RISCAuthority

administered by FPA Fire Protection Association

S6 Electronic security systems: guidance on keyholder selection and duties

Version 3 Published 2021

Acknowledgements

The assistance of the Association of Chief Police Officers (ACPO) and the British Security Industry Association (BSIA) is gratefully acknowledged.

Cover image: Getty Images/Sigefride

Contents

1 Purpose and scope

This guide covers keyholding and response and whilst it is primarily aimed at commercial premises, many of its recommendations will also be relevant to domestic premises.

By way of clarification, and to avoid unnecessary repetition/ qualification within the body of this document, the following terms are considered to mean:

- *Electronic security system (ESS)* – a system for detecting unauthorised access to premises. The most common type of ESS is an intruder alarm system remotely monitored by an alarm receiving centre (ARC), to which most of this document refers. However, other ESS systems exist that may require keyholders, such as remotely monitored video surveillance systems (VSS, formerly known as CCTV) or remotely monitored building management systems (incorporating intruder alarm, VSS or access control systems), to which parts of this guide will be of general application.
- *ESS company* – an individual or organisation responsible for the installation and/or maintenance of an ESS.
- *IAS/IAHAS* – 'intruder alarm system' or 'intruder and hold-up alarm system'.
- *ESS owner(s)* – those who own, or are otherwise in charge of, an ESS.
- *User(s)* – those who set/unset ESS, but are not necessarily designated as keyholders.
- *Keyholder(s)* – those tasked with attending premises protected by ESS after any reported activation or fault.
- *Commercial response company* – an organisation which, for a fee, agrees to fulfil the role of keyholders.

The purpose of this guide is to assist ESS owners in the selection of appropriate persons to act as ESS users/keyholders and to determine appropriate security and safety procedures/ training for them to follow.

There are various diverse requirements to be considered, some of which are mandatory, in order to comply with legislation, public policies or insurance policy requirements. ESS owners need to be particularly aware of these as well as the other recommendations outlined within this guide.

Relevant legislation and public policies include health and safety legislation, local authority requirements, and the security system policies of the Association of Chief Police Officers (ACPO) or the Association of Chief Police Officers in Scotland (ACPOS).

Since this guidance is broadly based, ESS owners should check with their ESS company, insurance provider, local police and local authority for any special requirements concerning the type of ESS installed or proposed, its operation (or limits on operation) and the nature of any response expected.

This guidance document has been prepared with the assistance of the Association of Chief Police Officers (ACPO) and the British Security Industry Association (BSIA).

2 Mandatory alarm and keyholder requirements

Requirements are placed on IAS/IAHAS owners and keyholders by legislation, the police and insurers. At all times it is advisable to check whether there are any specific variations to the general information offered in this section, by seeking advice from the relevant organisation.

2.1 Legal requirements

Legal requirements principally cover two areas:

- noise nuisance from audible IAS/IAHAS; and
- employers' health and safety duties to staff keyholders.

2.1.1 Noise nuisance from audible IAS/IAHAS

Local authorities have various statutory powers available to them to control the potential nuisance from intruder alarms, such as the repeat or continuous operation of alarm bells/ sirens. These powers are set out in the following pieces of legislation:

- *The Control of Pollution Act 1974* – Under this Act, the Secretary of State has powers to prepare and approve Codes of Practice giving guidance on noise minimisation. One resulting Code of Practice is targeted at audible IAS/IAHAS, namely:

  Code of Practice on Noise from Audible Intruder Alarms 1982

  This statutory Code of Practice covers the issues of noise/ nuisance and notification of keyholder details and response. The Code of Practice also encourages local authorities to use their powers under Section 58 of the Control of Pollution Act to require the fitting of automatic alarm cut-off devices in certain circumstances.

- *The Environmental Protection Act 1990* – This places a duty upon local authorities to deal with complaints arising from statutory nuisance, including noise emitted from premises. The local authority must investigate the complaint and, if it is satisfied that a nuisance exists, it must issue an abatement notice.

  In addition, anyone who is aggrieved by noise nuisance (such as a continuously sounding alarm) may apply to a Magistrates Court for an abatement order. If it seems to the Court that neither the owner nor the occupier can be found, the Court may instruct the local authority to take action itself to curtail the nuisance, and this may well involve forcing an entry to the premises. While there is a duty to re-secure the premises, it is doubtful whether this implies fully resetting the alarm, even supposing the local authority had the means to do so.

  It is a specific defence to a charge of noise nuisance for a business to show that it has complied with the Code of Practice on Noise from Audible Intruder Alarms 1982, through the introduction of a 20-minute sounder cut-off. It is anticipated that such a cut-off would, in practice, also be an acceptable defence against local authority action in connection with private residences. This defence does not apply in Scotland or Northern Ireland however, where local authorities will continue to refer to the provisions of the Control of Pollution Act 1974.

