Responding to Terrorist Incidents

Developing Effective Command and Control

SUPPLEMENTARY GUIDANCE – COMMUNICATION TECHNOLOGY

Preparing organisations for a terrorist incident

Edition 2, March 2023

National Protective Security Authority

Disclaimer

The information contained in this document is accurate as at the date it was created. It is intended as general guidance only and you should not rely on it. This information should be adapted for use in the specific circumstances required and you should seek specialist independent professional advice where appropriate before taking any action based on it. To the fullest extent permitted by law, National Protective Security Authority (NPSA) accept no liability whatsoever for any loss or damage incurred or arising as a result of any error or omission in the guidance or arising from any person acting, relying upon or otherwise using the guidance. Full terms and conditions governing the use of this guidance are available on our website at www.npsa.gov.uk

Freedom of Information Act (FOIA)

This information is supplied in confidence to the named reader and may not be disclosed further without prior approval from NPSA. This information is exempt from disclosure under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation.

Edition 2
March 2023

National Protective Security Authority

Home Office

NaCTSO NATIONAL COUNTER TERRORISM SECURITY OFFICE

Executive Summary

This document provides guidance about the different systems that can be used to improve communications within and between organisations and businesses responding to terrorist incidents. Lives will be saved when responding to terrorist incidents by introducing:

- Carefully selected communications systems.
- Relevant and effective training and frequent practice.
- Tried and tested policies and procedures.

The purpose of these communications systems is to share information and warn others of what is taking place, reducing the impact of an attack.

Reviews and analysis have been undertaken of how communications have been delivered in the immediate response to recent terrorist attacks. The findings have been combined with the outcomes of National Protective Security Authority (NPSA) simulated attacks to identify key issues.

Several different types of communication systems have been assessed. While most systems will operate effectively during business as usual or in response to minor incidents, only a small number of system types will work effectively during the immediate response to a terrorist incident.

While the most effective response is likely to be provided by a Security Control Room (SCR) with a minimum of three security operators, a range of systems can be used effectively in situations where there is no SCR.

Figure 1

Contents

1. Introduction

1. Introduction

Guidance about systems that can be used to improve communications when responding to terrorist incidents.

This document provides guidance about systems that can improve communications within and between organisations and businesses responding to terrorist incidents. The purpose of such systems is to rapidly share information and warn others that an attack is underway at a specific location, with the intention of saving life and preventing harm to others.

Detailed information is available from NPSA that will cover other aspects of planning to mitigate the response to a terrorist attack. It is recommended that before reading this guidance, readers should familiarise themselves with the NPSA MTA guidance titled:

Marauding Terrorist Attacks – Making your organisation ready.[1]

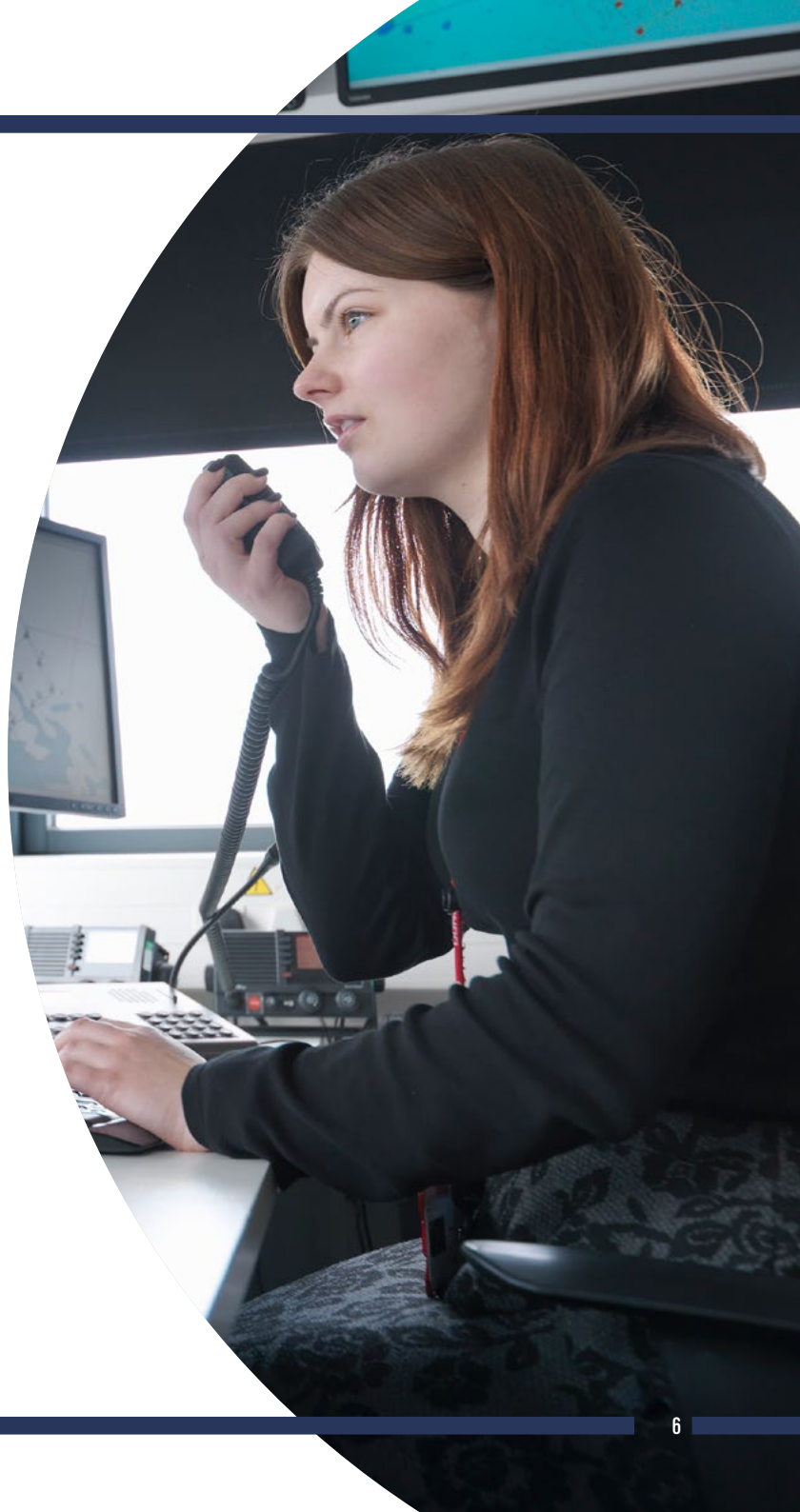
Detailed information is also available in relation to other aspects of responding to terrorist attacks. This includes:

Responding to Terrorist Incidents: Developing Effective Command and Control.
Guidance on how to enhance the capability of the Security Control Room (SCR) operator's response to a terrorist incident.[2]

Crisis Management For Terrorist Related Events.
A detailed guide for PR professionals to help mitigate the harmful effects of terrorist incident on brands, businesses and communities.[3]

Recent terrorist attacks have highlighted shortcomings in communications capabilities. Addressing these and other issues raised in this document will contribute to an organisation's ability to save lives and protect those they are responsible for.

NPSA will continue to provide updated guidance as further research and analysis are completed.



