Security

Generally the more valuable and portable an item, the more attractive it will be to thieves. Deterrence is the key to security. This is achieved by a combination of measures including physical and electronic protection, surveillance, and security marking items to make them difficult to dispose of.

Theft can result not only in the loss of contents but also in considerable damage to the building due to forced entry/exit by intruders. To minimise the risk of theft a security strategy should be developed with the aim of making it as difficult as possible for intruders to gain access to the property. Early detection of unauthorised visitors is also crucial.

Security assessment

To determine the security measures required to protect a property, it is first necessary to identify the theft risk from a security assessment, taking into account factors such as the value, portability and location of valuables, and the increased risks of damage to buildings posed by their presence.

When considering security it is best to examine security measures from the outside i.e. the site perimeter, and work inwards, making it progressively more difficult for intruders to gain entry and increasing the risk of detection from surveillance or intruder alarm protection.

Perimeter /site security

Whilst surrounding a building with substantial fencing/walling can significantly improve security and act as a psychological barrier by demarcating the site so intruders know they are trespassing, it should not be at the expense of external surveillance of the property. Where possible solid barriers, such as brick walls, which can act as a screen once scaled, should be avoided. Perimeter fencing should be at least 2.4 metres in height to have any real security value.

Common types of perimeter barriers available include:

- PVC/powder coated weldmesh or expanded metal fencing: This is difficult to overcome and maintains visibility but can be vulnerable to attack at fixing points to fencing posts.
- Timber panels: Economical to install, but do provide a screen once scaled and do not present much resistance to physical attack.
- Quickthorn hedging: This can be used in conjunction with other perimeter protections, has very low maintenance costs and once established acts as an effective deterrent where free from gaps.
- Chain link: This is readily available, relatively cheap and easy to install, but quite unattractive in appearance, easily distorts and is subject to localised collapse following cutting.
- Steel palisading: This is substantial and very effective.

Where perimeter fencing is erected matching gates should be installed to maintain security levels. Gates should be kept locked outside business hours, preferably using a hardened steel locking bar and a closed shackle padlock. Existing perimeter fencing/walling should be routinely inspected to identify any breaches, and reinstated or enhanced where necessary.

Barbed and razor wire or broken glass should not be used as part of perimeter protections.

Contractor / visitor controls

There should be clear signs directing contractors/visitors to a reception area. Other access points to the property should be locked or supervised. If you have large premises or do not arrange for contractors to be supervised at all times, identity badges should be issued on arrival and collected at the end of the visit. Details of contractors' vehicles, the person met, and their arrival and departure times, should be recorded. For contractors not known to you identification should always be requested and inspected/validated.

Vehicle access

Vehicular access points to the property should be restricted where possible. The use of retractable bollards, or one way plates, may offer a more aesthetically pleasing alternative to unsightly barriers. Designated parking areas should be well sign-posted, illuminated and located outside secure areas to the property.

The use of number plate recognition cameras at vehicular entrances may also prove a useful theft deterrent.

Security lighting

Security lighting can be operated by timer, photo-electric cell or by passive infra red unit. However, in the absence of reasonable surveillance its use is more likely to aid, than hinder, intruders. Security lights need to be carefully sited to ensure levels of illumination are as uniform as possible, avoiding the creation of shadows and gaps in which intruders could hide.

Landscaping

Avoid providing hiding places or natural ladders to upper floor levels. Prickly shrubs may keep trespassers away from vulnerable areas.

External metal

Whilst lead and copper values have since fallen from their peak in 2007/8 the rewards for thieves are still high and buildings continue to be targeted. Metal roof coverings, lightning conductors, pipework, electrical cabling and statues are all at risk. Financial losses extend beyond the cost of the stolen metal, including damage to stonework caused during the course of theft, and water damage to internal furnishings if it rains before the theft of roof coverings is discovered.

