RSA

SECURITY

Contents

Introduction

To prevent intruders and arsonists gaining access to any premises suitable security measures are essential. Some intruders will be opportunistic, but others are determined and organised intruders who will have done their homework in targeting the “weakest link in the chain”. This is why a “layered protection” approach is often the best plan to achieve a level of security commensurate with the risk.

This guide focuses on perimeter and building security. It makes reference to guidance and best practice published within the United Kingdom.

Essential Principles for Security of Property

There are generally no specific regulations to adopt set levels of perimeter and building security. Any references to regulations is typically related to maintaining emergency escape and preventing access to premises where danger may exist, i.e. a duty of care.

Security measures can be considered in terms of three broad categories:

- Physical security
- Electronic security
- Human security

Best practice when reviewing existing or planning new security can be found in Essential Principles for the Security of Property (S20) published by the RISCAuthority.

This covers security risk assessment, effective communication, reduction of intrinsic risk, strategy, active and pasive protection measures, selection of providers, training, maintenance, continuous review and the retention of records.

Physical Security - Locks

There are a wide range of security locks available to purchase. These include five-lever mortice deadlocks; cylinder locks and magnetic locks. The complexity and quality of lock design and manufacture is fundamental to the level of protection provided. A summary of related British / European standards is included within the Appendix to this guide.

Claims that a lock has been tested to a particular standard can only be relied upon where the test has been undertaken and "certified" by a recognised independent test body.

For the UK these include:

- British Standards Institute (Kitemark scheme) https://www.bsigroup.com/en-GB/kitemark/
- Master Locksmiths Association (Sold Secure scheme) www.soldsecure.com
- Building Research Establishment Limited (LPCB scheme) www.bre.co.uk

Doors

Doors especially those of lighter construction, can be vulnerable to attack by intruders even when they are fitted with the best quality locks and bolts. Door panels can be kicked-in or hand-tools used to cut a body-sized hole.

Even doors that appear solid are frequently found upon close inspection to be of only semi-solid construction and/or filled with lightweight material. It is therefore essential to reinforce such doors with sheet steel; particularly for external or internal doors in vulnerable or target risk areas.

Timber doors should be of external grade and a min thickness of 45mm, noting that hardwood is generally stronger than softwood.

The following specification is suitable for locksmiths or builders when over-cladding and improving door security:

- Doors to be clad on their external face with a single panel of sheet steel not less than 1.5mm fixed using coach-bolts of a minimum diameter of 6mm passing through the full thickness of the door and spaced at intervals not exceeding 150mm, all round the perimeter of the door.
- Coach-bolts to be fitted at similar intervals through the cross bracing and centre rails of the door.
- All securing nuts and washers to be on the inside of the door welded to the bolts, or alternatively the ends of the bolts should be modified (burred) so they can't be readily undone**.**
- If in exceptional circumstances, it is necessary to steel-reinforce the door on its internal face, 5.5mm diameter wood screws with non-return heads and at least 25mm in length should be used at intervals not exceeding 100mm in place of coach-bolts.
- Hinge bolts should be installed top and bottom. In order to carry the additional weight it may be necessary to fit additional hinges to the door.

An alternative is to install internal or external lockable steel bar/mesh gates, roller shutters, or internal collapsible (folding) steel grilles.
These should ideally be certified as meeting a recognised security standard, e.g. a suitable security level of the Loss Prevention Certification Board's LPS 1175 scheme.

Windows

Many burglars favour access via a window to gain unlawful entry.
Window locks offer a minimum level of protection that may be sufficient to deter an inexperienced opportunist, but they will not withstand a determined attempt at forced entry. Leverage a window frame with a hand-tool, or simply breaking and removing the glass pane will generally be sufficient to gain access.

It can therefore be desirable in many instances, to fit steel bar grilles to windows, particularly those in vulnerable locations.