- *Noise Act 1996* – This act is concerned with night-time (11pm to 7am) noise from a dwelling or licensed premises, such as noise from an intruder alarm system. Following the service of a warning notice, the person responsible may be liable to a fixed penalty or summary prosecution. If necessary, elements of the alarm system, in particular its sounder, may be removed and seized by a local authority officer acting under a warrant.

- *Clean Neighbourhoods and Environment Act 2005* – This is the latest legislation covering noise from audible intruder alarms. Under this Act, a local authority may create designated 'alarm notification areas'. These are areas in which the occupiers/ owners of premises with audible IAS/IAHAS must nominate keyholders and notify the local authority of their contact details.

The Act also empowers the local authority to enter problem premises, with force if necessary, and, once a warrant has been obtained, to deactivate a system that is causing a noise nuisance. These powers apply to any area, not just designated alarm notification areas. An authorised officer can take whatever steps are necessary to silence the alarm. This might include, for example, disabling the external sounder. Again, the officer is not required to reset the alarm (even if he/ she has the means to do so).

Further advice may be obtained from your IAS/IAHAS company or the local authority environmental health department.

Note: Failure to comply with legal requirements may lead to enforcement action and/or prosecution.

2.1.2 Employers' health and safety duties

Many employers request or require nominated employees to act as keyholders.

The Health and Safety at Work etc Act 1974 and the Management of Health and Safety at Work Regulations 1999 place a statutory duty on employers to safeguard, so far as is reasonably practicable, the health, safety and welfare of their employees. This legislation requires an employer to undertake risk assessments and then carry out effective planning, organisation, control, monitoring and review of the preventive and protective measures employed. An employee acting as a keyholder is doing so as part of their work, so risk assessments should include these duties.

Recorded instances of keyholders being injured during their duties are few and far between, but that does not mean the risk can be ignored. Indeed, according to the type of premises involved or the area in which it is located, the risk of injury may be envisaged as sufficiently serious to suggest the need for a commercial response company to be used rather than employees. Further practical advice on keyholder safety can be found in section 5.

There may also be a duty of care owed by an ESS owner or employer to visitors to the premises, such as an engineer or representative of the ESS company, responding police officers, staff of the commercial response company, or even trespassers, by virtue of the Occupiers Liability Acts 1957 and 1984.

Note: Failure to adequately address legal duties may lead to claims for compensation and/or prosecution.

2.2 Police requirements

Police response to ESS is governed by the Security Systems Policies (SSP) of the Association of Chief Police Officers (ACPO), or the Association of Chief Police Officers in Scotland (ACPOS), as adopted by each local police force. These are respectively entitled ACPO 'Policy on police response to security systems' and the ACPOS 'Security systems policy'.

One of the SSP requirements is that the ESS company shall ensure that details of the names, addresses and telephone numbers of at least two keyholders are provided to the alarm receiving centre or remote video receiving centre (ARC/RVRC). Some police forces also require these details to be supplied to the police force itself. This must be done when:

- installing a new system;
- taking over an existing system; or
- a change of keyholders takes place.

To further comply with the SSP, keyholders must:

- be trained to operate the alarm;
- be contactable by telephone;

- have adequate means of transport to attend the premises at all hours;
- be capable of attending within 20 minutes of being notified; and
- have access to all relevant parts of the protected premises.

Alternatively, details of a commercial response company may be provided, subject to it being:

- available at all times via a 24/7 central control room;
- be capable of attending within 20 minutes of being notified.

Note: Failure to comply with police requirements may lead to withdrawal of police response to alarm calls.

2.3 Insurance requirements

After assessing the risk, insurers may impose specific conditions in relation to the use of, and response to, an ESS. ESS owners should check the exact details with their insurer, but in general terms a typical insurance policy intruder alarm condition may require that:

- the policyholder shall appoint at least two keyholders and lodge written details (which must be kept up-to-date) with the IAS/IAHAS company and (if they so require) with the police;
- the keyholders must be available at all times to accept notification of alarm activations, attend promptly and allow access to the premises;
- in the event of notification of any activation of the IAS/IAHAS, or interruption of the means of monitored communication to the ARC during any period that the intruder alarm system is set, a keyholder shall attend as soon as reasonably possible;
- the premises shall not be left unattended until the IAS/IAHAS is set in its entirety, with the means of communication used to transmit alarm signals in full operation;
- any operating code is kept secret and any keys or other operating devices for the IAS/IAHAS are not left on site when the IAS/IAHAS is set; and
- the insurer be notified as soon as possible if IAS/IASHAS become inoperable or if police response is reduced or withdrawn.

Any problems in meeting an insurer's standard requirements should be discussed with the insurer and any alternative agreements recorded in writing.

Note: Failure to comply with an insurer's alarm condition may jeopardise insurance cover.

3 Criteria for appointing keyholders

Keyholders have an important duty to perform and their selection is a matter of considerable responsibility.

