RISCAuthority

administered by

FPA Fire Protection Association

S19 Security guidance for defence against robbery

Version 2 Published 2021

Cover image: Getty/vchal

IMPORTANT NOTICE

This document has been developed through RISCAuthority and published by the Fire Protection Association (FPA). RISCAuthority membership comprises a group of UK insurers that actively support a number of expert working groups developing and promulgating best practice for the protection of people, property, business and the environment from loss due to fire and other risks. The technical expertise for this document has been provided by the Technical Directorate of the FPA, external consultants, and experts from the insurance industry who together form the various RISCAuthority Working Groups. Although produced with insurer input it does not (and is not intended to) represent a pan-insurer perspective. Individual insurance companies will have their own requirements which may be different from or not reflected in the content of this document.

FPA has made extensive efforts to check the accuracy of the information and advice contained in this document and it is believed to be accurate at the time of printing. However, FPA makes no guarantee, representation or warranty (express or implied) as to the accuracy or completeness of any information or advice contained in this document. All advice and recommendations are presented in good faith on the basis of information, knowledge and technology as at the date of publication of this document.

Without prejudice to the generality of the foregoing, FPA makes no guarantee, representation or warranty (express or implied) that this document considers all systems, equipment and procedures or state-of-the-art technologies current at the date of this document.

Use of, or reliance upon, this document, or any part of its content, is voluntary and is at the user's own risk. Anyone considering using or implementing any recommendation or advice within this document should rely on his or her own personal judgement or, as appropriate, seek the advice of a competent professional and rely on that professional's advice. Nothing in this document replaces or excludes (nor is intended to replace or exclude), entirely or in part, mandatory and/or legal requirements howsoever arising (including without prejudice to the generality of the foregoing any such requirements for maintaining health and safety in the workplace).

Except to the extent that it is unlawful to exclude any liability, FPA accepts no liability whatsoever for any direct, indirect or consequential loss or damage arising in any way from the publication of this document or any part of it, or any use of, or reliance placed on, the content of this document or any part of it.

Contents

Scope 2

1 Introduction 2

2 Employee safety - a legal requirement 3

3 Evaluating the risk 3

4 Premises design 4

5 Physical protection 4

6 Cash security 5

7 Cash in transit 6

8 Safes 6

9 Electronic security systems 7

9.1 Video surveillance systems (VSS, formerly termed CCTV) 7

9.2 Intruder alarms 7

9.3 Hold-up (personal attack) alarms 8

9.4 Access control 8

9.5 Security fog devices 9

10 Forensic coding system 10

11 Policies and procedures 10

12 Staff training 11

13 Key holding 11

14 Summary 12

15 References 12

16 Further reading 13

Scope

This guide considers the defences available to commercial undertakings, typically retailers, who through the conduct of their business are exposed to the attention of potential assailants prepared to rob them of cash or property. It is not intended to cover theft not involving coercion against persons, eg burglary. However, at certain times the crime considered in this guide has been referred to as aggravated burglary. Outside the scope of this guide are the largest targets of the type that attract highly organised and resourced teams with very violent methods including ‘tiger kidnap’ hostage scenarios. Also outside the scope of this guide are the specific issues confronting locations with heavier risks of raids targeting cash such as cheque cashing outlets, bureaux de change, pawn brokers, sub post offices, bookmakers, jewellers, large retailers, casinos, building societies, banks and the like. Additional guidance for specific theft risks is availably in wider suite of RISCAuthority security guides, including S7 *Security guidance for fog devices* and S22 *Cash security a user’s guide*.

1 Introduction

Robbery attacks involving threatened, perceived or actual physical assault, resulting either directly or indirectly in the loss of property and cash from a variety of businesses is an important issue for insurers and their customers. There are several categories of robber from the professional to the opportunist or someone perhaps moving up from mugging or street robbery. Organised robberies will often involve considerable force, usually with more than one offender commonly holding weapons such as knives, pick-axe handles, baseball bats and, potentially, firearms. Drug and alcohol abuse related issues are often the main factors, resulting in unpredictable, and often violent, behaviour. Apart from the financial loss, there is the additional human cost in potential trauma, stress and physical injury. These effects combined could result in a small business failing to fully recover following such an attack.

