RiskSTOP

Instant Risk Guidance

TR 09a Premises Security

TR 09a Premises Security

Attention should be given to ensuring that the premises are adequately protected against intruders and malicious persons by the provision of appropriate physical and electronic security devices and systems commensurate with the risk, and that systems are designed, installed and maintained to relevant British Standards and other recognised Codes by third party accredited companies.

Physical Protections

As a minimum, all doors should be secured by thief resistant locks such as a mortice deadlock complying with BS 3621 or a padlock, conforming to *Security Grade 5 or 6 of BS EN 12320: Building hardware – padlocks and padlock fittings*, together with the manufacturer's corresponding locking bar and all accessible windows secured by key operated locks. In the case of doors, other than final exits or fire doors, key operated security bolts or heavy-duty barrel bolts may be employed. Depending on the risk, enhanced physical protections may be required, for example, sheet metal linings to doors, hinge bolts to doors with externally exposed hinges, window security grilles or shutters, etc.

When considering the security of fire doors, it is vitally important that under no circumstances must additional physical security measures be fitted without obtaining the prior approval of the Fire and Rescue Service.

Insurance companies will often have a minimum standard of security endorsement attaching to a policy. It is strongly recommended that when a new lock is considered that you ensure that the lock meets the relevant standard prior to its fitting.

Intruder Alarms

Most commercial and industrial premises are likely to require the installation of an intruder alarm as protection against theft and unlawful entry, in many cases as a direct result of the requirements of insurers. In most circumstances, this will require the provision of remote signalling to a third-party certificated alarm receiving centre.

It is normally required that an intruder alarm system be installed and maintained by a company which is acceptable to the Police and is approved by the National Security Inspectorate (NSI NACOSS Gold) or the Security Systems & Alarm Inspection Board (SSAIB).

The intruder alarm company should be instructed to ensure that the system will:

- Conform to at least Grade 3 in accordance with BS EN 50131-1, BS 8243 and BSI Published Document PD6662.
- Qualify for Level 1 Police response and be issued a Unique Reference Number (URN) as necessary.
- Be designed and configured such that when an intruder enters any part of the protected premises there is a high degree of certainty that the alarm system will deliver a sequentially confirmed message.
- Not employ the means of unsetting the system described in paragraph 6.4.4 of BS 8243 (whereby opening the initial entry door will disable all means of alarm confirmation throughout the protected premises).
- Incorporate remote signalling by a dual path Alarm Transmission System (ATS) operating at a performance level commensurate with the risk and which holds third party certification to the related requirements of BS EN 50136-1: 2012 + A1: 2018, or those of BS EN 50136-1: 2012 plus PD 6669: 2017.

Where an intruder alarm system has been specified by insurers, it is strongly advisable that a copy of the System Design Proposal is submitted to them for approval prior to any contract being signed.

Other common intruder alarm considerations include:

- The introduction of procedures to ensure that all movement detectors are able to supervise their intended fields of detection whenever the intruder alarm system is set. It must be positively established prior to each setting of the alarm that movement detectors are not masked, nor is their supervision range diminished by the placement of any stocks or other materials.

- The provision of personal attack devices. Each device must be sited so that it can be operated discreetly by a member of staff and in a location where it is not susceptible to accidental or mischievous activation. It is important to ensure that the operation of a personal attack device transmits a signal to the alarm receiving centre on a silent basis so that there is no audible warning at the point of threat.

It is important to ensure that operation and maintenance of the alarm system is correctly managed to avoid unwanted alarms. In cases where, owing to false calls, Police response has been withdrawn, insurers should be immediately notified and all necessary actions taken to enable Police response to be restored as soon as possible.

Where there is an existing alarm system which either has been installed to the previous standard BS 4737 which pre-dates the European grading requirements, or has been installed to Grade 2 standards, it is important that these systems are assessed to determine whether they are satisfactory or whether by adapting the existing system it can be considered suitable without having to install a completely new system. Areas to consider include, but are not limited to:

- Replacing detectors with anti-masking detectors in vulnerable areas within the buildings which contain attractive contents or areas which are frequented by third party delivery drivers or are directly accessed by the public.
- Increasing the coverage of the system in areas which are unprotected.

Other Protection Methods

Where governed by the risk profile, other forms of security may need to be considered as part of the overall scheme of protection such as security fencing, remotely monitored CCTV, security lighting, security fogging systems, secure cages or rooms for highly attractive and valuable contents and the provision of manned security guarding, etc.

