An introduction to protective security for owners and operators of publicly accessible locations

Recent years have seen an increase in terrorist attacks in publicly accessible locations, i.e. locations that people visit, congregate in, or transit through. A defining feature of such attacks is the targeting of people, whether randomly, or as representatives of specific groups (e.g. relating to race, religious beliefs, etc).

Any publicly accessible location is a potential target, and it is therefore essential that the owners and operators of all such locations understand the risks they face and consider appropriate mitigations.

This section is intended to introduce protective security for owners and operators of publicly accessible locations – whether businesses, or other organisations operating in permanent premises or the organisers of temporary events, or those with wider interests in public security such as public authorities.

It is worth noting that improvements made to security from a counter-terrorism (CT) perspective are likely to have wider benefits, potentially reducing other crime and antisocial behaviour. Similarly, existing or new security measures implemented for other purposes can have a counter-terrorism benefit.

An important tenet of protective security is that it should, wherever possible, utilise simple, affordable interventions that protect and reassure the public and deter would-be attackers, with no (or minimal) adverse impact on the site's operation or people's experience. Whilst an extensive pallet of countermeasures is available, many of the more complex and costly ones – particularly specialist physical security products – will be more relevant to larger sites likely to host higher visitor footfalls and/or crowds.

It is important to consider **security as a system**, a combination of physical and/or behavioural interventions deployed in a complementary manner to mitigate key risks. Getting the "people" aspects right (e.g. developing and sustaining a security culture, encouraging vigilance, and providing appropriate and effective training) is at least as important as selecting (and correctly installing) physical security measures (such as security doors, blast-resistant glazing, fences, bollards, CCTV, electronic access control and intruder detection systems). Further advice and guidance is available on the NaCTSO website or from your local Counter Terrorism Security Advisor (CTSA). Where you believe, based on your risk assessment, that you may need such measures, you may also wish to seek independent expert advice (https://www.cpni.gov.uk/cpni-working-security-professionals). Even where appropriate measures are selected that appear to match a site's needs, ensuring they are installed and operated to provide effective capability (and properly complement other security measures) is crucial.

Key initial steps are **understanding threat and risk:**

- Understanding the terrorist threat – noting that terrorist groups, their motivations and target preferences and attack methodologies can differ and tend to change over time.
    - A useful level of awareness can be achieved by following open source media reporting of recent attacks and their methodologies, understanding

    and monitoring the National Threat Level (https://www.gov.uk/terrorism-national-emergency), and browsing relevant government websites (e.g. https://www.cpni.gov.uk/terrorism).

- Understanding the specific risks the threat poses for your site and / or organisation - how and why your site / organisation might be affected, either by being targeted directly; or through indirect impacts, due to its location in a particular area or because of its proximity to neighbouring sites, businesses, or organisations that may be targeted.
    - You should undertake a risk assessment to identify and record terrorism risks and appropriate mitigations. This should be aligned with your organisation's / site's wider assessment of risks and their management.

In order to maximise their likelihood of success, terrorists are likely to undertake research and planning activity in preparation for an attack; this can include visiting potential target locations ("**hostile reconnaissance**"), as well as conducting research online.

Consider what you and your colleagues (whether employees, contractors or volunteers) can do to make it harder for a would-be terrorist to carry out a successful attack, for example by:

- Being alert to suspicious behaviours and activity in and around your site, such as people loitering or displaying an unusual level of interest in asking questions, or filming or photographing. Note that you and your staff are well placed to know what is "normal" in your environment, and hence what may be suspicious. Where it feels safe to do so, consider engaging the person in a welcoming and helpful manner; if you have any concerns, consider reporting them to the police. Similarly, you and your colleagues should be alert to abandoned bags and other left items, and report any you deem suspicious to the police.
- Being security-minded in your communications, particularly online. Wherever possible, include positive general messages demonstrating your commitment to ensuring the security and safety of visitors and staff. Avoid providing specific information that could help a terrorist plan an attack, for example floor plans containing more detail than is necessary to assist customers with planning their visit, or details of where and when security patrols do (and don't) take place.
- Encouraging and enabling a security culture in the workplace, for example ensuring that any concerns can easily be reported and will be acted upon and ensuring that managers lead by example and avoid giving mixed messages.

Consider how you and your staff would respond to an incident occurring outside or near to your building or site, or inside it. Remember that every second counts.

- How quickly would you become aware of what was going on?
- How would you respond?
- Would you and your staff be able to act quickly enough to move yourselves and visitors to safety?
- What can you do to prepare for such an eventuality?

ACT Awareness e-Learning (Action Counters Terrorism), has been developed by Counter Terrorism Policing to provide nationally recognised corporate CT guidance to help people better understand, and mitigate against, current terrorist methodology. It is available to all organisations, their staff and the general public (https://www.gov.uk/government/news/act-awareness-elearning).

For many organisations, security arrangements will be enhanced by developing relationships with neighbouring businesses and organisations, for example working together to make the local environment harder for would-be terrorists to operate in, including enabling the rapid exchange of information on suspicious activity and potential incidents. It is also advisable to engage with your local CTSA and neighbourhood policing team.

Take care to ensure that any security measures / plans don’t conflict with health and safety requirements and fire regulations.

Remember to **review and refresh** (where appropriate) your risk assessment, your plans and mitigations, including your staff’s awareness of the threat and how to respond. Routine reviews should be undertaken regularly, with reviews also carried out if there are changes to the threat – either in terms of national threat level (indicating the likelihood of an attack) or as a result of incidents that demonstrate a shift in attack methodology.

Further information

- Counter Terrorism Policing and its National Counter Terrorism Security Office (https://www.gov.uk/government/organisations/national-counter-terrorism-security-office)
- Centre for the Protection of National Infrastructure (www.cpni.gov.uk)