Businesses most at risk include those dealing in ‘traditional’ high-value, easily transportable goods that are of attraction to the criminal fraternity, for example jewellery, fashion clothing, mobile phones/PDAs, high specification computer equipment, off licences and convenience stores with cigarettes/tobacco and wines/spirits, and cash-related operations, including post offices, pawnbrokers, bookmakers and petrol filling stations. The presence of an ATM facility can also greatly increase the likelihood of an attack, particularly if this is a ‘merchant fill’ type, ie directly controlled by the business proprietor. Late night opening hours can also increase vulnerability and the likelihood of being targeted.

Exposure to attack and the subsequent loss can be significantly reduced by a combination of staff training, premises design and by the provision of suitable and appropriate physical and/ or electronic-based forms of protection systems. Whilst not exhaustive, this guide contains information on some of the possible courses of action that can be taken in order to reduce the overall exposure and impact of robbery attacks on vulnerable businesses.

2 Employee safety – a legal requirement

It is important to fully appreciate that management's responsibilities do not end at the safe preservation of property and monetary assets. The crime of robbery clearly also presents risks of physical and psychological injury to staff and other persons on the premises which management must take equally seriously. There is a legal requirement under the Health and Safety at Work Act to provide a safe place and safe systems of work and also to provide adequate training and instruction for employees. Under the Management of Health and Safety at Work Regulations it is a legal requirement to carry out written risk assessments for all significant and reasonably foreseeable risks. This is also good risk management practice and it helps prioritise risk control measures, making sure that the most important risks are tackled first. This important aspect of risk management is considered in more detail in this document in the section: Policies and procedures.

3 Evaluating the risk

Businesses, particularly larger operations and those involving multiple outlets, should look to prepare a robbery prevention plan with staff involved as necessary in its content to ensure maximum practical value. This would be based on a risk assessment considering a range of factors including the following:

- Location and crime profiles in the area. Most robberies occur in large metropolitan areas with inner cities generally suffering higher crime rates considered to be particularly at risk. (Local crime statistics are available from www.police.uk). You may also speak with your neighbourhood police officers to identify your local risk.
- Amount of potential target goods/cash held on site. Higher value property will attract the attention of more professional thieves with better planning and the potential for violent attacks.
- Type of business. Some businesses can be targeted because of the perception that large amounts of high-value goods and/or cash will be on site (whether or not the case).
- Working hours operated. Premises that are open during unsociable hours could be more vulnerable.
- Type and number of staff on site. Young, inexperienced staff could be more vulnerable. There should be an adequate number of staff available as evidence gathered by various police forces would indicate that the number of staff present can greatly assist in deterring attacks.
- Standards of security in place.
- Premises design and suitability.

Sharing of information with other businesses in the area can be beneficial, particularly joining an 'early warning' crime alert scheme which will often include mobile communication systems to quickly pass on information. Maintaining regular contact with local police will keep you informed of local crime trends, emerging patterns and ready access to crime prevention advice.

As part of the overall security review, it is important that the safety of employees is fully considered as part of the risk assessment and measures implemented take into account the requirement to provide, 'so far as is reasonably practicable', the health, safety and welfare of employees as required under health and safety legislation.

4 Premises design

Consideration should be given to the premises design externally and internally to identify and, where practicable, reduce any vulnerability. A layered approach to security measures is often the most effective strategy to defend against, and delay, attacks on target goods.

Externally, this can include effective perimeter fence/gate security where possible and restricting those areas that could provide opportunities for concealment and possibly impede the effectiveness of any closed circuit television system. This would include hidden recesses, obstruction of main approaches such as waste bins or excessive vegetation growth. Where such features are unavoidable, then these should be taken into account when establishing the opening/closing and response protocols.

External areas designed for staff smoking should carefully be considered for potential vulnerabilities to staff from attack with the possible intention of gaining entry to the premises by use of duress. External doors and windows are the next layer of protection and their construction and security need to be commensurate with the identified risk.

Internally, consideration should be given to the layout of any areas open to the general public, such as sales floors and point of sale counters. Ideally, the main entrance should be clearly visible with the point of sales area arranged to prevent, or at least restrict, unauthorised access.

