Issue No 12 – 1 December 2015 – Counter-Terrorism Special Bulletin

Dear Reader,

Our thanks to those of you who have passed feedback on our recent Corps Relay bulletins. We are pleased to announce that Corps Relay will now be circulated monthly to provide helpful information on all matters of high importance relating to security, crime, terrorism, and related topics.

We are taking this opportunity with this issue to provide you with ***Counter Terrorism Guidance Notes***. These notes are embedding within this message, together with two very informative documents provided by the Cross-sector Safety and Security Communications (CSSC) and the National Counter Terrorism Security Office (NaCTSO).

Although there may be some variances in writing style and content within these documents, we believe it is appropriate to provide our valued clients and customers with as much information as possible from responsible sources during these challenging times.

For further information, feel free to contact our Corps Relay team direct on:
07773 320234, or via e mail:
mbluestone@corpssecurity.co.uk

COUNTER-TERRORISM SPECIAL GUIDANCE NOTES

Are your Premises a Target for Terrorists?

Although terrorists are often keen to attack Government, State and Establishment targets, it is not uncommon for extremist terror groups to also target 'secondary' or 'soft' targets in order to make their point, or to grab media headlines. The current atrocities perpetrated against the Bataclan Theatre and restaurants in Paris are a classic example of the vulnerability of soft targets. In this regard, establishments such as theatres, restaurants, pubs, cinemas, museums, schools, colleges, shopping centres, transport hubs and places of worship may be perceived as soft targets by terrorist groups.

Sources and Nature of the Threats

The threat of international terrorism emanates from a diverse range of sources, including the so-called 'Islamic State' (IS), Al Qaeda and associated networks, and those who share this ideology but do not have direct contact with them. A threat could manifest itself from a lone individual or group, rather than a larger network.

The nature of terrorist threats can take a number of forms, as terrorists may use a variety of methods of attack to achieve their objectives. These may include explosive devices (IEDs and VBIEDs), firearms, missiles, kidnapping, infiltration and cyber-attacks.

IS and/or Al Qaeda linked terrorists now have a proven track recording in carrying out Mumbai style shooting attacks (now commonly referred to as "Marauding" or "Swarm" attacks). Sadly, we have in recent days witnessed in Paris marauding attacks, combined with suicide bombings, directed against a theatre, football stadium, restaurants, and bars.

In Northern Ireland, while the targets of dissident IRA groups generally focus on members of the Police and Prison Services of Northern Ireland, there is a risk that such groups could once again target key British institutions on the mainland. We should not forget this source of threat to the UK.

Hostile Reconnaissance

Given the current security situation, and particular recent events in Paris, Security teams should be increasing their high visibility presence through increased external patrols. It is also essential that security teams are trained and regularly briefed to identify the behavioural patterns and body language of potential terrorists, and those accomplices who gather pre-operational information, through hostile reconnaissance.

Security Patrols

Security patrol members who engage in external patrols should pay particular attention to the following potential indicators of hostile intent:

- Suspicious vehicles parked in restricted areas; or being driven erratically; or with occupants taking photographs or video footage from those vehicles
- Persons acting suspiciously who may be taking photographs or video footage; or who are asking intrusive questions about premises ownership, usage or security

Security teams can also be equipped with two-way radios, as well as mobile phones, body worn video(BWV), notebooks, high-visibility clothing and, where necessary, torches.

Security personnel should also be reminded never to place themselves in personal danger, where they perceive a serious physical threat. They must be reminded to report any suspicious activity without hesitation to their Security Controller or other relevant Manager (the Anti-Terror Hotline telephone number can be found at the end of this document).