[1] https://www.npsa.gov.uk/marauding-terrorist-attacks-1
[2] https://www.npsa.gov.uk/incident-response-command-control
[3] https://www.npsa.gov.uk/crisis-management-terrorist-related-events

1. Introduction

Benefits of introducing effective communications systems			
Attack in an iconic crowded place		**Attack in a busy city centre - shopping area or night-time economy**	
Ineffective communications	**Effective communications**	**Ineffective communications**	**Effective communications**
• No means of communicating with public to tell them of the threat and action to take. • Not all security officers have a radio. • Insufficient training provided on radios – key features, how to interrupt. • Neighbouring site's alerts, scene very noisy, hindering ability to communicate	• Effective communications in place to communicate with public. Informing them of threats and action to take. • All operational staff and security officers are equipped with radios. • All staff trained and practised in use of radios. • Radios have emergency buttons and interrupt facility that users know how to use. • Emergency communications plan tested and deconflicted with neighbours.	• No preparedness for the attack. • No formal arrangements for communicating between neighbours. • Unable to warn each other of an attack coming. • Some informal means of communicating between security officers, allowing limited steps to be taken.	• Each premises has a response plan • Area-wide plan as to how all neighbours should communicate with each other. • Early warning system in place and effective. • Formal networks have been developed on resilient systems that support immediate communications

Table 1

1.1 Scope

This document discusses:

- Systems to be used to communicate between personnel working either for an organisation or independently.
- The importance of effective communications during the incident response and incident management phases of a terrorist attack in order to prevent other people being harmed and generate the appropriate response.
- The communication paths that demonstrate how people can communicate.
- Types of communication flow that demonstrate who will deliver and receive communications.
- Available types of technology and the pros and cons of using them in responding to a terrorist incident.

Throughout the document, examples are provided of specific systems and technologies that are available for purchase. These are included solely as examples of systems, and no endorsement of these systems is implied or provided. At this time, NPSA has only undertaken limited testing, technical assessment and limited evaluation of such systems. The assessment provided is based on user operability trials and NPSA's findings from the ASCEND trials and research into terrorist incidents.

1. Introduction

1.2 Intended audience

The principles set out within the guidance are intended to be adaptable, scalable and relevant to any site. The site maybe a site with:

- A well-resourced SCR in a National Infrastructure (NI) Site, crowded place or major event site. These may have multiple operators and complex communications and security technology.
- A SCR with minimal resources, such as a single SCR operator.
- Security officers deployed to the site but working without an SCR.
- Small businesses or organisations run by a manager with no dedicated security resources and a low level of security awareness.

1.3 Terrorist Attacks – Special Considerations

Terrorist attacks are intended to cause fear and, in many cases, to cause serious harm to people. Communication has a key role to play in keeping everyone as safe as possible through:

- Providing information about the nature of the threat.
- Keeping people away from the threat or other hazards or other methods to keep people as safe as possible.
- Summon assistance (e.g. police or first aid).

It should be remembered that while terrorist attacks are fortunately rare, they are likely to have a very high impact when they do occur.

1.4 Building on Business as Usual

Systems should be in place that support communications through the Business as Usual (BAU) operations and then during the response to an attack when the requirements of communications technology are likely to be different.[4]

The benefits of using the same system during all phases are:

- Staff will be familiar with its use and therefore more likely to use it during an incident.
- Staff will be better at using the system, be more practised, and more likely to follow the defined protocols that they know work effectively. Reducing the burden on staff which will enable a better quality of communication.
- An attack may start with a BAU issue (e.g. abandoned bag), so communications might start as usual and then escalate as the incident develops. The system should be able to expand to manage the anticipated surge in demand.
- A single system will be the most cost-effective.
- The amount of equipment that needs to be carried will be minimised.

[4] However, mixing urgent messages with routine messages may lead to them being ignored.

2. The response

2. The response

NPSA continues to investigate communications technology to assist with managing the response to an attack. The primary aim is to reduce the risks to personnel in or near the attack. This can be done by:

- Alerting businesses, organisations and other site occupants; neighbours and others that need to know that an attack is taking place at or close to the site.
- Delivering clear information to those affected so they can make informed decisions as to how to respond promptly.
- Warning people who could enter the attack site to keep away.
- Providing updates to those affected so they can decide if they need to do something different.
- Passing information to the emergency services as quickly as possible.
- Enabling the delivery of first aid to victims.

Common failures have also been identified and these have included:

- Insufficient communications available to operational staff.
- Inexperience and a lack of training in using the available technology.
- Excessive radio chatter and poor radio procedures.

Sites should consider how the communications methods intended for use during the immediate response to an attack can be developed and improved. When conducting a review of existing capabilities, sites should consider how they communicate with both those within their own and their neighbouring sites.

2. The response

2.1 Attack phases

The response to any terrorist incident is split into several phases. These phases are set out within the NaCTSO Crowded Places guidance titled *Managing Risk, Business Continuity*[5] and summarised in table 2. This guidance is focused on the **Incident Response and Incident Management phases**.

	Phase	Description
	Business as usual	The site is running in its steady state. No response has been initiated. During this phase sites are encouraged to use deterrence and security minded communications.
The focus of this guidance	Incident response	Incident response deals with the immediate impact of an accident. It is a short phase that focuses on escalation and activation, ensuring people and the environment are supported and made safe wherever possible. This period will cover a site's immediate response and the attendance of the Emergency Services to resolve the incident.
	Incident management	IM refers to how the organisation will manage the consequences of the business interruption at the scene through command, control, coordinate and communication. (IM covers who is in charge, how to keep stakeholders informed, escalation processes, coordination of resources, etc.)
	Crisis management	Crisis management is about your arrangements to manage strategic, complex and unprecedented events. It is rarely standalone and will require integration with other disciplines.[6]
	Business continuity & resilience	These are the arrangements you should develop in order to maintain critical and urgent business activites to a pre-determined level i.e., what work your business must continue to do to survive the disruption from a terrorist attack.[7]
	Business recovery	A Business Recovery Plan usually takes place over a long duration, with wider stakeholder engagement and detailing the priorities for rebuild, recovery and restoration. It should detail how and in what order you will return to the new normality following a disruption.[8]

Table 2

[5] https://www.protectuk.police.uk/advice-and-guidance/risk/managing-risk-and-business-continuity
[6] For more information see https://www.npsa.gov.uk/crisis-management-terrorist-related-events
[7] For business continuity see https://www.npsa.gov.uk/content/business-continuity
[8] For both business continuity and recovery see https://www.gov.uk/topic/public-safety-emergencies/emergencies-preparation-response-recovery

2. The response

The phases will overlap; the tasks relevant to one phase are likely to be running as the tasks relevant to subsequent phases have been activated.

The nature of communication during each phase will change. During the business-as-usual phase, there is likely to be a lower intensity of communication. This will be focused on routine and non-urgent activity. There is likely to be a rapid and significant increase in communication as an incident is identified and the "incident response" phase commences. The communications technology highlighted within this document can be used across the phases. However, the effectiveness will vary. It is likely to be the number, type and method of communication that changes.

As the attack is discovered, people will be working under immense stress, and there is likely to be considerable confusion. As a result, communications may be unclear and confused. Users may forget procedures, and may struggle to articulate themselves (e.g. stuttering, freezing and rambling). Other tasks will become more difficult to complete and users will struggle with multitasking, such as taking notes whilst speaking. However, a person's ability to respond during this phase can be improved through preparation, training and effective practice. Keeping policies and procedures simple will make them easier to follow. Using Standard Operating Procedures (SOPs) that set out the actions that need to be taken will be of considerable benefit at moments of high pressure. SOPs can be reinforced by using action or prompt cards, which will provide a useful checklist of the key tasks to be completed.

During the incident management phase, the nature of the communications is likely to change. The situation will start to become under control as situational awareness increases and response procedures are implemented. Pressure on all those delivering the response will remain high. The need for them to make decisions will continue and the demand to provide detailed information is likely to rise.