The following specification is suitable for locksmiths or builders when installing window grille bars:

- Grilles to comprise vertical solid steel bars at least 20mm in diameter or square section spaced at not more than 100mm centres. The bars to pass through and be welded to tie bars of flat steel not less than 35mm x 6mm spaced not more than 600mm apart.
- Grilles to be fixed, preferably on the inside of a window opening, using one of the following methods:
    - Bars to be grouted into the brickwork at top and bottom to a depth of at least 50mm and set back at least 50mm from the surface of the wall.
    - Tie bars to be cut, splayed and grouted into brickwork to a depth of at least 50mm and set back at least 50mm from the surface of the wall.
    - The bars to be welded to a frame of angle iron with a minimum dimension of 35mm x 35mm x 3mm which must be fixed to the brickwork surrounding the window (not to the window frame) by either 75mm x 9mm proprietary anchor bolt for fixing into masonry (e.g. Rawlbolts) or 75mm 5.5mm diameter countersunk woodscrews with suitable proprietary wall plugs at 300mm intervals all round the opening. Bolts or screws to be spot welded to the frame.

Alternatively, consider internal or external lockable steel bar/mesh gates, roller shutters, or internal collapsible (folding) steel grilles.

These should ideally be certified as meeting a recognised security standard, e.g. a suitable security level of the Loss Prevention Certification Board's LPS 1175 scheme.

Further Guidance and information can be obtained from:

Master Locksmiths Association (MLA) - www.locksmiths.co.uk
Door and Hardware Federation (DHF) - http://www.dhfonline.org.uk/
Glass & Glazing Federation - www.ggf.org.uk

Intruder Alarms

Intruder alarms are often a prerequisite of insurance. They provide a high level of theft deterrent as well as early notification of unauthorised entry.

RSA recommends in the UK that the alarm system be installed and maintained by a company that is recognised as an installer of intruder alarms by either the National Security Inspectorate (NSI) or the Security Systems and Alarms Inspection Board (SSAIB). It must also be recognised as a Compliant Company by the relevant responding police force. Remote signalling (if incorporated) to connect to an Alarm Receiving Centre which is inspected and certified by NSI or SSAIB. (In some circumstances, a more restricted selection of installation, maintenance and / or monitoring companies may be warranted).

Unless more specifically confirmed, the security grading of the intruder alarm system (detection and control equipment) should be to Grade 3 according to BS EN 50131. Refer to RISCAuthority document “S14”, see Appendix.

The following provide good practice guidance suitable for most commercial and industrial premises:

- Except for ancillary control equipment (such as remote keypads and digital key readers), control and signalling equipment must be located in a position where it is concealed from general view and is least vulnerable to attack.
- Audible warning must be by either two external self-actuating audible warning devices or by one external self-actuating warning device and an internal self-actuating siren or two tone electronic sounder, each giving a sound emission of at least 100dB at 1 metre.
- Where it is not possible to install an external warning device above 3 metres (i.e. so that it would not be readily reached from ground level), two external self-actuating warning devices must be fitted. They should be sited on different elevations of the premises, where possible.
- Where the system has remote signalling, which is usually desirable, any internal warning device must be sited remotely from the control panel so as not to identify the position of the panel when activated. For the same reason, any internal sounders used as part of the alarm setting / unsetting procedure must also be sited remotely from the control panel.
- The means of unsetting to be via an entry door lock linked to the alarm, unless the entry route or premises are considered low risk, in which case, use of a remote control device (transmitter or fob) upon entry is acceptable.
- Confirmable intruder alarm systems should incorporate:
    - The whole system 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 confirmed alarm message.
    - Signalling by any Dual Path Remote Signalling product that has been tested and certificated to LPS1277 issue 3 as conforming to ATS5 configured as such and installed in accordance with annex C of that standard. For example: BT's Redcare Secure IP, Emizon's TCD DP Grade 4 and Chubb's eConnect

G4. Other signalling products complying with this standard may also be acceptable.

- Following the cancellation of an alarm signal the system must re-arm without any zone, sensor or detector being locked out, so that the whole system remains alert to signal further alarm information during the set period.
- To prevent tampering once the system has been set, all microphones and cameras intended for confirmation purposes must be located within areas covered by intruder alarm detection devices.
- All control and remote signalling equipment other than ancillary control equipment (such as remote keypads and digital key readers) must be located so that it cannot be accessed whilst the alarm is set, without creating a confirmed alarm condition.
- The alarm specification (system design proposal) must include the actions to be taken by the alarm receiving centre upon receipt of the following alarm messages or information:

    1. A confirmed alarm condition, including circumstances where the loss of one or more signalling paths contribute to the confirmation criteria.
    2. An unconfirmed alarm condition, including any variations according to whether or not the system can be rearmed in its entirety.
    3. A telecommunications failure, including the failure of one telecommunication path in a dual-path signalling system.

