Welcome back to all those businesses getting ready to reopen.

We are all delighted that you are able to step up preparations for a return of staff, visitors and customers.

As you get closer to restarting, we ask you to please remember all the good work we have done together over recent years to help protect crowded places from terrorism. The UK National Threat Level remains at SUBSTANTIAL, meaning an attack is likely.

We feel confident that terrorist activity in the UK will return to previous norms after restrictions to prevent the spread of the coronavirus are eased.

So when you are making plans for the reopening of your business, we ask that you think about security and build a security review into your 'to do' list.

Our 60-second check provides an easy guide to the things that you can think about now as you get ready to return to normal – or 'the new normal' as it will undoubtedly be for all of us.

Making arrangements for social distancing and extra hygiene precautions are going to be foremost in your mind, but don't forget there are always those who look to exploit situations when your attention may be elsewhere. Good counter terrorism measures also have benefits in deterring crime.

Here's what you should consider to help keep everyone safe and secure once you are back together with your colleagues:

• Is it clear who is appointed to make security decisions on the 'shop floor' and do they know what they should do in an emergency? Do your other staff know who that person is?

• How do you enter and exit your premises? Do you need to limit this to staff and, if so, is the route clear and secure? Are there any other doors or windows that may need checking?

• In the event of a terrorist attack, if it was not safe to evacuate and RUN, how would you lock down and secure your premises quickly to protect staff and customers? Where would you HIDE? How would you communicate with others and TELL the emergency services what was happening?

• Have you checked that any security equipment at your premises, such as CCTV, is in working order?

• Have you reminded your staff to display their company ID at all times and to review any company-specific security policies you have?

Having done the basics, you can find more detailed, sector-specific advice in [NaCTSO's Crowded Places Guidance](#).

Our colleagues from the Centre for the Protection of National Infrastructure (CPNI) have provided more detailed guidance for businesses preparing to return.

They reiterate that whilst the risk to health from COVID-19 is at the forefront of everyone's minds, the threat of terrorism and other security threats nonetheless remains substantial.

Their guidance points out that it is essential that businesses and other organisations remain cognisant of these threats as they look to adjust their operations,
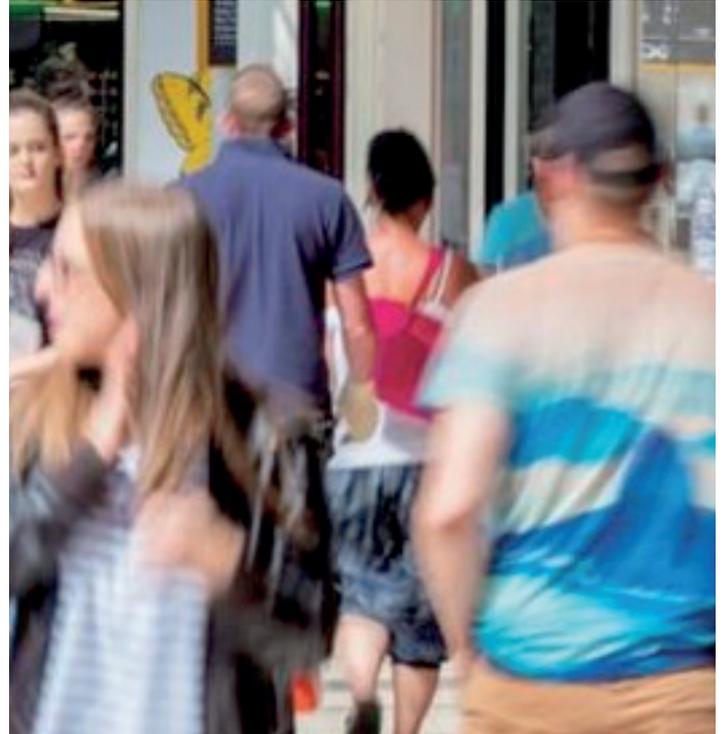
ensuring that security measures are proactively adapted to support and complement other changes.

Summary of guidance provided by the CPNI.

If you have a security department or manager, they should be consulted to help ensure good security is maintained as far as possible and that there are no unintended security consequences as a result of changes. This should be achieved by conducting a security risk assessment. For further information see the [Centre for Protection National Infrastructure](#) and [National Counter Terrorism Security Office](#) for specific security advice related to COVID-19

Overarching security considerations

Adapting to COVID-19 measures is inevitably going to result in changes to operating policies, processes and procedures of hotels, indoor, outdoor attractions and other business event venues. Any changes in these

COUNTER
TERRORISM
POLICING

UK Protect

Protective Security Information for the Business Community

NATIONAL BULLETIN

5 June 2020

should always be considered with regard to security implications. The security department or manager should be consulted and involved throughout to help ensure good security is maintained as far as possible and that there are not any unintended security consequences of these changes. This should be achieved by conducting a security risk assessment of any new measures or changes.