[9] https://www.npsa.gov.uk/Scan

2.2 Reporting suspicious activity

A person's actions or behaviour might attract attention, but it may not be immediately possible to gauge the reason for their suspicious actions. Is the person about to commit a terrorist attack? Are they involved in low-level criminality or are their actions unusual but without any malicious intent? A decision will need to be made quickly as to what action is proportionate and a key part of that decision making process should be communicating with others about what is being observed. From a different perspective, for example from the SCR where they have access to CCTV cameras, the actions may be explainable.

SCaN
SEE, CHECK AND NOTIFY

Training is available on the assessment of such situations through See Check and Notify (SCaN). SCaN aims to help businesses and organisations maximise safety and security using existing resources and is available at no cost. It empowers an organisation's staff to know what suspicious activity to look for and what to do when they encounter it. As a bonus, the skills they learn will help them to provide an enhanced customer experience.[9]

Sites cannot underestimate the importance of rapidly gathering information and then quickly passing it to people within and near the site. Individuals should use this information to enable them to make decisions concerning their own safety and organisations should use it to decide how they can most effectively protect their assets.

3. Command and control systems

3. Command and control systems

Command and control capability will vary considerably from site to site. Sites with a higher level of security, safety or operational risk are more likely to have an SCR and deliver a more impactive level of communication to their staff and other occupants. They should have plans in place to enable a comprehensive response to a terrorist incident.

At the other extreme, there will be small businesses and organisations where there is no SCR or other structured command and control capability and no dedicated security resource.

In all cases, the procedures introduced should be straightforward and easy to implement.

The level of automation or operational involvement required is an important consideration when selecting a communications system. Automation is likely to be of considerable benefit where there is little or no SCR capacity. The use of any system is likely to require:

- Staff to be trained in its use.
- Systems to be reliable and regularly updated, tested and maintained.
- An element of operational input when responding to an attack or other incident.

An assessment should be made of the security risks associated with your site and the level of mitigation that is delivered through the use of existing communications systems and processes. This may identify the need for additional measures to be introduced. The assessment should consider:

- The security threats that are considered to be of greatest risk.
- The operating environment.
- The identity and number of stakeholders.
- The availability of SCR operators or other decision makers during the response to an incident.
- The level of resilience that is required and the need to have multiple systems.
- If systems need to be site-specific or shared over several sites. For example, multiple sites could use radios operating on a single frequency.

The assessment is likely to identify that a single system is unlikely to provide sufficient capability to provide a resilient system that can cover all the communications requirements that will be identified, several systems may therefore need to be introduced. However, some businesses may simply only have one capability deployed to the site. In such circumstance, it is even more important to ensure that it works and that the appropriate training and exercising opportunities are provided.

4. Identifiying communication paths and flows

4. Identifiying communication paths and flows

Careful planning is required to introduce the most appropriate communications systems for sites. Each site should define their requirements for communications capability before deciding which solution they need.

During the planning process consideration should be given to the following factors:

- √ What type of message is being shared?
- √ In the event of an attack, what information should be immediately communicated?
- √ Who is delivering it?
- √ Who are messages being communicated to?
  - Staff
  - Management
  - Visitors
  - Neighbours
  - Public
- √ How do they receive the message? Do they have disabilities (deaf or hearing impaired/blind or partially sighted)? Do they understand English (in an airport, this may not be the case)?
- √ Are you communicating to other organisations who may have their own control room or individuals who may be working alone?
- √ How many people need to receive the message (capacity)?
- √ How quickly do people need to be alerted to the message being sent?
- √ Where does the message need to be delivered to (coverage)?
- √ Is a response required?
- √ How is the message being delivered?
- √ Will there be permanent monitoring of the system?
- √ How will systems be affected by a surge in communications?

4. Identifiying communication paths and flows

The site should also consider the following:

- ✓ How much time will a system take to administer and keep up to date?
- ✓ What is the user training requirement? Sites with a high turnover of staff will need to develop a training plan that is able to provide new staff with the information they require.
- ✓ How are data protection risks being managed?

Figure 2 provides a high-level framework to establish what is required for a site incident communications plan.

4. Identifiying communication paths and flows

Consider: In answering the questions listed it is also useful to consider the following issues that have been identified through NPSA's analysis into the immediate response to recent terrorist attacks and learning from the ASCEND trials.

- Lack of clear, concise messages, leading to misunderstandings or confusion.
- Overtalking on the radio, caused by poor radio discipline.
- Lack of communication between neighbouring businesses, arrangements are often ad-hoc.
- Lack of planning of what, why, to who and when information needs to be communicated.
- Failing to build resilient systems, with a lack of a secondary means of communication.
- Not all security officers are issued with a means of communication. Can they communicate and respond effectively when there is an urgent need if they do not have immediate access to a radio?
- Operating environments may not always allow the operator to identify a notification for some time after they have received it.

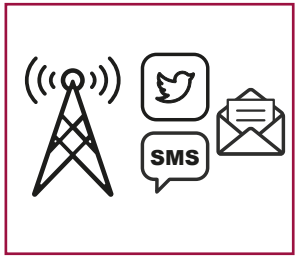
To make sure these issues are not manifested at a site, a carefully formulated plan will be required that considers the use of the right people, processes and technology.

The answers to the above questions and analysis of the current situation will enable a site to establish a high-level requirement for enhancing or adding communications systems.

5. Summary of communication technologies

5. Summary of communication technologies

Emergency communication systems



5.1 Mass notification systems

- MNS apps (5.1.1)
- SMS messaging (5.1.2)
- Social media (5.1.3)
- Cell broadcasting (5.1.4)

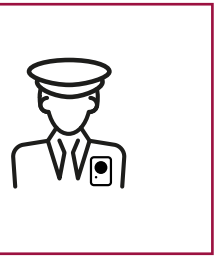
5.2 Push-to-talk communications

- Legacy radio comms (5.2.1)
- Push to talk over cellular (5.2.2)

5.3 Audible warning devices

- PA systems (5.3.1)
- VA systems (5.3.2)
- Loud hailers (5.3.3)
- Bells and sirens (5.3.4)