Keyholders should be reliable and trustworthy individuals. For that reason they are usually selected from amongst ESS owners or their employees, family, friends or neighbours (termed 'non- commercial response') or, failing that, a commercial response company can be engaged.

Whoever is appointed, it is vital that the ESS company be immediately notified of any changes to keyholders and/or their contact details. Additionally, where a security system is eligible for police response, the police criteria for keyholders must be met.

In choosing keyholders there are certain factors that need to be considered, as outlined below.

3.1 Non-commercial response

Keyholders should:

- be willing and able to undertake the task responsibly;
- be adequate in number (ideally at least four should be appointed to cover illness, holidays, etc);
- be chosen for their proximity to the premises, ideally within a maximum travel time of 20 minutes;
- be able to access all parts of the ESS protected premises;
- be appropriately trained in all of the processes and procedures for:
  - setting and unsetting the ESS;
  - aborting false alarm calls;
  - allowing authorised engineer access; and
  - using any codes or other devices necessary for operating the ESS and for communicating with the ARC; and
- possess, or be provided with, mobile telephones to allow them to contact:
  - other keyholders;
  - the ARC;
  - the ESS company;
  - the ESS owners or other senior personnel, for example to authorise repairs;
  - the police; and
  - emergency tradesmen, such as glaziers and builders.

The telephone numbers for each of the above should ideally be programmed into the memories of keyholders' mobile telephones.

3.2 Commercial response

Commercial response services have become more widespread in recent years, with market demand driven by hardening police attitudes to attending false alarms and increased employer concerns for the health and safety of non commercial keyholders, for example, employees.

Commercial response companies are usually engaged on the basis of payment of an annual retainer fee plus any call out charges. They are usually engaged to attend alongside, or instead of, other nominated keyholders such as employees, but may also be engaged to act instead of the police as the 'first response'.

Where such companies attend and find nothing untoward, they will usually re-secure the premises and reset the ESS. If the premises cannot be re-secured and/or the ESS cannot be reset in its entirety, arrangements must be put in place for the commercial response company to contact other nominated keyholders or representatives of the ESS owner, who must then attend and take appropriate remedial action in accordance with any legal, police or insurer requirements.

3.2.1 Engaging commercial response companies

Where commercial response services are sought, ESS owners should:

- consult with their insurers;
- ensure that the prospective service supplier complies in full with:
  - BS 7984: Keyholding and response services. Code of practice, which gives recommendations for the storage and management of keys, staffing, operation and management of organisations providing such services on a contractual basis;

- the Security Industry Authority licensing regulations in relation to keyholding and response services, which may be evidenced by the company holding 'Approved Contractor Scheme (ACS) status; and
- the ACPO/ACPOS SSP requirements for keyholders;

- not agree to the storage of premises keys and/or alarm operating devices in an on site key box – see 3.2.2 below; and
- provide the commercial response company with a separate identifiable ESS user code/ unsetting device (once the company's services have been engaged).

The most reliable means of ensuring that a commercial response company complies with the above criteria is to choose one which is approved for keyholding and alarm response services by the National Security Inspectorate (NSI) under their Guarding Gold or Guarding Silver approval schemes, or one approved by the Security Systems and Alarms Inspection Board (SSAIB).

It is important to ensure that where the ESS is eligible for police response, the commercial response company can comply with the police requirement for attendance within 20 minutes, as failure to do so after a police call out may result in withdrawal of police response.

Prior to the commissioning of the ESS, details of the commercial response company will need to be forwarded to the ESS company, who in turn will forward these details to the ARC/RVRC and, where necessary, the local police.

It is particularly important that the use of a commercial response company be referred to the relevant insurer for approval if they are to provide the 'first response' to signals from the ESS (that is, to take the place of any police response for which the ESS may otherwise be eligible). Failure to do so may mean that insurance protection may not operate in the event of a claim.

Note: Failure to comply with an insurer's keyholder and/or ESS response requirements may jeopardise insurance cover.

3.2.2 Commercial response companies – key storage arrangements

Commercial response companies operating to BS7984, and inspected by NSI or SSAIB, can be expected to adhere fully to BS7984, part of which deals with secure storage of keys to customers premises and alarm systems.

In the past, BS7984 only permitted storage of customer's keys in commercial response companies' own suitably protected premises or roving response vehicles. However, the 2008 version of BS7984 now permits storage of keys at the customer's premises within a site key box, subject to the customer signing an acknowledgement of the potential security risks of such an arrangement.

As an increasing number of ESS have a physical unsetting device which will need to be stored in such a key box (rather than a code which could be kept secretly elsewhere), the security risks are significant. Potential intruders gaining access to the key box, either by opening it in situ or removing it from the wall (then opening it elsewhere and returning) will have the means both to unlock the entry door and turn off the ESS.

This risk is further compounded by BS7984 making no requirement for the security quality of the key box or its installation.

