Picture credit: Shutterstock.com

RED ALERT

Jamie Fretwell, *explains why alarm receiving centres play a vital role in protecting against intruders by providing a rapid signal identification and actioning service*

Since the advent of electronic CCTV and access control technology, alarm receiving centres (ARCs) have been mainstays of the security industry. Commonly defined as remote monitoring facilities where security operators receive data, signals and alarms, ARCs are usually manned by trained experts on a 24/7 basis, where they can assess a situation as it's happening and decide on the best course of action to deal with an incident.

Intruder alarms are widely recognised by insurance companies and, in some cases, considered a prerequisite to obtaining cover. However, with locally signalled systems activation is usually only indicated by an audible warning, such as a siren, which is located on the outside of a premises. Response to such systems relies on someone nearby both hearing the alarm and then taking action to investigate its cause or alert others.

Although an intruder alarm can act as a deterrent, alert property owners to emergencies and indicate that action needs to be taken, they are often ignored. A 2015 survey by GoCompare revealed that 76 percent of the 2,070 UK residents questioned had ignored a building's intruder alarm. The most common reason was that the person 'wasn't sure what to do' (26 percent), while 24 percent said they thought somebody else would deal with it.

So, although traditional alarms may alert staff or passers-by to an incident, they offer limited protection when used on their own. This is where an ARC comes in, as it can vet an incoming alarm signal and initiate agreed escalation procedures, if registered for police response, notify them so that necessary action can be taken.

False alarms generated from traditional security systems can result in the police response being removed from those sites

Although no two ARCs are the same, there are minimum standards that they have to be built and operated to. That said, when choosing an ARC it is vital to select one with the requisite industry accreditations. BS 5979 and the more recently introduced BS EN 50518, which has superseded BS 5979, and BS 9518 are recognised and accepted by the police service and security auditing bodies, while BS 8418 covers the installation and remote monitoring of detector activated surveillance technology.

BS EN 50518 specifies the minimum requirements for monitoring, receiving and processing alarms generated from alarm systems. In the latest edition of the standard, which came in October 2019, ARCS are divided into two categories with different levels of requirements. A Category I ARC will be designed and operated to a higher standard with respect to construction, security and integrity than a Category II ARC. Category I ARCs therefore handle security system signalling whereas Category II ARCs handle signalling from non-security systems. BS EN 50518 also addresses risk assessment, as well as operational safety such as standby power supplies. It contains technical requirements and information for performance on alarm handling, as well as requirements on daily operations, staffing, training, tests and access to an ARC.

ARCs can also hold National Security Inspectorate (NSI) and Security Systems and Alarms Inspection Board (SSAIB) certifications. To obtain these accreditations ARCs have to adhere to all relevant British and European standards for technical competency, operate formal internal procedures and audit processes to give greater customer assurance, demonstrate a long-term track record of performance and provide evidence of reliability and stability.

Eliminating false alarms is increasingly important and reputable ARCs can filter them out to ensure that only genuine emergencies are escalated. False alarms generated from traditional security systems can result in the police response being removed from those sites, while the time and effort required to gain reinstatement takes up resources and can leave sites exposed for significant periods of time.

The National Police Chiefs' Council's (NPCC) Police Requirements & Response to Security Systems policy sets conditions on the use of an allocated unique reference number (URN) when requesting attendance at an incident. To obtain a police URN there are certain conditions that must be achieved relating to the alarm system installed, the company used to install and maintain it, the type of signalling system used and the ARC connected to the alarm system. An immediate police response is obtained if a verified alarm signal from an ARC issued with a URN is triggered, and an ARC is able to use a direct phone line to the regional police to obtain assistance, rather than going through a national switchboard.

Greater collaboration and cooperation between the emergency services and ARC operators helps to deter crime and facilitates a faster police response. Funded by the private sector, the Electronic Call Handling Operations (ECHO) project is a significant technological advancement in the handling of intruder and hold-up alarm signals. It is available to emergency services across the UK that are ready to accept transmissions.

In the event of an activation from a monitored installation, an ECHO-connected ARC receives a digital alarm signal transmission direct from the premises. The signal is verified and transmitted directly to the relevant police service via ECHO, negating human intervention and enhancing the potential for rapid intervention by responders. In line with NPCC requirements for alarms to be delivered electronically to police control rooms, the number of ECHO-connected ARCs has grown significantly and signals from over 100,000 intruder and hold-up alarm systems registered with the Metropolitan Police, Avon and Somerset Constabulary and Essex Police are now being transmitted via its automated signalling service.