Response to be by the police, at the highest response level provided for by the responding force's Security System Policy (SSP) and keyholders owners / staff or an Security Industry Association (SIA http://www.sia.homeoffice.gov.uk/Pages/home.aspx) approved professional key-holding response company.

Insurance representatives must be informed immediately if there is a notification of a reduced level or withdrawal of Police response to the intruder alarm system. The premises must not be left unattended, unless physically secured and the alarm system is fully set including the designated methods of remote signalling.

If the alarm is activated (whether the activation is confirmed or not), or any signalling path is lost, the appointed key-holder must attend the premises immediately to investigate the reason for the activation. If there is a fault with the alarm system or an alarm signalling path, an alarm technician should be called and the keyholder should not leave the premises unattended until they are fully re-secured, with the alarm system and its signalling paths fully reset.

Failure to both fully secure and alarm the premises may invalidate insurance cover.

See Appendix for further guidance.

Closed Circuit Television (CCTV)

The presence of a CCTV system is widely accepted as a useful means to deter, or otherwise help to detect and limit, unauthorised access and criminal activity.

There are many types of CCTV system available however whatever type of system is used, it is important that it is reliable, resilient against interference, has adequate coverage. All at risk areas should be covered i.e. areas attractive to trespassers/criminals. A suitable method of 'real time' monitoring and response to viewed events is essential.

Detector-activated CCTV systems monitored at a remote video response centre, allow intrusion to be detected and observed without the need for continuous on site monitoring or expensive guarding.

Prior to installation of CCTV systems, careful analysis should be made in consultation with insurers. Suitable standards are available from the National Security Inspectorate **NSI** or The Security Systems Alarms Inspection Board (**SSAIB**). See Appendix for references.

Cash Security and Defence Against Robbery

Cash continues to be one of the most thief-attractive commodities and where possible the amount of cash held should be minimised. Cash holdings can be reduced by making/receiving payments by cheque or electronic transfer. Staff involved with cash exposures, even those not directly handling cash can find themselves involved in a threatening situations simply through their presence at the scene of a criminal attack.

Businesses most at risk include those dealing with high value easily transportable goods such as jewellery, designer clothing, portable electronic devices, tobacco products, wines and spirits. Cash related operations such as post offices, pawnbrokers, book makers and petrol filling stations are also at high risk of being targeted. Cash dispensing machines also increase the likelihood of an attack. Late night working hours may increase the likelihood of being targeted.

Further information and guidance is available within the Appendix below.

Security Fencing

Security fencing particularly, when used in conjunction with static guards and/or security lighting and CCTV is a very useful first line of defence.

There are two main types of fencing: perimeter fencing, such as chain-link, welded mesh, and steel-palisade and electrified security fencing.

The relevant British Standard is BS1722. Parts 10, 12 and 14 cover perimeter fencing and part 17 covers electrified security fencing.

Maintenance of security fencing is very important and procedures should be in place whereby the fence is inspected in its entirety on a regular basis, e.g. once a day, week or month according to the degree of risk.

Any breaks, holes or other damage should be repaired without delay. Wherever possible, trees and undergrowth should not be permitted to grow close to the fence (on either side) as these can provide concealment and possibly be an aid to scaling the fence. For the same reasons, pallets, material storage, outbuildings, skips, etc. should not be positioned close to a security fence.

Gates in security fencing should be installed with a commensurate level of security to the fence itself.

The hinge pins of security gates should be capped by a disc of mild steel welded to the top of the pin to prevent the gates being lifted off their hinges.

Alarm signalling on fences may be local (audible) to an on-site security facility, or remote to an Alarm Receiving Centre. Where response to fence activations involves contracted security personnel the personnel should be suitably licensed e.g. in the UK SIA or SSAIB see appendix.

Computer Security

Computer and other electronic office equipment in business premises are particularly attractive to thieves. The impact of theft is not just related to loss of hardware but may also compromise data security. In environments where thieves may operate, which includes open plan office environments, portable computer equipment should be locked safely away or secured to the workstation when not attended. Care should be taken that securing equipment is compatible with the computer equipment and associated warranties.