5.4 Visual warning devices



5.5 Body worn cameras

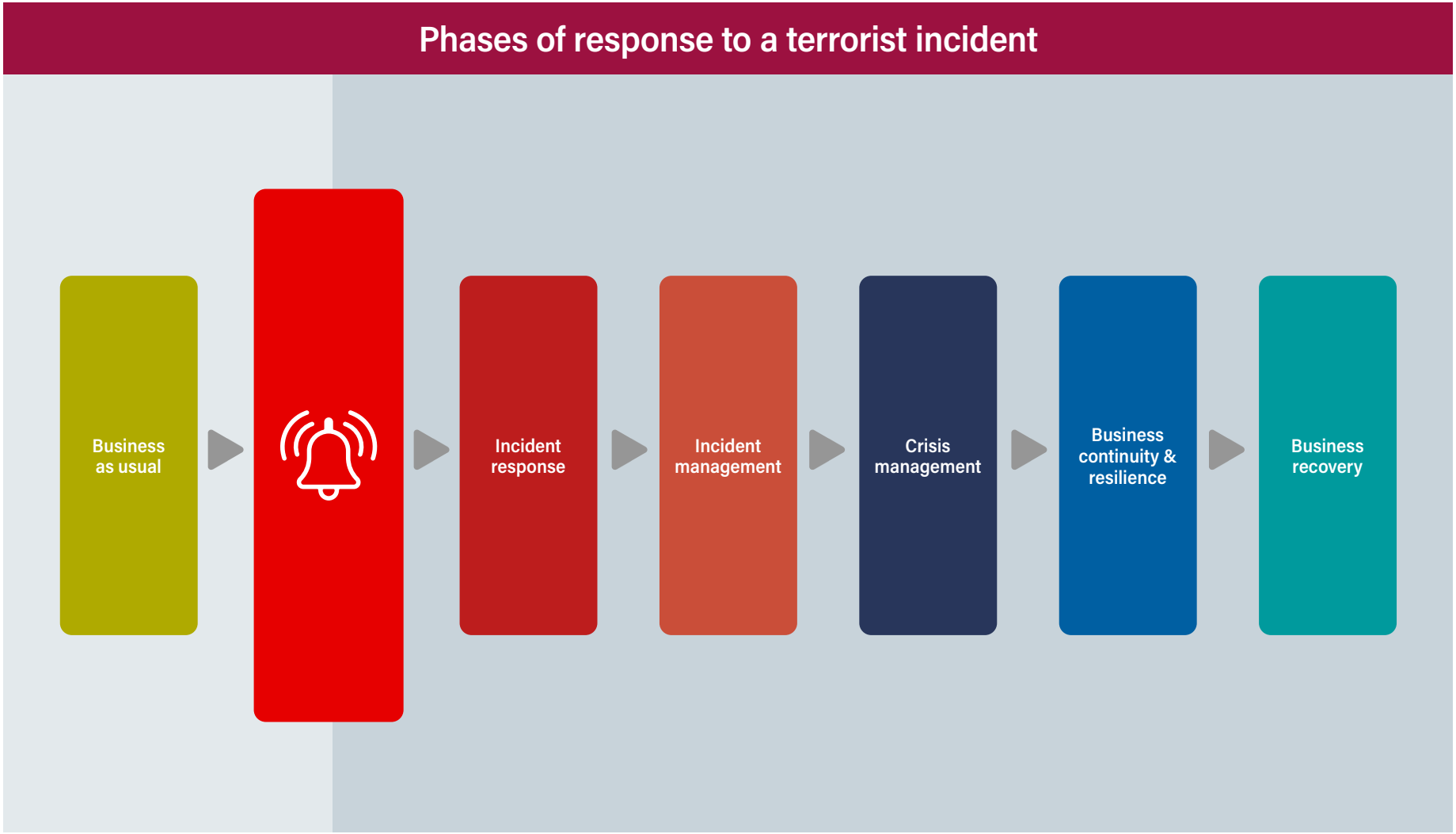
5.6 Personal safety apps

The following section describes several mass communication methods that have been identified. The systems are divided into six groups.

A summary is provided for each capability. This includes:

- The phase of greatest viability - An assessment of which attack phase the capability will work effectively.
- The pros and cons in relation to using that capability during the response to a terrorist incident.

5. Summary of communication technologies



5.1 Mass notification systems

Mass notification systems provide a capability to communicate across a range of different technologies to multiple people. The systems can communicate with an entire workforce, specific groups or individuals depending on the nature of the incident. If connected to PA systems or external audio/visual devices, sites can deliver communication to the public and neighbouring organisations.

Mass messaging should not be relied upon as a primary communication method to alert people to an attack, but it could supplement other technologies and effectively provide updates about an ongoing incident.

5.1 Mass notification systems

5.1.1 Mass notification system apps

Phase of greatest viability:

Pros	Cons
■ Can be used over multiple different communications technologies. ■ Messages can be presented on phone, tablet or PC. ■ Inexpensive to maintain. ■ Pre-set messages are quick to send. ■ Support non-urgent and time critical communications. ■ May provide a warning to those away from the immediate vicinity of the incident. ■ Bulk messages can be sent. ■ Works via the mobile network and venue Wi-Fi.	■ Requires constant monitoring by the recipient to identify an alert. ■ Primarily created for one directional communication. ■ Messages prepared during the attack will take time to write up and send. ■ Will not reach the public unless they have downloaded the app in advance. ■ Requires regular updating and administration. ■ Urgent messages may get missed amongst other routine messages. ■ Difficult to transmit and receive messages on the move. ■ Unless the SCR is heavily resourced, this is likely to distract the SCR operator from other key tasks.

Several mass notification apps can send messages within either a single organisation or be deployed where multiple organisations are connected to a shared Wi-Fi network and have a centralised body responsible for managing the system.

Example: A shopping centre could have a system where all employees and outlets within the centre could be connected to the app to receive notifications.

Furthermore, encouraging the public to use the app and connect to the Wi-Fi network would enable communications with them. Each app is likely to offer slightly different functionality and offer different modes of messaging. Everbridge is an example of a mass notification system app that can broadcast to a wide range of devices using predefined messages to multiple contact groups.

The successful use of a mass notification app will be partly dependent on the target audience's uptake. App use will likely need to be promoted, and uptake encouraged. A site recently reported that having implemented a new app-based system they had achieved an uptake of about 15%.

5.1 Mass notification systems

5.1.2 SMS messaging

Phase of greatest viability:

Business as usual | ~~Incident response~~ | Incident management | Crisis management | Business continuity & resilience | Business recovery

Pros	Cons
■ Inexpensive to operate. ■ Minimal training required. ■ Sends bulk messages.	■ Single routing of communications via mobile phone network and mobile phones. ■ Requires constant monitoring by the recipient to identify an alert. ■ Messages written during the attack will take time to write up and send. ■ Difficult to provide a live response to changing events. ■ Single route for communications. ■ Dependent on mobile network coverage. ■ Requires registration and regular updating of users. ■ Difficult to transmit and receive messages on the move. ■ Unless the SCR is heavily resourced this is likely to distract the SCR operator from other key tasks.

During a security incident, the SCR could use SMS messages to communicate as part of a mass notification system. SMS messages are a relatively cost-effective means of communication. SMS messaging can be used to send text-based messages to individuals or groups. Organisations could use SMS messages to communicate with their employees or neighbouring organisations during a security incident. However, SMS messaging cannot normally be used to alert the public. (see Cell Broadcasting).

5.1 Mass notification systems

5.1.3 Social media platforms

Phase of greatest viability:

Pros	Cons
■ Inexpensive to use and maintain. ■ Minimal training required. ■ Can be used over multiple different communications technologies. Messages can be presented on a phone, tablet or PC. ■ Pre-set messages are quick to send. ■ May provide a warning to those away from the immediate vicinity of the incident. ■ Bulk messages can be sent. ■ Available to all who register the app being used.	■ Dependent on all recipients having chosen app or multiple apps downloaded. ■ Requires continual monitoring by the recipient to identify an alert. ■ Primarily created for one-directional communication. ■ Free text messages will take time to write up and send. ■ Difficult to provide a live response to developing incidents. ■ Single route for communications. ■ Requires access to social media applications. ■ Critical messages may be missed amongst other messages. ■ Difficult to transmit and receive messages on the move. ■ Widely broadcast messages might inform a hostile who is monitoring responses.

Social media platforms have very high engagement figures and offer a means to communicate with many users. Some of the world's largest social media platforms have implemented a range of tools to assist in emergency communication.

5.1 Mass notification systems

5.1.4 Cell broadcasting

Phase of greatest viability:

Pros	Cons
■ Able to target all people carrying a mobile phone within a defined area. ■ Cheap to operate.	■ Currently not available in the UK. ■ Delay will be caused by seeking HMG authorisation. ■ Requires mobile phone and mobile phone network coverage. ■ Subsequent messages will take time to authorise, complete and send. ■ Single route for communications. ■ Messages will be high level. ■ Difficult to receive messages on the move.

