CORPS RELAY

Prepared by: Mike Bluestone CSyP & Neil Shanks CSyP
James Henderson MSyl
Date: November 2022

CORPS
Est. 1859
SECURITY

The Conflict between Ukraine and Russia

The war in Ukraine has had a large impact on international energy availability and this is an area that will need to be monitored in the approach to winter. The UK have shown support for Ukraine throughout the conflict but, despite claims to the contrary from Russia, the UK have not engaged in any direct military action against Russia. Russia has made several threats suggesting the potential use of nuclear weapons to defend Russia, however, Russia's ambassador to Britain, Andrei Kelin, has said that this will not happen.

Russia has reportedly destroyed 30% of Ukraine's power stations and continue to use their control of the Nord Stream gas pipelines as leverage, forcing Europe to seek gas supplies from elsewhere in the world. The result is increased gas prices and slower supply times, although the milder than usual weather in October has resulted in many countries building up some gas reserves.

Corps Consult continues to monitor the situation and provide updates, as appropriate, through further special bulletins.

Threat of UK Power Outages

The energy crisis in the UK may be set to move beyond increased prices to the consumer, to reduction of service, as the Government warn of potential power outages due to shortages in gas supply. Approximately 50% of the electricity in the National Grid comes from gas fuelled power stations and the UK is exploring contingencies in the event the supply is insufficient. Supply could become a problem if there are further impediments in importing gas, but also if there are unexpected increases to electricity demands in the UK e.g. additional requirements due to severe cold weather increasing heating in domestic and commercial properties. Ofgem have warned that Britain could face severe gas shortages this winter and, whilst Programme Yarrow details plans to mitigate the risks of power outages, where power outages do occur they have the potential to impact on the security and operational provision for businesses. Please note certain businesses, such as hospitals, will be protected.

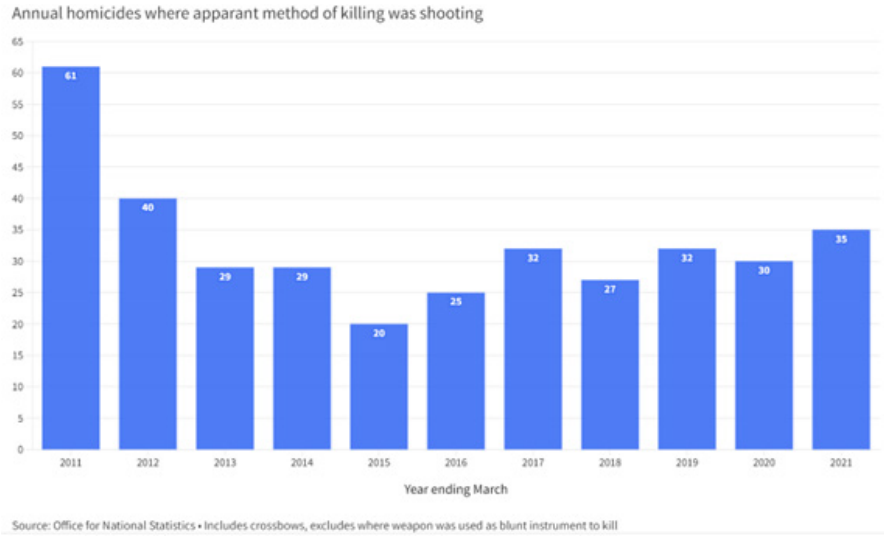
The Government has mooted the possibility of power outages lasting 3hours being shared across the UK on a rolling schedule. The schedule looks to group the UK into eight regions and impact each for 3 hours per day, with times varying across the week. Businesses should consider the impact this could have on their sites, including, but not limited to:

- CCTV Systems
- Security Alarm Systems
- Access Control Systems
- IT Systems/Data Centres
- Fire Alarm Systems
- Communications systems

Considerations should include, but not be limited to:

- Will my system still operate?
- Am I dependent on other locations that may be affected separately (e.g. remote servers)
- Do I have a back-up system (generator, UPS, battery system)?
- How long will my back-up last and do I need to limit my back-up to key systems only?
- Will my locks fail open or locked, and if the former, can I mechanically secure them?
- Do I need additional staff to secure my premises?
- Will site systems reset automatically, or do they need an intervention?

