# Maintaining a security minded approach during the pandemic

**Threat of terrorist attack has not gone away, with socially distanced queues of people outside buildings a new concern. Highway authorities must keep security high on the agenda.**

Crowded spaces can be attractive sites for terrorist attack, with vehicles used as weapons against people on the roadside – as seen on Westminster Bridge and London Bridge in 2017.

In the Government's response to the Coroner's report into the London Bridge & Borough Market attack there was an action for highway authorities to be provided with guidance.

Since then the Department for Transport has been working with the UK Roads Liaison Group and the Centre for the Protection of National Infrastructure (CPNI) to provide additional help to local highway authorities across the UK.

New guidance now published builds on previous advice for highway authorities contained in the 'Well Managed Highway Infrastructure' code of practice. The new guidance is available on the UKRLG website and is summarised here.

In essence, it says that highway authorities across the UK should adopt a 'security minded approach' to their assets, information and people to ensure appropriate and proportionate security measures are applied to deter and/or disrupt hostile, malicious, fraudulent and criminal behaviours or activities.

Three key sections of the guidance cover 'culture and governance', 'major schemes and maintenance renewals' and 'developing an integrated security network'.

↑ **Street furniture can protect against hostile vehicle attack as seen here in Stratford-upon-Avon** CPNI

## Culture and governance

Culture is about encouraging behaviours or installing internal mechanisms or procedures to embed a security minded approach within an organisation. There are two broad steps for this:

1. Governance: an important step to achieving a security culture is to have a senior level official responsible for security, and;
2. Providing training and support to staff to help deliver a security minded culture.

Governance is important for security, so this means identifying who is accountable for security at the highest board or executive level – either a designated point of contact or a virtual security 'team' of people throughout an organisation.

A board level executive should be appointed as a senior risk owner for security, who has corporate responsibility for security and ensures a clear security governance process within the organisation so that risks can be owned, managed and reviewed regularly.

Visible senior leadership helps to promote positive security behaviours and ensure security processes and procedures are adopted throughout a business, thereby establishing a security culture.

CPNI's 'Passport to Good Security for Senior Executives' sets out the key themes for top down best practice and provides relevant prompts for the actions needed to be taken. It helps authorities to identify, assess and mitigate the threats to their organisation.

Highway authorities should also develop an appropriate security strategy and embed this in their organisation; CPNI's 5Es approach (educate, enable environment, encourage and evaluate) is a recommended approach to delivery. Ensuring that all front line staff are trained in being vigilant and understanding how to respond to unusual activity or items is essential for good security.

Highway authorities should undertake training of their staff and those in their supply chain, for example, encouraging their parking enforcement officers, street cleaning and refuse collection staff

UK ROADS LIAISON GROUP

**c/o CIHT, 119 Britannia Walk**
**London N1 7JE**
**web:** *ukroadsliaisongroup.org*

**email:** info@ciht.org.uk
**tel:** 0207 336 1555
**twitter:** *@ukrlg*

**UKRLG Chair:** Stephen Fidler

**UKRLG Board Chairs:**
**Roads:** James Bailey
**Lighting:** David Denner
**Bridges:** Liz Kirkham
**Network Management:** Mark Kemp
**Asset Management:** Garry Sterritt

**Senior Policy Officer:**
Justin Ward
**email:** *justin.ward@ciht.org.uk*
**tel:** 0207 336 1584

to remain vigilant and immediately report any suspicious looking activity, behaviour or objects.

This training could involve putting all staff through the ACT 'Awareness e-Learning' developed by National Counter Terrorism Office and security specialists, which is freely available. In addition to staff knowing what to look out for, it is essential that issues are reported to the appropriate authorities and management must positively thank staff when issues are reported.

Authorities may wish to develop their own triage process before items are reported to the police either locally or through national counter terrorism policing mechanisms such as the ACT app. This app provides access to the latest messaging, advice and protective security documents created by counter terrorism police.

The value and effectiveness of security measures can be significantly enhanced if their existence is publicised. This can be a deterrent to those seeking to cause harm, while simultaneously reassuring the public by, for instance, publicising the installation or renewal of hostile vehicle mitigation (HVM) and other measures such as CCTV as part of enhancement to an area or urban realm. It would signal to those seeking to cause harm that those measures exist and may deter them from continuing with their plans.

While it is valuable to publicise that security measures are in place, a security minded approach should be taken for all public information and communications. You should avoid publishing specific technical details (especially online) that could be useful for those carrying out research as part of an attack planning process.

Training in how to adopt a security minded communications approach can be arranged by your local counter terrorism security advisor (CTSA) as part of the 'See, Check & Notify' training programme. The free training is suitable for communications professionals, subject matter experts and policy teams. It provides simple and easy to apply guidance to maximise safety and security and deny those with malicious intent the information they need to plan operations effectively.

↑ A camera monitoring activity in the street

PRES PANAYOTOV – SHUTTERSTOCK

↑ Barriers have been installed on several London bridges to protect pedestrians

LENSCAP PHOTOGRAPHY – SHUTTERSTOCK

## Major schemes / maintenance renewals

Security mindedness should inform both the design and maintenance of major highway works, such as integrating security measures in the public realm at project inception.

It is also important to protect critical infrastructure (such as telecoms/gas/electricity) rather than leaving it accessible or vulnerable during a maintenance process, which is particularly important in crowded spaces such as a railway station or shopping district – where HVM measures should be considered as appropriate during any refurbishment or new build project.

Measures can also be taken in temporarily crowded places for a time limited period and 'socketed' systems could be considered if a site is to be protected temporarily on repeated occasions. Further advice on security measures can always be obtained from your local counter terrorism security advisor.

It is worth noting that not all security enhancements require major civil engineering, such as HVM. Using CPNI's Operational Requirements process will help highway authorities identify and proportionally mitigate the risks.

Advice is also available on how to blend in physical features to prevent against vehicles being used as weapons (HVM). In considering appropriate physical security measures the potential for negative impacts on the aesthetics of the public realm should be considered, for example using specially designed planters and artwork rather than a row of bollards.

Other measures are available that provide protection while blending in with the surrounding architecture and streetscape, helping to retain a sense of place without compromising security.

Local authorities, along with their consultants and contractors, should consider the advice available as part of the design process.

Where work is being undertaken using digital engineering processes such as building information modelling or other concepts such as 'smart cities' and interconnectivity of assets are being considered, a security minded approach should be taken in relation to the generation, processing, sharing and storage of information.

## Developing an integrated security network

Highway authorities should consider their whole network in terms of security risks and seek security advice in doing this. Highway authorities can seek advice from their local police force counter terrorism security advisors to ensure an awareness of the potential risks they face.

A local authority should consider undertaking a 'security considerations assessment' (SCA) to assess how well security is understood and embedded across its organisation as well as how it is considered in the work it undertakes across the assets it manages.

As we have seen with vehicle as a weapon attacks in 2017, threats can shift (such as where the vehicle occupants cause further disruption on foot).

Highway authorities should give due regard to shifting attack methodologies when considering their security posture and network.

Authorities should also look for opportunities to work with partners to agree on a common approach to addressing security, for example by attending security meetings at major railway stations. There is useful guidance that highway authorities would also benefit from on reducing security vulnerabilities at rail, bus, and coach stations.

Further guidance is also available around protective security considerations for high street hospitality and minimising the risk to pedestrian queues from a vehicle used in a weapon attack.