Reviewing Security Measures and Procedures

It is essential for public and private organisations to regularly review their security policies, procedures, and physical security measures in relation to access to their premises.
We pose some questions below which we hope will assist you to take practical steps to mitigate the threats from terrorism:

- *Are you satisfied with your existing access control physical measures?*
- *Is entry to your premises or estates adequately controlled?*
- *Who has ownership of access policies and procedures?*
- *Who has operational control?*
- *Are appropriate preventative measures in place?*
- *Are your personnel trained to understand and identify hostile reconnaissance?*
- *What contingency plans exist to address situations where someone or something worrying or suspicious is discovered?*
- *Do you have updated evacuation and invacuation contingency plans?*
- *Are reporting procedures adequate in terms of escalation of concerns, and police support?*

- *Is staff 'security awareness' training up to date?*
- *Do people know what they are looking for?*
- *Do you have search processes in place?*
- *If so, is the search training adequate, or in need of a refresh?*

Whilst we at Corps Security recognise that risk and threat levels will vary amongst our customer base, there are nevertheless some generic steps, or *'Top Tips'* that can be taken to help when thinking about our customers' individual and specific counter-terrorism measures and programmes:

'Top Tips':

- *Maintain a good flow of intelligence and information, including close liaison with local Police and Counter-Terrorism advisors*
- *Have the right calibre of trained people in place, including well trained Security teams, and run Security Awareness programmes for all staff and personnel*
- *Select appropriate technical solutions, especially to enable robust access control measures*
- *Implement effective operational procedures*
- *Ensure that control and supervision protocols are in place*
- *Carry out regular tests (including Penetration Tests) and drills of all security and safety systems*
- *Implement both internal and external security audits*
- *Ensure that Contingency and Emergency plans are in place and are easily accessible for all relevant personnel*
- ***Always ensure that Security teams are alert to suspicious behaviour and activity in or around your subject premises or environment! The Paris attack shows that the terrorists had done their homework, and had carried out pre-operational reconnaissance on their target premises…***
- ***REMEMBER! It is vital that Access Control and anti-tailgating measures are as robust as possible, and that unauthorised persons are not allowed to gain access to your premises!***

Tailgating

What is tailgating? Tailgating is a method of unauthorised entry to premises whereby the 'tailgater' will exploit a physical gap in security, or exploit the misplaced trust of an authorised person to gain entry into a site or premises to which they are not authorised. Examples of tailgating include the tailgater taking advantage of 'sneaking in' behind an authorised entrant who has accessed premises via a door or barrier. This frequently occurs when a bone fide entrant enters through a door and the closing mechanism of the door is too slow, thereby allowing an unauthorised person or persons to

slip past. Other examples can include an over-trusting authorised entrant who may hold a door open for an individual whom he or she believes to be bone fide. Such actions often reflect a poor security culture, and lack of security awareness on the part of corporate personnel. It is therefore particularly important at times of security alerts and terrorist threats to take all necessary steps to eliminate tailgating, and educate corporate personnel of the risks and threats.

Many electronic access control systems have built-in anti-passback features, which help prevent tailgating.

Keeping the wrong people out of your site or premises is a basic but essential element of mitigating the threat from terrorist attacks.

Evacuation or Invacuation?

One of the most consistent attack methodologies is the use of multiple and co-ordinated attacks to cause mass casualties. This in itself brings into focus what we should do in the event of a terrorist attack on premises. Automatic evacuation could mean taking those who are in the relative safety of a building out into a highly dangerous environment of secondary fragmentation and falling glass and of course possibly into another explosion.

Of course great care must be employed when deciding whether to advise invacuation as the automatic response, especially if the building is on fire or in danger of collapse.

What is Invacuation?

Invacuation is the opposite to evacuation, i.e. refuge is sought within the building following an attack, as opposed to evacuating the building to the relevant assembly point. If invacuation is necessary, this should be carried out according to directions of the responsible manager or decision making team.

