO) can give free, impartial and site-specific advice. You can also visit the website www.securedbydesign.com for more details.

The Building Shell

Examine the shell of the building closely when carrying out a risk assessment. This includes all roofs, walls, basements/cellars, doors and windows, and any other area where intruders can gain access.

Although doors and windows are the usual entry points for burglars, insulation, metal foil construction or even single-skin brick walls can easily be cut through with saws or disc-cutters. Criminals can exploit flat roofs with roof-lights, adjoining cellars, access hatches and even sewer tunnels if the perceived gain is great enough.

Doors

Although most internal doors should be closed to stop the spread of fire, they should not necessarily be locked. Burglars can cause a great deal of damage to doors and frames just to find out if a room contains property worth stealing.

In buildings that need high security (such as IT offices, in-house travel agencies or banks) it is advisable to fit robust doors and locks as well as caging. In certain circumstances, it may be better to use a safe to store valuable items or documents.

Guidelines for Doors:

- They should be flush with the building line avoiding recesses
- They should fit their frame well enough to prevent them being forced open with jemmyes or crowbars
- Frames should be strong and as securely fixed as the door itself, ideally with metal anchors into the surrounding brickwork or timber
- Wooden doors should be at least 44mm thick
- Materials such as aluminium and UPVC can be less strong than reinforced steel so consideration and care should be taken when using them
- External hinges should be protected and made non-removable
- External fire doors should have the outside handle removed
- Any glazing in doors should be of laminated glass to prevent accidents and to deny entry by breaking of the glass
- External doors and security doors should be fitted with a closer. This should always be on the inside face of the door
- Security doors must meet the Product Assessment Specification (PAS) 024

Locks

The simplest form of lock is a mechanical lock that uses a key to control one door. The principle of suites of locks, allowing senior staff to access a range of doors throughout the building with a single key, but limiting other staff to their zones of responsibility, is a more sophisticated use of key locking. Potential disadvantages of such systems include the need for stringent key management, and the fact that lost keys may place the security of the entire building at risk.

Digital code locks, mechanical locks or electronic locks can be more appropriate, but the locking mechanisms may provide poor security. Door codes should be changed regularly so that they do not become known to potential offenders, and to make sure that passers-by do not learn the numbers by seeing them being keyed into external doors. Numerical key-pads should be cleaned regularly as prolonged use can leave fingerprints over the keys being used enabling an intruder to identify the code.

If the main entry door or staff door is locked during the day only with a single rim latch, consider upgrading to a mortice latch. Many thefts occur after normal working hours but when there are still staff in the building. A mortice-type lock will help improve the security of these doors and stop them being overcome by an opportunistic intruder.

Access Control

Keys and Key Management

Where keys are used, it is important that they are closely controlled and accounted for.

Only trusted members of staff should have access to master and sub-master sets of keys.

You should allocate keys to specific key-holders, and check regularly that none of the keys have been mislaid. It is advisable to use keys that are registered to a company or organisation that will demand detailed information before they will produce duplicates.

You will need to appoint nominated staff members as key-holders to attend out of hours in the event of fire, crime or other emergency.

Many alarm and security companies provide a holding service for keys. Some companies will organise urgent repairs, boarding up etc. on your behalf. They will usually do this in conjunction with your alarm company, to comply with police alarm response policy.

Be careful to ensure that key-holders are not compromised or called to the building under a false pretence, only to be threatened and forced to allow access to the building and switch off alarms.

Electronic access control is becoming more common. Door entry phones, many with visual verification by small video cameras, or swipe cards or tags that are read by computer operated detectors are all readily available

Card Access and Tags

Smart cards, tokens or fobs are easier to control than keys. Lost cards or fobs can simply be deleted from the system, and a new one issued to a legitimate user.

These systems should have an anti pass-back facility to ensure that the same card, token or fob cannot be used twice to enter a building unless it has been used to exit the building first.

These cards can be used to control, restrict access to, and restrict movement around a building, including gates, barriers, lifts and doors. Management and security staff should be able to access all parts of the building, whilst other personnel should be allowed access only to parts of the building deemed appropriate to their work.

Evening cleaning staff can be given an exit-only card that does not allow them to re-enter the building. Visitors or outside contractors can be given a card or token that is valid only for given areas at given times.

For greater security a video entry system can be installed allowing those inside the building to view any visitor and request identification to be shown prior to being granted access.