Access control

Access to the property should be restricted to a manned reception where possible. Unsupervised doors should be self closing, self locking and where possible devoid of any external fittings. Doors could be additionally secured using digital keypad or electronic access control locks, passage through which can only be achieved with a known code, authorised swipe card/proximity fob or using biometrics. The advantage of access control locks is that codes are easily changed if cards are lost or staff leave your employ. However, such locks often offer limited physical strength and should only be utilised as a secondary locking system.

The number of door keys issued should be kept to a minimum and a key register retained. The copying of keys by staff should be prohibited. Identifying labels on keys should be avoided; use a key numbering system instead.

Keys held on site must be stored securely to deter unauthorised access. Where a significant number of keys are held on the premises consider installing a proprietary key cabinet in a secure, central location.

Physical security

Where possible external doors should either be constructed of solid timber at least 45 mm thick, or steel, and secured using a mortice or cylinder rim lock conforming to BS3621 (identifiable from a BSI Kitemark on the lock face).

However, a wide range of locks are now available on the market and insurers may accept alternative locking systems. Advice on suitable locking systems for your property can be sought from a locksmith or your local crime reduction officer. Details of locksmiths in your area can be found on the Master Locksmiths Association website, www.locksmiths.co.uk/.

Security of doors not used as final exits, or designated fire doors, may be improved by fitting two mortice rack bolts or two key operated security bolts in addition to the existing fastenings. Outward opening doors should also be secured using hinge bolts, sited near the existing hinges.

The protection of vulnerable doors can be improved by fitting a secondary door i.e. a roller shutter or gate, provided any fire exit doors are not compromised.

Security of existing doors can also be enhanced by reinforcing with sheet steel or timber linings.

Accessible opening windows should be secured using proprietary key operated window locks or restrictors limiting their opening width to no more than 100 mm. In high risk theft areas the use of either fixed internal bars or sliding/collapsible grilles to secure windows should be considered.

The protection of skylights and rooflights should not be overlooked. These should be protected internally, using metal bars or grilles, where located in vulnerable or readily accessible areas.

Cast iron drainpipes can take the weight of two people and could be used to gain access to upper floor levels. Consider relocating drainpipes where appropriate or the use of anti-climb paint to restrict access to roofing. If you use anti-climb paint this should not be applied below a height of 2 metres and warning notices, highlighting its use, should be prominently displayed.

Target areas

These may include areas containing high value, and easily disposable, portable equipment such as tablets, computers and data projectors. Where possible such target areas should not be located on the ground floor. Doors should be constructed of solid timber, at least 45 mm thick, and secured by mortice deadlocks or cylinder rim locks to BS 3621. Accessible opening windows should be secured using key operated window locks as a minimum, but with internal bars or sliding/ collapsible grilles if possible. Where collapsible grilles are used these should be certified to LPS 1175. These areas should be kept locked when not in use and access strictly controlled.

Where it is difficult to introduce adequate physical security measures, consider using intruder alarm protection for specific vulnerable items.

Where possible, high value portable items should be visibly security marked and / or electronically security tagged to deter theft. Though not a visual deterrent, you could use ultra-violet marking which may help in the identification and recovery of stolen items.

Intruder alarms

As well as localised sounders, intruder alarm systems should also incorporate remote signalling to inform authorised persons of an intrusion to the premises.

Where fitted prior to 1 June 2012, systems should have been installed in accordance with BS 4737 Part 1, or PD 6662 and DD 243 or BS 8243 in accordance with the (then) Association of Chief Police Officers (ACPO) Policy on Police Response to Security Systems. In respect of DD 243 and BS 8243, the system should NOT BE configured in such a way as to allow the mere opening (including by force) to disable the alarm and all means of confirmation.

Since 2012 all systems should be installed to PD 6662:2010, BS 8243:2010, DD 263:2010, and in accordance with the National Police Chiefs Council (NPCC) Policy on Police Response to Security Systems. Since August 2017 systems can also be designed and installed to PD6662:2017, BS8243 and BS9263. From 31May 2019 all new PD6662 systems will have to comply with these standards.

