Major Incident Preparation, Management and Recovery

This document has been prepared following a Waterloo based Major Incident Exercise. It contains information on how to prepare for a major incident, management of the event, and how to recover and return to normal after the event. The advice set out in this document is not exhaustive but provides a guide of some important actions which can help your business improve existing measures.

1. Preparation

1.1 Communication

1.1.1 CSSC (Cross Sector Safety and Security Communications)

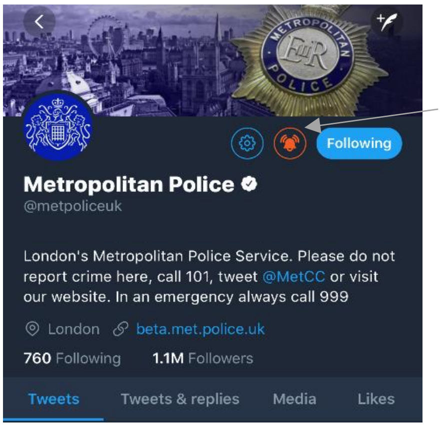
The CSSC is an initiative which was created to facilitate communications between the private and public sectors, on issues surrounding security and business resilience. It is a partnership between law enforcement agencies, local and national government organisations and private sector businesses. The information provided is accurate, reliable and free, via email and/or text.
Sign up here: https://www.thecssc.com/membership-form/

If appropriate, these communications should be shared internally via email once they reach your business.

1.1.2 Twitter

Twitter can be utilised to obtain reliable information, as soon as it's available, via trustworthy sources. Additionally, critical notifications can be easily created which alert the user to an incident via a push notification, without the user having to check Twitter.

It is recommended that @MetPoliceUK, @BTP, @LondonProtect and your local metropolitan neighbourhood team(s) are followed on Twitter. Critical alert notifications can be set up for both @MetPoliceUK, and @BTP.



Metropolitan Police
@metpoliceuk

London's Metropolitan Police Service. Please do not report crime here, call 101, tweet @MetCC or visit our website. In an emergency always call 999

London beta.met.police.uk

760 Following 1.1M Followers

This is achieved by clicking on the circled alarm on the profile page of each account. Once active, it will turn from blue to orange. Please note, this feature is only currently available for these accounts, of the ones listed above.

This will enable a push notification to be sent to your phone in the case of a major incident.

The @MetPoliceUK is the most reliable source of information. News and media outlets may be quicker at providing information in the event of a major incident, but this may be unverified information. @MetPoliceUK will only provide verified information.

1.1.3 Apps

Other apps can provide critical information in an emergency situation. It is recommended that the following are downloaded:

- Emergency by British Red Cross – Real time personalised alerts and advice around severe weather and other UK emergencies

- citizenAID – A simple and clear teaching aid of immediate actions and First Aid for a variety of major incidents including stabbing, mass shooting and bombing.

1.1.4 News Reports

Stay aware of crime and security related news reports which may have a direct or indirect impact on your business. An incident which occurs outside of London still may have potential to impact London at a later date, especially with Waterloo Station acting as a central transport hub into London.

1.2 Training

1.2.1 Act Awareness E-Learning

Act Awareness e-learning training is a free, online, government approved, counter-terrorism training package, which takes a maximum of 45 minutes to complete. All staff should undertake this training. This is nationally accredited counter terror guidance to help staff better understand, and mitigate against, current terrorist methodology. Access has been provided specifically for WeAreWaterloo BID members via the login details below.

Website: https://ct.highfieldelearning.com PIN: **232716**

Additionally, staff should watch this 4 minute video outlining “Run Hide Tell”
https://www.youtube.com/watch?v=CYPyZ3ErFy0

1.2.2 Act Awareness – Classroom Session

Act Awareness Classroom sessions are available, which has recently replaced Project Griffin. The session is delivered by a metropolitan police counter terrorism officer and is available free of charge. The session can be delivered to groups of thirty and are more suitable for senior members of staff. Contact alex@wearewaterloo.co.uk to find out when the next Act Awareness session is, or for the BID to organise and facilitate a session.

1.2.3 Emergency Procedures

Staff should be briefed and should fully understand their role in the site’s emergency procedures. These should include:

- Evacuation
- Invacuation
- Dynamic Lockdown

Emergency Procedure Template (Please note, shelter-in-place is the Americanism for invacuation):
https://www.fema.gov/media-library-data/1388775706419-f977cdebbefcd545dfc7808c3e9385fc/Business_EmergencyResponsePlans_10pg_2014.pdf

1.2.4 Emergency Information on Display

To reinforce training, literature should be available and on display (only in staff areas). Such examples include Run Hide Tell: https://www.kent.police.uk/getmedia/aff208be-98bc-4237-9b8b-0b65de0b72f0/Run-Hide-Tell-poster-(English).pdf

HOT (Hidden Obvious Typical):
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/563349/HOT_Poster_NaCTSO.pdf

1.2.5 Crowded Places Guidance

More information and guidance is available for security and general managers of each sector (retail/late night economy) on how to improve their protective security:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/701910/170614_crowded-places-guidance_v1a.pdf
This information is provided by the National Counter Terrorism Security Office.

