CRISIS MANAGEMENT FOR TERRORIST RELATED EVENTS

CIPR CHARTERED INSTITUTE OF PUBLIC RELATIONS

CPNI Centre for the Protection of National Infrastructure

CONTENTS

CIPR FOREWORD

Emma Leech
President of the CIPR

The value of public relations is found throughout the organisations we serve. Effective, strategic relationship and reputation management is fundamental to the attainment of organisational objectives and the effect is far deeper than the surface impact of technically excellent communication. A responsive, communicative, thinking organisation is one which can thrive in this uncertain and volatile modern era.

Crisis response is the sharp end of our professional service, where communication, strategic planning and professional judgement coincide. Whilst it is just one of the ways in which professional public relations strengthens organisations, it is one of the most important, with the potential to protect and sustain value in uniquely difficult circumstances.

As professionals we train to respond in a crisis and in turn we train others within our organisations to adapt a plan to meet the threats a crisis will bring. This is a well worn routine. Sometimes, the crisis is of our own making. An issue, created by how we work or do business, causes strife in our nexus of stakeholder relationships and when it surfaces it can escalate into a crisis.

But in a volatile and uncertain world a crisis can also come from a less predictable place. Hostile actors – by which we mean those who want to attack or disrupt an organisation for profit or to make a political or ideological point- pose what seems to be an increasing threat to organisations – particularly those who serve communities, provide leisure and recreation, work with large numbers of people and create spaces for gatherings which celebrate culture and sport. Think of the Manchester Arena bombing, the attack on Borough Market, the 7/7 attack on the London Underground and 2019 shootings in Christchurch, New Zealand as well as attacks in cyber space, like the WannaCry incident. These, and many other terror-related incidents manifested themselves as a crisis for the organisations responsible for the places where they happened, for the emergency and security services, for the hospitals and for the agencies of local and national government who had to deal with them.

As professionals, working in these and other contexts, the fear and horror we feel when people and places we work for or represent are targeted by terrorists, has to be separated from the way in which we manage communication in a time of unique crisis. It demands a calm response, coordination across several agencies and clear communication with the public and others. At many CIPR awards events, up and down the country, we have been called on to acknowledge the achievement of communications teams who have faced exactly this type of crisis. We have been tested and we will be tested again.

ABOUT OUR PARTNERSHIP WITH CPNI

That's why CIPR is working with the Centre for the Protection of National Infrastructure (CPNI) on guidance to help organisations prepare for crises arising from terrorist events. CPNI works closely with government departments responsible for policy on National Security Strategy, National Risk Register and Counter Terrorism Strategy.

This guide is aimed at PR professionals who work in house for, or as agencies contracted to, organisations vulnerable to a crisis resulting from factors outside their control. No matter how large, or small the organisation or consultancy, a plan is needed. We wanted to demonstrate how an organisation can use communication to make itself less vulnerable to attack in the first instance. We researched handling of past crises, including a number of high-profile terrorist incidents and brought new learnings from those incidents together with best practice in handling crisis communication.

As well as providing a guide there will be additional resources to support members and we want to lead a debate with our partners in the business community and beyond. We must consider how, now and in future, the source of the crisis could be external as well as internal and it could be hostile and terror-related. We need to think, as the guidance suggests, that there is a way to communicate that can help to deter a terrorist enterprise. We need to know with whom we should coordinate, should it happen to us. We need to learn from the experiences of the people who created the communications response in similarly testing circumstances and I am pleased to say this guide has been thoroughly researched for that purpose.

Above all we must never overlook the fact that these incidents are a crisis not only for the organisation but for the innocent people involved, their families and their communities. These are the people we serve first in a crisis of this kind. We owe it to them to provide the most professional service we can.

RESEARCH TO INFORM THE GUIDANCE

CPNI commissioned original research to inform the guidance material. In-depth interviews were conducted with 30 communications heads and security professionals representing 24 organisations. They comprised a combination of organisations who had first-hand experience of communications during a terrorist incident and those who could face such an incident in the future.

The research participants were very open with us and shared their learnings – good and bad.

We are very grateful to them for this and pleased to be able to pass on their experiences to help organisations better plan, handle and recover from potential terrorist incidents.

The lessons learned are broadly applicable but provide important pointers for handling a terrorist incident specifically.

The research was undertaken between December 2018 and March 2019 by Agfora, specialists in business-to-business research.

KEY FINDINGS FROM THE RESEARCH

A gap was identified for guidance materials that covered the specific aspects of a terrorist-related incident and the initiative was welcomed by the communications and security professionals alike.

Although most organisations felt they were well prepared for a crisis, there was general acknowledgement that they could always do, or have done, more. Communications, in the main, is recognised as of strategic importance and increasingly so since the tragic event in Manchester.

Critical to the success of the communications function, however, is the strength of the security culture within the organisation and its ability to align closely to the security operation within the organisation. Communications and security professionals are not always well acquainted, nor mutually respected, and this can prove a challenge.

The learnings have been incorporated in the advice we have given to practitioners in the ‘Communications Toolkit’ section of this guidance.

For details of the research sample and method, please see Annex 1.

WHAT'S AT STAKE?

Introduction by Director, CPNI

CPNI AND ITS ROLE

The Centre for the Protection of National Infrastructure is the government authority for protective security advice to the UK national infrastructure. Its role is to protect national security by helping to reduce the vulnerability of the national infrastructure and other assets and events to terrorism and other threats.

CPNI, Counter-Terrorism Policing and the UK Government cannot protect the UK alone. It relies on partnerships with industry, academia and international partners.

It is with this backdrop that CPNI has worked with the industry's lead professional body, the Chartered Institute of Public Relations, to produce the first ever bespoke guidance material for terrorist-related events.

WHO IT'S FOR

Given an attack in the UK could occur anywhere, at any time, and likely with little or no warning, the guidance is relevant to all organisations running sites and venues UK-wide, where employees and the public may be present. From sporting and music venues, restaurants, bars, hotels and nightclubs to transport hubs and carriers, they all represent potentially 'soft' targets for terrorists.

The profile of hostile actors is broad encompassing terrorists, organised crime and cyber criminals and hacktivists.

So this guidance will also be relevant to organisations looking to protect their computer systems from interference by cyber hackers. Whether you are an employer of people or a provider of a public space or customer services, it will provide valuable advice to help you prepare and manage for a threat from a hostile actor in physical or cyber space.

Our guidance will help your organisation deploy communications to mitigate the harmful, and often "longtail" effects of a terrorist incident on brand and business reputation, value and continuity.

But our guidance doesn't stop, or even start there. Communications can be effective in helping to deter a terrorist incident in the first instance.