Fuel Crime

Above ground diesel tanks at farms, goods storage locations and domestic premises are a target for thieves. Collateral damage following fuel theft can often lead to fuel leaks contaminating the ground with associated high clean-up costs.

Given this theft risk all fuel storage facilities should be subject to a suitable risk assessment.

Fuel tank theft security measures include:

- Isolation of electric pumps
- Closed shackle padlocks on filler caps
- Anti-siphon devices
- Minimising fuel levels
- Access controls, fencing and lighting
- CCTV
- Intruder alarms (where practical)

Manned Guarding

Traditional manned security guarding remains a mainstay in security strategy. To help ensure that security guards provide a good quality defence they should be subject to suitable background checks and certifications, and suitable onsite systems such as guard tour verification and lone worker controls.

In the UK licensed security personnel can be contracted from firms that are approved by the National Security Inspectorate (NSI), Security Systems and Alarms inspection Board (SSAIB) or the Security Industry Authority Approved Contractor Scheme (SIA-ACS).

Metal Theft

The rising worldwide demand for metals has resulted in a significant increase in their market value which in turn has led to a very serious rise in the number of metal related thefts, particularly of non-ferrous metals such as copper and lead.

Many of the losses have involved thieves targeting unoccupied buildings for copper cabling, pipe-work, sanitary fittings and lead from roofs.

In addition to the cost of replacing stolen property, the damage caused to the fabric of the building through its forced removal can also incur very large repair bills. Where the theft of lead from roofs has not been detected quickly enough, losses have been greatly increased due to subsequent damage caused following rainwater ingress.

Security Fog

A Security Fog Device is an electronically operated security system, which on activation produces a dense “fog” in order to disorientate a potential thief and deter/hinder further access into the protected area.

Fog is produced by passing glycol (or other fluid) through a heating block, where it vaporises before being emitted into the area to be protected. The fluid may be pumped through the heating block or released from a pressure container. As the vapour is released into the atmosphere it instantly condenses to form a dense white fog. Glycol based products are considered to be non-toxic.

Security fog may be combined with flashing lights and sirens to further disorientate potential thieves. These systems are typically used in retail environments and careful consideration must be given to employee and customer safety.

Security Fog Devices should be designed, installed and maintained in accordance with the manufacturers specifications and conform to BSEN50131-8 Alarm Systems Intrusion and hold up systems – part 8 Security Fog Device/Systems in conjunction with insurers requirements.

Protection of Unoccupied Buildings

Fire, theft and malicious damage in empty premises is a significant cause of loss.

There is evidence to suggest that once a building has been vandalised, further attacks can occur within a short period of time.

Good management procedures including regular inspection visits (at least once a week), regular maintenance of the property and fire and security systems can help to prevent criminal attack and also reduce the eventual cost of remedial work should a loss occur.

It is important to ensure that the fabric of the building is maintained in good order. Without regular maintenance an unoccupied property can quickly become run-down and attract unwelcome attention, such as from vandals and fly-tippers. Graffiti should be removed and any damage repaired without delay.

Unoccupied buildings are an attractive playground to children. Children and other trespassers are owed a duty of care such that even unoccupied buildings need to be maintained as safe environments as far as reasonably practicable. Unoccupied buildings should of course be maintained as safe environments for those with legitimate access.

Best practice precautions should include the removal of all non-essential contents and services. However adequate physical security and alarms should be maintained.

Appendix

The following standards are based on United Kingdom guide and best practice from UK sources.

Relevant Standards

BS1722:10 Specification for chain-link and welded mesh anti-intruder fences
This type of fence can be considered suitable as a general purpose or low security fence. Where enhanced levels of security are required BS1722 part 12 or 14 should be specified.

BS1722:12 Specification for Steel Palisade anti-intruder fences
This type of fence can be considered suitable for all types of fencing from general purpose to extra high security fencing.

BS1722:14 Specification for open mesh steel panel fences
This standard specifies the requirements for four standards of open mesh steel panel fence ranging from fences suitable for boundary and general purpose to fences suitable for extra high security.

BS1722:17 Specification for electric security fencing - design, installation and maintenance
This standard specifies the requirements for electric security fencing.