As previously mentioned, it is important that protections are designed, installed and maintained to relevant British Standards and other recognised Codes by third party accredited companies. Third party accreditation should also apply to manned guarding and other providers of security services.

Access Control

In addition to security out of business hours, the matter of access control to the premises as a whole should be addressed and the appropriate measures and systems introduced.

Security Fog Devices

A security fog device (sometimes referred to as a 'smoke' security) consists of an electronic security device which, on activation by an intruder alarm system, produces an impenetrable cloud of dense 'fog' with the objective of disorientating a potential thief and to deter / hinder further access into the protected area.

Originally designed primarily to combat out of hours 'smash and grab' style theft where more conventional security devices might fail to prevent losses, security fog devices are nowadays also regarded as providing valuable protection during the time period between the activation of an intruder alarm and the arrival of response personnel such as police and / or keyholders.

It is important to recognise that in normal circumstances, security fogging is unlikely to be installed in isolation, but as an effective component of an overall scheme of physical and electronic protections.

Whilst in the early days of their development, some concerns may have arisen over the damage to the contents of the premises arising from the occasional over-production of fog, considerable improvements in the reliability and effectiveness of these devices have been made to the extent where they have become generally accepted by many specifiers and insurance providers.

It is essential that security fog devices are designed, installed, operated and maintained in accordance with *BS EN 50131-8: Alarm systems. Intrusion and hold-up systems. Security fog devices.*

Detailed guidance on smoke fog devices can be found in RISCAuthority publication S07: *Security guidance for fog devices*, available at [S07 - Security guidance for fog devices]

It is of paramount importance that the relevant police authority and fire and rescue service are advised in writing of a proposed installation of a security fog system. Both services have developed guidelines for their personnel for when attending premises in which a security fog system has activated.

Ram Raid Protection

Recent years have seen a significant increase in the crime of 'ram raiding'. Whilst traditionally targeting retail premises, criminals have moved towards focusing on ram raid attacks of ATMs and industrial premises, employing mechanical diggers and other heavy vehicles, influenced by the growing presence of modern buildings with lightweight construction.

As well as the theft of contents, significant collateral damage to the building fabric, and subsequent business interruption often arises.

Targets for ram raid attack include, but are not limited to:

- ATMs
- Computer and electrical products
- Designer clothing
- Electronic goods
- Non-ferrous metals
- Cigarettes and spirits

Measures employed with the objective of deterring / frustrating a ram raid attack (which should be determined by a risk assessment) include:

- The installation of proprietary products across potential points of attack such as posts, fixed or retractable bollards, fixed or moveable barriers, girders or gantries.
- The use of natural barriers such as ditches, mounds or embankments, or civic obstacles such as stone or concrete structures.

The risk may also be reduced by the placement of the bulk supply of target commodities in an internal physically secure area, well away from potential points of perimeter attack.

It should be remembered that some forms of external ram raid protection will require local authority planning consent before installation. Planning consent will also be required for the installation of street furniture such as posts, bollards or planters on any public thoroughfare. In respect of private property, such restrictions may not apply, however where the property is tenanted, the permission of the property owners will be needed.

Anti-ram raid bollards should be certified to *BSI PAS 68: Impact test specification for vehicle security barrier systems,* and selected and installed in accordance with *BSI PAS 69: Guidance for the selection, installation and use of vehicle security barrier systems.* It is also recommended that companies involved in the manufacture and installation of such products should be selected from those that are registered members of the Perimeter Security Suppliers Association -Ǎhttps://www.pssasecurity.org/

For detailed information and guidance on ram raid protection, reference should be made to RISCAuthority publication S10: *Guidance for protection of premises against attacks using vehicles (ram raid)*, available at S10 - Guidance for protection of premises against vehicle attacks (Ram Raids)

Protections Management

At risk of stating the obvious, it is vitally important that close attention is given to ensuring that all physical and electronic protections are maintained in an operative state and that they are placed in force as appropriate on close of business each day.

Keyholding should be restricted to a minimum number of trusted persons for whom the appropriate closedown instructions should be given and an up to date register of all keyholders kept.

Where taking occupation of newly acquired premises, all external door locks, alarm codes, etc. should be changed as necessary. This should also apply in circumstances such as when keys are lost or misplaced and may also be required where keyholders are no longer employed.

Additional Information

Detailed information on a wide range of security measures are available at https://www.thefpa.co.uk/advice-and-guidance/free-documents?category=10