Target sales stock should ideally be with in staff attended sections of the sales area and consideration should be given to using 'dummy' stock or packaging with the real items retained in a secure store or cabinets under the control of authorised staff.

There should be a good overall level of illumination, both externally and internally. Use of mirrors, both decorative as fitted to pillars and other structural features, as well as purpose-designed security mirrors, can be of great assistance in maintaining effective surveillance as well as acting as a possible deterrent.

5 Physical protection

The risk of a person or persons breaking into a premises whilst occupied to commit robbery, or prior to opening in order to await the arrival of staff to hold them under duress whilst robbery is committed, needs to be considered. The appropriate levels of building perimeter physical security need to be put in place, especially in places which could be accessed to gain entry to restricted areas of the premises that are not generally available to the public. This would include perimeter doors fitted with suitable, good quality locks and vulnerable windows secured with security shutters, steel bars, security screens or security glazing.

High-value target goods should be specifically protected where possible, which could include suitably secured steel weld mesh cages in stock rooms, lock down enclosures for computer equipment or robust counter units on sales floors.

Display cases housing high-value target items should be of strong, attack-resistant types. Sufficiently strong cases can often compensate for limitations in other security elements. The main considerations for such display cases are:

- **Locks.** These need to be robust and resistant to picking and direct physical attack; ideally they should be hidden from view.
- **Hinges.** Need to be of a similar standard, being well secured to the case.
- **Framing.** Construction of the frame should be such that an attack will not affect the overall integrity of the case.
- **Glazing.** The most vulnerable part of the case, the glazing, needs to be laminated and set well into the frame.

The level of protection provided by display cases should take account of the value and attractiveness of the object to be displayed but other factors will always need to be considered in the assessment, for example the quality of the supervision, the physical and electronic security of the premises and where the case is located. In the event of a display case with high attack resisting qualities being needed, the following aspects should be considered:

- the glass should conform to an appropriate category of BS EN 356: *Glass in building. Security glazing. Testing and classification of resistance against manual attack*;
- the case should be steel framed with flanged corners to hold the glass in place. These flanges should have at least 20mm overlap around the glass to prevent a levering attack on the corners of the case;
- unglazed sides to the case may need to be of steel. MDF type materials are unsuitable;
- the case to be secured with good quality, high security locks. Generally at least two locks should be fitted to each opening in the case. Ideally, locks should be concealed and protected from direct attack;
- lighting should be housed in a separate light box compartment secured by different locks to the main display section which will enable the lighting system to be maintained without opening the display section. The case should be constructed to prevent access to the contents via the light box compartment;
- ideally, hinges should be concealed and thereby protected from direct attack. However, if they are exposed they need to be supported by steel hinge bolts and resistant to attack through the hinge pins being driven out; and
- owners of cabinets with target contents likely to provoke a sustained attack should consider using a cabinet certificated as having been tested to a suitable security rating of a scheme such as LPS 1175 or LPS 1270.

6 Cash security

Operators of businesses with significant amounts of cash at risk are strongly advised to obtain guidance from their insurer.

Cash is, of course, highly theft-attractive and the target in many robbery attacks. Wherever practicable, the amounts of cash held on the premises and cash handling should be kept to a minimum with non-cash transactions encouraged whenever possible, use of direct bank transfers (BACS) or cheques instead of cash payments to staff and regular banking or collections by professional cash carrying companies.

Where a till is used for cash control, a till limit needs to be applied. The till limit should be set as low as is reasonably practicable for the individual business (some modern electronic point of sale tills can be programmed to provide either a visual and/or audible warning on reaching a preset limit). Specific cash till controls include the use of anti-grab till screens designed to fit around the till drawers to make access difficult when the till is open. Access to the rear of counter areas should be restricted and controlled.

Counter caches can be used as a useful method to store cash (usually bank notes) thereby reducing the holding in a till prior to collection and deposit within the safe (see section 8). Such devices should be securely fixed.