Cell broadcasting and location-based SMS (LB-SMS) messaging are one-to-many communication methods which send mass messages to mobile telephones within a specified geographic area. Cell broadcasting utilises a dedicated channel within the mobile telephone network separate to the networks' regular telephone calls and messaging services. Whereas LB-SMS messages are delivered using the standard communication network.

5.2 Push-to-talk (PTT) communications

There are two primary types of Push-to-Talk (PTT) voice communications. They are described as follows:

- Legacy radio communication systems
- PTT of cellular (PoC) using the Long Term Evolution (LTE)

Each can be operated with or without a control room function, as provided by an SCR.

Some PTT devices incorporate emergency alert buttons on the handsets. These are generally designed for lone workers to broadcast an emergency alert to their network but could be incorporated into a warning system for use during a security incident. A "call interrupt" function is also available to allow control rooms to stop long transmissions and allow for time-critical messages to be broadcast as a priority.

There have recently been considerable developments in the technology available as to how two-way radios work. Careful consideration will need to be given and expert advice obtained to establish which option meets the requirements for each site.

The amount of radio use at sites varies considerably. Some sites will use radios as an essential part of their day-to-day operation, while others will occasionally use them to support the response to incidents.

Examples of where they may only be used occasionally are where they are issued through community schemes, such as Shopwatch or Pubwatch, to alert members to incidents within their neighbourhood and there is a low level of use. Where users do not make regular use of them, this can cause a significant problem as they may have had a minimal level of training and be unfamiliar with protocols for radio use and with the technical capability of the radio they have been issued.

Sites should provide training and practice opportunities to all radio users to enable them to operate using the correct radio protocols and understand the system's functionality.

To support training, sites should always adopt strict radio protocols in the operational environment. This will increase the likelihood that when radio discipline is most important during the response to an incident, their use will have become embedded as learned behaviours. Information is provided in annex B in relation to radio protocols.

5.2 Push-to-talk (PTT) communications

5.2.1 Legacy radio communication systems

Phase of greatest viability:

Business as usual	Incident response	Incident management	Crisis management	Business continuity & resilience	Business recovery

Pros	Cons
■ Rapid communication to all those equipped with a handheld device. ■ Minimal training required. ■ Secure operation. ■ Able to communicate one-to-one and one-to-many. ■ Two-way communications. ■ Reliable technology. ■ Able to transmit and receive messages on the move.	■ Expensive to operate. ■ Limits on coverage. ■ No public access.

Legacy radio communication systems or Land Mobile Radio (LMR) have commonly been used by the emergency services, manned guarding personnel, and multiple other users. They enable communication between SCRs, individuals and groups over a dedicated network.

Such systems are generally suited to communicating between individuals or small groups. The ability to communicate with specific groups, such as security guards and facilities staff is likely to be of considerable benefit during any security incident. For example, all personnel responsible for security within neighbouring organisations could share important updates within that group.

5.2 Push-to-talk (PTT) communications

5.2.2 Push to talk over cellular (PoC) using the Long Term Evolution (LTE)

Phase of greatest viability:

Business as usual	Incident response	Incident management	Crisis management	Business continuity & resilience	Business recovery

Pros	Cons
■ Rapid communication to all those equipped with a handheld device. ■ Minimal training required. ■ Secure operation. ■ Communicate one-to-one and one-to-many. ■ Two-way communications. ■ Cost effective when loaded onto a smart mobile device. ■ Reduced infrastructure costs. ■ Wider area coverage than LMR systems. ■ Transmit and receive messages on the move.	■ No public access. ■ Expensive when operating on a specialist hardware-based device.

Push-to-talk over cellular (PoC) devices operate similarly to legacy radio communications except they do not require a radio network to operate. They operate over cellular or Wi-Fi networks.

PoC solutions can be hardware or software-based.

- Hardware-based solutions may offer higher quality devices, for example, more rugged, better audio devices, longer-lasting batteries, etc., compared to software-based solutions.
- A software-based solution, installed onto a mobile device such as a mobile phone via an app, could be significantly more cost-effective for organisations to implement, as many individuals will already use a mobile phone.
- The infrastructure costs of a PoC system are significantly reduced compared to legacy radio communications as PoC systems utilise existing mobile telephone infrastructure.

An example of such a system is *Zello*, a system that operates using either a PoC device or other smart device and operates by mixing Wi-Fi or data networks.

PoC apps that also provide video and text messaging alongside voice communications can also be deployed and are likely to provide additional situational awareness during a security incident beyond that achieved by voice communications alone.

Considerable additional functionality will be available if a PoC device is managed through an SCR. For example, *TRBOnet* provides a dispatch console which will add considerable additional functionality, including the ability to cross patch two or more channels on a temporary or permanent basis. This function would enable neighbouring sites to be linked together during the response to an incident.

5.3 Audible warning devices

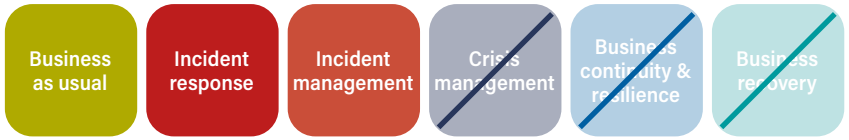
Audible warning devices can either be simple standalone devices such as loud hailers, or a bell/siren, or they can form part of more complex systems such as a Public Address – Voice Announcement systems (PA-VA) system. Detailed information about making announcements is provided in the supplement titled, *Marauding Terrorist Attacks Supplementary Guidance: Announcements*. PA-VA systems may be used separately or together.

Audio technologies provide one of the most effective methods by which those in the vicinity of an incident may be alerted on a one-to-many basis. Such systems can be used to notify an organisation's employees, the public or, with appropriately deployed equipment, neighbouring organisations. The systems can be linked to, or run alongside, mass notification systems to assist with delivering alerts to those caught up in the incident or within the surrounding vicinity.

5.3 Audible warning devices

5.3.1 Public Address (PA) systems

Phase of greatest viability:

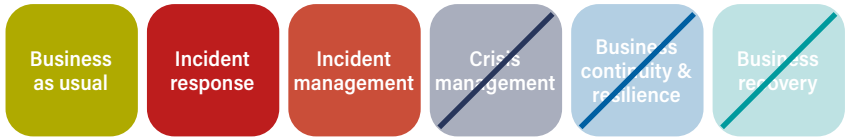


Pros	Cons
■ Quick to operate. ■ Messages broadcast one-to-many. ■ Can cover a wider area. ■ Messages can be regularly and quickly updated and adapted. ■ Able to receive messages on the move. ■ Ability to convey urgency.	■ Requires a dedicated SCR operator. ■ Regular training and practice required for the operator. ■ Announcements may be heard by the attackers. ■ No feedback route immediately available.

Public Address (PA) systems may be used to deliver specifically tailored verbal alerts to all individuals within the systems' coverage – including employees and the public. However, messages may be heard by the attackers.

5.3.2 Voice Alarm systems (VA)

Phase of greatest viability:



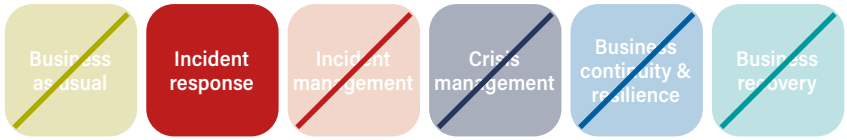
Pros	Cons
■ Very quick and easy to operate. ■ Messages broadcast one-to-many. ■ Can cover a wider area. ■ May be fully automated. ■ Able to receive messages on the move. ■ Effective in initiating an evacuation.	■ Regular training and practice required for the operator. ■ Announcements may be heard by the attackers. ■ No feedback route immediately available. ■ Only preset messages available. ■ If left on can create confusing background noise.