Deterrence Communications: thwarting hostile actors from targeting your site or organisation

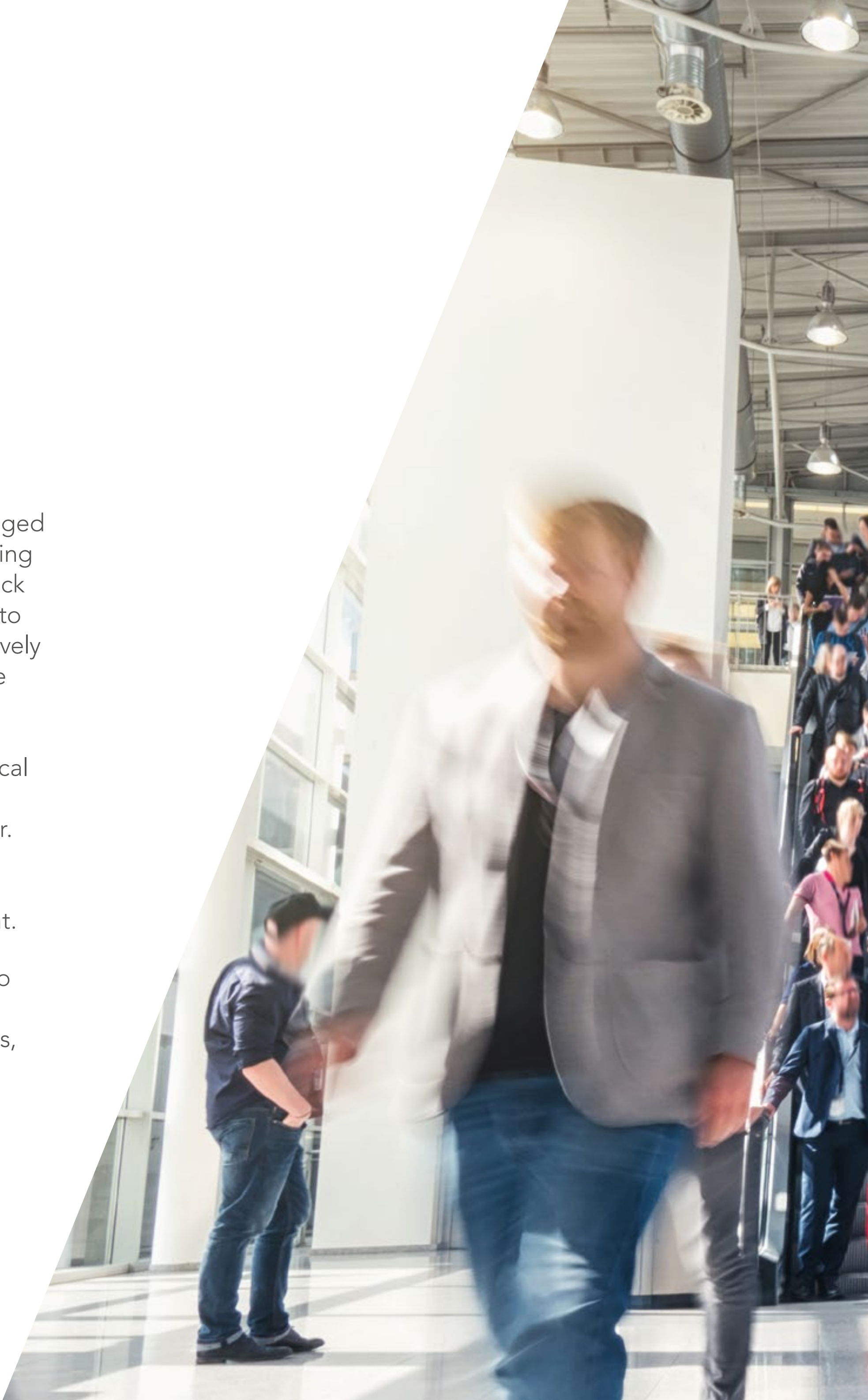
COMMUNICATIONS CAN HELP DETER TERRORISTS

A hostile actor will plan and prepare for an attack. Once a hostile has fixed on the site, sites or organisation they wish to target for a potential attack, they will want to make sure that they give themselves every chance of success. To that end, they will gather information from a range of sources including people, online research and physical reconnaissance to inform their plans. And it is this information that is within the gift of communications professionals to control and manage.

What this will take is thinking like a hostile and asking the question "What can we say that will put off a hostile, but not upset our normal customer or site user?". The answer to the question is the use of 'security-minded' communications to deter; dissemination of messages that will hint at security measures in place without giving the game away.

Hostiles will not necessarily be discouraged by security provision, per se; simply having CCTV, guards or a particular fence or lock will not suffice. An organisation needs to promote these security measures effectively to the hostile. If a hostile believes a site has excellent security measures due to what they've read online, seen on a poster or witnessed through their physical reconnaissance, it may be enough to deter them from their target altogether. This process has the added benefit of reassuring staff and visitors; they will feel that they are in a safer environment.

CPNI has helped organisations develop 'Security-Minded Communications' messaging and campaigns. These assets, along with guidance materials, can be provided by CPNI; see Annex 2.



SEE IT.
Trust your instincts if something doesn't look right.
SAY IT.
Notify staff or police.
SORTED.
We'll take you seriously. And we'll sort it.
CRITICAL
THREAT LEVEL
Together, we've got it covered.
Department
for Transport

PARTNERSHIP: POLICE, PUBLIC AND INDUSTRY

The cooperation between the police, public and industry is a powerful defence against terrorism. Consequently, attacks have been prevented and lives saved.

Public vigilance campaigns can be a powerful deterrent.

Action Counters Terrorism (ACT) is the overarching brand which incorporates all Counter Terrorism Policing campaigns that warn, inform and reassure.

See Annex 3 for details.

COMMUNICATIONS TOOLKIT

WORKING WITH THE POLICE*

Fundamental to handling a terrorist incident on the ground is the police lead on communication; organisations should **not** communicate directly to external audiences on anything related to the incident. Police forces work to a shared 'Major Incident Plan' and as such are set up to communicate directly to the public en masse during a major incident.

What is incumbent on the organisation is to have a relationship in place with the local police prior to any incident occurring. This will include understanding the well-rehearsed procedures and processes the police have in place for the operational and communications aspects of a terrorist incident.

For example, the organisation will be required to work closely with the police to disseminate police-originated communication; this will ensure information is accurate and anything placed in the public domain does not compromise a criminal investigation.

The same rules will apply for any major incident where there is a criminal element or a natural disaster, such as fire, flooding where the circumstances are outside of the organisation's control. All risks should be considered as part of the organisation's risk assessment and preparedness. The police will always be the first port of call, but depending on the incident, it may be that a government agency will take the lead; your local police contacts will be able to advise you on the correct protocol given the nature and cause of the incident.

*in a non-cyber incident.

