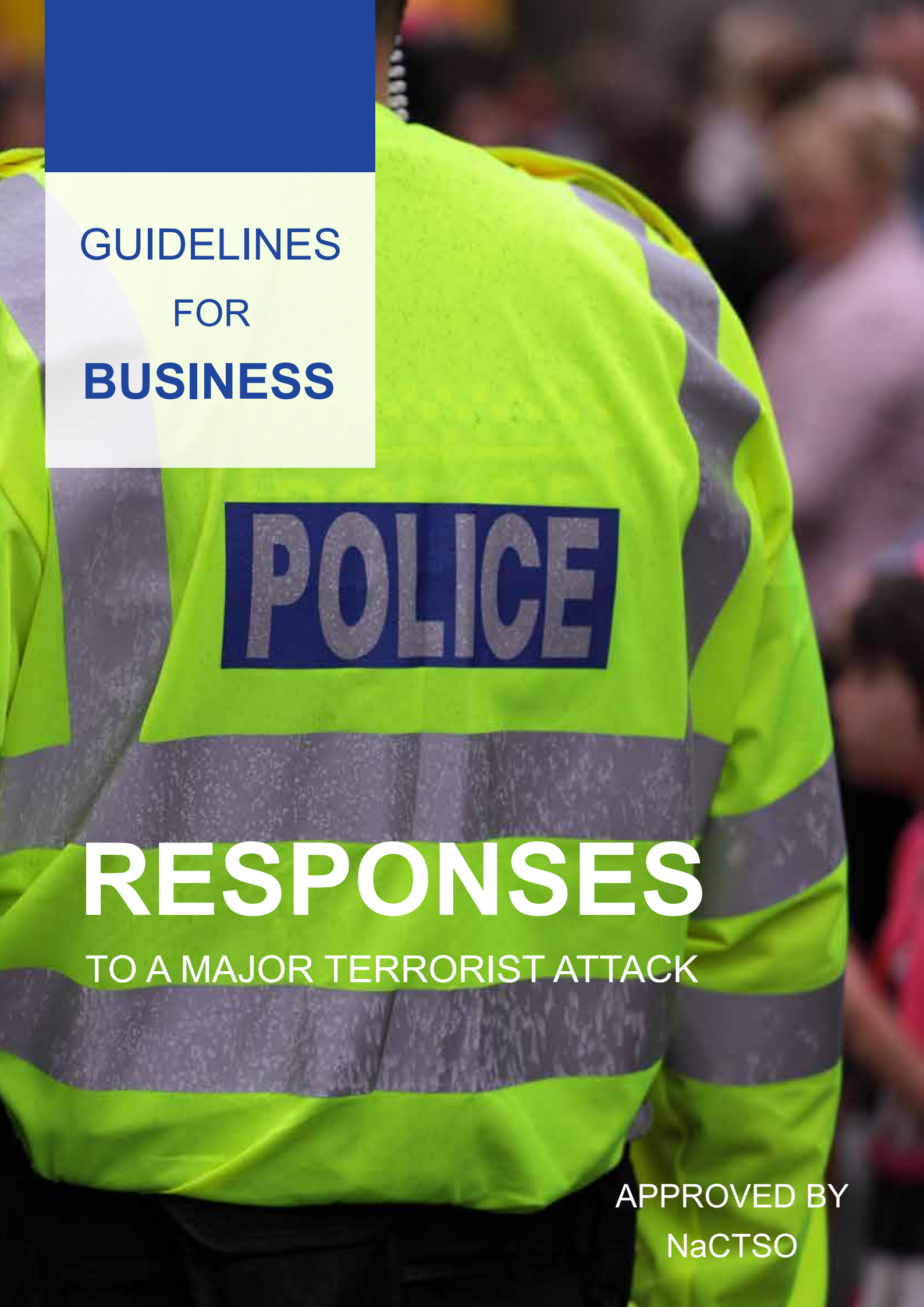
GUIDELINES

FOR

BUSINESS



RESPONSES

TO A MAJOR TERRORIST ATTACK

APPROVED BY

NaCTSO

RESPONSES

TO A MAJOR TERRORIST ATTACK

GUIDELINES FOR BUSINESS: RESPONSES TO A MAJOR TERRORIST ATTACK

Introduction

This advice and guidance is offered to businesses in support of the publicly available 'Stay Safe' counter-terrorism video, approved and promoted by NaCTSO. The message in this document is designed to help businesses with their responses before, during and immediately after a major terrorist incident.

Should a major terrorist attack occur or be expected imminently, the authorities may change the official terrorism threat alert level to **'Critical'**. This change will be announced by central government (COBR) on advice from the Joint Terrorism Analysis Centre (JTAC).

However, it is important to remember that there is no need to wait for an official government announcement before changing building 'response levels' or implementing enhanced security arrangements if early indications appear serious, impacting and in proximity to the business.

Background

Previous declarations of **'Critical'** have been sector specific and have typically lasted 3-4 days (i.e. 10-13 Aug 2006 for the foiled transatlantic airlines plot, 30 Jun-4 Jul 2007 for the TigerTiger attacks in London and at Glasgow Airport, and on 23- 27 May 2017 for the Manchester Arena attack).

In the light of developing terrorist threats, there is a possibility that a protracted period at a **'Critical'** level could occur in the future, for example, as a result of a wide-scale manhunt.

