CORPS RELAY

Prepared by: Mike Bluestone & Neil Shanks

Date: August 2021

CORPS SECURITY

COVID-19: Lockdown Restrictions Lifting

Reports suggest that August 2021 will see the lifting of the majority of COVID-19 restrictions across the UK. Wales, Scotland and England are removing the greatest number of restrictions (from 7th August, 9th August, and 16th August respectively), with social distancing and mask wearing being recommended but no longer mandatory, no more restrictions on indoor mixing, and venues returning to their pre-COVID occupancy numbers. Furthermore, under-18s and adults that have received two vaccinations will no longer be required to self-isolate when returning from Amber List Countries, nor will fully vaccinated adults be required to self-isolate after contact with someone with a confirmed case of COVID-19. Adults are expected and encouraged to return to the workplace. Scotland is expected to maintain some restrictions including face covering for public transport and some areas are still requiring venues to collect customer details.

The Northern Ireland Executive are expected to discuss their COVID restrictions further on the 12th August however, until then, up to ten people from three households can meet indoors, up to fifteen people can meet outdoors (no limit on households), and close-contact services are open, amongst other reduced restrictions.

Bank Fraud Investigations

Monzo, the UK-based digital bank, announced in their annual report that they are being investigated by the Financial Conduct Authority (FCA) over compliance with UK money laundering regulations. Records from 01/10/2018-30/04/2021 are currently being examined following an increase of £2.7m in compensation paid by Monzo to compensate customers that have been victims of fraud. The total compensation paid to Monzo customers that were victims of fraud in the last financial year was £9.5m. The bank have previously admitted concerns over their procedures for preventing financial crime.

£61 Million Privacy Settlement by Zoom

Zoom were undoubtedly one of the most recognisable emerging names from the COVID-19 pandemic. However, despite their popularity and the perceived security of the Zoom platform, the company has settled a £61 million ($85 million) class-action lawsuit in the US related to a series of privacy breaches. These include allegations that Zoom mislead users into believing the platform offered end-to-end encryption, failed to prevent breaches that resulted in sharing millions of users' data with other companies (including Facebook, Google and LinkedIn), and failing to prevent non-authorised/invited individuals from joining calls (also known as 'Zoombombing'). Whilst Zoom have maintained their innocence despite reaching the settlement, they have committed to increasing their security procedures. It should also be noted that Zoom were previously investigated by the National Crime Agency in relation to Zoom calls being hijacked by individuals that streamed inappropriate images of children and a separate issue of abuse footage to children taking part in a Zoom fitness class.

Rise in Drug Poisoning Related Deaths

The Office for National Statistics (ONS) have published a report detailing the trends of deaths resulting from drug poisoning up to 2020. The Deaths related to drug poisoning in England and Wales: 2020 registrations shows that not only have the deaths related to drug poisoning increased but they are at their highest point since records began in 1993. Approximately 65% of these deaths are linked to substance misuse, accounting for 52.3 deaths per million people. The North-East of England has the highest rates of drug related deaths for the eighth consecutive year, whilst London has the lowest of any region. Males are shown to be twice as likely to die of drug poisoning as females. This trend continues in Scotland and Northern Ireland, where drug related deaths have also been increasing year on year.

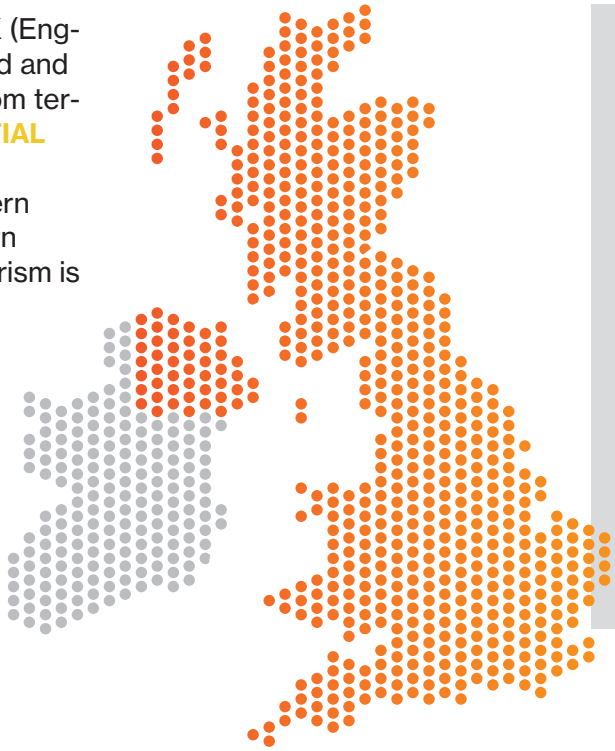
Access Control Systems Code of Practice (3rd Edition)