A key precaution is to ensure that the aggregate of cash found in the public area is limited and kept under control. As the contents of tills, caches etc reach their limits the contents should be removed to a secure room (a cash office) in which the cash is processed (eg counted) out of sight of visitors and made secure, for example deposited in a secure container, usually a safe. The cash office should have a location as near as possible to the centre of the premises and, if possible, on an upper floor. The construction of the cash office and the security of the door(s) and any window(s) should be commensurate with the highest value in cash that it ever contains. Realistically this may mean, for larger amounts, reinforced door(s) with lock(s) to a recognised high security standard, blanked over window(s) etc.

Where large amounts of cash are held within an automated teller machine (ATM), special precautions need to be taken to mitigate the risk. For further guidance in the use and operation of ATMs reference should be made to RISCAuthority Guidance Document: S3: *Convenience ATMs Recommended Security Measures for Business*.

7 Cash in transit

Where staff are used for banking or other cash in transit activities then it is essential that sufficient personnel are chosen as escorts with times of transfer varied, as should the vehicles and routes used. A thorough risk assessment is necessary to determine the actual arrangements that are necessary and these will also hinge on the amounts at risk and any insurance company policy requirements.

Proprietary transfer bags should be considered which may include portable transmitters linked to devices which emit a dye or cloud of smoke should the bag be snatched, for example.

The Personal Protective Equipment at Work Regulations state that protective equipment is to be supplied and used at work wherever there are risks to health and safety that cannot adequately be controlled in other ways. Where there is significant potential for an aggravated attack on collection/delivery staff with serious consequences resulting in bodily injury or fatality, even with procedural control measures in place, Personal Protective Equipment (PPE) such as stab or bullet resistant vests should seriously be considered in order to reduce the risk to employees so far as is reasonably practicable.

However, the use of a professional Cash in Transit company should be considered where there are large amounts of cash involved. Any such company needs to operate in accordance with BS 7872. They should also be inspected and approved by a third party UKAS accredited approval body such as the National Security Inspectorate (NSI) and Security Systems and Alarms Inspection Board (SSAIB).

8 Safes

Safes should be suitably located in an area of the premises out of public sight, access to which is controlled and restricted to authorised persons only. The safe should be kept closed and locked at all times other than when immediate access is required.

Any safe in use needs to have an adequate cash limit suitable for the proposed maximum value of cash required to be retained. It is strongly recommended that the insurance company is approached for advice and guidance on suitability and installation before a safe is purchased.

As time is normally a crucial factor in aggravated robberies, an option is for the safe to be fitted with a time delay lock with a delay of at least five minutes, but longer if work practice allows. As a deterrent, signs warning of the use of safe time devices, and the fact staff do not have access to the safe, should be displayed prominently at locations likely to be within view of anyone disposed to attempting a raid.

Safes are available with a deposit facility which quickly and easily denies access to the cash without the safe having to be opened. The facility is available to non key holding staff, and is particularly useful in retail environments and those involving late opening/ extended business hours.

For significant amounts at risk, safes with multiple locking arrangements are available and should be considered in order to be able to have different key holders to each lock so that for a safe with two locks two persons must be in attendance to unlock it, reducing exposure to out of hours 'duress' types of attack. Safe keys should be retained by designated persons at all times and removed from the premises outside business hours. Keys should never be left in the key lock or within a drawer or cabinet.

Combination locking can improve overall control of access to the safe, eliminating the possible use of a duplicate key. This also has the added advantage of ease of change of the combination in the event of a previously authorised member of staff leaving the company.

9 Electronic security systems

Electronic security equipment and devices can be used and specifically designed to prevent or deter violent crime.

9.1 Video surveillance systems (VSS, formerly termed CCTV)

Installation of a VSS system with adequate monitoring and recording can provide an effective tool not only to locally or remotely alert appropriate personnel to an attack taking place, but to also provide subsequent evidence of a committed crime and act as a deterrent by improving the perception of security within premises.

VSS systems should be designed, fitted and maintained by a company inspected and approved by a UKAS accredited approval body such as the National Security Inspectorate (NSI) and Security Systems and Alarms Inspection Board (SSAIB). Where they are designed to transmit images remotely to a third party off site monitoring service, the system should be connected to a similarly approved alarm receiving centre (ARC).Alternatively, where the installation is designed to comply with BS 8418, the connection should be made to an approved remote video response centre (RVRC).