A TOOLKIT IN THREE STAGES: PREPARATION FOR, DURING AND POST AN INCIDENT

Preparing for an incident

PLANNING FOR THE WORST

By planning in advance, having relationships and initial key outputs in place, organisations can ensure they are taking a leadership position as soon as a crisis occurs.

Recent high profile incidents have moved security higher up the agenda for organisations. Transport hubs, energy infrastructure and areas that host large public events and gatherings, from shopping malls to stadia and arenas, are all potential targets.

These events have changed public perception. Research has shown that people are more accepting of security measures such as bag checks, surveillance and an increase in visible security staff. There is an expectation that these measures exist and that organisations are prepared for the worst.

In a world of rolling news coverage, social media and citizen journalism, businesses are scrutinised more than ever. Communication has never been more important, both in terms of deterrence (see page 9) and how organisations react to a crisis.

For terrorist-related incidents, reputational damage will be caused if the organisation handles the issue badly, for example communicating insensitively, poorly or not at all. Alternatively, for something like a cyber-attack, the organisation's IT policies and security will be examined and they are more likely to be held responsible.

THE IMPORTANCE OF LEADERSHIP

An essential part of being prepared is having the right communications leader in place. They will head up the crisis team and be expected to make fast, clear decisions under pressure, manage resources effectively and demonstrate a range of responses on behalf of the organisation they represent, both practical and emotional.

The organisational leader, for example the CEO, must also demonstrate leadership in a crisis. As the most senior representative of the business, they are expected to show compassion and reassure stakeholders that the organisation is in control. They will need to work closely with the communications leader both during and after the crisis to ensure that the organisation is as effective as possible.

Good leadership starts before a crisis. A strong security conscious culture must be embedded within the business from the start. This can help prevent a potential crisis and ensures that the foundations are in place if something does happen. Communicators should contribute to contingency plans, lead the crisis communications strategy, put the right skills and resources in place, and develop positive relationships with key partners and stakeholders in advance.

Other factors that contribute to a security focused culture include:

- **Empowerment:** staff should know how they can contribute to security in terms of precautionary action, ongoing maintenance and response to incidents
- **Awareness:** customers/visitors should understand the need for security, how it will impact on their experience and what to do if they suspect a problem
- **Relationships:** strong relationships should be cultivated at all levels within the business, and with external stakeholders including contractors, suppliers, local authorities, the police and other emergency services, community groups and nearby businesses.

The ultimate aim is that organisations are doing all in their gift to deter potential hostile actors from targeting them, and are fully prepared if an incident does happen.

MAKE A PLAN

A crisis communication plan should be a core component of any organisation's risk preparations. It should be developed following a detailed risk analysis looking at potential issues and possible solutions. Typically, these issues relate to an organisation's people, assets, property and operations, and the plan is there to guide action and communications.

For incidents involving hostile actors on the ground, further preparation is required. As with other crises, these happen without warning. However, as they often involve public safety, there is further pressure to get things right; understanding how police processes and protocols work is key to planning.

It is important that the plan is adapted over time. This should reflect changes in the organisation, new potential risks, updated guidance, and insights gained from test incidents and crises elsewhere.

While the course of action will vary for different crises, the principles of the plan will be the same.

Suggested areas for inclusion are:

- **Communications policy:** the communications process for an incident, internal chain of command, police protocols, expectations of staff, and activities (including relevant channels)
- **Holding statements:** a selection of responses suitable for a range of incidents, ready for issue (with minor amendment) in the initial phase of the crisis
- **Roles and responsibilities:** within the organisation, including the designated person for emergency planning and managing crises. Identifying spokespeople and team member's specific job roles, and externally, with appropriate partners.
- **Wellbeing:** the crisis lifecycle can be lengthy and involve 24/7 working. Shift patterns and recovery time should be identified. Potential partners (e.g. extra resource from an external agency or another internal department, such as marketing or HR) should be included.
- **Contact list:** key team members and external stakeholders, including media (as required)
- **Systems:** details of logins, process for corporate channels (e.g. amending website or switching to dark site), technical guides, building access details
- **Resources:** templates, action plans, corporate imagery and briefing materials (e.g. fact sheets), communications log, email and WhatsApp groups, "grab bags" (e.g. phone charger, water, change of clothes, basic toiletries, information packs). If the police are taking the lead there will still be a requirement for the organisation to provide supporting resources, but your comms will not be in the front line for communication to the media.

This plan should also cover what to do after the initial crisis, including how to help the team and organisation recover (see page 22 for more).

PUTTING IT INTO PRACTICE

Once the plan has been approved, it is important to test it. Training and desktop exercises are a great way of doing this. It involves bringing the team together that will be working together in the event of a crisis.

The internal team should include:

- Communications department
- Other company departments, relevant to the crisis, e.g.
  - Designated person for managing the crisis
  - Security
  - Legal
  - IT department (if it is a cyber-attack)
- Core management team and executive board
- External PR support (if the plan requires it, for example at the recovery stage)

Externally, familiarise yourself with the role of your Local Resilience Forum (LRF). LRFs are multi-agency partnerships made up of representatives from local public services, including the emergency services, local authorities/councils, the NHS, the Environment Agency and others. These agencies are known as Category 1 Responders, as defined by the Civil Contingencies Act. They work in emergency preparedness, and take the lead on training. LRFs have a communications sub-group and they will be your main point of contact for your own incident planning.

It is important to do this in "peace-time." This allows you to test processes and, more importantly, build relationships with the people you will be working with if something goes wrong. This effort will be hugely beneficial if a crisis does occur; the key people will already know each other and have a level of rapport. They will also already have tested out the systems and processes and spotted any gaps or issues that need to be addressed.

It is also a good idea to look beyond the organisation and the crisis team, and build relationships with any nearby residents or businesses. They will also be affected in the event of an attack, and will look to the organisation for guidance and reassurance.

TOP FIVE LESSONS LEARNT:

1. Communications team is aligned with operations within the business and key decision makers, from management through to key department heads
2. Security culture has been built and is consistently reinforced
3. Relationships have been built in advance with strategic partners (e.g. police and other emergency services)
4. Detailed plan is in place, including policy, holding statements (including provision for following the police lead), roles and responsibilities and resources
5. Crisis plan is regularly revisited and tested

Communication during an incident

By planning well, practising frequently and having in place a co-ordinated effort; as well as understanding the vital role of strategic communications; a crisis can be well handled and well communicated.

Communicating bad news well, is now expected of all major organisations. As the result of actions of a hostile actor, the police will have the lead role in communicating to external audiences in an effective and timely fashion. However, the target organisation will remain important and should reinforce messaging and ensure that consistency and accuracy are maintained. If the police, or government department are not the designated point of contact for the media, the organisation should act quickly to take the lead, and position itself as a source of truth.

