ProtectUK

Introduction

Original publication date
02/11/2020

The threat we face from terrorism is significant. As we have seen in the UK and across Europe, attacks can happen at any time and any place without warning. Having better security for all these areas makes it harder for terrorists to plan and carry out attacks. It also helps reduce the risk of other threats such as organised crime.

This document provides protective security advice in a number of sectors and scenarios. It has been developed through extensive research and analysis of previous incidents, and the assessment of current known threats. It covers the key forms of protective security: physical, personnel, cyber and personal, and helps give guidance on how different sectors can act to help make their business, institutions or organisations safer.

This guidance is primarily aimed at those in the security sector and those who own or run businesses, organisations, amenities or utilities. Some of the wording may be new to some readers, but we hope the advice can also be of use to anyone who wishes to improve their own security. To deliver protective security effectively a security plan is essential along with a full risk assessment. It is important to identify an individual responsible for security and to identify what are the important assets, people, products, services, processes and information within your organisation. You can then begin to introduce mitigation to reduce vulnerabilities. A strong security culture must be supported and endorsed from a senior level.

1.1 Physical security

Effective physical security is best achieved by multi-layering different measures. A terrorist will attempt to identify and exploit perceived weaknesses. The core principles for protecting an asset are Deter, Detect, Delay and initiate an effective response.

1.2 Personnel and people security

To achieve effective personnel security, a system of policies and procedures are required to reduce the risk of an organisation’s assets from being exploited by bringing together aspects of physical, personnel, people and cyber security. This guidance signposts business towards the objective of vigilant staff and an effective security culture. Organisations should determine how to get the best from their staff in security matters and disrupting hostile reconnaissance and insider threats.

1.3 Cyber security

The National Cyber Security Centre’s role is to reduce the cyber security risk to the UK by improving its cyber security and cyber resilience. They work together with UK organisations, businesses and individuals to provide authoritative and coherent cyber security advice and cyber incident management. They are able to provide effective incident response to minimise harm to the UK, help with recovery, and learn lessons for the future.

1.4 Personal security

Our own security, and the safety of those close to us, is of utmost importance. The more individuals do to protect themselves, the safer they and their families will be. There are three key areas that can affect an individual's safety. These are physical security, an individual's situational awareness and online security. Exactly which security measures are adopted will depend on the extent, or level of threat an individual is likely to encounter and their vulnerabilities. This may be dependent upon their profession or role, a specific threat, the location of their work and or their personal history. No one has more responsibility for an individual's personal security than themselves. With an evolving threat we must all consider our own personal security, particularly when in public places.

2. How to use this guide

The publicly accessible locations guidance has been reviewed by protective security experts from the National Protective Security Authority (NPSA formerly CPNI), the National Counter Terrorism Security Office (NaCTSO) and practitioners from a range of businesses, trade bodies and associations.

While it can be read page by page, it has been designed for the user to jump to the page most relevant to their interest or enquiry.

The guidance is divided into sections that discuss different types of terrorist attacks and their effective

mitigation. It is worth bearing in mind that a number of these attack-types can be carried out at varying times when a crowded location is in use. An attack can be carried out in crowds of people or during a specific event (such as during a concert, or during the opening hours of a shopping centre). Some attacks may lead to ‘preparatory acts’ being carried out prior to the presence of any crowds (e.g. timed explosives).

We would caution against undue emphasis being placed on the timing of any particular attack and that the possibility of attacks taking place at different times is considered in the planning and preparation to mitigate the likelihood of attacks.

Essential mitigations against certain types of attack, or indeed prepared hostile reconnaissance, such as identifying and notifying supervisors or the police about suspicious behaviour are relevant steps you can take against acts of terrorism throughout an event or the lifecycle of a site. Use should be made of examples in tabletop exercises and discussions in order for the site operators and relevant third-party contractors (e.g. security staff, facilities management) to work through their processes and emergency procedures in a range of scenarios that consider different types of attack taking place at different times.

KEYWORDS
PALS GUIDANCE
PALS
PUBLICLY ACCESSIBLE LOCATIONS
PUBLICLY ACCESSIBLE PLACES
PHYSICAL SECURITY
CYBER SECURITY
PERSONNEL SECURITY