There are various responsibilities, accountabilities and constraints imposed by privacy legislation, namely the Data Protection Act 1998 and accompanying Code of Practice, of which operators of VSS systems need to be aware. A copy of the Code of Practice can be obtained from the Information Commissioner's Office.

Before installing a VSS system it is helpful to speak to your local police or Crime Prevention Design Advisor to identify appropriate areas of coverage and police requirements for images. A properly installed system that captures good images of the face of any person visiting the premises will be more effective in the identification and prosecution of offenders.

Monitoring of the system should ideally be at a remote location or at least from locations within the premises separate from the primary area of risk where an appropriate emergency response and assistance can be called upon without this being evident to the attacker.

The VSS system should be recording at all times. It should capture good quality images, incorporating a detailed record of the date, time and place of each image. An assessment of the lighting conditions for both day and night times will need to be undertaken to ensure lights levels are sufficient to provide the desired image. Recording hardware should be kept in a secured, restricted access area, preferably protected by an intruder alarm system.

Additional security value can be gained by connecting deliberately operated devices, such as hold-up devices/personal attack alarms, so that images are transmitted in real time to an alarm receiving centre or remote video response centre for immediate analysis. This significantly benefits the overall effectiveness of the system and police response times.

To facilitate maximum deterrent value, high profile warning notices and signs (a legal requirement under the Data Protection Act 1998) should be displayed prominently both externally and internally drawing attention to the use of the system. NB: Police experts do not support the use of monitors in the public area as a deterrent, because they reveal the location and coverage of cameras and such use can be in breach of Data Protection principles.

9.2 Intruder alarms

This document concentrates on robbery rather than burglary of unattended premises, therefore the design and installation of intruder alarm systems is not covered in detail with such additional guidance available from the RISCAuthority document S9: *Intrusion and hold-up alarm systems (I&HAS)*.

However, certain applications of an intruder alarm system can be used both to deter, and possibly detect, the risk of violent attacks as follows:

- Emergency exits can be permanently alarmed by connecting to a 24-hour operating circuit designed to audibly alert staff upon the unauthorised opening of the protected door. Advisory signs to this effect should be placed on such protected doors to provide additional deterrent value and control unauthorised use as an exit door.

- Depending on the Grade of alarm, a duress code can be programmed into the alarm control panel, the use of which is designed to silently alert the monitoring alarm receiving centre of a possible situation whereby the authorised key/code holder is being forced under duress to unset the alarm system.
- As a further measure to counter possible unsetting of the system due to duress, in conjunction with the alarm receiving centre, monitoring of pre-agreed alarm opening/closing times of the installed system can be arranged whereby any unexpected unsetting or delayed setting would generate an appropriate pre-agreed response by the alarm receiving centre.
- Specific protection can be provided to cash safes either by safe ‘limpet’ or movement detection.

9.3 Hold-up (personal attack) alarms

Deliberately operated hold-up alarms, commonly referred to as personal attack (PA) alarms, are used to silently alert police, via an alarm receiving centre, of the need for an emergency response to a violent or threatening event. Whilst such devices may be fitted as ‘stand-alone’ systems, they more usually form part of a general intruder alarm system.

Use of a hold-up alarm system can only be justified if a risk assessment demonstrates a clear need and benefit. The assessment should also identify the required type, ie either fixed or portable, and the best locations for the devices. The location of devices should preferably include areas away from the point of high risk to allow for safe use by persons who are unlikely to be directly affected yet be in a position to view any incident. The system should operate silently (ie not trigger an audible warning device) to limit the risk of a violent response.

Training needs to be provided to all users where such devices are installed, including third parties such as cleaners, to prevent accidental misuse and false calls to the police. In order to reduce the risk of false alarms, only dual action devices are permitted which require the simultaneous depression of two buttons to transmit an activation.

Where a hold-up alarm utilises landline communications to transmit signals to an alarm receiving centre, there may be a risk that this link could be cut prior to an attack (in an attempt to prevent transmission of any subsequent hold-up alarm signals). To counter this, dual path signalling should always be used to provide a back-up form of communication in the event of loss of one of the signals.