> *"The person in charge of communications must have the gravitas, confidence and experience to be able to contest and suggest messages."*
>
> **Laurie Bell, Wiltshire Council.**

PUTTING THE PLAN INTO ACTION

As we have said on page 15, practising your plan for an incident is vital. For now, when the incident has hit, you need to ensure your role as the lead communicator is conducting a well-rehearsed orchestra, not scrabbling around for the music stands.

> *"You cannot do enough planning. If the computers are down, you need to have a hard copy of the communications plan. Grab bags with phone chargers, boots and waterproofs etc. At Parsons Green I was there for 12 hours. And you need to know where the car parks are near your base if public transport is down."*
>
> **Jo Hall, Police force.**

If you have not practised, this stage will be worse than difficult. The research report states the importance of 'Practice. Practice. Practice'.

Your plan should be clear, concise and most importantly have very clearly stated roles and responsibilities.

Ensuring everyone knows who oversees what, and who has authorising powers is vital. Even in non-hierarchical organisations, you must now employ command and control methods to remain in control of the messaging to your staff, and be appraised of police communication.

WORKING WITH THE POLICE

During a terrorist-related incident on the ground, organisations will be required to disseminate police-originated communication; this will ensure the information is accurate and anything placed in the public domain does not compromise the criminal investigation.

The police will have a pre-prepared, and rehearsed, communications plan including messages, holding statements and lists of media contacts. It will be down to them to communicate around the incident, whether that be telling the public what they should do if they are caught up in the incident, or providing reassuring messages. Sensitive communication around casualties is strictly controlled by the emergency services.

DO NOT FORGET THE INTERNAL AUDIENCE

Any organisation has an internal audience who can quickly become external detractors, or advocates. You will have very little time to get them involved. The golden hour (which may be a much shorter period) is used to describe the window available for ensuring lines of communications are open and active for staff. Dedicated channels should be established, with backups if access to the organisation's intranet or message channels is limited (for example if the intranet is restricted due to criminal investigations), if the network is overloaded, or if it has been the target of the attack.

You must provide information for your staff and resources so that they can help deliver the plan. Your internal audience will inevitably cross over into your external audience, so what messages do you want them to carry home with them to their external networks, families and friends? Remember that social media is a potential area where this crossover may occur.

"It was embarrassing, the first internal message at 2am and then no updates until 2pm."

Police force.

LOOK AFTER YOUR TEAM

The communications team are likely to need back up, for example to triage media calls and, updating of website, or circulation of hard copy information internally if online systems fail. Ensure you have that in place and call on it. This may include shadow members of staff, drawn from elsewhere in the business and with an understanding of how the communications function works. Send some of your team home as soon as the incident hits, it will be hard for them, but you will need at least one experienced communications lead for every shift.

Be aware that in terrorist attacks, some of the team may be concerned about work colleagues or their own family members; be on hyper alert and ensure there is support from across the organisation and from partner agencies.

"Sending press officers to the scene – not sure that was such a good idea as they can be traumatised later and unable to do their jobs as fully as they might."

Police force.

Think carefully about what staff may see when visiting the incident site. In a terrorist incident, it may not be necessary to send a member of staff to the site. However, if a visit is necessary, it is often valuable to buddy up a communications team member with an operational member of staff or member of your security team. Ensure consideration is given to the provision of ongoing professional counselling support.

WORKING IN PARTNERSHIP

It is more common for public sector and networked organisations to have arrangements in place to share staff when a hostile act occurs e.g. terrorism attacks. Police forces will move communications staff around the country to support other forces, and the NHS has a long history of sending in staff from other organisations to support the organisation under attack. Ensuring they can hit the ground running is vital. If your organisation is part of a network, e.g. local CBI, Chamber of Commerce or Small Business Forum consider calling on colleagues to assist you. The Chartered Institute of Public Relations may also have contacts who can assist. Do not be afraid to ask for help.

"To keep continual relationships with stakeholders (i.e. local businesses, emergency services etc) so that if there IS a crisis, you know the people and can count on their immediate support."

Leisure.

(For additional staff brought in to support the team) *"have packs ready of stuff they need to know – where the toilets are, and the canteen, logins for access to email."*

Police.

SOCIAL MEDIA

Be guided by police advice on social media use.

The public is looking for personality from social media. Organisations must show some emotion in times of attack, but should lay down ground rules for what is acceptable. The police will be on hand to advise on what should be shared with the public, but avoid images of the incident itself or traumatised members of the public. Instead, focus on safety (e.g. police onsite), tributes or recovery.

Twitter is first, then Facebook.
Keep consistency and keep in control.
Even if you have nothing to update, say so.

If the organisation is issuing its own media statements, be prepared for more complex sign off, especially if the situation becomes a criminal incident or one of national importance. Her Majesty's Government (HMG) will get involved if this is the case.

"It is a play off between speed of messaging and accuracy. People expect information immediately. It does not matter if it is totally accurate – but it is important to acknowledge something is happening immediately. Operations colleagues prefer to wait for all the information and then put out a message. But it doesn't work."

Transport.

TOP FIVE LESSONS LEARNT:

1. Review your resources and try to have a back-up team in place, from a partnership organisation, other parts of your own organisation, or an external source.

2. Look after the communications team and ensure consistent internal communications.

3. Do not be over reliant on online networks, have a Plan B for technological failures.

4. Ensure there are clear roles, responsibilities and sign-off procedures; for both internal and external communications.

5. Do not underestimate the scale of an incident including the level of interest from the media, (national and international) and the public, nor its duration.

ENHANCED
SEARCHES
IN PLACE

Communication after an incident

Restoration, not promotion is a strong theme for communications activities following a major incident. It is also important to take time to reflect after an incident, especially one by hostile actors. This may be a first for your organisation and any debrief can play a multifaceted role. It is important to take the opportunity to learn from what worked well and what could have gone better, embedding new ways of working, actively listening and responding to comments and views from your customers and staff; as well as providing an opportunity for all participants to reflect on their experiences.

Once the storm has passed, for many organisations it is tempting to start to rebuild exactly what was lost. A mature organisation will take the opportunity to review if a new, or different structure is needed. It is also important to remember individually and corporately, there will be weaknesses and the need for recovery. It is therefore important, that the recommendations for ensuring robust team structures and support are in place, in case there is a second wave.

GETTING THE TONE RIGHT

After an incident has passed for your organisation, it may still be ongoing for the investigators, the victims and for some of your staff. The communications team must continue to be linked in with customer services, marketing, HR and operations colleagues; at times it will be the role of the communicator to advise that 'business as usual' cannot continue e.g. running a price increase campaign at this time would be damaging if service continuity has been interrupted.

Ensure communications is continuing to monitor feedback and has an active listening role. The perception may be that the organisation was lacking and therefore was weakened before the incident occurred; this is particularly the case for cyber incidents.

