S12
First published 2009
Version 01

# Security

## Police response intruder alarm systems: ten-step guide for purchasers

RISCAuthority

administered by FPA Fire Protection Association

## Acknowledgements

The assistance of the following with the supply of images for this guidance document is gratefully acknowledged:

Cooper Security Ltd
Pyronix Ltd

## IMPORTANT NOTICE



## CONTENTS

## 1. INTRODUCTION

Intruder alarm systems are an effective means of protecting both commercial and domestic premises against theft, robbery, malicious damage and arson. As such, premises owners or occupiers may find that their insurers make certain types of insurance cover conditional upon having such a system, and most often one with police response. In doing so, insurers will usually require an alarm system to meet certain requirements, as outlined in this guide.

Alarm systems can be a complex and significant investment in security and the adage 'you get what you pay for' should be kept in mind. Time spent researching the topic should help inform your discussions with prospective alarm installers, and thus help you choose the most appropriate alarm system.

This ten-step guide outlines insurers' likely main requirements/ recommendations for a new police response alarm system. By following them you will help ensure that any new alarm system is both acceptable to your insurer and is a reliable and sound investment.

A simple summary of the guidance is included as Appendix 1.

**Note:** If you require further information on the design and use of these, or other types of, alarm systems, there are several RISCAuthority guides on intruder alarm systems and related matters, which are available as free downloads from the RISCAuthority website *www.riscauthority.co.uk*

## 2. BASIC ELEMENTS OF AN ALARM SYSTEM

Alarm systems consist of three basic elements: detection devices, control equipment and the signalling equipment. The detection devices (typically including door contacts, movement or vibration detectors and sometimes 'hold up' buttons), together with alarm signalling equipment are connected to the control equipment (the 'panel') – which acts as the 'nerve centre' of the system.

Although performing a distinct, separate function, the signalling equipment is often incorporated into the panel. The purpose of the signalling equipment is to transmit a signal if the alarm activates. It can do this 'locally', eg by operating sounders on the outside and/or inside of the building, or 'remotely', eg by sending signals to a police recognised Alarm Receiving Centre (ARC). Most police response alarm systems have both local and remote signalling.

## 3. TEN-STEP GUIDE TO BUYING A POLICE RESPONSE ALARM SYSTEM

### 3.1 Step 1 – Selecting an installer

To ensure that alarm systems are properly designed, installed, maintained (under a service contract) by trained, competent and security vetted personnel, and connected to a suitably regulated/ police approved ARC, you should only select installers who are on the approved list of one of two regulatory bodies, namely the National Security Inspectorate (NSI) or the Security Systems and Alarms Inspection Board (SSAIB).

For further information and details of approved installers in your area, please visit *www.nsi.org.uk* (tel: 0845 006 3003) and/or *www.ssaib.org* (tel: 0191 296 3242).

### 3.2 Step 2 – Consulting your insurer

Not all property will be insured but where insurers are interested they may stipulate alarm system requirements, or otherwise provide general advice.

It is recommended that you contact your insurer for advice, and then pass their suggestions to an installer, rather than expect the installer to contact them directly. If you are uncertain who your insurer is, contact your insurance broker.

One advantage of obtaining prior insurer guidance is that prospective installers will be competing against a backdrop of common basic requirements, thus reducing the dangerous temptation to cut specifications down to produce the cheapest quotation.

**Important note:** An insurance policy may contain a condition that requires:

- a particular type of alarm installer, system, signalling and response;
- an emergency/routine maintenance contract being kept in force;
- provision to the installer and others of keyholders' details;
- the insurer's prior approval for any changes to the system;
- the insurer to be notified if police response is reduced or withdrawn;
- full setting of the alarm system, including all means of communication with the ARC, whenever the premises are left unattended (and possibly partial setting at other times);
- keeping any alarm operating codes secret and not leaving alarm operating devices at the premises when they are unattended; and
- prompt keyholder attendance after any reported alarm activation or fault.

Policy conditions vary between insurers, so you should check your own policy for details of any such condition, and whether failure to comply could jeopardise insurance cover.

### 3.3 Step 3 – Security grades and the risk assessment process

When designing an alarm system, installers regulated by the NSI or SSAIB are required to conduct a formal security risk assessment. This is to help determine a security 'grade' for the system (detection and control equipment) and signalling, plus other system design features, most appropriate to each customer's circumstances. Insurers treat grade of system and grade of signalling as separate issues and their likely stance on each can be summarised as:

- **System (detection and control equipment)**

  Grade 1 – inadequate for insurers' needs;

  Grade 2 – suitable for most domestic and some low risk commercial premises;

  Grade 3 – suitable for most commercial, and some high risk, domestic premises; and

  Grade 4 – suitable for very high risk premises.