Remote signalling systems should contact the alarm company's alarm receiving centre, which is manned 24 hours per day, and conforms to BS 5979 Category II or BS EN 50518.

To comply with the NPCC Policy on Police Response to Security Systems, all intruder alarm systems installed after 1 October 2001, and those systems installed prior to this date but which have subsequently lost police response, must be capable of generating confirmed alarm conditions.

Whilst the NPCC Policy specifies three types of alarm confirmation, Ecclesiastical require that the alarm be sequentially confirmed unless otherwise agreed.

If the installation of an intruder alarm is a requirement of your insurance you will be advised by Ecclesiastical, and the specification must be agreed prior to installation or contracts being signed. The system must be installed and maintained by a company on the official list of recognised firms of a UKAS accredited Inspectorate body i.e. National Security Inspectorate (NSI) or Security Systems and Alarm Inspection Board (SSAIB) and must also appear on the local police force list of compliant companies. For details of NSI or SSAIB listed companies in your area visit their websites, www.nsi.org.uk or www.ssaib.org respectively. The commissioning, maintenance and remote support of intruder alarm systems must be in accordance with the code of practice BS9263:2016.

Closed circuit television (CCTV)

If you have extensive premises where surveillance is difficult, CCTV can be an effective deterrent to intruders.

CCTV permits the continual monitoring of an area using cameras, which is usually linked to a digital recording system or monitored by security personnel. Several considerations should be noted:

- The quality of camera varies tremendously
- Systems can be expensive
- Systems need effective monitoring
- Systems are limited to what the camera can 'see'
- Data protection, civil liberties and human rights issues.

However, such systems can be successful in monitoring car parks and main entrances.

BS 8418 provides a Code of Practice for the installation and remote monitoring of detector activated CCTV.

Cash handling

The possibility of threats of violence to you and employees is as important as the theft of money itself.

To reduce the chances of being attacked by thieves you should consider the following:

- Limit the amount of cash held on your premises as much as possible.
- Pay wages directly into bank accounts using the BACS system.
- Other than for small amounts, at least two able bodied employees should accompany cash in transit. Any policy conditions must be adhered to.
- Where possible vary the time and route taken by staff when banking cash.
- Use a professional cash carrying company for large amounts of cash and certainly for single transits in excess of £10,000.
- Carry out cash counting/handling in a secure internal room (cash office). Our team of specialist in-house surveyors can provide further advice on the design, construction and location of cash offices.
- Provide any persons at risk with personal attack alarms.
- Use a safe for any cash kept on the premises.
- The provision of Automated Telling Machines (ATMs), including convenience ATMs, can attract determined professional attacks which could cause substantial damage to your building, or threats to personnel.

Security guarding

Where there is a high risk of theft, the use of security personnel may be considered. Security guards may be provided in-house or contracted from licensed security contractors. Where in-house security guards are employed, care needs to be taken in their recruitment. Appropriate vetting to establish reliability, integrity and medical fitness should be undertaken. Guidance in this respect is available in the Code of Practice for Static Site Guarding and Mobile Patrol Service – BS 7499.

Where contracted security guards are used, these must be licensed in accordance with the requirements of the Private Security Industry Act 2001. We will also require them to be either NSI or SSAIB approved contractors for the delivery of guarding services.

Additional information

Further useful information is available from RISCAuthority.

RISCAuthority is an annually funded research scheme, supported by a significant group of UK insurers, that conducts research in support of the development and dissemination of best practice on the protection of property and business.

Need to contact us?

For further advice Ecclesiastical customers can call our risk advice line on **0345 600 7531** (Monday to Friday 9am - 5pm, excluding bank holidays) or email us at **risk.advice@ecclesiastical.com** and one of our experts will call you back within 24 hours.

ecclesiastical

Ecclesiastical Insurance Office plc (EIO) Reg. No. 24869. Registered in England at Benefact House, 2000, Pioneer Avenue, Gloucester Business Park, Brockworth, Gloucester, GL3 4AW, United Kingdom. EIO is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Firm Reference Number 113848.