1.2.6 Recognising the Terrorist Threat

Detailed government approved advice from the National Counter Terrorism Security Office covering many more terrorist threat types and protective procedures are available here:
https://www.gov.uk/government/publications/recognising-the-terrorist-threat/recognising-the-terrorist-threat

1.3 Raised Threat Level

The current terrorist threat level is at “severe”. Businesses should be able to distinguish between how their businesses operate at “severe” or “critical”, with enhanced security measures in place at “critical”. This usually occurs immediately after a terrorist attack. “Critical” threat levels do not last for long, as the additional security measures are generally unsustainable. The threat levels are expected to stay between severe and critical for the next ten years.

Threat Level	Meaning	Response Level
Critical	Attack expected imminently	**Exceptional** - Maximum protective security measures to meet specific threats and to minimise vulnerability and risk – unsustainable in the long term.
Severe	Attack is highly likely	**Heightened** - Additional and sustainable protective security measures reflecting the broad nature of the threat combined with specific business and geographical vulnerabilities
Substantial	Attack a strong possibility	
Moderate	Attack possible but not likely	**Normal** - Routine protective security measures appropriate to the business concerned
Low	Attack unlikely	

Examples of enhanced security measures can include (but are not limited to):
- External bag checks
- Complete control over building entrances and exits
- Strict adherence to building regulations (i.e. smoking in designated areas, and general improvements in housekeeping measures)
- Visible and active security to deter threats
- Increased staff vigilance to spot and report suspicious behaviour

For those who are office based, it should be considered if staff can work from home.

The National Counter Terrorism Security Office have provided this succinct guide for security managers during a raised threat level to “critical”:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/616572/Threat_Levels_advice.pdf

2. Management

2.1 Dynamic Lockdown

Dynamic lockdown is the ability to quickly restrict access and egress to a site or building (or part of) through physical measures in response to a threat, either external or internal. The aim of lockdown is to prevent people moving into danger areas and preventing the attackers accessing a site (or part of). A dynamic assessment should be made of any situation to see what the best course of action is, which could be a dynamic lockdown.

2.1.1 Planning a Dynamic Lockdown

- You should identify all access and egress points in both public and private areas of the site (,access points may be more than just doors and gates).
- Identify how to quickly and physically secure access/egress points
- Identify how your site can be sectored to allow specific areas to be locked down
- Staff roles and responsibilities should be included in the plans.
- Staff must be trained to act effectively and made aware of their responsibilities
- Stopping people leaving or entering the site – direct people away from danger
- Ability to disable lifts without returning them to the ground floor should be considered
- Processes need to be flexible enough to cope with and compliment in-vacuation and evacuation

Dynamic lockdowns should be practised with staff taking responsibility for their roles in the procedure. The process should also be embedded: how would it be executed if key persons were not on site?

2.1.2 Informing Staff and Customers

The site occupants can be informed through a variety of options depending on the nature and occupancy of the site, these can include:
- Public Address (PA) system
- Existing internal messaging systems; text, email, staff phones etc.
- “Pop up” on employees computers / internal messaging systems
- Dedicated “Lockdown” alarm tone
- Word of mouth

Note: Use of fire alarms should be avoided to reduce incorrect response to an incident.

2.1.3 Dynamic Lockdown Advice

In depth advice on Dynamic Lockdowns from the National Counter Terrorism Security Office is available here: https://www.gov.uk/government/publications/developing-dynamic-lockdown-procedures

During a major incident the most reliable and up-to-date information will come from: @MetPoliceUK

3. Recovery

3.1 Business Continuity Plan

A Business Continuity Plan will enable your business to continue operating whilst your workspace is unavailable. Some businesses were unable to access their premises for 11 days after the Borough Market attacks. Key points for your business continuity plan are below:

- Have a contact list for your managers and ensure those managers have a contact list for all staff
- Identify “Critical Functions” i.e. the processes that must happen for the business to continue. Understand how you keep these functions active until you can resume business as normal.
- Keep a list of key contacts, suppliers, insurers etc.
- Agree a back-up location for short term working and have critical business information available (on a password protected/secure memory stick). Ensure access to social media/emails so you can inform customers of the situation
- Roleplay scenarios where you are unable to access the premises, cash, IT systems, and how you cope without them. Check with nearby businesses to see if they can help you, or if you can help them.
- All business continuity information and items should be easily accessible in a “grab bag”. One should be held on-site and one off-site, as the primary premises may not be accessible. A list of emergency items which should be present in the grab bag are here: http://www.kent.fire-uk.org/your-safety/business-safety/top-tips-

for-businesses/preparing-an-emergency-grab-bag/

A template business continuity plan is available here. This will automatically download on clicking the link: http://www.wearewaterloo.co.uk/sites/default/files/business_continuity_template.doc

3.2 The BID’s role after a major incident

After a major incident, the BID will endeavour to:
- Provide a space for businesses to work (and liaise with larger businesses to understand if they can offer workspace to smaller businesses)
- Provide business continuity advice
- Liaise with local authorities to understand restrictions around cordons, and timeframes on a return to normality
- Support businesses with insurance claims