VA systems are often used to instigate a building's evacuation during a fire, providing pre-recorded voice alerts alongside audible warning alarms. The systems are usually automated but can be manually overridden as required. Such systems can provide scripted instructions to a building's occupants based on the building's design and the nature of the incident.

5.3 Audible warning devices

5.3.3 Loud hailers

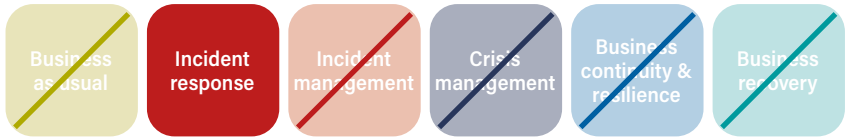
Phase of greatest viability:



Pros	Cons
■ Cheap to operate. ■ Messages can be transmitted on the move.	■ Requires regular maintenance, batteries may fail. ■ Limited coverage, only suitable for a small and confined area. ■ There may be a delay getting the loud hailer into the right place to use. ■ If not immediately available, the person using it may be unable to get to the place that it is most needed.

5.3.4 Bells and sirens

Phase of greatest viability:



Pros	Cons
■ Very quick and easy to operate. ■ Broadcast one-to-many. ■ Can cover a wider area. ■ People are able to receive alarms when in transit. ■ Air horns or similar devices will be easy and quick to deploy.	■ Can be heard by many but they may not know what the alarm sound means. ■ Regular briefing and practice required for the building occupants. ■ May be heard by the attackers. ■ No feedback route available. ■ No ability to change message. ■ May be left on and create confusing background noise. ■ May be misunderstood. Visitors may follow their own training and experience, which may be contrary to the site's instruction.

A handheld airhorn or siren could also be used. They are unlikely to have the range of a permanently wired device but could possibly be used to alert people in a temporary site such as a street market or other open air event.

5.4 Visual warning devices

5.4 Visual warning devices

Pros	Cons
■ Very quick and easy to operate on preset message. ■ Can cover a wider area. ■ May be of particular benefit to those ■ that have impaired hearing (Possibly caused by the incident).	■ Can only potentially be seen by a limited number of people in a defined area. ■ Can be seen by many but they may not know what a visual warning light means. ■ Regular briefing and practice required. ■ May be seen by the attackers. ■ No feedback route available. ■ Take a long time to change the message. ■ Text is difficult to read when moving at speed unless very large and brief messages. May cause people to stop and read the message.

Visual alerts can be delivered via a range of output devices, including televisions, computer workstations, LED displays, strobes, and beacons. They are generally delivered on a one-to-many basis and can be used by organisations to effectively communicate directly with their staff, the public and neighbouring organisations. They can provide an effective method of communicating with those in sight of the display if the lighting conditions are correct and they can understand what the warning means.

Systems could be linked to, or run alongside, mass notification systems to assist with delivering alerts to those caught up in an incident or deployed as standalone local systems. At their simplest, this may involve flashing beacons, illuminated 'exit' or 'stay-put' signs, and emergency lighting systems. Whilst some Wi-Fi enabled lights are available, most are hardwired to the switching mechanisms, with switches either manually operated or automated.

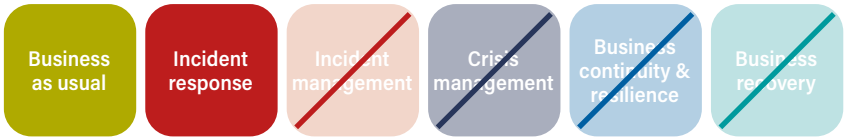
Carefully positioned digital and LED displays can be used to provide more detailed information to recipients regarding the incident and guidance as to what action to take. They are likely to be more effective if large screens can be used in crowded places to deliver simple instructions.

Hybrid audio-visual products integrate audio warnings alongside flashing beacons and text-based displays can be used to maximise the chance a user will observe the notification.

5.5 Body worn cameras

5.5 Body worn cameras

Phase of greatest viability:



Pros	Cons
■ Can be used to increase the situational awareness of the SCR and others. ■ May provide direct evidence of the incident to responding police officers. ■ Can transmit on the move.	■ Difficult to transfer images to the SCR and then the police in the event of an incident. ■ They can only collect detailed images of people and images within close proximity. ■ Unlikely to be able to capture detailed images of people who are more than a few meters away from them

Body-worn cameras are increasingly used within the emergency services and those providing manned guarding services to provide a means of evidence gathering and act as a deterrent (through fear of evidence capture).

5.6 Personal safety apps

5.6 Personal safety apps

Pros	Cons
■ Provides capability for staff to report they are safe in the event of an incident. ■ Able to send messages one-to-many.	■ Requires regular updating of staff information. ■ No communication with the public. ■ Difficult to transmit and receive messages on the move.

Several different personal safety apps are available. They have been designed to enable users to send alerts to their contacts in an emergency. In the event of an incident, they could potentially play their part in enabling employees, for example, to notify their employer of their status.

Common features include:

- Panic buttons – enabling alerts to be sent to emergency contacts. Some also send GPS locations and permit recipients to access the sender's camera or microphone to gain information.
- Check-in – users can either set times when they should check into a destination, or users can request their contacts to provide status updates.

6. Conclusions

6. Conclusions

Communicating effectively during and after a terrorist attack can save lives. The following information summarises the key points that should be considered by those responsible for ensuring that the appropriate communications systems are in place to support the delivery of an effective response to a terrorist attack.

This information is divided into three crucial areas:

PLANNING

Detailed planning should take place to identify the requirements for communications systems that will support the response to a terrorist attack.

A comprehensive planning process will be required to either review and develop existing arrangements or build a new capability from scratch. For a large National Infrastructure (NI) site this work is likely to be resource intensive and involve considerable engagement across the businesses and organisations who operate within and adjacent to the site.

USERS

Time must be spent to identify the people who will generate and receive the communications made in response to a terrorist attack. It must be established where they are and how many of them there are before decisions can be made as to what messages need to be communicated and the most appropriate method of communication.

A significant part of the planning process will be the identification of those that will deliver messages and the intended recipients. The requirements will vary depending on the number of users, the scale of the site, the sophistication of their technical training and the type of business being run. However, the high-level challenges of communicating rapidly with staff, visitors and neighbours are the same. It is the scale and the mechanisms that will vary.

COMMUNICATION METHODS

There is a wide range of communications systems available to support the response to terrorist attacks. A detailed operational requirement should be completed prior to making a decision as to what should be procured.

There have been significant developments in communications technology over recent years and it is likely that this market will continue to develop rapidly in the future. It is therefore important to take time to carefully identify the user requirements before decisions are made as to the most appropriate equipment to be used.

The requirement will vary between the phases of an incident and it is unlikely that a single system will meet all the user requirements and deliver sufficient resilience. Annex C provides a summary of some of the available capabilities and the constraints on their operation.

Annex A
Example scenarios

Annex A – Example scenarios

The following examples are intended to show how different organisations and businesses may need to adapt their communications to meet the needs of different groups working within or close to the areas they are responsible for.

It is not feasible to describe all the different types of communications capabilities for every type of different venue that could be impacted by a terrorist incident. The examples are intended to provide a high and low level example of how organisations and businesses could position their communications to support their response to a terrorist incident. The high level example uses a shopping centre management company and the low end example uses a single site premises located within a city centre high street.