The National Security Inspectorate (NSI) have published their third edition of the Code of Practice for the Design, Installation, Commissioning and Maintenance of Access Control Systems (NCP 109). The revision was necessary due to advancements and changes with the technology used in access control since the second edition was published. These include new considerations around cyber security measures and new requirements for IP network installation. The third edition will become mandatory for all NSI NACOSS Gold and Systems Silver approved companies from 31 May 2022.

Current National Threat Level

The threat to the UK (England, Wales, Scotland and Northern Ireland) from terrorism is **SUBSTANTIAL**

The threat to Northern Ireland from Northern Ireland-related terrorism is **SEVERE**



NOTE:

Threat levels are designed to give a broad indication of the likelihood of a terrorist attack

LOW means an attack is highly unlikely

MODERATE means an attack is possible, but not likely

SUBSTANTIAL means an attack is likely

SEVERE means an attack is highly likely

CRITICAL means an attack is highly likely in the near future

Recent Developments

Role of the Taliban as UK and US forces leave Afghanistan Threat from Daesh in Africa

Whilst the conflict in Afghanistan has been a controversial point within British politics, the threat to the West posed by extremist groups has rarely been disputed. The threats are not only those of physical harm through terrorist attacks, but also more subtle attacks on Western ideologies through anti-Western propaganda. As the US and UK withdrawal continues, Chief of Defence Staff, General Sir Nick Carter points out that UK involvement in Afghanistan prevented further attacks like the 9/11 attack. Presently there is a significant degree of fighting taking place in Afghanistan, with the Taliban believed to be holding approximately 30% of the country at present, whilst actively trying to take major cities by force. This appears to come as part of the Taliban's move towards taking Helmand, once the centre of British operations in the country. If they are successful in deposing the sitting government and taking control of Afghanistan, the impact this could have on security in countries that actively opposed them will require careful monitoring.

Recent Developments

Iranian Cyber Attack Research

A file of classified documents alleged to have been written by the Shahid Keveh, a unit that is part of the Iranian Islamic Revolutionary Guard Corps' (IRGC) cyber command. The documents, which were obtained by journalists at Sky News, show particular focus on companies/activities in the UK, US, France, and other Western Countries. The documents include a list of various buildings and infrastructure where they can remotely control various aspects including heating, lighting, and ventilation. Furthermore, there is evidence that the files show the collection of targets that can be attacked at an opportune moment for the attacker, the point of which is not detailed. The more concerning contents of the documents includes suggestions of how cyber attacks could be used to target and sink cargo ships, supported by information collected about the global shipping industry satellite communications device, as well as how an attack could be used to blow up a petrol pump.

Notable Dates/Events

Key Religious or National Celebrations

There are significant days for several religions and nations throughout August. It is not only important to be mindful of these dates to celebrate our diverse society, but also because several terrorist groups have been known to select these days to carry out their actions.

For a full list of key dates, events and demonstrations, please view the "Corps Events Calendar" in CorpsSecure, our online customer portal or app.