Insurers will not generally sanction site key storage, as it will be in clear violation of many standard intruder alarm condition wordings that typically require customers to:

- 'maintain secrecy of codes and security of keys and setting/ unsetting devices for the operation of the intruder alarm system';

also to ensure that:

- 'all keys and other setting/unsetting devices for the intruder alarm system are removed from the premises when they are left unattended'.

Where insurers are asked to consider key box use they will wish to consider the nature of the risk and the likelihood of potential intruders taking the trouble to compromise a key box at the premises in question.

For example:

- *At low risk premises where, for example, an alarm system is not an insurer requirement:* Here use of a good quality site key box may not be felt to greatly compromise overall security. For example, the premises or its contents may be regarded as low value with consequent basic physical security, such that there are many potentially weaker access points for intruders to tackle than the key box and its associated premises entry door.
- *At medium risk premises, for example, where an alarm is a routine insurer requirement:* Here the implementation of some mitigating measures, such as alarm protection of the actual key box and/or monitoring of agreed alarm system 'open and closing times' at the ARC – with keyholder notification of any deviations, may make their use acceptable.
- *At high risk premises, for example, where an alarm is a critical insurer requirement:* Here their use should be prohibited.

Insurance arrangements aside, site key storage should not be considered without considering the physical and ESS protection of the proposed key box, for example:

Physical security

Whilst key box suppliers may make security claims for their products, ESS owners should look for some independent certification, to a recognised relevant standard, of any claims made. In the absence of a specific key box security standard, possible candidates for such independent testing might include one of the existing standards aimed at safes, safe cabinets or other physical security devices.

In this regard the 'Sold Secure' scheme (run by the Master Locksmiths' Association) test for safe cabinets has recently been modified (at the basic 'Bronze' security level – three-minute attack resistance) to specifically recognise keyboxes. It is also possible that the European Safe/Safe Cabinet Standards BS EN 1143/ BS EN 14450 respectively, or the Loss Prevention Certification Board (LPCB) test standard LPS 1175, may, at a suitable test level, also be considered as providing a suitable indication of key box security.

However, whatever the inherent strength of a key box, due regard must always be given to the nature of the fixings holding a key box to the wall, whether the key box is surface mounted or (ideally) recessed, as well as the nature of the wall itself.

Electronic security

The degree of security risk is related to the type of ESS and the method used to unset it. Unsetting methods that involve a code unset are the least vulnerable as the code can conceivably be kept elsewhere than in the key box. Thus, even if intruders gained access to a physical operating device within the key box and initiated a partial unset, they would not be able to fully unset the system. After the expiry of the designated entry time the system may be able to signal this fact to the ARC/RVRC – who should then be in a position to notify keyholders.

The following precautions are advised, based on the type of IAS/ IAHAS installed:

For a non-confirmation system:

- if an alarm code is used, it should not be kept in the box;
- if a key is used (only likely in very old systems) the system should be upgraded to use a code – see above; and
- detection against opening/removal should be provided to the key box.

At higher risk premises and/or when above cannot be achieved:

- arrangements should be made for the ARC to monitor agreed site open and close times – see 5.3.

For a confirmation system (designed to meet DD243 – soon to be British Standard 8243):

- if only a key is used (the means of unsetting in DD243 paragraph 6.4.2 is employed), the system should be changed to use the means of unsetting in paragraph 6.4.3 – see below;
- if a key and alarm code are used (the means of unsetting in DD243 paragraph 6.4.3 is employed), the code should not be kept in the box;
- if only a fob is used (the means of unsetting in DD243 paragraph 6.4.5 is employed), the system should be changed to the method in 6.4.3 – see above; and
- detection against opening/removal should be provided to the key box.

At higher risk premises and/or when above cannot be achieved:

- arrangements should be made for the ARC to monitor agreed site open and close times – see 5.3.

Note: Failure to comply with an insurer's keyholder and/or alarm system response requirements may jeopardise insurance cover.

4 Managing the system

4.1 Control of false alarms

False activations can be a major nuisance and lead those expected to respond to ESS to lose confidence in them. A well- designed ESS, properly installed and managed, should function without false alarms but unwanted activations are often the result of factors that were not recognised and addressed at the time of system design (system issues), or problems when setting/ unsetting (user issues).

Some examples of common causes of false activations are mentioned in 4.3 below.

If the system causes unwanted activations which exceed the thresholds laid down in the responding police force's SSP, the police may downgrade or withdraw response.

Owners should therefore ensure that arrangements are in place to fully investigate any false activations and promptly cure any problem found in an attempt to prevent further false alarms that may quickly lead to police response being withdrawn.

It should be noted that most police forces have for some time insisted that all new IAS/ IAHAS, and those requiring restoration of police response after its withdrawal, must have a confirmation capability provided if they are to be eligible for police response.

The fundamental difference between traditional 'non-confirmation' IAS and systems with a confirmation capability is that the first intruder activation of a confirmation system must be supported by the activation of a second detection device, or some additional corroborative evidence, before the police can be asked to attend.