> *"Cyber is seen as something the organisation SHOULD have defended against so less seen as 'victim' and less sympathy. [It would be] unwise to play the victim card."*
>
> **Consultancy.**

POLICE

THE VALUE AND ROLE OF DEBRIEFING

Debriefing is a vital part of the lifespan of any issue and incident. It is not, and should not be allowed to become, an opportunity to apportion blame. Consider external facilitation and do not shy away from challenging and difficult conversations.

> *"You have to listen to what colleagues on the ground say. We did have a debrief with colleagues from (undisclosed organisation) and that was a very difficult meeting, it exposed tensions that were already there."*
>
> **Health.**

Ensure all staff, not only those who have been on the frontline of the incident, have access to support and be aware that it may be some time before people realise they need support; organisations should have a rolling programme of easy to access, confidential support.

From the research undertaken, a police force found that 10% of staff had accessed support of some kind (with more coming forward) following a recent mass terrorist attack.

It may be useful for a leader to share their own experience. Some senior leaders have said only when they shared that they had taken up the offer of support that their teams felt able to do the same. It is important to show humanity; as an organisation to your stakeholders, but also to your staff.

> *"Internal staff had never featured in the plan, but 10% have accessed support of some kind. There are still people coming forward."*
>
> **Police force.**

Make sure you undertake some evaluation. Debriefing and allowing people to talk is important. Ensure you capture what went well and what could you do better next time; and reiterate the offers of help to staff.

CONSISTENTLY CONSISTENT

Keep monitoring social media, and ensure that you are continuing to offer messages of reassurance and assurance that your organisation is learning from the incident and changing the way it operates.

The leadership team must be visible to staff and stakeholders, consistently communicating that a comprehensive action plan is in place, supported by a strong two-way communications plan to rebuild trust with all of those who've been affected; service users, customers, stakeholders, regulators, et al.

If it is still very sensitive, perhaps your organisation is under investigation itself; mobilise your stakeholders to speak on your behalf. It is important that there is a rhythm of communications. Do not allow holes to appear, where someone will fill the void, often with miscommunication.

DON'T PLAY INTO THE HOSTILE'S HANDS

It is important to use the right language and not to glorify, nor to make value judgements or exercise partiality when it comes to descriptors around terrorism.

For example, use of the word "terrorist" to describe the perpetrator is generally not advised.

See Annex 3 for links to further information on this.

Dealing with different types of incidents

A MASS TERRORIST ATTACK

Terrorist attacks tend to aim at one of two things; places where there are large gatherings of people, such as stadia, music venues or shopping centres, and sites that have strategic value, such as government buildings, energy infrastructure or transport hubs. Their aim is to create chaos and fear.

The perpetrator can be acting alone or as part of a terrorist group, or cell and will have different motives and methods for their attack.

It means that a wide variety of organisations, and by extension, communications professionals need to be prepared for this eventuality.

Where a terror attack differs from another crisis is:

- Scrutiny is higher as it involves public safety
- The police will take the lead
- It is often on a larger scale, and media interest will be ramped up domestically and internationally– speed is of the essence
- It involves a wider range of stakeholders, including emergency services and government
- Messaging must not create panic and should reassure where possible
- Information is harder to get (and verify) and the organisation is unlikely to lead on communications
- The organisation is likely to be viewed sympathetically, but this can change if communication is poor

The media will seek to explain why the attack happened, looking at:

- ○ The hostile actor's/actors' background. This may raise issues around religion, politics, gender, mental health, etc. or look for previous relationships with the organisation
- ○ The security of the location and whether the organisation is liable and failed in its duty of care (for example, if a gunman enters a school)

These are all sensitive issues from a communications perspective, both if asked to comment on the perpetrator or on the organisation's own security and procedures. Avoid commenting on the personal details or offering up any opinions or speculation. Communications should stick to the facts and prioritise the needs of victims and other important stakeholders, providing the information and support that they need.

> *"Do not demonise following the event. Do not handle it as if it was whole sectors of society that committed the atrocity."*
>
> **Consultancy.**

In addition, the organisation may need to evacuate and shutdown operations. A clear process should be in place to manage this, including contingency plans if technology fails. Paper back-ups, an offsite command centre and arrangements for communicating with staff/personnel may be required.

Elements such as a dedicated webpage, a specific hashtag and a crisis line for people to call, are all tactics that help direct people to relevant information that is being distributed by the organisation. Information should also be shared from other partners, such as the police. This is important as it helps establish the organisation as a source of truth; there will be many rumours, especially on social media.

However, organisations will be limited in what they can say as there will be criminal proceedings and sometimes an inquest after the incident occurs.

And, once the crisis has passed, the communications do not stop. There could be an ongoing requirement to continue messaging; for example, as investigations progress, as victims are identified and family support is required, and as the organisation recovers (which could include new security measures, construction, and staff wellbeing). In future, the event will also be revisited, both for anniversaries and if similar incidents occur elsewhere.

Furthermore, the incident may last longer, for example if it turns into a hostage situation or the hostile actor evades capture.

There can also be a ripple effect, with further attacks creating an impact on other similar sites.

"The first incident was challenging, but the whole dynamic changed in the 2nd incident as someone had died."

Laurie Bell, Wiltshire Council.

A CYBER ATTACK

Cyber attacks bring the focus onto the organisation

Cyber attacks come in a range of forms. Examples include:

- Denial of Service (DoS) attack, which seeks to "crash" websites by having multiple traffic sources accessing the server at the same time
- A virus that infects the network causing systems failures
- Data breaches, where compromising information is accessed, such as staff records or customer payment details

There is a different dynamic with cyber attacks as the IT department often takes the lead and not the police. However, the communications team should not be overlooked. The same approach described elsewhere should be followed, with communications professionals bringing the relevant people together to prepare for and manage the crisis.

Using a data breach as an example, speed is of the essence as it often compromises user privacy. It is important to understand the potential nature and scale of the incident quickly. There will also be possible repercussions, in terms of both the impact on the data subject and the impact on the organisation's reputation.

In terms of the data subject, their security is at risk. They should be contacted as soon as possible to say their data may have been compromised, so that they take precautions while the organisation investigates more fully. This is both good practice and a requirement under GDPR, which states a duty to report personal data breaches to the relevant authorities within 72 hours.

Further communications should follow, sharing the findings of any investigations and how further breaches will be prevented.

Challenges with a cyber attack:

- The problem can originate as a result of non-compliance by a third party, for example an operator of the system, or supplier testing the relationship
- The involvement of suppliers and third parties in the technical space can obfuscate roles and responsibilities for comms teams
- NDAs may be in place which constrain communications, preventing full transparency and the dissemination of information

In addition, information disclosure can be of benefit to the hostile actor, making it difficult to communicate truthfully.