In order to be eligible for police response, an intruder and hold up alarm system incorporating remote signalling would require to conform to the current Association of Chief Police Officers’ (ACPO) policy on electronic security systems and will therefore need to conform to DD 243 or BS 8243: 2010 (superseded DD 243) and PD 6662: 2010. Any PA system should be designed, installed and maintained by a company inspected and approved by a third party UKAS accredited approval body such as by the National Security Inspectorate (NSI) and Security Systems and Alarms Inspection Board (SSAIB).

9.4 Access control

Procedures should be in place as far as practicable to ensure all third parties entering the site or premises, such as visitors, contractors and deliveries, are required to report and sign in/out at a designated point which has restricted access to the rest of the premises, eg reception or delivery office and, where necessary, be escorted by the relevant person(s). Training should be provided to employees to encourage the questioning of any unaccompanied and unknown third parties walking around the premises with the use of visitor badges being considered so employees can clearly identify who is legitimately on site.

Staff should be discouraged from using doors not designated for regular entrance/egress, such as emergency exits, and as noted above, these can have signs to this effect and be permanently alarmed to audibly alert staff upon the unauthorised opening of a protected door.

Where appropriate, consideration should be given to the provision of controlled entry using suitable and appropriate remotely controlled electronic/electrically operated door locking systems fitted to the main public entrances to the premises. Suitable and appropriate devices should be used to verify the identity of callers prior to admittance. This can be done by door viewers, audio systems or visual systems using a wide angle lens camera with a monitor unit adjacent to the door. Preferably, there should be a combination of these.

Where there are internal doors leading from public areas restricted to authorised access only, access control locking systems, such as electronic digital code locks, can be used. Such doors should also be fitted with a suitable self-closing device.

Where internal doors lead to vulnerable areas eg the cash office/safe room, consideration may be given to incorporating a duress code into the access control facilities. This allows staff under duress to raise the alarm when entering the vulnerable area and in some circumstances may be the only opportunity to do so. However this is not a method approved by police for conveying a hold up alarm signal to them via a hold-up alarm system. Operation of a police approved hold-up device by another member of staff (or a call using the emergency service) would be necessary if it is clear that the individual is indeed under duress.

For high-risk situations, such as jewellers and cash handling businesses, public access can be controlled by installation of an ‘airlock’ door system, using remotely controlled electronic/electrically operated locking systems, whereby both an outer and inner door are interfaced so only one door can be opened at a time, effectively providing an additional layer of security to allow both control of entry of authorised persons and a deterrent by delaying a quick escape. Use of secured window-style serving facilities can be particularly beneficial in late night opening establishments, such as petrol filling stations, thereby negating the need for customers to enter the premises.

9.5 Security fog devices

A security fog device (often also referred to as a ‘smoke’ generating security device) is a security system which, on activation, quickly discharges a harmless dense ‘fog’ filling the protected area in a matter of seconds so that visibility is reduced practically to zero. This is designed to disorientate a potential thief and deter/hinder further access into the protected area. These devices can either be configured as a stand-alone system or, more usually, be integrated as an extension of an intruder alarm system or an intruder and hold-up alarm system.

Any security fog device should be designed, installed and maintained in accordance with BS EN 50131-8: 2009. The relevant police force and fire service should be advised in writing of the proposed installation of such a system as both organisations are likely to have guidelines for their personnel when attending premises where a system may have activated. It is also important that details of the proposed installation of such a device be referred to any interested insurance company for approval or comment prior to acceptance and installation.

These systems have three primary applications:

- automatic activation to protect the premises outside hours of occupancy against a break-in to allow time between an intruder alarm activating and the arrival of key holders and police;
- automatic activation to protect defined areas of the premises, more usually display windows holding high-value goods, in the event of an attack during business trading hours;
- manual activation by use of an appropriate deliberately operated hold-up device to protect against aggravated robbery during normal hours of business when staff are present.

In respect of the latter, protection is achieved by deploying a short controlled activation to create a ‘fog’ curtain between the attacker and the staff and/or goods with the intention of forcing the attackers to retreat from the premises. The application of a dense ‘fog’ aimed directionally, means that the attackers should still have a corridor by which to leave the premises to help ensure the safety of the staff and to limit any property damage. Adequate warning signs displayed at normal entry/exit points of the premises improve the initial deterrent value.