Actions to be considered during an attack include:

- Taking immediate cover away from windows and doors, which should remain closed
- Staff and visitors should only leave when directed to do so by the Emergency Services. Clear instructions and procedures must be put in place to ensure all staff/visitors are aware of the need to stay indoors, and where the safest place would be

- ***The safest place would generally be towards the centre of the building away from glass or external doors, <u>but</u> you should seek advise from a structural engineer to identify protected spaces within your building***

Practical Considerations for Evacuation and Invacuation

- Consideration should be given to access to water and toilet facilities if sheltering for extended periods of time
- You should agree your evacuation/invacuation plans with the Police and other Emergency services, and your trusted neighbours
- Ensure that all staff are aware of the plans and that appropriate measure are in place to assist any disabled colleagues
- We know that terrorists will sometimes use an attack method where they set off one explosion in order to get potential victims to evacuate themselves to a more open environment, where they can be easier to attack either with a secondary device, and/or firearms
- The recent use of firearms seen in Paris for example ('Swarm Attack'), also brings into question our usual response to an emergency
- The natural reaction to evacuate from a building could potentially increase the death toll, as well as increase the fear value associated with the attack
- In Bali, for example, a small device was exploded inside a nightclub to move victims outside into the path of a large car bomb (VBIED) causing catastrophic loss of life

Sharding Glass

We also know that in urban environments (such as the Manchester bombing in 1996) flying (sharding) glass has often caused the <u>majority</u> of injuries in a bomb blast, hence the evolution of 'invacuation' as a contingency.

Useful Equipment for Contingencies and Emergencies

'Grab Bags' and Emergency Equipment

- *List of Contacts (laminated) staff, head office, etc.*
- *Emergency Plans and Floor plans*
- *Incident Log (consider dictaphone), notebook, pens, markers, etc.*
- *First aid kit (designed for major emergencies) consider large bandages, burn shields or cling film, large sterile strips, cold packs, baby wipes as well as standard equipment*
- *Torches and spare batteries (or wind up)*

- *Glow sticks*
- *Radios for monitoring media (plus spare batteries)*
- *Two-way Radios (fully charged plus spare batteries)*
- *High visibility jackets*
- *Loud hailer and spare batteries*
- *Hazard and cordon tape*
- *Plastic macs/foil blankets/bin liners*
- *Dust/toxic fume masks*
- *Water (plastic container) and chocolate/glucose tablets*
- *Computer back-up tapes/disks/USB memory sticks or flash drives*

Consideration to be given in the case of premises fire and/or collapse

In circumstances where evacuation is the obvious answer, those in key areas within businesses must be aware of the potential consequences of each option so that they can make an informed decision. Businesses should also understand that they will be responsible for their staff and customers (if a terrorist attack takes place), and have appropriate evacuation and invacuation plans.

Businesses should develop a 'security culture', with buy-in from all levels of the business including the very top (often the most difficult to persuade). Staff should be trained to understand what is expected of them in an emergency.

Dynamic Lockdown

Embedded within these notes is a separate National Counter Terrorism Security Office (NaCTSO) Guidance Note, which covers the important issue of premises lockdowns.

Defined as a 'Dynamic Lockdown', the NaCTSO document addresses the ability to quickly restrict access and egress to a site or building (or part of it) through physical measures in response to a threat, either external or internal.

We know that many clients and customers have questions and concerns about lockdowns, and indeed, as recognised by NaCTSO, due to the differences between the vast array of sites in the UK, it is not possible to provide prescriptive advice. For this reason we urge you to take careful note of the NaCTSO guide. It is appropriate, however, for your own particular premises or site lockdown

procedures to be bespoke developed in conjunction with professional security managers and qualified advisors.

Report it! Report it!

You may end up saving a life or lives... and there is nothing more rewarding than that.....

Remember! Everyone should always remain alert to the danger of terrorism and report any suspicious activity to the police on 999 or the anti-terrorist hotline: 0800 789 321

For further information, feel free to contact our Corps Relay team direct on:

07773 320234, or via e mail:

mbluestone@corpssecurity.co.uk

CORPS
CONSULT