Quick Guide to Hostile Incursions / Marauding Terrorist Attacks

CPNI
Centre for the Protection of National Infrastructure

1. COMMON THEMES FROM INCIDENTS

- Attack planning is always undertaken and usually this involves reconnaissance of targets.
- Attacks may use bladed weapons, firearms, IEDs, vehicles (as a weapon), fire or combinations of above.
- Attacks are fast moving and often last only several minutes, although can last much longer if it results in a siege or stronghold.
- Common themes from previous world wide attacks: confusing picture, conflicting information, people not recognising an attack underway, poor communications (between security personnel and also to those caught up in the incident – personnel not knowing what action to take).

2. CPNI RECOMMENDED 7 KEY STEPS FOR ORGANISATIONS

1. Anticipate the threat and assess the risk. Involve all key stakeholders when assessing risks and mitigations. Tabletop exercises can greatly assist in the understanding of risk and gaps in mitigations.

2. Develop a strategy for the delivery and maintaining the long term effectiveness of mitigations. For many, the mitigations will be wide ranging sitting across many business areas. The effectiveness of mitigations are likely to degrade over time and should be addressed.

3. Prepare your people. Security personnel need appropriate training and should regularly practice their response. All other occupants need to know what to do and should rehearse their response, as for fire.

4. Disrupt hostile reconnaissance. Make it difficult for a hostile to obtain useful information about your site and personnel. Deter them by demonstrating a good security posture.

5. Detect, delay and protect. Early detection of an attack is critical, consider technology to assist and rehearse detecting incidents. Delay the progress of attackers by using physical barriers and active delay systems (see lockdown). Protect critical assets, such as control rooms, to ensure they remain operational during an incident.

6. Response. Develop, exercise and rehearse response plans and test security systems. Consider how and what you will communicate to personnel during the incident. Consider how you will interact with the police and assist them with their tasks, including tracking the attacker(s), opening doors, communicating with the control room etc.

7. Recover. Plan for how the organisation will recover from the incident, including the welfare needs of staff.

3. STAY SAFE

- NaCTSO have published guidance for general personnel on what do in the event of a firearms or weapons attack – STAY SAFE. It recommends **RUN, HIDE TELL**
- A STAY SAFE video has been produced and is an excellent way to provide a basic awareness to staff.

4. LOCKDOWN

Lockdown means securing **all** building doors, windows etc to restrict / prevent the movement of hostiles. Partial or zonal lockdown applies to predefined zone/area(s) only, such as an entry point(s). It is usually a quicker, easier and often safer alternative to full lockdown.

The following key issues must be considered when invoking full or zonal lockdown:

- The safety of personnel and their need to escape.
- What types of barriers are to be used (including active delay systems) and how this will be effected/controlled.
- The timeliness of activation.
- The needs of police firearms officers.
- Communications within building / between occupants.
- Fire detection and suppression systems and their activation.
- Remember that you cannot force personnel to remain in place during lockdown.