> *"We had to strike the right balance of how much disclosure; on the one hand we wanted to be truthful and honourable but without giving ammunition to the bad guys. We were ahead and in control of the story and this stopped some of the negative points being used against us. It is a balancing act in the communications sphere."*
>
> **Cyber.**

The way the organisation handles this situation has the biggest impact on reputation. If poor processes have resulted in the issue then blame will be apportioned. A proactive response to solve this issue can mitigate this and help the organisation move forward from the crisis.

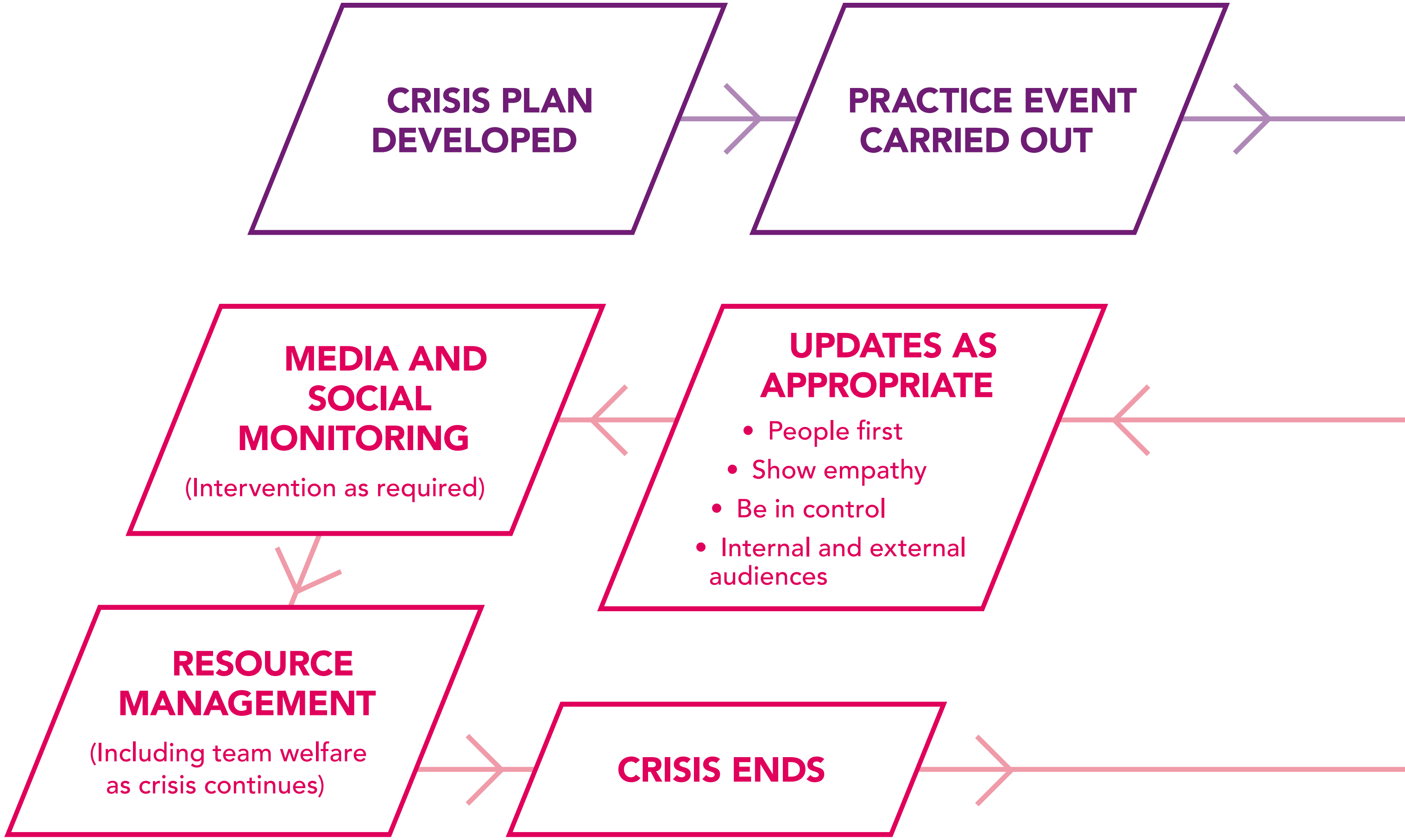
THE STAGES OF A CRISIS

Flowchart

The flowchart below sets out the key considerations for the planning, handling and recovery stages of a crisis.

> *While every crisis has its differences, these actions should all occur in some form. It is important that consideration is given to both the operational and emotional needs of the organisation and its stakeholders, and sufficient time is allocated for planning and recovery.*

Source: CIPR



CRISIS PLAN DEVELOPED

PRACTICE EVENT CARRIED OUT

UPDATES AS APPROPRIATE

- People first
- Show empathy
- Be in control
- Internal and external audiences

MEDIA AND SOCIAL MONITORING

(Intervention as required)