However, advisors and specifiers such as consultants and insurers must carry out a careful risk assessment before sanctioning or lending any degree of support for the technology in this application; an assessment that takes account not only of the rationale and expectations for the system but also the impact on legitimate occupiers of the premises (staff, visitors and customers).

It is suggested that satisfactory completion of a sufficiently thorough assessment would require collaboration with the manufacturer's representative and the installer of any triggering (ie hold-up alarm) system. The fog products differ in their operation and it will be necessary to evaluate whether the operational requirement can be met by the way the equipment is expected to operate including the required pattern of fog emission and the time that elapses before the fog in the intended area of operation reaches the required density. Experience suggests that in the hold-up application rapid obscuration by fog emission is essential.

The advisor or specifier should also take steps to establish that the installer of the triggering system will integrate and connect both systems in accordance with manufacturers' instructions, will correctly commission the equipment and will ensure that the equipment is fully functional at all necessary times (eg is not left deactivated in error following maintenance).

Further more detailed guidance on security fog devices can be found in the RISCAuthority document S7 *Security fog devices*.

10 Forensic coding system

This denotes a unique 'tagging' system consisting of specially formulated chemicals which are virtually undetectable when deployed, but which contain a long lasting 'trace' element unique to the premises.

These systems can be deliberately applied to high-value goods or, more usually, as with smoke generating devices, can be deliberately activated during an attack to harmlessly contaminate either the goods or, more usually, dispersed to fall onto the attacker. This forensically confirms that the person was present on the premises at the time of the attack and can be used in evidence in a possible subsequent prosecution.

11 Policies and procedures

In addition to the physical and electronic control measures in place, security and staff safety against robbery rely heavily on the support of the appropriate procedural processes. Where reasonably foreseeable risks evaluated as part of the risk assessments called for under the Health and Safety at Work Act and Health and Safety at Work Regulations involve staff exposure – as incurred in tasks such as the cash in transit and handling operations – a documented safe working procedure (SWP) to support the employee(s) in adopting the required working method must be developed. The safe system of work will often comprise an aggregate of physical and electronic security measures combined with procedural working methods.

Where there is a significant risk of robbery, a formal system of written security policies, procedures and safe operating practices based on written risk assessments needs to be developed and periodically reviewed. These policies should include staff vetting procedures such as criminal records and also cover post incident trauma counselling and assistance.

Policies and procedures should not be limited to staff actions or behaviours. Policies could include limiting the value of stock in a single window or display cabinet, standards of secure cabinets etc.

12 Staff training

This should be supported by recorded training programmes on all the policies and procedures required to be carried out plus general security awareness.

Staff should be instructed and trained in the detail of security plans and their intended execution, including the practical operation of security systems, devices and procedures. The level and design of such systems and equipment would need to take into account practicality and the ease of use by staff.

They should include guidance on how to be vigilant and identify, record and report any suspicions or unusual behaviour that gives cause for concern and what to do in the event of a hold-up or robbery.

When information indicates that there is an increased risk or that an offence has taken place locally, a staff briefing should take place. The briefing should pass on relevant information including descriptions, vehicle registrations and methods used. The briefing should reinforce the need for increased alertness and the necessity of following policies and procedures.

In the event of an attack, instructions should be clearly provided to staff on how they should respond. The best defence against physical assault is to comply promptly with demands, as this is strongly recommended by the police:

- do not resist;
- do not argue;
- do not fight back;
- do not use, or threaten to use, a weapon; and
- do not follow a robber out of the premises.

During an attack, staff should be trained to try to remain vigilant, noting any distinguishing features such as physical appearance, clothing and the like. After an attack the police should be notified immediately and any witnesses, if agreeable, requested to await their arrival or provide their contact details. The scene should not be disturbed so as to secure the maximum benefit from the gathering of possible forensic evidence.

Employee records should show the content and date of the training and employees should sign an acknowledgement to indicate they have received the training given. Training records are to be maintained for all employees to assist in the review process and also to provide evidence that training has been given as these may assist in defence of any potential civil claims. For risks such as cash in transit, specific training and qualifications can be considered such as the NOCN Level 2 Award in Cash and Valuables in Transit.

