ProtectUK

Physical security

Original publication date
02/11/2020

1. Introduction

Physical security is important to consider when protecting against a range of threats and vulnerabilities, including terrorism.

When planning the introduction of any physical security measures, it's imperative both safety and emergency responses are considered.

Effective physical security of a Publicly Accessible Location is best achieved by multi-layering a variety of measures. This is what is commonly referred to as 'defence-in-depth'. The concept is based on the principle that should one line of defence be compromised, the additional layers and measures in place would make sure the threat didn't slip through.

In order to achieve success, a hostile will attempt to identify and exploit weaknesses within your protective security measures. The NPSA (formerly CPNI) principles of Deter, Detect and Delay, supported by an effective response plan, will help to frustrate and disrupt any potential hostile.

Considering the physical security requirements at the outset of the venue's planning and design phase, will often result in more effective and cost-efficient security. The risk assessment will determine which measures should be adopted. It is essential that the threats faced by the venue or site are understood; effective security depends on a proportionate response to the threat.

2. Operational requirements

The NPSA Operational Requirements process helps organisations make intelligent investments in security, enabling them to implement measures which are in proportion to the risks they face. By following the process, security managers and practitioners are able to assess, develop and justify the

actions their organisation needs to take, and the investments they need to make, to protect their critical assets against security threats.

3. Security awareness

Vigilance by staff and visitors at all Publicly Accessible Locations is essential to the protective measures. Staff will know their own work areas well and should be encouraged to be alert to unusual behaviour or items that are out of place. They must have the confidence to report any suspicions, and know that reports, including false alarms, will be taken seriously.

3.1 Training

Training is therefore particularly important. Staff should be briefed to look out for packages, bags or other items in odd places, carefully placed (rather than dropped), items in rubbish bins, unusual interest shown by strangers in less accessible places and suspicious behaviour.

Read more about Hostile Reconnaissance to learn about what suspicious behaviour might look like.

Read more about Personnel Security Training and Good Practice to learn about developing a strong security culture.

3.2 Deterrence

Hostiles will not necessarily be automatically deterred from a Publicly Accessible Location simply because it has CCTV, guards or a particular fence or lock. Instead, an organisation needs to use these security measures in an effective manner. Effective security measures with an alert and professional guardforce and staff will require hostiles or criminals to conduct further attack planning and pose an extra risk of detection, which they may be unwilling to accept. If a hostile assesses a site that has excellent security measures due to the information available online, on a poster or witnessed in operation, it may be enough to deter them from their target altogether.

Read more about deterrence comms to learn about communicating a strong security culture online.

3.3 Patrolling, guarding and security officers

Routine searching and patrolling of premises represents another level of security and may cover both internal and external areas. Make sure patrols are carried out regularly, but at unpredictable times. Staff must have clearly defined roles and responsibilities which are linked to clear policies and procedures for them to follow. Such measures must be underpinned by training, rehearsal and exercising.

Read more about personnel security training and good practice

4. Access control

Controlling access into a site or venue may include either people, items or vehicles and is an essential layer of protective security. An efficient entry system creates a smoother flow into a crowded place. Make sure that the boundary between public and private areas of your venue are secure and clearly signed. Make sure there are appropriately trained and briefed security personnel to manage access control points.

Consideration should be given to how vehicle access could be controlled at the point of entry, particularly in relation to the searching or screening of vehicles in response to a specific threat. Larger sites may additionally have ‘crash’ gates which will require a strict security regime to make sure they are not breached. Access points should be kept to a minimum, with any boundary fences or demarcation lines clearly signed.

Read more about Search Planning to learn about how to successfully carry out searches of people and vehicles on site.

Access control systems and locks are designed to control who can go where and when. These systems integrate with physical barriers to provide delay and detection against hostiles trying to access your site. Controlling access can be done via:

- Automatic Access Control Systems (AACS) which control a number of doors across a single or multiple site
- locks (electronic or mechanical) which control access to a single door

Consideration should be given to investing in good quality access control systems that are not only physically robust, but also cyber secure.

To learn more about key management and security passes, go to our Access Control.