Those IAS/IAHAS that do not provide confirmed activations, and were granted police response prior to confirmation being required for new systems, can usually retain response until undue false alarms occur. For such a system vigorous control of false alarms is the best way to avoid the cost and inconvenience of a subsequent requirement to convert it to a confirmation system.

Anyone able to set or unset an alarm system must be comprehensively trained and totally competent in its operation. Only trained keyholders should hold keys to the premises.

Note: ESS owners who receive a letter warning that police response may be, or has been, downgraded or withdrawn must inform their insurers immediately. Failure to do so may jeopardise insurance cover.

4.2 Codes/unsetting devices

Any codes or other unsetting device, such as a proximity fob or key, used in connection with the alarm system should not be available to anyone other than authorised users or keyholders.

Users and keyholders should be advised to take care of their codes and unsetting devices and report compromise or loss immediately to the ESS owner. It is good security practice to keep keys and fobs separate so that loss of either one of these does not result in the total loss of control over secure access to the premises as would the loss of both together.

Where a key-pad type of control is used, care must be taken to ensure that others cannot see the command digits being entered. The use of individual (as opposed to shared) codes is recommended, as it allows those who create problems to be readily identified and retrained.

Codes should be changed periodically and whenever someone with access to them ceases to be a user or keyholder. Similarly fobs should be returned and/or deleted from the system once a user or keyholder ceases to act for the ESS owner.

Note: Failure to exercise reasonable care and caution with regard to code/unsetting device security may jeopardise insurance cover.

4.3 Securing the premises

Keyholders must, before leaving the premises, ensure that the premises are physically secure, that the alarm is fully set, including signalling systems, and that any indicated faults are rectified, unless some other responsible person remains on the premises.

4.3.1 Checklist for keyholders when leaving the premises

Prior to setting the alarm system, keyholders should ensure that:

- all doors and windows are closed and securely locked;
- there are no staff, contractors, customers or visitors remaining in the premises (apart from any staff who may be acting as escorts to the keyholder – see section 5);
- there is nothing in an area covered by ESS movement detectors which is likely to cause false alarms, for example swinging signs, badly stacked stock which may fall over or temporary heaters left on;
- there is nothing that may limit the area normally covered by an ESS detector, for example, stock or other items stored in front of it; and
- keyholders are ready to leave as soon as the setting procedure is initiated.

Note: If the alarm cannot be set in its entirety (including all means of signalling), the alarm company must be called. The premises should not be left unattended until the fault has been put right and the alarm has been correctly and fully set. If keyholders do not fully set the ESS in accordance with the insurer's requirements and intruders then break in, any subsequent insurance claim may not be paid.

4.4 Abort process

Many IAS/IAHAS have an abort procedure, enabling keyholders to immediately notify the ARC that a transmitted alarm signal was in fact a false activation, particularly if this occurs during opening or closing routines. In most cases, by unsetting the system in the normal manner, automatic abort of a false activation, and any related possibility of a police response, will be achieved if the unset is completed within 120 seconds. For some systems, it may be necessary to telephone the ARC in order to abort a false alarm call, and in such cases a telephone should be made available close to the setting/unsetting equipment.

4.5 Testing and maintenance

Most ESS allow owners to test certain functions periodically. For example, most IAS movement detectors contain test indicator lights, enabling owners to 'walk-test' the devices to ensure that they are providing adequate coverage. Testing in this manner at frequent intervals is important to ensure that movement detectors have not been masked or sabotaged, and are not otherwise in a faulty condition.

ESS owners should ensure that such tests are carried out at recommended intervals and that any problems identified are reported to the ESS company without delay.

The ESS company will usually be responsible for making regular inspections of the ESS, but owners should make sure that a maintenance contract providing for this is in force, and that the inspections are duly carried out and recorded in the maintenance logbook.

Visits by the ESS company to a customer's site should only be permitted by owners by appointment, as it is important to ensure that any person wishing to work on the system is properly authorised to do so. The credentials of the visiting engineer should be checked with the ESS company using their established telephone numbers rather than any number supplied by the visitor.

Note: An ESS maintenance contract is usually a condition of insurance provision.

4.6 Action following an ESS activation

If the ESS activates, a keyholder must attend the premises without delay. If the circumstances giving rise to the activation do not allow the ARC/RVRC to permit the system to be reset without the attendance of an ESS company engineer (in accordance with prevailing conditions specified in relevant British Standards and/or police SSP), or the ESS is in some way damaged, then a keyholder must remain on the premises until the engineer has attended and carried out the required remedial actions, allowing the system to be reset in its entirety.

Whether or not the activation was caused by an actual break- in, keyholders must, before leaving the premises, ensure that the premises are physically secure, that the ESS has been fully reset, including signalling systems, and that any indicated faults have been rectified, unless some other responsible person remains on the premises.

