Management of Intruder Alarms

The modern intruder alarm system is a valuable, sophisticated weapon in the fight against crime. However, like any technology-based supervisory system that depends upon human interaction and intervention to fulfil its purpose, its value is very significantly influenced by the quality and rigour of management control applied.

It is most important that the greatest benefit be obtained from your intruder alarm system by correct operation and setting in its entirety when your premises are left unattended. Should you be unable to set the system in its entirety (for example, a signalling communication path is unavailable or some other part of the system is in a fault condition) you must call the alarm company immediately and not leave the premises unattended until the fault has been put right and the alarm has been fully set.

False Alarms and Withdrawal of Police Response

The issue of False Alarms is a major one for police. Installers are now required to install to the Intruder Alarm Policy set by the Association of Chief Police Officers (ACPO). It is now required that all new alarms are "confirmed". This means that 2 signals must be sent within a 30 to 60 minute period, before the central station will ask the police to attend.

Each police force will modify the ACPO policy to fit, but there is a threshold of three false alarms within a 12 month rolling period, beyond which the police will not respond. This is reduced to two if it's the case of a panic alarm that is not genuine. The police forces in England, Wales and Northern Ireland, will normally downgrade their response from Level 1 (immediately) to Level 2 (response is desirable but attendance may be delayed, e.g. due to resource availability) to any system which generates 2 false calls in any 12 month period. Following 3 false calls in any 12 month period Level 3 (no police attendance, keyholder response only) will normally apply.

It is the alarm users' responsibility to manage the system in a way that does not cause false alarms.

In some parts of the country, lower false alarm thresholds may apply and you need to be aware of the thresholds applicable in your local area.

If you receive a letter warning you that police response to your system may be downgraded or withdrawn you must inform GJIS Limited or your insurance adviser immediately. Failure to do so may invalidate your insurance cover.

Note: with effect from 2008 the police (in the UK) have indicated their intention to reduce the level of false alarms to 1 only and will not resume response to the systems until they have been up-graded to a confirmed system. At this stage it is also likely that they will also require hold-up alarm activations to be confirmed! Currently technology does not permit this. It is never going to be easy to keep up with changes with the policing authorities therefore it is important to ensure that your intruder alarm system is regularly serviced and updated to keep a breast.

You must make sure that everyone authorised to set and unset the system has been fully trained in its operation. This should include where applicable the walk testing of movement detectors to ensure they are effective and that the field of cover is not obscured or restricted. GJIS Limited has a Checklist for Keyholders available for users of the system as an aid to prevent false activations.

Keyholder Response

The system must be allocated a police Unique Reference Number (URN) and thus benefit from police attendance to alarm activations in accordance with the Force Intruder Alarm Policy. If there is notification of a reduced level or withdrawal of Police response to the System GJIS Ltd must be informed immediately.

The premises must not be left unattended unless physically secured and the alarm system is fully set including the designated methods of remote signalling.

If the alarm is activated (whether the activation is confirmed or not), or any signalling path is lost, the appointed key-holder must attend the premises immediately to investigate the reason for the activation.

Confirmed systems require two detectors to activate but if one activates insurers normally expect the keyholder to attend which will be without police back-up. In view of this and the possible risk of injury to the keyholders combined with the health and safety implications it is recommended that a keyholding service is used to attend either in place of or in addition to the Assureds keyholder. The likelihood or possibility that thieves are working a ruse to get the owner or keyholder to the Jewellery premises should always be considered and therefore a minimum of two keyholders or persons should attend.

If there is a fault with the alarm system or an alarm signalling path, an engineer should be called and the keyholder should not leave the premises unattended until they are fully re-secured, with the alarm system and its signalling paths fully reset. Failure to both fully secure and alarm the premises may invalidate your insurance cover.

Key holding nominations and arrangements must ensure that someone is always contactable should a response be required. Delays in contacting keyholders can result in thieves having longer to steal or damage your property. It should also be remembered that the police cannot enter and check your premises unless a keyholder is present. Most police forces require that keyholders must be able to be at the premises within 20 minutes of being contacted. Failure to comply may lead to withdrawal of police response.

The GJIS Limited "Checklist for Keyholders" is available for users of the system as an aid to list key contact points and telephone numbers in the event of an activation.

Key Holding companies

Regulations in London for commercial premises require either two non-professional keyholders of one professional keyholder able to respond to an alarm 24/7 and within 20 minutes of the intruder alarm being activated.

Instead of asking a member of staff to respond during the night or out of hours, a key holding company can have a trained warden attend and execute a security check. If a break-in has occurred then the keyholding company will liaise with the police, organise for contractors to attend, make good any damage and ensure that the property is left secure.

With new lone worker health and safety requirements it is often now necessary to employ a professional keyholder.

Telecommunication Failure

British Telecom provides various grades of breakdown response cover on telephone lines to the local exchange. Customers whose alarm systems signal via British Telecom lines are strongly recommended to subscribe to their Total Care contract which will ensure that the best response is obtained when there is a fault on the line.

Code Words

Caution must be exercised over the issue and management of code numbers used in operating the alarm system, and any passwords agreed with the alarm company. These are very important to the security of your system. Never leave a note of them on the premises, even in places that are not normally available to unauthorised persons and do not reveal them to any third parties who may be working temporarily at the premises (e.g. contractors). To do so may put your insurance cover at risk. Individually allocated codes provide the greatest security.

If you have been given a code to abort a false alarm consider now how to act:

- in the heat of the moment
- as quickly as possible
- With the least risk of disclosing this important code to unauthorised persons.

If you have a key-pad type control, never let others see the command digits being entered.

System Management Codes

If you have a code to authorise the remote centre to change agreed opening or closing times of your premises observe the same confidentiality rules as above. Remember the credibility of your system is at stake and altering these instructions over the telephone carries risks. You should arrange to keep to the agreed times and use your code only in exceptional or emergency situations.

Checking the Identity of an Alarm Company Representative

Make sure that you always check the identity and authorisation of visitors claiming to represent the alarm company. Remember even if you know the person, they may have changed jobs and no longer be authorised to attend your installation.

Always:

Ensure the visitor is referred to the person who is responsible for your alarm system

Establish the reason for the visit

Insist on seeing an identity card and check the photograph

If in any doubt, deny the visitor access to any part of the system until you have telephoned the alarm company and obtained confirmation of the details of the identity card/document and that the person's visit is known and authorised. REMEMBER, don't rely on a telephone number given to you by the visitor - only use the alarm company's published number.

If a criminal obtains access to your system when it is not set he may tamper with it and reduce your security. You are entitled to check with the alarm company EVERY TIME their representative visits. There may be special technical controls fitted into the control box that oblige engineers to telephone their company before working on your system.

For further assistance on this or any other risk management topic, please contact GJIS Limited.