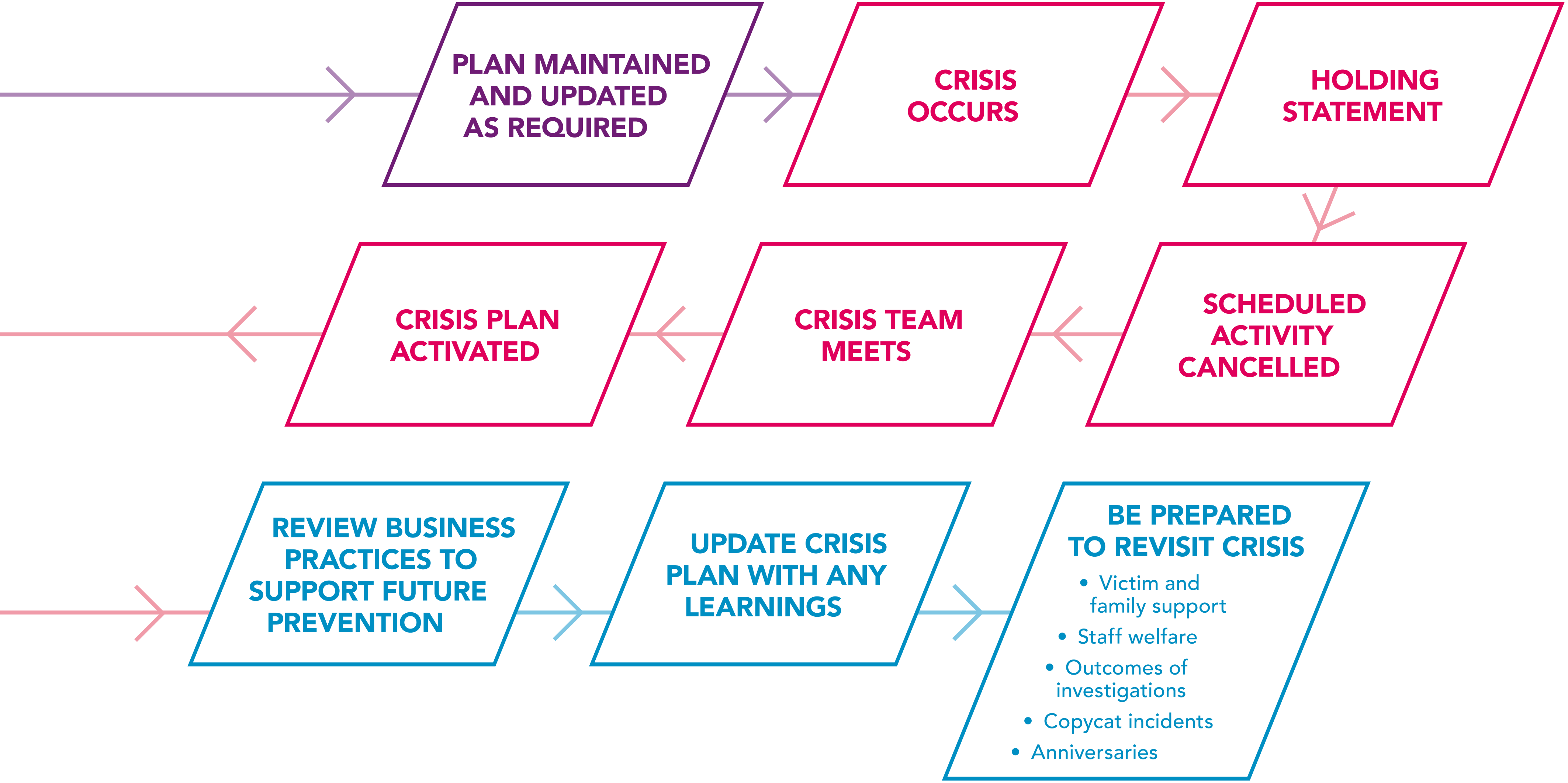
RESOURCE MANAGEMENT

(Including team welfare as crisis continues)

CRISIS ENDS

KEY:

■ Before ■ During ■ After



PLAN MAINTAINED AND UPDATED AS REQUIRED

CRISIS OCCURS

HOLDING STATEMENT

SCHEDULED ACTIVITY CANCELLED

CRISIS TEAM MEETS

CRISIS PLAN ACTIVATED

REVIEW BUSINESS PRACTICES TO SUPPORT FUTURE PREVENTION

UPDATE CRISIS PLAN WITH ANY LEARNINGS

BE PREPARED TO REVISIT CRISIS

- Victim and family support
- Staff welfare
- Outcomes of investigations
- Copycat incidents
- Anniversaries

WHAT THE FUTURE HOLDS

From the CIPR and CPNI

As this guidance goes to press the threat level for the UK from international terrorism – i.e. from groups such as the Islamic State in Iraq and the Levant (ISIL) and Al Qaida–as set by the Joint Terrorism Analysis Centre (JTAC) is 'severe' which means "an attack is highly likely". But as the recent events of Christchurch New Zealand have thrown into sharp relief, the threat is not just from international terrorism but from "extremist, right-wing" terrorism.

It is a stark reminder of the breadth and depth of terrorist causes in the UK and around the world. No organisation can afford to be complacent to their potential vulnerability. The UK – its citizens and businesses – need to be vigilant and on their guard for activities in public places and in the corporate environment that strike them as being unusual or suspicious. The role of your publics–staff and customers alike – is key here. And while it is never going to always thwart the planning of a hostile act, it is possible on the one hand to reduce vulnerability to being the target of one, and on the other to plan for the worst. Planning for a terrorist-inspired incident – whether in the physical or cyber world – makes good sense in terms of risk management and communications readiness.

Although there are some fundamental differences between a terrorist incident and a more conventional crisis compromising product or service operation – the principle of having a communications plan in place and rehearsed is no different. The impact of a terrorist attack on your organisation or site is no less damaging on business continuity, reputation and share price than a conventional crisis but with the added dimension of human loss and complexity. It is to be expected that there will be a multiplicity of stakeholders involved from central government, the counter-terrorism and security agencies and the emergency services.

We hope by dint of our endeavours we can make ourselves less of a target. This guidance is a first and marks the beginning of the work the CIPR and CPNI are doing jointly to educate and train the twin professions of communications and security. Both organisations lead the way and provide best practice in their fields and the partnership we have forged through this initiative will pave the way for a range of training and publicity activities.

The CIPR has communicated this guidance to its members, and through them to the organisations they work for as well as to a network of representative organisations across the UK. CPNI likewise will be rolling out the guidance to its security fraternity. CIPR is planning a Webinar followed by a series of practitioner workshops; at these we will share what organisations have told us worked well and less well in their handling of crises. The guidance will also be publicised widely within the communications and security industries.

Fundamental to the success of this work, and ultimately the improved readiness of UK-based business for a terrorist incident, is the need for collaboration between the security and communications functions. And although the partnership between CIPR and CPNI will facilitate this, it is up to seniors representing these functions to make that collaboration work in practice. The research undertaken to inform this guidance material shows that relationships between security and communications professionals are at best tenuous. Without them, and even with the best will in the world, the advent of a security-threatening incident would challenge the best prepared communications team.

And it goes beyond the strength of these internal relationships. The research pointed to the importance of close relationships with external stakeholders and the benefits of forging these in "peacetime".

The CIPR, supported by CPNI, are here to support you over the coming months to embed the guidance in communications practice. And whether you are a communications professional in-house, or a consultant, you can benefit from this ground-breaking new guidance as much as we have enjoyed researching and putting it together for our industries.

Our thank you goes to the authors and CIPR members – Sarah Pinch Chart.PR FCIPR MIoD, Dan Gerrella Dip CIPR, Chart.PR, MCIPR and Claire Spencer, FCIPR, DipCam and consultant to CPNI.

Annex 1 – About the research

ABOUT THE RESEARCH

METHOD & SAMPLE	ORGANISATIONS & SECTORS	PROFILE OF ORGANISATION & CRISIS HANDLED
In-depth Interviews – 30 respondents	**24 organisations interviewed**	**13 had experience of terrorist incident**
Heads of communication Security managers Consultants/consultancies and subject matter experts	Transport Retail & Leisure Health Critical National Infrastructure Police forces Local Authority Education	**Incidents experienced:-** • Manchester Arena • Westminster Bridge • London Bridge • Borough Market • Oxford St. (suspected incident) • Parsons Green • Finsbury Park • 7/7 (2005, London bombings) • Salisbury novichok poisoning • Cyber attacks including WannaCry

Note – Market Research Society (MRS) guidelines and respondent requests for anonymity preclude disclosure of further information on research participants.