Specific security implications are likely to be around queueing, search and screening, maintaining vigilance for potential threats and access controls. Each of these will be examined in turn.

Queues and social distancing

Whilst dense crowding is unlikely if social distancing is operating correctly, the revised layout of spaces may present new security risks, particularly where multiple queues are created. Considerations include:

• Operators should try and organise queuing within existing protected areas; Operators should NOT remove any security features or useful street furniture items without considering protective security in the round.

• If queuing is only possible outside of protected areas then consider and mitigate the vulnerabilities by: routing queues behind permanent physical structures (e.g. street furniture, bollards, trolley parks & bike racks) to provide a visual deterrent and delay; closing off vehicle access to shared spaces; adjusting servicing and delivery times; reducing the opportunities for vehicles (including potentially hostile vehicles) to interact with pedestrians; erecting robust barriers; introducing a reduced speed limit mandated using traffic calming

• In any messaging, both at the site and particularly on-line, be mindful of how detailed information about queue locations, times and number of people or removal of security features such as street furniture,

bollards etc at specific times can be very useful and motivating information for those with hostile intent. Operators should avoid giving credible, detailed information that could identify an attractive target, especially if the queue is forming outside of any protective security measures.

Search and screening

For sites that conduct physical search and screening of staff/visitors this will be challenging to undertake in particular with social distancing measures.

• To maintain effective security and deterrence, search and screening should still be conducted as appropriate and in line with the organisation's policies.

• Ensure security staff feel safe, e.g. having access to appropriate PPE and hand-washing facilities, and that they are able and confident to raise any concerns

• CPNI has published guidance on adapting existing search and screening processes to take account of physical distancing. Details are available from your local Police Counter Terrorism Security Advisor (CTSA).

Staff, security officers and stewarding

It is vital for staff to remain vigilant for and act on potential security threats including terrorism and wider criminality as these threats have not gone away:

• Continue to ensure that awareness of security threats is raised alongside safety and health risks through staff briefings.

• Whilst stewards and security officers may be focussed on managing people and queues for COVID-19 safety reasons, they should continue to remain vigilant for and report any suspicious activity as soon as possible.

• Ideally consider providing separate stewarding to manage the social distancing and other safety aspects

to enable your security staff to focus on their core responsibilities to keep the site safe from threats.

- Ensure there is a good communication system in place to inform people of any incident. Carry out a short exercise or test to check procedures and equipment for this are working correctly.

Restricted entry points

Restricted access entry points, such as those facilitated by keypad, biometrics and/or pass should remain fully in operation. They should not be deactivated.

- Pin pads and biometrics should be highlighted as "touch points" and cleaned regularly (note: they are touched less than door handles)

- Access control (staff) proximity cards will work up to 10cm from the reader. Staff can be informed that there is no need to physically touch the card on the reader.

Personnel and people security issues

CPNI has produced a series of CV-19 specifc personnel people security guidance to assist with a wide range of issues that have or are likely to occur because of changes in working practices and individual employee situations.

Currently most organisations will have a larger number of people working from home than normal, which introduces additional risk. Encouraging your employees to take personal responsibility and to think and act in a security conscious way is crucial at this time. This can help prevent incidents and breaches from happening.

During COVID-19, poor employment screening processes could enable an insider to recognise the value in being able to access sensitive information or equipment. Having a strong security culture will act as a deterrent to insider activity by ensuring the workforce have a good understanding of security awareness, and ensure they understand how to report concerns where

they notice behaviour of concern. The way in which you employ people may also have changed during this period. As restrictions have been put in place for personal interviews as a response to the COVID-19 pandemic, it is increasingly likely that interviews for either recruitment, HR, vetting purposes or even line managers will be required to be undertaken via a telephone or online.

It is important to preserve the trust already established with employees, despite serious disruptions caused by such events as the COVID-19 pandemic. Disruption can have a negative effect on how some employees perceive or trust their employers, especially in how the latter responds to the crisis. If there is a breakdown in trust and employees see limited efforts to support them during the crisis, some might seek to undertake unauthorised insider acts for their own benefit or even just to exact revenge against their employers.

Hostile actors and criminals may act anonymously online in an attempt to connect with people who have access to valuable or sensitive information and one of the biggest threats that's has emerged during the pandemic so far is the use of online phishing techniques by hostile actors to exploit concerns about COVID-19.

If you want to help your staff make an even greater contribution to your organisation's security, our 45-minute free online Action Counters Terrorism e-Learning course can be done at any time from home on a laptop or tablet.

You can also download our free Action Counters Terrorism App, containing clear links to our protective security advice, from Google or Apple.

Our best wishes to you and your teams over the coming weeks, and thanks as always for your support

The NaCTSO team