13 Key holding

For those persons appointed as premises key holders required to open and close the premises or attend the premises in response to intruder alarm system activations, a formal protocol should be established and staff provided with instruction and training.

Where possible, keys for the premises and any safes, should be split between two or more designated senior members of staff to reduce exposure to single person duress.

For opening and closing procedures, this can include having more than one person to allow for surveillance of the immediate area and having an established method of verification to safeguard against attack on arrival at the premises, eg a system of telephone calls to designated persons within a defined time, with failure to receive the call prompting contact with the police.

For responding to alarm activations, again ideally using two persons attending, a call can be verified as genuine by contacting the alarm receiving centre before leaving for the premises. Alternatively, the services of a professional key holding company could be considered. Any company used should operate in accordance with the relevant Codes of Practice ie BS 7499, BS 7858 and BS 7984. They should be inspected and approved by a third party UKAS accredited approval body such as the National Security Inspectorate (NSI) and the Security Systems and Alarms Inspection Board (SSAIB).

For further information, refer to RISCAuthority guidance document S6 *Electronic security systems: Guidance on key holder selection and duties*.

14 Summary

There is, unfortunately, no single effective solution to counter both the threat and the actual impact of an attack involving either force or the perceived threat of force.

However, a combination of undertaking relevant training and appropriate deployment of some of the above detailed suggested courses of action would both deter and significantly reduce exposure to robbery, thereby offering improved safety and peace of mind to employees who are increasingly exposed to this very unpleasant crime which all too frequently can have very serious, if not devastating, consequences.

In summary, carrying out a risk assessment to take fully into account the potential exposure and vulnerabilty to this form of crime and, based on this, putting in place suitable and appropriate physical and electronic security protections supported by formal policies and procedures, should help to reduce and mitigate the overall risk.

15 References

RISCAuthority

1. S3: *Convenience ATMs: Recommended security measures*.
2. S5: *Alarm signalling using the Internet Protocol Part 2 – Considerations for insurers*.
3. S6: *Electronic security systems: guidance on key holder selection and duties*.
4. S7: *Security fog devices*.
5. S9: *Intrusion and hold-up alarm systems (I&HAS): considerations for installers and other stakeholders*.
6. S10: *Guidance for the protection of premises against attacks using vehicles (ram raids).*
7. S33: *Intruder alarm systems: Ten-step guide for purchasers*.
8. S22: *Cash security a user's guide.*

These documents may be downloaded free of charge from the website: www.riscauthority.co.uk.

16 Further reading

British Standards Institution (BSI) standards

1. DD 243: 2004: *Installation and configuration of intruder alarm systems designed to generate confirmed alarm conditions. Code of practice*.
2. BS 8243: *Installation and configuration of intruder alarm systems designed to generate confirmed alarm conditions. Code of Practice*.
3. PD 6662: *Scheme for the application of European standards for intrusion and hold-up alarm systems*.
4. BS 8418: *Design, installation, commissioning and maintenance of detector-activated video surveillance systems (VSS). Code of practice*.
5. BS EN 50131-8: *Alarm systems. Intrusion and hold-up systems. Security fog device/ systems*.
6. BS 7499: *Static guarding and mobile patrol services. Code of practice*.
7. BS 7858: *Security screening of individuals employed in a security environment. Code of practice*.
8. BS 7872: *Manned security services. Cash and valuables in transit services (collection and delivery). Code of practice*.
9. BS 7984: *Key holding and response services. Code of practice*.

Loss Prevention Certification Board/Loss Prevention standards

10. LPS 1175: *Requirements and testing procedures for the LPCB approval and listing of intruder resistant building components, strong points, security enclosures and free-standing barriers.*
11. LPS 1270: *Requirements and testing procedures for the LPCB approval and listing of intruder resistant security glazing units*.

HSE risk assessment

12. *www.hse.gov.uk/pubns/indg423.pdf*

RISCAuthority

administered by

FPA Fire Protection Association

Fire Protection Association
London Road
Moreton in Marsh
Gloucestershire GL56 0RH
Tel: +44 (0)1608 812500
Email: info@riscauthority.co.uk
Website: www.riscauthority.co.uk