Notable dates in August include:

- 10th August – Al-Hijra/Islamic New Year & Muharram – an Islamic celebration
- 14th August – Anniversary of the Westminster Car Attack– key event anniversary
- 15th August – Assumption of Mary – a Christian celebration
- 22nd August – Raksha Bandhan – a Hindu celebration
- 30h August - Janmashtami – a Hindu celebration
- 30h August – Eid-al-Adha - Islamic celebration

Demonstrations

- 1st August – The annual African Reparations Protest event, hosted by The Reparations March UK group and supported by Stop the Maangamizi (African Holocaust), is to take place at Windrush Square, Brixton from 10:00. This event has previously been a march, however it is believed this year will be a static protest the same as it was last year.
- 1st August – pro-Palestinian event entitled “Big Ride For Palestine” culminates in the final leg from Luton to London (Mile End Park, Tower Hamlets at approximately 16:00)
- 1st August – Animal Rights Protest – Kingston-upon-Thames
- 3rd August – Pro-Palestinian protest by Palestine Action, Palestine Solidarity Campaign and Oldham Peace and Justice outside Elbit Ferranti (Cairo House, Oldham). This has been advertised as a repeat event taking place every Tuesday.
- 4th August – Animal Rights Protest – Carnaby Street (Westminster)
- 7th August – Animal Rights Protest – Cardiff, Yeovil, & Leicester Square (Westminster)
- 7th August – Anti-Dairy Protest entitled “Dairy Still Kills” are to hold an outreach event in Leicester City Centre followed by leafletting at an unknown location north of the city
- 7th August – Norwich Livestock Market Animal Vigils are to stage a protest at the Livestock Market on Hall Road, Norwich, coinciding with the “Fur and Feather Sale” at the market at 11:00
- 15th-20th August – Anti HS2 Protest “Roll Back The Tracks” Bike Ride from Wigan to Birmingham. Details as yet unknown.
- 23rd August – Believed to be the starting point of Extinction Rebellion’s “Summer Rebellion 2021”. London is believed to be the target of this action as it coincides with a further reading of the Climate and Ecological Emergency Bill and the passage of the Police, Crime, Sentencing and Courts Bill to the House of Lords.

The Insider Threat Revisited

Corps Focus: Security Issue of the Month

The Insider Threat is an area of continuing risk to businesses. Despite the fact that the October 2020 Edition of Corps Relay included this as the Issue of the Month, correctly identifying it as a present and growing risk to business, the evolution of this risk justifies it being revisited. The Insider Threat has proved to be one of the main security risks throughout the COVID-19 pandemic as it has evolved with the changes in working practices.

Research suggests that there has been a significant growth in data breaches caused by insiders, with the Verizon 2021 Data Breach Investigation Report suggesting Insiders could be responsible for around 22% of security incidents. This supports other research suggesting that the increase in frequency of incidents involving Insider Threat rose by 47% between 2018-2020. Current predictions for 2021, based around the rise in remote working, suggest that Insiders could be responsible for up to 33% of security incidents. If this prediction is accurate it means a 100% rise in Insider Threat driven security breaches.

There are many things that businesses can do to help prevent themselves from falling victim to the Insider Threat. These include, but are not limited to:

- *Reviewing and updating the Insider Threat Risk Assessment*
- *Reviewing the lone working, remote working, and management supervision policies/ procedures to ensure they meet the businesses current requirements/operating style*
- *Ensure that all relevant cyber security precautions are taken and where this may clash with certain systems, a resolution is found that does not leave the system vulnerable to attack*
- *Ensure that all devices have up-to-date software*
- *Educate staff on the Insider Threat, including the dangers of social media (this includes LinkedIn)*
- *Educate staff about staying safe on-line, including password safety and selection*
- *Encourage all staff to complete the ACT counter terrorism training to assist them in what keys to identify if someone/something does not seem to be right*
- *Ensure that employees are engaged with regularly and, where possible, in person*
- *Where engagement occurs virtually, ensure that there remains full engagement with staff and staff are encouraged to identify anything that doesn't seem right – This may not always be linked to the Insider Threat, but it may help identify someone that needs additional support*
- *Ensure that management supervision is completed, and this includes engaging with employees about their welfare*
- *Ensure that devices, such as removable storage, cannot be used on work devices unless they have been encrypted and issued by the Company*
- *Ensure all staff are aware of the process for reporting lost work devices*
- *Ensure all work issued devices are password protected, not just laptops*

Market House
85 Cowcross St
London
EC1M 6PF

07890 590352
Neil Shanks

intel@corpssecurity.co.uk
www.corpssecurity.co.uk