UK Lock Standards

Of the various UK test standards that can apply to locks, the one most commonly cited by UK insurers over the years has been BS 3621, evolving into the x621 Series and sits alongside European Standards for door locks (EN 12209 and EN 1303).

BSEN 12209
This is a UK version of a European Standard for door locks. Numerous different combinations (Grades) of lockcase/lock mechanism and key security are available, plus related testing for attack resistance, force, durability, fire and safety. The x621 Series up to Security Grade 7, Key Security B - the latter only for lever locks. If a cylinder is used reference is made instead to BSEN 1303.

BSEN 1303
This is a UK version of a European Standard for lock cylinders. Various security levels against attack and for key security are available. The x621 Series up to Key Security Grade 5, Attack Grade 2.

TS007
This is a UK Standard developed to recognise and protect against the risk of ‘snapping attacks’ on door lock cylinders. Snapping attacks relate to a form of criminal attack whereby a protruding cylinder is gripped by a wrench, or similar tool, and twisted until it snaps in its narrow middle section. TS 007 cylinders with a 3 Star rating can resist such attacks on their own, but a 1 Star cylinder needs to be married up with a 2 Star surrounding door handle to give an overall 3 Star level of protection.

TS008
A UK Standard for testing letter flaps for resistance to external access/manipulation of internal door lock mechanisms.

PAS 24
Applies to manual attack testing of single leaf domestic doorsets and windows, including locks (but excluding picking/sawing) and hinges. Any glazing must be laminated if the door/window could be opened from inside without a key, and similarly any letter flap must defeat external manipulation of a door lock release.

BS 8607
This is a UK Standard for mechanically operated push button locksets. A Grade 4 rating is intended to be comparable to a x621 series lock.

BSEN 12320
This standard reflects a European Standard for padlocks and staples (padbars) of all types, i.e. open and closed shackle. Security Grades range from 1-6, 6 being the highest.

BSEN 179 & BSEN 1125
These standards are UK versions of European Standards for emergency escape door mechanisms at premises where, respectively, no panic is likely to occur, e.g. a factory/office, and those where it might, e.g. a shop or club/pub. Where an external keylock is incorporated, it should be tested to a security level chosen from BS EN 12209 (for external attack only).

Further information and guidance can be obtained from:

ATM Recommended Security Measures (S3)

Audible Only Intruder Alarm Systems Summary for Insurers Typical Requirements (S13)

Cash Risk Assessment an Insurers Guide (S18)

Cash Security a Users Guide (S22)

Code of Practice for the Protection of Empty Buildings Fire Safety and Security (BDM10)

Electronic Security Systems guidance on Keyholder and Selection Duties (S6)

Guide to Electronic Access Control System (S29)

Guide to Shop Front Protection (S16)

Guidance for Specifiers of CCTV in Security Applications (S23)

Intrusion and Hold Up Alarm Systems (S9)

Measures for the Control of Metal Theft (S21)

Physical Security for Homes (S25)

Physical Security for Homes: Guidance for Occupiers (S24)

Police Response Intruder Alarm Systems 10 Step Guide for Purchasers (S12)

Police Response Intruder Alarm Systems Summary of Insurers Typical Requirements (S14)

Security and Arson Prevention (S1)

Security of Emergency Exit Doors in Non-Residential Premises (S11)

Security Guidance for Defence Against Robert (S19)

Security Guidance for Fog Devices (S7)

The Selection and Use of Electronic Security Systems in Empty Buildings (S4)

British Standards Institution www.bsi-global.com

European Fencing Industry Association - http://www.efia.co.uk/ or Tel 0845 450 4898

Fence Contractors Association - www.fencingcontractors.org or Tel 07000 560722

Loss Prevention Certification Board - www.redbooklive.com

Secured By Design (SBD) - www.securedbydesign.com

Security Industry Authority - http://www.sia.homeoffice.gov.uk/Pages/WelcomePage.aspx

The National Security Inspectorate (NSI) - www.nsi.org.uk Tel 0845 006 3003

The Security Systems and Alarms Inspection Board (SSAIB) - www.ssaib.org or Tel 0191 296 3242

The RISCAuthority (the UK insurers' technical advice body) www.riscauthority.co.uk

Vacant Property Security - http://www.vpsgroup.com/