Annex 2 – 'Security-Minded Communications'

Security-Minded Communications is an approach developed by CPNI. It is designed to equip organisations that manage sites, venues and events with the ability to utilise communications as part of their protective security measures. Security-Minded Communications is designed to help disrupt the hostile actor and therefore reduce the likelihood of criminal activity from taking place.

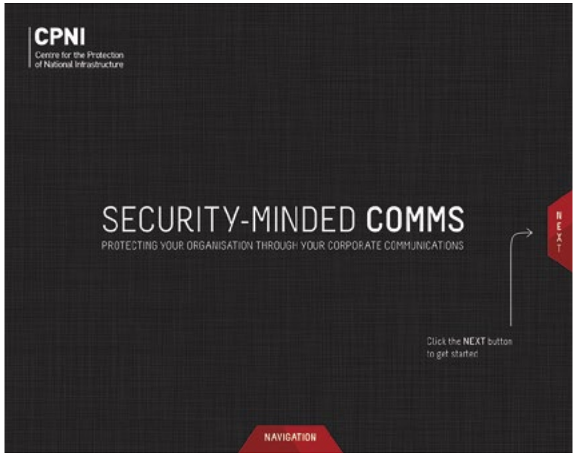
It is an approach that many organisations have taken to help deter hostile actors from targeting them. One such is a leading events organiser, whose Security Manager says of Security-Minded Communications: "It is the most cost-effective security measure we have implemented." However, for the approach to be successful the communications team has to work closely with the security team to implement. Furthermore, security minded communications is only as good as the security provision that underpins it.

Communications assets that organisations can use to discourage and deter, including the 'See it. Say it. Sorted.' posters that are used widely on the rail network, can be provided.

What characterises communications undertaken by organisations in furtherance of this approach is the active and visible promotion of the security provision at the site/s. Typically activity will comprise a mix of digital and ambient communications that disseminate security messaging, including but not limited to:-

- Digital channels
    - Organisation/site website
        - E.g. banners on the home page with links to a page that provides more security related information
    - Social media channels: original content and reposting of relevant content from partners, emergency services and police
    - Emails to customers and visitors
- Promotional materials and advertising
    - Electronic notice boards
    - Printed cards
    - Outdoor media: posters and banners

Exemplars of messaging and content, as well as creative assets, have been developed by CPNI to help deter hostile actors. In addition, CPNI has a range of useful tools and guidance for organisations; based on years of detailed research, it will help set strategy and shape security messaging. The guidance can be requested by emailing detercomms@cpni.gov.uk



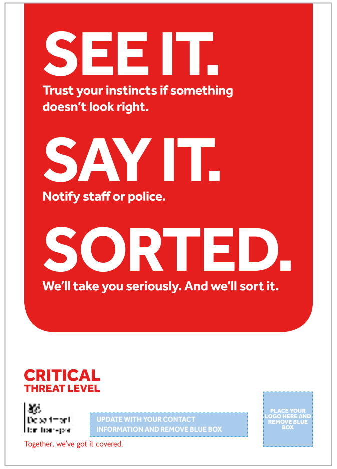
CPNI
Centre for the Protection of National Infrastructure

SECURITY-MINDED **COMMS**

PROTECTING YOUR ORGANISATION THROUGH YOUR CORPORATE COMMUNICATIONS

Click the **NEXT** button to get started

Security-Minded Comms – interactive PDF.



SEE IT.
Trust your instincts if something doesn't look right.

SAY IT.
Notify staff or police.

SORTED.
We'll take you seriously. And we'll sort it.

CRITICAL
THREAT LEVEL

UPDATE WITH YOUR CONTACT INFORMATION AND REMOVE BLUE BOX

PLACE YOUR LOGO HERE AND REMOVE BLUE BOX

Together, we've got it covered.

See It. Say It. Sorted. – template poster.

Annex 3 – Resources and further reading

FROM CPNI:-

Embedding Security Behaviour Change:
https://www.cpni.gov.uk/embedding-security-behaviour-change

Developing a Security Culture:
https://www.cpni.gov.uk/developing-security-culture

Identifying the Right Security Behaviours:
https://www.cpni.gov.uk/identifying-right-security-behaviours

Secure online presence:
https://www.cpni.gov.uk/secure-online-presence

Understanding Hostile Reconnaissance:
https://www.cpni.gov.uk/understanding-hostile-reconnaissance

Recognising the Terrorist Threat:
https://www.gov.uk/government/publications/recognising-the-terrorist-threat

FROM THE POLICE:-

Action Counters Terrorism:
https://act.campaign.gov.uk/

ACT E-Learning:
https://www.gov.uk/government/news/act-awareness-elearning

ACT Awareness eLearning is a CT awareness product that provides nationally recognised corporate CT guidance to help industry better understand, and mitigate against, current terrorist methodology.

Reporting terrorist activity:
www.gov.uk/ACT

Every year thousands of reports from the public help the police tackle the terrorist threat. If you see or hear something unusual or suspicious trust your instincts and ACT by reporting it in confidence at gov.uk/ACT. Reporting won’t ruin lives, but it could save them. Action Counters Terrorism. Remember, in an emergency, always dial 999.

OTHER RESOURCES:-

Local Resilience Forums:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62277/The_role_of_Local_Resilience_Forums-_A_reference_document_v2_July_2013.pdf

Emergency Preparedness: Communicating with the Public:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61030/Chapter-7-Communicating-with-the-Public_18042012.pdf

Lexicon around the subject matter:-
https://theglobalcoalition.org/en/counter-daesh-dictionary/ & https://www.bbc.co.uk/editorialguidelines/guidance/terrorism-language/guidance-full

FROM THE CIPR:-

Books:

Griffin, A (2014) ***'Crisis, Issues and Risk Management'*** Kogan Page

Griffin, A (2009) ***'New Strategies for Reputation Management: Gaining Control of Issues, Crises & Corporate Social Responsibility'*** Kogan Page

Regester, M, Larkin, J (4th Edition 2008) ***'Risk Issues and Crisis Management in Public Relations: A Casebook of Best Practice'*** Kogan Page

Skills Guides:

(available to CIPR Members, via www.cipr.co.uk)

Crisis and risk management

Crisis planning

Social media in crisis/issues management

Training Courses:

(available from CIPR via www.cipr.co.uk)

Creating your crisis communications plan

Crisis communication

Risk issues management & crisis

Social & digital crisis management

Qualifications:

(available via www.cipr.co.uk)

Specialist Diploma (Crisis Communications)

CIPR CHARTERED INSTITUTE OF PUBLIC RELATIONS

www.cipr.co.uk

CPNI

Centre for the Protection
of National Infrastructure

www.cpni.gov.uk

aml Designed by AML Group
www.aml-group.com