- **Signalling system**

  Grade 4 dual path remote signalling will usually be required, plus an external alarm sounder.

Installers can't be expected to anticipate every aspect of an individual customer's risk exposure, so you should fully co-operate in the risk assessment process. If you are not asked about certain issues that seem relevant to you, for example, after reading this guide or based on your own perception of risk, ask the installer to take them into account, or explain to you why they do not think they are relevant. Some matters that may be overlooked include:

- **Insurer requirements:** has your insurer made any requirements or offered advice?
- **Risk of sabotage of equipment or signalling:** has the installer fully accounted, for example, for the risk that movement detectors could be covered, or that phone lines used for signalling could be cut?
- **Business interruption:** monetary values of target items are not the only indictor of the need for a higher grade system. Has the installer considered the risk of lost trading or damage to business reputation, for example following theft of important items or records, and/or damage to the premises or vital production machinery, for example following possible arson or malicious damage?
- **Future risk:** in view of the often marginal increase in costs for Grade 3 versus Grade 2 equipment it may, if it is likely that you might acquire more/different target items, be worth buying a higher grade system now, as this could avoid later upgrade costs.
- **Police response and keyholder safety:** the aim should always be to obtain a police response early on in any break-in; not only to reduce the size of any loss or increase the chance of an arrest, but also to provide timely assistance and reassurance to keyholders. If you use employees as keyholders, you will have health and safety responsibilities in this area. As such, the risks of attending alone ('lone working') should always be considered in determining alarm system design.

**Important note:** Selecting the correct grade of system and signalling at the outset is very important, as the grade of equipment cannot usually be later changed to another grade without buying replacement components.

### 3.4 Step 4 – Choosing system and signalling grades

When it comes to grades of system (detection and control equipment) the common choice at most premises is likely to be between Grades 2 and 3. The main differences between them are that Grade 3 systems can record more information in their memory (event log), have better mains power monitoring and battery back-up and, significantly, have movement detectors that:

- prevent or detect re-orientation (changed field of view); and
- detect 'masking' (blocking or covering the detector).

At many commercial, and a few domestic, premises the nature and value of the property at risk will be such that a Grade 3 system will clearly be appropriate.

In cases of doubt, a factor that may suggest the need for a Grade 3 system is the risk of interference with alarm equipment when the alarm is unset (particularly movement detectors), either by members of the public or by staff. This can be a particular risk with, for example, premises such as shops, pubs, clubs, car showrooms or leisure facilities etc, where the public may have unsupervised access during business hours, or for those businesses that have a large or transient workforce – perhaps of uncertain trustworthiness.

**Figure 1: Movement sensors can be vulnerable to interference**

When it comes to grades of signalling, installers may simply suggest a grade of signalling that matches that of the system. However, there are significant differences between the grades of remote signalling; principally in how quickly any failure, for example, cutting of the telephone line, will be detected and notified to the ARC.

With Grade 4, this is a maximum time interval of 3 minutes, but with Grade 3 and 2 the intervals are 5 and 25 hours respectively. Faced with this, and given the importance of remote signalling to the overall effectiveness of the system, Grade 4 signalling will very often clearly be the most appropriate choice, whatever the underlying grade (2 or 3) of the system.

**Important note:** In cases of doubt as to which system and signalling grade is appropriate, the safe insurance default is to select system Grade 3 and dual path signalling at Grade 4.

### 3.5 Step 5 – Sequential confirmation (system design)

To minimise the risk of police being called out to false alarms, new police response alarm systems must be of a type capable of generating what are called 'confirmed activations'. Sequential confirmation is the format most used and, in simple terms, requires that the ARC receive two or more alarm-related conditions, within a certain time period, before they can ask the police to attend.

Whilst the police will only respond to confirmed activations, keyholders are expected to respond to both confirmed and unconfirmed activations. To help ensure that keyholders are not called out without the police, it is important that the design of a confirmation alarm system ensures that:

- there are sufficient detection devices to ensure that a confirmed activation is obtained early on during any break-in;
- any detrimental security impact that might result from the designated alarm 'entry/exit' door being forced open by intruders is minimised; and
- suitable dual path signalling is provided.

These issues are each expanded upon below.

#### *3.5.1 Detection and control equipment*

Insurers will be looking to see that systems have been designed to generate a confirmed activation from all 'at risk areas' (areas containing 'target items', that is items which are expected to be of attraction to criminals) as soon as possible after an intruder enters them. This typically involves having at least two different forms of detection device at, or near, each possible entry point.