5. The perimeter

There should be measures in place to ensure that a venue or site can exercise a degree of control over the activities that take place within their property boundaries. Defensible space is created by deciding which areas around a property are public and which areas are private. Simply put, boundaries should clearly define the difference between public and private space. This is particularly important when challenging protests and unlawful activity. There should be measures in place to ensure that an occupier can exercise a degree of control over the activities that take place within their property boundaries.

Fencing

Fencing is often used as a perimeter, providing a line of demarcation; it is an important security measure, both for deterring criminal activity and enhancing safety. Once installed, it should be regularly checked to ensure that it is in good repair and fit for its intended purpose. Perimeter Intrusion Detection Systems (PIDS) may be used at the perimeter to alert security officers that the perimeter has been breached.

Hostile Vehicle Mitigation

Read more about Hostile Vehicle Mitigation (HVM) on our website or contact a CTSA who will be able to advise you on keeping your site safe from hostile vehicles.

6. Control rooms

Security Control Rooms (SCRs) form the hub of a site's security. The control room's main function should be security; non-security responsibilities should be discouraged. The set-up of the control room should ideally allow serious incidents and crisis situations to be handled within them, without compromising the ability to deliver normal security functions.

For further information, seek specialist advice and refer to the NPSA website.

7. Structural framing, walls and floors

Buildings in the UK are commonly constructed using a structural frame, typically steel, concrete or timber, or are built from unframed masonry. There are many different types of walls and floor systems that are used within buildings, but together these elements play an important role in protecting occupants and assets from the effects of blast and other security threats. For many, a primary security concern is for the building to remain standing, or for damage to be limited to defined zones following an attack involving explosives, impact and/or fire.

Designing structural framing, walls and floors for buildings so that they incorporate physical security requirements from the outset, will help deliver strong and resilient business operations. Where it is necessary to retrofit or adapt existing structures, physical security needs should form a central part of the project's 'Operational Requirement'.

8. External doors and windows

Good quality external doors and windows are essential to building security. Advice on standards is available through the Secured by Design or NPSA websites, or via a local CTSAs. Consideration should also be given to intruder detection systems. Remember that glazed doors are only as strong as their weakest point, which may be the glazing. All accessible windows should have good-quality key-operated locks.

Many injuries involving explosive devices are caused by flying glass. Glazing protection is an important measure to reduce casualties. Extensive research has been carried out on the effects of blasts on glass. There are technologies which minimise the shattering effect and therefore reduce the severity of injury. Anti-shatter film, which holds fragmented pieces of glass together, offers a relatively cheap and rapid improvement to existing glazing. If installing new windows, consider laminated glass, but before undertaking any improvements, seek specialist advice through a CTSA.

Working from a security threat and risk assessment, it should be determined which of the following types of attack the door and windows need to mitigate against:

- blast

- ballistic – people either trying to shoot at occupants through the door, or to damage the door/door hardware in order to gain entry
- manual forced entry – attackers using tools to try and force entry through the door
- surreptitious entry – an attacker trying to infiltrate through the door leaving no indication of compromise

Doors

Doors form an essential part of physical security and are often required to perform several functions, including to:

- control access, permitting access only to authorised personnel
- permit an appropriate flow of people/materials etc.
- work in conjunction with intruder detection systems (IDS), to detect unauthorised access
- provide a barrier to delay the progress of a hostile
- provide protection from specific types of threat, such as blast or ballistic
- provide protection from fire and/or smoke ingress
- provide a means of escape in an emergency

Security doors should also integrate with sensors for intrusion detection and access control systems, making sure the earliest possible alert to a potential compromise. Whether they are part of the external façade, or form part of the boundary around a space within the building, it is important to define the security requirements for each door.



Windows

Windows comprise a number of components and their security resistance is linked to how these components perform as a whole system. Consequently, when specifying the level of protection required of the window, it should relate to the whole system, not just the glass. When identifying glazing, there are various types of glass to select from, each of which has different properties:

- **Annealed/float glass** – traditional window glass which forms sharp glass shards when broken. It is not recommended for use in any security solution.
- **Toughened glass, also known as tempered glass** – the production process produces glass that is approximately five times stronger than regular annealed glass. It will break into small chunks instead of glass shards.
- **Heat strengthened glass** – this is similar to toughened glass but is only twice the strength of regular annealed glass
- **Laminated glass sandwiches** – an interlayer between layers of glass designed to hold together when the glass shatters

- **Polycarbonate** – significantly stronger and lighter than glass and hard to break



Laminated glass is the preferred option for most security applications. Care should be taken to make sure that the correct type of laminate is specified and used. It is also important to make sure that the rest of the glazing system, for example the support structure and fixings, are specified and installed correctly.