All incidents should be fully recorded in the alarm record book.

4.7 Responding to alarm signalling path faults

A fault on the telephone line or other signalling path connected to the ESS may prevent a message from reaching its destination. It is therefore very important that keyholders appreciate that any such 'fault', where indicated or otherwise suspected, may have been caused deliberately by someone planning to break in.

In the event of notification of a fault in the signalling system from the ARC/RVRC, police, telephone company, or the system itself (for example, a warning light or message on the alarm control panel or other device), remedial action must be taken at once.

Arrangements should be made for a responsible person to remain on the premises until the fault is rectified, whether or not other signalling paths (for example, in a dual signalling system) are thought to be unaffected.

To minimise the downtime of a faulty telephone link, owners should subscribe to an enhanced corrective maintenance service, where available. This will reduce the amount of time that the premises will have to be occupied in the event of a communications fault. Details will be available from the relevant telecommunications provider.

Note: Insurance cover may be jeopardised if the premises are left unattended with any signalling path in a faulty condition.

5 Safety of keyholders attending the premises

As mentioned in section 1, employers as ESS owners have a duty of care to keyholders. The most effective means of providing for their safety is to follow systematic and structured processes of risk identification, assessment, training, management and monitoring.

Resulting safety measures can be written into a clear policy and procedure to be followed by keyholders when attending the premises, either under normal circumstances (that is, opening and closing of the premises), or in the event of unexpected activations. The following situations should be considered when conducting the assessment and management audit of the risks to keyholders:

- opening up the premises at the start of working hours, and closing them up at the end of normal working hours – at these times, there may only be a limited number of staff on the premises;
- carrying keys to or from the premises – in some circumstances there may even be risks posed by keys being held at keyholders' private residences;
- keyholders receiving a bogus call-out message from criminals who are impersonating the police or the ARC/RVRC; and
- responding to a call-out and attending the premises out of normal business hours, possibly without the police in attendance.

In order to consider the appropriate level of protection necessary, employers will need to assess the degree of risk involved in each situation.

It is most important that keyholders understand that they are not required to expose themselves to unreasonable levels of risk. They should always be satisfied that it is safe to enter the premises and, should they have reasonable cause to feel threatened, they should contact the police and wait for their arrival, or follow their instructions, before proceeding. Instructions to this effect should be stated in the employer's health and safety policy and related written instructions to keyholders.

An increased risk of harm to keyholders (from assault, duress or hold up) may be likely in any of the following circumstances:

- where the premises is in an area with a high level of crime/ deprivation;
- where the contents are particularly attractive to gangs of criminals, for example where the goods stored in the premises are of high value and fairly portable, for example consumer electrical goods or fashion clothing; and
- at premises such as banks, building societies and large retail stores where there are high values of cash or other portable valuable property in safes or cash centres, enabling thieves to steal a very high amount in a very short time should the keyholders be compromised.

Risks such as these are referred to as 'target risks' within the remainder of this guidance document.

It should be noted that keyholder risk may be generally increased when responding to an unconfirmed alarm activation from a IAS that has a confirmation capability, as police attendance will not have been sought by the ARC.

5.1 Normal opening

Keyholders should ideally not be left in a position where they are on the premises on their own. It is strongly recommended that, as a matter of routine, keyholders meet with another keyholder or colleague at a place away from the premises so that the two may enter together. Alternatively, keyholders should wait at the premises for a second person to arrive before entering.

If exterior lighting during the hours of darkness does not continuously illuminate the area outside the final door, lighting automatically operated by means of a movement sensor should be fitted to give assistance to keyholders.

On arrival at the premises, keyholders (especially if unaccompanied) should observe the premises from a safe distance and be alert for anything suspicious, for example unrecognised persons waiting near the entrance or in vehicles nearby. If in doubt, they should seek assistance and/or wait until a colleague arrives. On approaching the premises, they should make a careful examination of the entrance door and the outside of the property, making sure that everything is in order. If there is evidence of an intruder having been on the premises, the police should be called at once and the keyholder (or other staff) should not enter until police have attended in case of danger or contamination of a possible crime scene.

In the case of 'target risks', it is possible that intruders may already be on the premises (having previously forced an entry) in order to overcome keyholders or employees as they arrive, one by one. This possibility should always be taken into account. A sensible precaution is to implement a system whereby one person enters, while another stands some distance away and waits until they receive a pre-arranged 'all-clear' signal before entry.

For 'target risks', keyholders and/or escort should be provided with portable personal attack alarms which will operate in the vicinity of the premises, as well as inside them. These alarms should operate silently, triggering the premises' alarm to send a special personal attack message directly to the ARC/RVRC. These types of alarms should preferably be capable of locating and reporting exactly where the member of staff is situated.