In addition, the alarm system control and signalling equipment should be located in an area concealed from external view, and alarm protected in such a way that intruders cannot reach it without creating a full alarm activation.

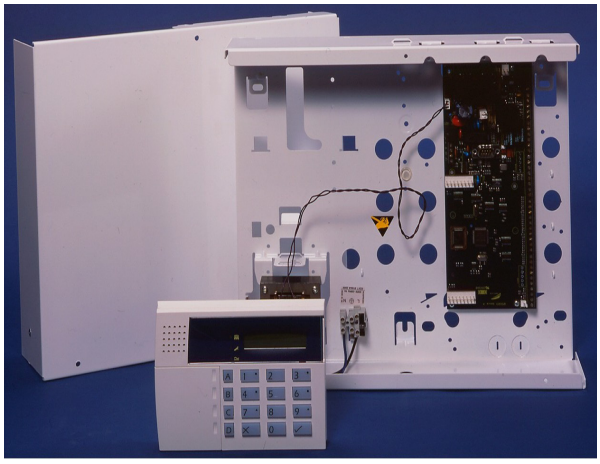

**Figure 2: The control and remote signalling equipment should be installed out of sight and in a secure area**

#### *3.5.2 Unsetting*

Alarm users need to have a way of switching off an alarm system without causing a false alarm. There are a variety of ways that this can be done but it is likely that the installer will propose one of two methods, often referred to by the clause numbers in the relevant standard (DD243: *Installation and configuration of intruder and hold-up alarm systems designed to generate confirmed alarm conditions – Code of practice*). In simple terms, these two options are:

- **Using a door lock linked to the alarm (Clause 6.4.3):** when alarm users unlock a designated entry door (fitted with a lock electronically linked to the alarm), the alarm system turns off its confirmation capabilities. Thereafter, the user can enter the premises and fully unset the system by entering a security code at a keypad.

  **Note:** An intruder forcing open the entry door will immediately start the process of generating a confirmed alarm. Insurers generally prefer this means of unsetting.

- **Using a digital key to unset the system (Clause 6.4.5):** the system is unset by operating a hand-held transmitter (similar to a car remote control key) or by presenting a proximity card or token ('fob') to an electronic 'reader'. There is a designated entry door through which the user must enter, and an entry timer device. During the entry time alarm sensors covering the entry route will be activated by users, but any resultant alarm activation is held on site to allow the user time to unset the system. If the system is not correctly unset at expiry of the entry time, an unconfirmed alarm will be transmitted to the ARC. After expiry of the entry time, and a further false alarm abort time, a confirmed alarm can be generated – but only after further detectors not covering the designated entry/exit route have activated. With this form of unsetting, depending upon the layout of the premises and the alarm detection, creation of a confirmed alarm activation may either prove impossible to obtain or be obtained too late during a break-in to be really effective.

  **Note:** An intruder forcing open the alarm entry door will be treated by the system as a potential user, and any confirmed alarm may be either delayed or not obtained at all. Whilst insurers will generally accept this method, they may not do so at premises where significant values of 'target items' are within easy reach of the entry door.

**Figure 3: A typical portable transmitter**

### *3.5.3 Signalling*

To help ensure that alarm events can still be sent to the ARC after, for example, a phone line has been cut, signalling products used in conjunction with sequential confirmation systems need two connections (paths) to the ARC, each using a different type of signalling technology, for example, telephone and radio. Such systems are termed 'dual path' signalling systems.

A critical feature of dual path signalling systems is how soon, if at all, the ARC will become aware of failure of either or both paths, as this may indicate criminal activity and permit them to promptly call the police alongside keyholders.

With remote signalling potentially the weakest link in any alarm system, insurers will usually require a Grade 4 dual path signalling system to be used, whatever the underlying grade (2 or 3) of the system.

In addition to the remote signalling, insurers will still usually want an external alarm sounder installed for its local deterrent and warning effect. Such sounders can also help police locate the premises to which they are being called. Sounders should be installed at a height above ground, and in such a location, that they cannot easily be reached by intruders and attacked.

Figure 4(a)

Figure 4(b)

**Figure 4: External sounders should be installed at high level, eg 4m above ground, as shown in (a), not (b)**

### 3.6 Step 6 – Hold-up (personal attack) alarms

Hold-up alarms, commonly referred to as personal attack (PA) alarms, are used to alert police to the need for an emergency response to a violent or threatening event.