Estimates indicate a saving of up to four minutes in response time. This could prove critical in helping to quickly apprehend offenders, provide greater assurance to home and property owners and even save lives in critical emergencies where every second counts. Being ECHO connected offers ARCs a clear tangible commercial and performance benefit, while making sure customers receive the fastest possible response.

ALARM RECEIVING CENTRES VET INCOMING WARNING SIGNALS AND INITIATE PROCEDURES

Although ARCs are primarily used for the monitoring of intruder, CCTV, access control and fire detection systems, they are increasingly being used in a wide range of other applications. These include lone worker safety solutions via smartphone apps, dedicated safety devices and body-worn cameras, environmental monitoring such as temperature sensors and lift alarms, gas alarms in waste treatment plants, freezer alarms in shops and patient safety systems in healthcare environments. Other services include remotely assisting clients that wish to set and unset their sites depending on occupancy and activities being carried out.

Using an ARC can also introduce greater operational efficiencies. For example, it isn't necessary to assign manned guards to operate barriers for the occasional site visitor, carry out temperature checks, conduct internal patrols or provide CCTV monitoring and alarm setting. Similarly, using two person teams to manage access control and complete site patrols on an alternating basis is not usually required. Instead, using an ARC results in reduced resources and therefore costs required on site.

In retail environments, using remote investigation, whereby CCTV cameras move into pre-set configurations to provide an instant overview of what's happening, is highly effective. A centralised management system also provides an audit trail so that, if required, it is possible to prove that a predefined strategy was adhered to.

Some ARCs also specialise in providing services for lone worker protection. For example, if an individual feels that they are entering into a situation that poses a potential risk, they can send a pre-activation message to inform the ARC. This could be invaluable for a lone shop worker who is confronted with a potential risk situation, such as a customer who is behaving suspiciously or erratically but is not a definitive threat. In this situation the ARC could monitor the audio and/or video feed

to help verify the threat and take action if necessary. Over the last few years there has been a seismic shift in the level of technology incorporated into ARCs and the security systems they are connected to. The cloud allows shared resources, software and information to be provided to devices as a utility over the internet, rather than being loaded on to an individual computer or a physical server.

It offers the potential to create value, flexibility, greater resiliency and enhanced services through off-site storage, better control, real-time monitoring, remote service, maintenance and support, an enhanced end-user experience and faster integration with other disciplines such as video verification. It has been embraced by leading ARCs and a security system is now considered an internet of things (IoT) based solution.

REPUTABLE ARCS FILTER OUT FALSE ALARMS SO ONLY REAL EMERGENCIES ARE ESCALATED

Artificial intelligence and machine learning are also having an impact, with the former creating deep learning algorithms that can differentiate between genuine and false alarms, and allow ARCs to significantly increase their accuracy. At the same time, video analytics technology facilitates the aggregation and analysis of data by presenting information in statistical reports and graphs to identify when and where, for example, incidents are likely to occur, events are commonly triggered and who is using particular lone worker safety devices.

Companies that offer ARC services must be able to demonstrate to customers that their data is protected, accessible and stored securely. The most effective way to do this is via certification to ISO 27001 – the international standard for information security management systems (ISMS). An ARC with ISO 27001 certification will be able to guarantee that only authorised, competent and security screened personnel are provided with access to data for retention and/or processing, and can demonstrate robust policies around information security management.

As part of a Data Protection Impact Assessment (DPIA), a service provider should describe the nature, scope, context and purposes of the processing; assess necessity, proportionality and compliance measures; identify and assess risks to individuals; and identify any additional measures to mitigate those risks. Once a DPIA has been completed, a client must then decide whether the service provider can reduce information security risks to an acceptable level, appropriately protect information, ensure that employees comply with applicable legislative and regulatory requirements, and provide documentary evidence in the form of records to show that the processes are being followed correctly.

There is no 'one size fits all' when it comes to selecting an ARC and organisations looking to procure these services need to carry out a thorough assessment of what a potential partner can offer and, just as importantly, ask the right questions. BS EN 50518 and ISO 27001 are vital, as is SSAIB and/or NSI certification, while without an URN the police may not respond immediately. Utilising an ARC means that no matter the time of day, someone is watching and, when needed, can ensure a better level of emergency service ●

Jamie Fretwell is Head of Monitoring & Lone Worker Operations at Reliance High-Tech. He has over 20 years' experience working within the Security Industry managing ARC's, spanning a broad range of monitoring systems and technologies and end user applications. He has also represented employers on BSIA/BSI committees over many years.

When choosing an ARC it is vital to select one with the requisite industry accreditations

Picture credit: Shutterstock.com