Once premises are occupied, but not yet trading normally, care should be taken in respect of the arrival of unrecognised persons/ personnel, for example, contract cleaners seeking access. Keyholders and other staff should be trained to request and verify the identification of such persons before allowing them entry to the premises.

5.2 Normal closing

Keyholders should preferably not be left in a position where they are on the premises on their own. It is strongly recommended that, as a matter of routine, keyholders lock up with another keyholder or colleague acting as escort until they jointly leave the vicinity with the premises keys. The escort should remain with them if they are unexpectedly delayed leaving. For example, if the keyholders' personal vehicle is disabled, this may have been done deliberately so that the keyholder is left alone in the vicinity of the premises.

If exterior lighting during the hours of darkness does not continuously illuminate the area outside the final door, lighting automatically operated by means of a movement sensor should be fitted to give assistance to keyholders.

Before exiting the premises to operate shutters or grilles, or to complete the final lock up, keyholders should look around outside the building for anything that appears suspicious. If there is any cause for concern, the police should be contacted.

For 'target risks', particularly those situated in areas with a high crime rate, it is recommended that a mutual support scheme is arranged so that other local traders who overlook the premises are asked to be vigilant while the premises are being locked up.

Where premises are closed for normal trading, but still occupied – perhaps at much reduced manning levels, particular care should be taken in respect of the arrival of unrecognised persons/ personnel, for example, contract cleaners seeking access. Keyholders and other staff should be trained to request and verify the identification of such persons before allowing them entry to the premises.

5.3 Monitored opening and closing

Where there is an ESS with remote signalling to an ARC/RVRC, arrangements can usually be made with the ARC/RVRC to monitor the pre-agreed 'opening and closing' times of the premises via the routine unsetting/setting of the ESS.

A degree of tolerance to normal deviation in such times is usually recognised by the ARC/RVRC to avoid false alerts and is typically 30 minutes either side of the agreed times.

Any 'opening or closing' of the premises outside the agreed time parameters can then be regarded by the ARC/RVRC as a suspicious event, which will be notified to the ESS owners or keyholders.

This facility can be useful where there is a risk that those tasked with setting the alarm may fail to do so (for example contract cleaners), either through neglect or through succumbing to attack before normal alarm setting can take place. It is also useful where there is a risk of keyholders being brought to site under duress outside normal business hours, and then being forced to open the premises.

Where this system is in operation, legitimate changes to the usual 'opening and closing' times must be pre-notified to the ARC/ RVRC.

For 'target risks', where the ARC procedures involve them making a check call to the premises before alerting others, keyholders should be supplied by the ESS company with a special codeword to be used if they have been forced by criminals to open up the premises under duress.

Some IAS/IAHAS control panels allow keyholders to send a 'duress code' signal (for example, by entering a certain sequence of characters on a keypad). This sends a unique and dedicated signal to the ARC, indicating that a duress situation exists at the premises.

Where a kidnap or duress situation is a significant possibility, the employer should have in place specific security related health and safety policies and procedures to reduce the risk. These can be established in consultation with the local police, insurers and usual sources of health and safety advice.

Note: *Kidnap and duress.* The kidnap or duress of a keyholder (or other potential target) is not common. However, the security and safety risks should always be considered, particularly in the case of target risk premises.

5.4 Personal attack and duress codes

Where IAHAS are installed, a personal attack facility will be incorporated to allow a request to be made via an ARC for a priority police response. Although such systems are usually expected to be available for staff use during trading hours, it is possible that they may on occasion be useful to keyholders attending premises in response to an emergency call out.

With such systems if the ARC receives a call from a personal attack device or receives a coded message which indicates duress it will, where permitted to pass such calls, notify the police using a special message format which alerts them to the fact that a hold-up is in progress or that someone on the premises is under criminal duress.

Such systems should operate silently, that is without a bell or other audible warning being sounded at the premises, as such devices could alert criminals to their use and cause them to react more violently.

5.5 Intervention

ACPO have been worried over a long period about possible indiscriminate installation and over-use of personal attack facilities such as duress codes and PA buttons/devices.

Use of duress codes has been tightened up by the police by restricting them to high security systems only, that is those that meet BS 7042 or BS EN 50131 at security grade 4.

For some time now PA buttons have needed to be of a dual action (two button) type to minimise accidental false activations but escalating misuse of PA facilities to summon the police to a variety of incidents, which the police do not regard as emergencies, has led to most ACPO forces adopting a limit of only two false activations before response is withdrawn. Furthermore, since 1 April 2008 ACPO has required a form of 'intervention' to be in place before reinstatement of response can be entertained for a system with suspended response.

There are various currently recognised forms of intervention available:

Call back

This method requires the ARC to telephone the premises to ascertain the reason why a PA button has been activated, the recipient of the call being required to give an agreed password to prevent the ARC calling the police.

Clearly, it is a method fraught with difficulties for the ARC and those at the premises. Nevertheless, in limited circumstances – for example, if there is an agreed non-switchboard telephone phone number for the ARC to call that should be answered by someone unlikely to be involved in a robbery/attack event (but who can see it if it was occurring) – it may be a viable form of intervention.