PA facilities can be an important feature of alarm systems but, because of the risk of (often well-intentioned) misuse, and the consequent impact on police resources, they should only be provided if there is a real risk of an attack. Dual action push button devices are usual, and should be located adjacent to the expected area of an attack (to permit their use by someone viewing, but not directly involved in, the attack).

### 3.7 Step 7 – Alarm response

Insurers value police attendance to alarms as only they have the authority, back-up resources and potential timeliness of response to effectively deal with criminal events, and also provide related safety and support for keyholders. To obtain it, arrangements for an immediate 'level 1' police response, or the next best available level ('level 2'), need to be put in place by applying for a police Unique Reference Number (URN). Your installer will arrange this for you. URNs are issued (and, in the event of undue false alarms, withdrawn) in accordance with the responding police force's Security System Policy (SSP). Details of available response levels and the SSP can be obtained from alarm installers and your local police force headquarters.

In addition to the expected police response, some keyholders (either non-commercial or commercial) need to be appointed for every alarm system to respond to all (confirmed and unconfirmed) alarm activations and faults, allow others access (the police, for example), and then take any necessary remedial action, including checking that the alarm system can be fully reset, before leaving the premises.

#### *3.7.1 Non-commercial keyholders*

Non-commercial keyholders will typically be the alarm owner or persons associated with them, for example, members of staff, friends or neighbours.

Keyholders should reside within a reasonable travel time of the alarmed premises (a maximum of 20 minutes for alarm systems with a URN), and be fully trained in the operation of the alarm system and associated security procedures.

With personal safety in mind, all non-commercial keyholders should be advised to:

- carry a mobile phone;
- attend with someone else (another keyholder, colleague or spouse/partner etc);
- take care upon arrival at the premises to survey the immediate scene; and
- call for police assistance via the 999 telephone system if there are clear signs of a break-in, and/or if intruders can be seen within.

If you cannot find anyone to act as a non-commercial keyholder or feel that those available may not attend reliably, cannot do so within a reasonable time, or health and safety considerations warrant a complementary or alternative response, you may need to consider appointing a commercial response company.

### *3.7.2 Commercial keyholders*

For a fee, commercial response companies will undertake to act as keyholders.

Insurers are usually happy for commercial response companies to be used instead of non-commercial keyholders, but generally recommend that the company holds NSI/SSAIB approval, or otherwise complies with Security Industry Authority (SIA) licensing requirements (most readily ascertained by choosing a company holding SIA Approved Contractor Scheme (ACS) status).

In an effort to provide what they claim can be a quicker response time, as it will avoid the need to retrieve premises keys from an operating base/roving operational vehicle, some commercial response companies may offer to store premises keys within a key box (sometimes referred to as a 'key vault') attached to, or embedded in, an external wall of the premises. Notwithstanding the 'quality' of the key box used or its fixings, such a practice could compromise security as criminals, should they attack and gain access to the contents of the key box, may not only possess the means (typically a door key) to let themselves in but also the means (typically an alarm fob) to turn off the alarm system.

**Important note:** The use of key boxes is a clear security risk and is likely to contravene your insurer's policy alarm condition.

### 3.8 Step 8 – Alarm receiving centres.

Your installer will usually arrange for a suitable ARC to handle alarm signals. Some installers have their own in-house ARC, others appoint an independent one.

ARCs will usually handle alarm activations/faults in accordance with their own standard alarm event handling procedures. These will be detailed in a formal 'response agreement', a copy of which should be made available to you.

It can reasonably be assumed that an ARC will notify the police (alongside keyholders) of all alarm activations where it is appropriate to do so. However, you should check that the ARC will inform keyholders immediately of events where a police response may not be available, in particular:

- receipt of any unconfirmed activations (when the system is set);
- receipt of any alarm or power system faults that could affect the operation of the alarm system (when the system is set); and
- failure of any signalling path (at any time).

**Important note:** Where ARC procedures do not match those noted above, and the ARC will not agree to change them, reference should be made to your insurer.

### 3.9 Step 9 – Making your choice

At the end of the risk assessment and design process, installers will make their written proposals (see Appendix 2) to customers, who then have to consider if they meet their (and their insurer's) needs. This can be a difficult decision, especially as it is unlikely that any two installers will come up with identical proposals.

At this stage, price, although an important consideration, should not be the sole determining factor. Instead, attention should be paid to the nature and extent of proposed alarm coverage, the ability of the system to produce the required response early on during any attack and its resilience to deliberate interference. In short, in a break-in or attack, will the alarm system do what you expect, or be found wanting?

### 3.10 Step 10 – Training and use

Your alarm system will not perform well if those who use it do not understand how it works and should be used. Training will help maintain your intended level of security and avoid many common causes of false alarms.