Integrated Access Control Systems

Such a system can be expanded to control automatic locks, alarms, smoke and fire detectors, building up a complete management and reporting package.

Computer control of these systems potentially offers far wider applications than security, as they can also help you to locate staff more easily, or record their times of entering and leaving the building.

Tagging all equipment also makes a computerised inventory of the entire business simple to set up and manage.

Internal Environment

Reception Area

Your reception area should be the first line of defence against intruders during normal business hours. To maximise the security benefits of your reception area:

- Never leave the reception area unattended
- Sign every visitor to your premises in and out, and issue them with identification against a signature. There are many good quality visitor pass products on the market ranging from simple paper-based systems to more advanced computer-produced versions that can include the photograph of the wearer
- Pick up all visitors from reception, and escort them back there: do not leave them to find their own way, or allow them to wander around the building alone
- Train your receptionist/s in security, so that they can recognise suspicious behaviour and are aware of techniques intruders commonly use, such as 'tailgating'
- Make sure reception staff cannot be threatened or placed under duress to allow unauthorised entry if you use them to control access from a public reception area into more secure parts of the building. The reception area should always be equipped with a personal attack/emergency button.

Entering a building and hiding until it is closed and empty is a common method intruders use to gain access. Your premises should be searched properly before it is locked up.

For more information on how to prevent unauthorised access, please see our section on access control.

Lighting

Make sure that your premises are well lit, inside and outside. Boost your interior lighting, if only by increasing the bulb wattage.

When installing exterior lighting, consider the surveillance that external lighting will enable. If the lighting will

only enable criminals to work with increased visibility, improved lighting may not be the answer.

Alarms and Alarm Communication

About Alarms

Alarm design and technology is continually improving. False alarms are being reduced, and higher degrees of security are being provided.

Alarms can be audible-only and/or monitored remotely by a monitoring station arranged by your installer. Monitored systems are strongly recommended for business users, as many now provide verification that intruders are on the premises via additional signals to the monitoring station. An alternate option is to install an auto-dialler which either through your phone-line or GSM sends an automated message to a designated number if the system is tripped.

Verified alarm activations improve the chances of catching intruders and minimising false alarms. All monitored alarm systems installed after 1 October 2001 must include some form of verification that activation is genuine before the police will respond.

Selecting an Alarm Installer

Many insurance companies now require customers to use approved installers if they wish to benefit from lower premiums. Check your insurance company's requirements before choosing your alarm installer.

To get a balanced view of what is on offer, get quotations from at least three companies who are subject to independent inspection by an approval body recognised by the police.

These include the:

- National Security Inspectorate (NSI)
- Security Systems and Alarms Inspection Board (SSAIB)

Whilst all independently inspected alarm companies will have to ensure that they adhere to stringent standards on installation and equipment, which includes fitting to BS4737, you should make sure that you ask the following questions:

- Are there any maintenance and/or monitoring contracts or additional hidden extras, such as call-out charges?
- Do you own the system, or rent it?
- How long does the guarantee last, and what happens if there is a problem after that?
- Is there a 24-hour call-out service and emergency attendance within four hours?

False Alarms

A disciplined approach to alarm setting and un-setting must be implemented to ensure that false alarms are kept to a minimum. If the business is utilising a Police Response Alarm and has suffered a number of false alarms, they may be removed from the list meaning Police will not respond if the system is triggered. It is up to the business and the alarm installer to ensure the system is cannot trigger by accident.

(Businesses should check with their local Police Force as to their stance on false alarms as procedures can differ nationally)

It is essential to make sure that nominated people who attend the premises if an alarm has been activated cannot be compromised and forced to unset the alarm. Alarms are now available with built-in duress codes. These will unset the alarm, but will also alert the monitoring station that the entry is unauthorised.

Whilst the physical security of premises is important to the success of a business, the ICT equipment in place must also be secure.

Many businesses overlook the threats to the business from e-crime, internal theft and data loss.

For an in-depth, free and impartial security audit of your ICT equipment or for a complete assessment of your buildings security, call the Business Crime Reduction Centre.

Call on 0114 275 1343, email on z.wharton@bcrc-uk.org or visit www.bcrc-uk.org

Crime prevention advice from Business Crime Reduction Centre is independent and is given free of charge without the intention of creating a contract. Business Crime Reduction Centre cannot take any legal responsibility for the advice given.

© People United Against Crime 2010