Call back requires no changes to alarm systems, merely access to a suitable telephone and a change in ARC procedures. There is obviously a personnel safety risk at many premises that call back could alert attackers to the fact that someone has summoned help. Equally, there is a security risk if those being attacked are instructed to take the call and indicate that all is 'OK'.

Audio intervention

This method requires that use of a PA device activates a microphone fitted nearby. When the ARC receive the PA call, they open up an audio channel to the premises and, by listening to the pre- and post-alarm event sounds emanating from the area, they may be able to determine if a police response is appropriate. Some ARCs make use of a two-way system to audibly ask anyone present whether they need assistance.

There is, of course, a risk that any doubt on the part of the ARC over sounds heard will result in them falsely calling the police or, if a two-way system is used, alerting the attackers and provoking them. Conversely, the risk of those being attacked being instructed by the attackers to say all is 'OK' is perhaps less than with a call back, as the ARC should clearly hear such a conversation.

Visual intervention

This method is similar to audio confirmation, except that a VSS camera allows the ARC operator to view pre- and post-alarm event images from the area where the PA signal originated. Subject to suitable VSS coverage from cameras that are either hidden or not otherwise vulnerable to deliberate re-orientation, it should be a fairly straightforward matter for the ARC operator to determine the nature of the situation and whether a police response is appropriate.

Visual intervention has the dual advantage of not alerting attackers and also of providing useful information on the situation that any despatched police officers might face on arrival, for example, number and type of persons carrying out the attack.

5.6 Emergency call-out

If keyholders receive a call-out message outside normal business hours, they should check that it is a genuine message. If the caller says they are from an ARC/RVRC, keyholders can confirm this by exchanging codes with the ARC, or if their telephone has a caller ID facility, checking that the telephone number being used to make the call to them is recognised by them as belonging to the stated caller.

Alternatively, keyholders could telephone the ARC to make sure the call was valid before leaving for the premises. If doing so, they should telephone the originally recorded number for the ARC and not rely on information given by the caller. If there is any suspicion that the call-out message is bogus, keyholders should immediately telephone the police and follow their instructions.

On arrival at the premises, and if a police response is expected, keyholders should wait at a safe distance, but within sight of the premises, until the police arrive. If the police do not arrive within a reasonable time, keyholders should contact the local police station for advice before approaching the premises. Keyholders should specifically request the attendance of the police and not enter the premises alone unless satisfied that it is safe to do so. Since not all police stations are open continuously, keyholders should have the number of the nearest police station that is open 24 hours a day.

5.7 Keyholder on premises when the system cannot be reset

If the system cannot be reset following an activation, keyholders need to remain on the premises until this can be rectified, unless they are relieved by an appropriate person. However, while waiting at the premises keyholders may be vulnerable, and special procedures must be followed:

- wherever possible, keyholders should telephone another employee or a member of the management or security staff directly to seek additional support; and
- the premises should be secured from the inside and tradesmen or others admitted only if the visit has been pre-arranged and they can show appropriate identification.

It may be possible, via neighbourhood watch schemes or by a mutual aid arrangement with other local businesses, for security staff at neighbouring premises to be alerted so that they may keep the premises under observation and give assistance if required.

Assistance may also be obtained from professional security companies who may be able to provide:

- security guards to support or relieve keyholders;
- visits from patrols; and
- regular contact by telephone.

It will be necessary to make contingency arrangements beforehand for such services to be quickly available.

5.8 Mobile telephones

Keyholders must be in possession of mobile telephones. Their batteries should be maintained at a high state of charge so that, for example, a voice call to a colleague may be left open throughout vulnerable operations, especially if opening ‘target risks’ after an ESS activation.

5.9 Cash and valuable property in safes

It is advisable that, where there are safes/strongrooms, etc, containing significant amounts of cash or other valuables within a premises, keyholders having charge of the premises keys should not routinely bring keys to these secure areas with them during a call out. For ‘target risks’ keyholders should ideally not hold the safe keys, or be aware of any safe combination number.

If it is necessary for the holder of the premises keys to also hold safe keys, the safe should have a dual locking system, with one person keeping one key (or combination number) and a second person having the other key (or combination number), so that they must both be present before the safe can be opened.

Alternatively, a time lock should be provided, so that even with the appropriate key or combination number, the safe cannot be opened until the pre-set time has been reached. Where a time lock is used, the time set for opening should be after the premises are fully occupied, and not when keyholders first arrive to open up.

As a deterrent to criminals, special anti-hold-up measures, such as time locks and time delay locks (which delay access to the contents of a safe for a predetermined period), should be publicised by an official notice posted on the safe or in the vicinity of it. Staff members should also be informed of these special security measures and be trained as to how to respond to criminals in the event of a hold-up.

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