False alarms are not only troublesome but can be expensive to resolve, particularly if they lead to the withdrawal of police response – a situation that can also affect your insurance cover.

Your installer should offer full training in the scope and correct use of the alarm system, and you should ensure that all those likely to use it receive this

## APPENDIX 1 – SUMMARY OF INSURERS' TYPICAL REQUIREMENTS FOR A POLICE RESPONSE ALARM SYSTEM

Insurers' likely main requirements/recommendations for a new remotely monitored police response intruder alarm system are listed below.

- **Installation/maintenance to be by:**
  - a National Security Inspectorate (NSI)* or the Security Systems and Alarms Inspection Board (SSAIB)* listed installer, eligible to apply for a police URN with the force in whose area the alarmed premises are located; and
  - with a contract for emergency and routine maintenance in force.
- **Security grading of system (detection and control equipment) to be:**
  - Grade 3 for most commercial risks, Grade 2 for most domestic risks.
- **Sequential confirmation system to be designed, with:**
  - control and signalling equipment installed out of sight, and not located in an area used as an alarm entry-exit route;
  - two appropriate forms of detection[1] in each 'at risk area'[2]; and
  - means of unsetting to be via an entry door lock linked to the alarm unless the entry route or premises are considered low risk, in which case, use of a remote control device (transmitter or fob) upon entry is acceptable.
- **Hold-up alarm facilities (where required):**
  - dual action attack devices sited adjacent to expected attack area.
- **Signalling to comprise:**
  - a Grade 4, dual path, remote signalling product (ideally one independently certified as meeting Grade 4, but in any case as agreed by the insurer); and
  - with a supplementary external self powered audible warning device (sounder).
- **Monitoring to be by an Alarm Receiving Centre (ARC), with:**
  - NSI/SSAIB approval; and
  - the ARC notifying the police (where eligible) and keyholders of all alarm events/faults, including signalling path failures, immediately upon receipt.
- **Response to be by:**
  - the police, at the highest response level provided for by the responding force's Security System Policy (SSP); and
  - your keyholders (owners/staff/friends, etc or a response company).

**Note:** If a response company is used, NSI/SSAIB listed companies are preferred. Response companies must not store alarm operating codes or devices at your premises, eg in a key box, without insurer approval.

* For further information and details of listed installers in your area, please visit *www.nsi.org.uk* (tel 0845 006 3003) or *www.ssaib.org* (tel 0191 296 3242).

[1] Typical detection devices are door contacts, movement sensors – such as passive infra-red detectors (PIRs), dual technology devices ('Dualtechs') or twin motion detectors (TMD) – and vibration sensors.

[2] Areas containing 'target items', that is items which are expected to be of attraction to criminals.

## APPENDIX 2 – ALARM SYSTEM DOCUMENTATION

Installers are required to document various aspects of alarm systems, as follows.

### Security risk assessments

Although you need to be aware of its outcome, it is not a requirement that an installer shows you their risk assessment. However, most installers will disclose it, and some will ask you to sign it.

Insurers will not normally wish to see the installer's risk assessment if it accords with the suggestions of their own guidelines (or specific requirements following a site visit). However, it may be helpful to provide a copy of the installer's risk assessment if you wish to follow a course of action that is contrary to the insurer's general or specific requirements/recommendations.

### Specifications

Installers are required to prepare documents detailing the type and position of equipment used in alarm systems. Traditionally called alarm 'specifications', such documents are more correctly referred to as:

- 'system design proposals' (SDPs) – for proposed systems; and
- 'as fitted documents' (AFDs) – for installed systems.

Where an intruder alarm is required by an insurer as a condition of cover, they may ask to see a copy of the SDP or AFD to ensure that the system meets their needs. A copy layout/detection plan should be requested from the installer as part of (or to augment) the SDP/AFD, as this will greatly assist insurers in making their decision.

### ARC response agreement

You will need to complete a document for the installer/ARC providing details of at least two keyholders (and preferably more, to allow for holidays, illness etc).

A further document should also be made available, if full details are not included in the SDP, detailing what steps the ARC will take in response to various types of alarm related events or faults.

Fire Protection Association
London Road, Moreton in Marsh
Gloucestershire GL56 0RH, UK
Tel: +44 (0)1608 812500  Fax: +44 (0)1608 812501
Email: administrator@riscauthority.co.uk
Website: www.riscauthority.co.uk



Hard copies of this document may be obtained from the publications department of the FPA at the above address.

Electronic copies may be obtained from www.riscauthority.co.uk.

RISCAuthority

administered by FPA Fire Protection Association