Anti-shatter film, fitted alongside bomb blast net curtains may be used in conjunction with any of the types of glazing. Additional measures such as bars and grilles may also be incorporated to provide enhanced security. Thought should be given to whether these are placed inside or outside the glazing. Concealment measures can be used to reduce both the threat of ballistic attacks and unauthorised observation. In the case of ballistic attacks, such measures will prevent aimed shots but may not stop un-aimed fire. The construction details of glazing therefore needs to be considered to determine whether they will withstand bullets from the selected threats.

Go to the NPSA guidance on Windows and Glazed Facades

9. Heating, ventilation and air conditioning systems (HVAC)

In order to maintain a comfortable indoor environment, occupied buildings will feature some form of ventilation and heating or cooling. This may be achieved through natural ventilation, mechanical ventilation (e.g. fans or blowers) or hybrid ventilation systems.

Modern, commercial buildings such as shopping centres, airport terminals and sports venues typically use a distributed (mechanical) heating, ventilation and air-conditioning (HVAC) system. HVAC systems, which can have many points of access, potentially provide a viable, rudimentary means of dispersing chemical or biological agents, and so a consideration of measures to reduce this risk may be required:

- review the design and physical security of the air-handling systems, such as access to intakes and outlets
- improve air filters or upgrade the air-handling systems, as necessary

Read more about Chemical, Biological and Radiological (CBR) attacks guidance to learn more about this particular threat.



10. Integrated security systems

Intruder alarms, CCTV and lighting are commonly used to deter crime, detect hostiles and delay their actions. All these systems must be integrated so that they work together in an effective and co-ordinated manner. Intrusion detection technology can play an important role in an integrated security system; it is as much a deterrent as a means of protection.



Read more about CCTV guidance to learn more about implementing a secure video surveillance system.

10.1 Alarms

The National Police Chiefs Council (NPCC) security systems policy sets out the police requirements for alarm systems installed by compliant companies to gain a police response to premises. Compliant companies can apply for a police Unique Reference Number (URN) which is used to identify an individual security system within the police database to make sure an alarm activation has an immediate response. Make sure that the security system company is police compliant and they can supply a URN.

The NPCC requires security systems companies to be certified by an inspectorate accredited by United Kingdom Accreditation Services (UKAS) to EN 45011 and to relevant British Standards listed in the NPCC security systems policy. The two inspectorates approved by the NPCC are:

- National Security Inspectorate (NSI)
- Security Systems and Alarms Inspection Board (SSAIB).

Using CCTV can help clarify whether a security alert is real and is often vital in post-incident investigations.

10.2 Lights

External lighting provides an obvious means of deterrence as well as detection, but take into account the impact of additional light pollution on neighbours. If it is carefully designed and used, external lighting will help security staff and improve the capabilities of CCTV systems. Remember however, that CCTV is only effective if it is properly monitored and maintained.

10.3 Designing out crime officers and Counter Terrorism Security Advisors

Designing Out Crime Officers (DOCOs) and Counter Terrorism Security Advisors (CTSAs) both provide advice and guidance on physical security. DOCOs are the ‘gatekeeper’ to security within the planning system. Their role is vital to the process of identifying, as early as possible, any future development that has, or may have, any counter terrorism concerns. While CTSAs provide advice to counter terrorist threats, DOCOs provide advice and guidance to counter other criminality and they work closely together throughout the UK. Consult the appropriate website for further Information on who best to provide advice for a specific requirement.

11. Further information

Go to the BRE website to learn about design regulations to help keep buildings secure.

Contact a local CTSA for advice on standards.

Go to the NPSA website for guidance on a wide range of security measures

Go to the Secured by Design website who can give guidance on making a site or building secure.

KEYWORDS
PUBLICLY ACCESSIBLE PLACES
PHYSICAL SECURITY
SECURITY
SECURITY MEASURES
ACCESS CONTROL
PALS GUIDANCE
PALS
PUBLICLY ACCESSIBLE LOCATIONS