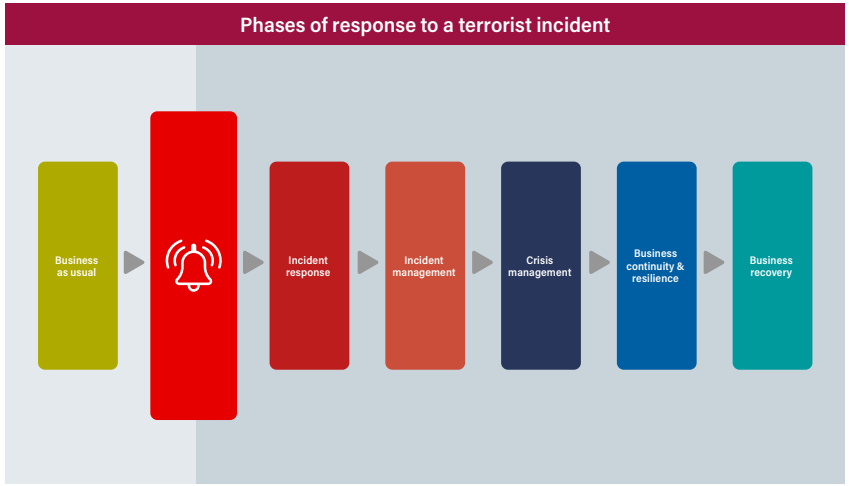
The situation

It is a busy afternoon and all the above outlets are open and busy.

A marauding terrorist attack involving three attackers armed with automatic weapons and knives commences in the main public pedestrian access to the shopping centre.

The following identifies the different communications systems that may be most effective during the different attack phases at the sites.

For the purposes of this exercise the Crisis Management, Business Continuity and Business Recovery phases are combined into post incident phases.



Annex A – Example 1: A large shopping centre

A large shopping centre that is owned and operated by a large multinational company. The shopping centre contains about 200 commercial units. This is made up of:

- 4 large flagship stores
- A multi-screen cinema
- 50 restaurants bars, cafes, restaurants and takeaway outlets
- 150 commercial retail outlets.
- Public transport hub
- An underground multi-storey carpark.

The centre is situated within a busy city centre area that contains multiple further retail, entertainment and business premises.

Business as usual

Open for business

The shopping centre will focus its communications on the following local stakeholders:

- The customers attending the site.
- The staff working at the multiple units within the centre.
- Their own security and facilities teams.
- Their neighbours.

Their intention during BAU is to provide shoppers and other users with a safe and comfortable visit to the centre.

It is recognised that the centre may have other stakeholders with wider interests at national and international levels. However, this exercise is only intended to consider those stakeholders whose safety and security could be directly and immediately effected by the incident.

Communications to – Customers visiting the centre

The primary tool of communication is likely to be a mass notification system app.

The centre may use social media apps such as Facebook, to communicate to members of the public visiting the centre. Providing similar but potentially less targeted messages to the above. One-to-many.

They could use visual warning displays to provide routine information in relation to the opening and closing of the site and any issues with the local transport network. One-to-many.

The PA-VA system can be used to communicate important messages to customers. This may be used to provide notice that shops are about to open or close or to promote local events. One-to-many.

While focused on improving the customer experience, all the above systems should be used to provide proactive safety and security messages. They can be used to provide a wide range of crime prevention and security awareness messages, intended to improve the security awareness of the customers, without increasing their level of fear.

Annex A – Example 1: A large shopping centre

Communications to – Staff working at the multiple units across the centre

The centre may use a mass notification system app to communicate to staff working for multiple different businesses and organisations across the site. This type of system will send a combination of emails, texts, and smartphone notifications to all staff about all routine site management issues. These can include safety and security issues (One-to-many).

They may have a radio (Push to Talk) network using a dedicated channel to communicate with all outlets and businesses who subscribe to this capability. This radio may be held by security officers working for individual outlets, outlet duty managers and a member of staff of the small retail and entertainment venues. This may be operated under a Shopwatch scheme. Allowing for either one-to-one, one-to-many or many-to-many communications.

Communications to – Security and other operational facilities staff employed by the shopping centre

The centre may use a mass notification system app to communicate to their own staff. This will send a combination of emails, texts, and smartphone notifications to all staff about a wide range of site issues.

They will have a private site-specific PTT radio system using several dedicated channels to communicate with different staff groups. There is likely to be a dedicated channel for security staff, sites may also have a shared channel dedicated to the management of incidents. Radios should be issued to all security staff, customer care staff and others working in key positions that are likely to identify or provide an immediate response to an incident.

Communications to – Neighbours

Communications with neighbouring businesses and organisations may be by use of a different radio system that would need to be operated by the SCR. During this phase, it would be used for passing information about low-level incidents and events taking place within the area. It is likely to be uncontrolled.

Annex A – Example 1: A large shopping centre

Incident response

Attack starts

Communications to – Customers visiting the centre

They will communicate using the following systems:

- PA-VA
- Alarm bells and sirens
- Visual display boards

The requirement for communications during this phase is that they are able to alert all customers to what is going on immediately, their safety is at risk and that they need to take immediate action. All three methods can be used but their use must be coordinated. If bells and sirens are used it is critical that their use does not interfere with the use of the PA-VA and that they can be silenced when necessary. The extended sounding of alarms is likely to lead to confusion.

The use of the PA-VA is likely to be the most effective means of communicating to customers.

Communications to – Staff working at the multiple units across the centre

As soon as it has been established that an attack is taking place this will switch to:

- The continued use of radios
- PA-VA
- Alarm bells and sirens
- Visual display boards

Up until this point, it may be possible for an SCR with only three operators to manage a number of radio channels and still undertake their other functions. However, as soon as an attack begins this capacity will be seriously reduced and it is likely that only a single channel can be managed. This may mean that a number of channels will need to be linked. Either the security channel or a dedicated incident channel should be used. It is important that all radio users are aware as to which channel is used.

Annex A – Example 1: A large shopping centre

Mass notification systems can be used during this phase, but they are unlikely to be fully effective. This is because of the lack of certainty that the message will be immediately picked up by the recipient. Such systems will operate on a one-to-many basis and are likely to only broadcast generic pre-prepared messages.

Communications to – Security and other operational facilities staff employed by the shopping centre

During this phase, the same capabilities would be used to communicate to other security staff working on the site as described above. The radio channels will need to be linked as soon as the demand on the SCR to complete tasks rises.

They will use the:

- Site's security and dedicated radio channels
- PA-VA
- Alarm bells and sirens
- Visual display boards

Communications to – Neighbours

Communications during the incident response phase are likely to be very limited as a result of the direct involvement of those in the SCR managing the incident. However, provided a limited message is transmitted making neighbours aware that a major incident is underway and providing brief details of the type of incident taking place that is likely to be sufficient for them to initiate their own response and then wait for further information to be passed.

The neighbours will also be able to continue to communicate directly with each other as they develop an understanding of what is taking place.

Incident management **Response develops**

Communications to – Customers visiting the centre

During this phase, the use of the PA-VA will continue to be the most effective method of communicating across the centre. The use of this system will enable the provision of rapid and tailor made updates to the customers. Directing them to take action and telling how to avoid the areas of danger.

PA-VA can also be used to warn people in the surrounding area to keep out of the attack area.

Alarm bells and sirens will cause confusion if they are used for an extended period and should be switched off during this phase unless a new danger is identified and a change of action is required by the customers.

It is unlikely that SCR operators will be able to update visual display boards or that customers inside the centre will be able to read them.

Annex A – Example 1: A large shopping centre

Communications to – Staff working at the multiple units across the centre

Radio and PA-VA will continue to be the most effective forms of communication at this point with the SCR likely to have little or no capacity to update MNS apps or visual displays.