In response to a **'Critical'** announcement by the authorities, businesses may choose to raise their building (estate) response level using alternative words such as 'Exceptional' or 'Heightened'. The application of other intermediate stages may provide greater granularity and flexibility.

Pre-Actions

- Advice around a **'Critical'** announcement should be prepared and communicated to employees to create a culture of awareness. If appropriate and depending on building design, this messaging should reinforce the principle that seeking refuge within the building could be far safer than evacuating onto the streets or transport network after an incident, subject to the scenario.

- While staff cannot legally be prevented from leaving a building (even if advised to the contrary) they can be prevented from re-entering. This may be important in a CBRN incident when contamination could be an issue. However, staff should be pre-warned of such potential action.

- The ‘Stay Safe’ video is a good resource (see Reference 1). The central message is ‘Run, Hide, Tell’. It is recognised that this message cannot address every potential circumstance or locality e.g. actions if trapped in a confined building or a train where flight may be restricted. The implications and sensitivities around any supplementary message should be considered carefully by dynamic assessment.

- Invacuation areas or citadels should be identified and plans for use need to be rehearsed. (Qualified building surveyors may be necessary to assess such areas.)

- Help-lines to out-sourced post-trauma counselling services could be established if possible and fundable.

- In case intruders try to set off alarms, it may be possible to put ground-floor break glass on ‘double-knock’ where an initial activation is silent for a brief period of time and hence avoid premature evacuation. Ground-floor staff should be made aware of this.

Notification (if any)

- Early unofficial notification of a security incident is likely to come through media outlets and social media. Certain sectors may receive notice from trade associations, external security consultants or departmental contacts.

- However, as media chatter can often be inaccurate, it is important to verify details as far as possible. Official police reporting or contact and CSSC messaging will help.

- Following an incident, initial information available to the emergency and security services may be unclear and unconfirmed and an official account therefore not immediately available. It will, however, be a priority and essential part of the response.

Immediate Actions

- Minimise any casualties by directing people in the immediate vicinity away from the danger zone.

- Direct first-aiders to casualties only when safe to do so. (Ground-floor areas should have supplemented first-aid packs to cater for multiple injuries.)

- Consider a lock-down of access and fire doors, as well as loading bays. Any reception staff should evacuate with others once lock-down is activated.

- Lifts should be grounded. This action should not set off fire alarms.
- Consideration of the actions of others in a multi-tenanted building should be afforded.
- Notify the police (999) of the situation as soon as possible and safe to do so.
- Control-room staff should monitor any CCTV systems (where possible) to gain as clear a picture of events as possible. They should zoom in to critical areas where possible for post-evidential use, and provide continual updates to security managers and emergency services if appropriate.
- The incident should be managed as effectively as possible until external assistance arrives. (The Crisis Management Team should be notified and activated, possibly off-site.)
- Invacuation to safe areas (citadels) should be managed. Advice to staff to stay away from windows, close blinds and shelter on the opposite side of the building to the local threat should be conveyed. Move to higher floors if possible via stairwells.
- Ground-floor amenities e.g. coffee shops should be closed if possible and appropriate.
- Security staffing and perimeter patrols should be increased until a clearer picture emerges - unless a current and specific threat exists.
- The primary focus should be on communicating the situation with employees. It is important to alert but not alarm. The message also needs to be conveyed to contractors including delivery agents, clients, and visitors (on site).
- While internal messaging via email and text notification is one route, this may be inappropriate in more complicated and bespoke attacks. Use of an intercom system may be possible but the planned content of the message, issued by a reassuring and authoritative voice, will be important. (Avoid referring to terrorists, weaponry or casualties in order to avoid alarming staff unduly.)
- Contacting and accounting for staff who are both incoming travellers and those stranded outside as a result of the restricted access protocol should be the next immediate priority. (An external office could be given this task to alleviate the work load.)
- An appropriate message should be placed on an automated messaging systems on a central telephone number (hotline). This can help answer employee

queries and concerns.

- The official announcement of a move to **'Critical'** may bring with it specific official measures that may steer internal messaging. The escalation may help validate decision-making with the C-Suite. (The more information obtained from a trusted source the more power to security managers have to justify their decision-making and the more trust and respect commanded from staff.)

- If the situation becomes protracted and people are confined to the building, consideration must be given to arrangements for catering and refreshments.

- If staff have been allowed home, guidance on when to come back to work should be relayed. (The automated messaging system may help.) Instigate work-from-home procedures if an extended period of closure is envisaged.

- Offer guidance to non-essential and volunteer staff as to work arrangements.

- If **'Critical'** lasts for any extended period then security manning levels will need to be reviewed. Consider the difficulty of hiring extra staff when others will be doing the same.

- Additional signage and barriers may be needed.

- Maintain log of actions for post-event lessons and any subsequent enquiry.

- A summary of actions around responses to changing threat levels is at Reference 2.

Post Actions ('Severe' Threat Level)

- Review risk categorisations of buildings. Perhaps restrict access points.

- Review security incident procedures.

- Review search options for all visitors.

- Reinvigorate staff vigilance campaigns. Audit staff receipt of briefings.

- Review working-from-home and out-of-hours procedures.

- Consider use of security awareness materials, e.g. posters, and contracts for extra security staff.

- Liaise with partners and neighbours to home emergency procedures in the light of events.

- Check buildings and adjacent properties for any evidence of the incident, including a review CCTV footage.

References

NaCTSO Guidance Note 2/2015 - Reviewing your Protective Security

London First Aide Memoire - Responses to Threat Level Changes