Communications to – Centre security and other operational staff

As above, radio and PA-VA will remain the means of communication to internal staff.

Communications to – Neighbours

Communications will continue via the radio and enable the site to continue to implement their own response to the incident and when appropriate provide support to those at the venue of the attack by providing shelter and first aid.

Post incident

The attack is halted

Communications to – Customers visiting the centre

At this stage, most of the customers will have left the centre and are safe. They will be focused on staying safe, finding out if the people they were within the centre are safe and securing their own property. If they arrived by car they may want to return to their vehicles. Communications with this group are now no longer urgent.

The most effective means of communication is likely to be through the PA-VA, but this may not have coverage in the areas they have been evacuated to. Therefore once the SCR are able to update other communications capabilities that were in place during business as usual, they are likely to prove useful.

Communications to – Staff working at the multiple units across the centre and Centre security and other operational staff

The radio is likely to provide the most effective and immediate means of communication but as with the communications to customers.

Communications to – Neighbours

Those organisations on the radio are still likely to be operating without communication from those at the scene, as they are too busy dealing directly with the incident. They will be able to continue to protect their own sites and communicate to their staff on site or those who may unwittingly be about to walk into the attack site.

As the recovery develops, it is likely that those in the centre's SCR can use the radio again. They may be able to ask for support from those in surrounding businesses and organisations. The support requested will depend on the nature of the incident.

Annex A – Example 2: A high street premises

A single and small high street retail, business or hospitality outlet.

Such a site is unlikely to have its own security staff and responsibility for the premises is likely to fall to the manager or senior member of staff on the premises. A small retail outlet or business is likely to focus its communications on:

- The customers,
- Staff on the premises,
- Their neighbours.

The communications capabilities are likely to be relatively simple and during all phases of a terrorist incident the communications with the staff and customers on the premises are likely to be through the use of verbal commands.

Business as usual

Open for business

Communications to – Customers

During the BAU phase this is likely to be through quiet and orderly conversations with the staff and customers.

Communications to – Neighbours

The premises may have a radio as part of a local Shopwatch or similar scheme for communicating with other businesses and organisations who may subscribe to the service. It is likely that any radio communications are limited and focused on dealing with minor incidents of crime and disorder. Communications are likely to be two-way and one–to-many. Radio users may lack confidence in using the radio and be unaware of the full technical capability of the device available to them.

The monitoring of the radio is likely to be of secondary importance to the overall delivery of business.

In addition, there may be a social media app such as *WhatsApp*. This will provide a no cost capability that can be used for informal communications between neighbouring businesses. Messages will only be picked up and read when the recipient has seen there is an incoming message and is available to read it.

The premises may use a social media app such as *INSTAGRAM* or *their website* to communicate changes in opening hours and other news to their customers.

Annex A – Example 2: A high street premises

Incident response | Incident management | Post incident | All attack phases

Communications to – Customers

Due to the limited size and the low level of staff and customers on the premises it is unlikely to be necessary to have any additional means of internal communication. The manager and other staff are likely to be able to use verbal commands to instruct both staff and customers as to what they should do if an incident develops.

Communicating to – Neighbours

The use of a radio is likely to be the only viable means of communicating very rapidly and safely with the neighbouring premises, to either warn them of the incident or other critical information. As the radio channel is un-controlled and the users are not used to using a radio during a major incident it is likely that communications may be confused and difficult to understand. Those transmitting messages are unlikely to follow the necessary radio protocols or use language that can be easily understood.

Annex B
Radio protocols

Annex B – Radio protocols

NPSA's analysis has highlighted that security and front-line personnel seldom practice radio communications in the context of an emergency. People talk over one another, broadcast unnecessarily long, rambling messages blocking others on the channel and ask for updates rather than trusting that updates will be provided when available.

The following points are intended to improve radio protocols:

- √ Each day - check equipment; battery charged; check all parts are in working order.
- √ Use of the phonetic alphabet enables quick identification of individuals; enables spelling of words during transmissions to avoid misunderstandings.
- √ Establish local protocols for identifying an emergency incident. State "urgent message", state location and brief details of the incident.
- √ People must be concise in conveying information and be fluent in an organisation's radio protocol (e.g. saying 'over' if ending a transmission if a reply is expected and 'out' if ending an exchange)
- √ Key messages, conveying vital updates or instructions should be repeated, and confirmation sought from the recipient that they have been received and acknowledged. This will reduce the likelihood that important information will not inadvertently be ignored.
- √ Users should make sure they identify themselves and their location.
- √ Effective communication undoubtedly becomes more difficult under pressure, and this skill should be regularly practised following training.
- √ Always release the PTT button whenever you stop talking. If you forget and keep it pushed down while you are trying to think of something to say, the radio continues to transmit, making your battery run down faster and making " dead air " so that nobody else can speak or be heard.
- √ Train users in features of radio handset, including, less used capabilities such as emergency assist.

The following mnemonics provide some simple guidance for all users to remember:

Rhythm, Speed, Volume and Pitch (RSVP)

Helps improve operator procedure and technique.

Rhythm	Speak in a consistent rhythm
Speed	Speak slowly enough to be clearly understood
Volume	Normal conversational volume is required
Pitch	A very low pitched voice is difficult to understand when transmitted by radio

Accuracy, Brevity, Clarity (ABC)

Provides three important rules about message content.

Ask yourself "do I need to transmit this, or can it wait?" and spend a moment thinking of the clearest way to communicate what you are trying to say.

A	B	C
Accuracy	**Brevity**	**Clarity**

Annex C
Summary technologies

Annex C – Summary technologies

TYPE:	MASS NOTIFICATION SYSTEMS				PUSH-TO-TALK (PTT) COMMUNICATIONS		AUDIBLE WARNING DEVICES			VISUAL WARNING DEVICES	BODY WORN CAMERAS	PERSONAL SAFETY APPS
Subtype:	MNS APP	SMS	SOCIAL MEDIA	CELL BROAD-CASTING	LEGACY RADIO COMMS	PUSH TO TALK OVER CELLULAR	LOUD HAILERS	PA-VA	BELLS AND SIRENS	-	-	-
SCR Operator required	✓	✓	✗	✓	✗	✗	✗	✓	✗	✗	✗	✓
Recipient needs to monitor	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓
Quick to send	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✓
User training	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Recipient training	✓	✗	✗	✗	✓	✓	✗	✗	✓	✓	✓	✓
Automated	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✓
Level of investment	MEDIUM	LOW	LOW	HIGH	HIGH	MEDIUM	LOW	LOW	LOW	LOW	MEDIUM	MEDIUM
Audio/Visual	VISUAL	VISUAL	VISUAL	VISUAL	AUDIO	AUDIO	AUDIO	AUDIO	VISUAL	AUDIO	VISUAL	VISUAL
Targeted/Private	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	✓
Blanket/Public	✗	✗	✓	✓	✗	✗	✓	✓	✓	✓	✗	✗
One or two way	TWO-WAY	TWO-WAY	TWO-WAY	ONE-WAY	TWO-WAY	TWO-WAY	ONE-WAY	ONE-WAY	ONE-WAY	ONE-WAY	ONE-WAY	ONE-WAY
Recipient requires												
Infrastructure required												
Integrates with other systems	✓	✓	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗
Used on the move	✗	✗	✗	✗	✓	✓	✗	✓	✓	✓	✓	✗

Icon key:

 Smart device

 Mobile phone

 Radio/push to talk device

 Hearing

 Sight

 Wi-fi reception

 Mobile network coverage

 Radio transmission

 Loud haler

 PAVA speaker

 Audible alarm bell or siren

 Visual warning device