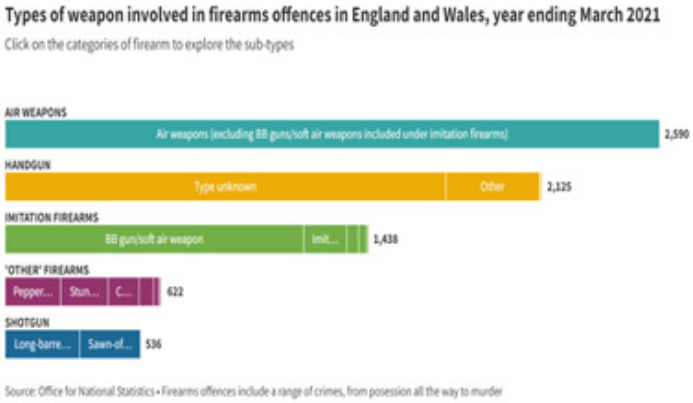
Increases in Gun Related Crime in the UK



The latest Office for National Statistics (ONS) figures on homicides (murders and manslaughters) involving shootings only cover the year ending March 2021 (2020/2021). These show an increase in shooting homicides that year across England and Wales – despite a drop in both overall homicides and firearms offences in general during Covid. There were 35 killings in 2020/21, five more than during 2019/20 and a nine-year high (see graph above).

Whilst crime statistics previously showed a 10% decrease in firearms offences in the year up to June 2022, this was then followed by eight fatal shootings reported in England and Wales between 19th July and 22nd August 2022. These included four in London, three in Liverpool and one in Manchester. The rate of shootings during that period was twice the daily average for 2020/21 at 0.2 per day (figures for Northern Ireland and Scotland are published separately).

The ONS also publishes statistics on firearm offences, the latest of which cover the year to March 2022. These show there was a slight annual increase in the number of gun crimes recorded by police in England and Wales in 2021/22 – 5,752, up from 5,715 the year before (+1%). This does not include offences involving air weapons, of which there are thousands each year.



Whilst these figures show very high levels of weapons involved in firearms offences, some sources suggest that there is also a link to improved recording of crimes.

The National Crime Agency (NCA) are currently running a campaign to raise awareness of the UK's firearms legislation and stop illegal firearms from entering the country. The NCA state if you have information on the whereabouts of illegal firearms, please contact the police or get in touch with the independent charity Crimestoppers online or on 0800 555 111 to stay 100% anonymous.

The Cost of Living Crisis, Recession, and UK Crime

Is the increased pressure of the cost of living crisis likely to have an impact on criminal activity within the UK? Will this be exacerbated by reports that although the number of food banks are at record highs, they are struggling to get sufficient donations to service their patrons? Will the reports from the Bank of England suggesting the UK is entering a recession that could last two years have an impact as this is yet another factor that has a direct relationship with criminal activity?

The most recent crime statistics for England and Wales, which cover June 2021-June 2022, show some interesting trends. The main headlines are:

- There appears to be a continuation of the reduction in thefts from the COVID-19 period, with theft showing a 19% reduction compared with year ending March 2020.
- Reports of fraud have significantly increased during COVID-19 and are back at their pre-pandemic levels (the same as the year ending March 2020)
- The Telephone-operated Crime Survey for England and Wales (TCSEW) identified an increase in computer misuse offences during COVID-19, however, the rise during the pandemic has been countered by an approximate 27% drop post-pandemic, suggesting that it was a feature of the pandemic rather than a permanent culture shift in criminal activity

The statistics currently available do not include the crime rates from July 2022 onwards, and as such, are yet to include the sharp increase in the cost of living due to inflation and all of the 8 rises to the Bank of England Bank Rate from Just 2021-June 2022. The Bank Rate is 12 times higher than it was in December 2021 and poses a genuine threat to individuals with high borrowing (including mortgages). This is compounded further when the value of properties is considered, as these have not just stopped increasing in value, but in many cases have started to reduce.

The result of increased financial demands, a recession, and a devaluation of high value assets means there is potential for job losses within some businesses, further driving the risk of individuals turning to crime to make money. Fraud is likely to continue to increase, and the risk of insider threat from employees under increased pressure financially is also increased.

Businesses should ensure they take reasonable steps to protect themselves and their employees from both fraud and the insider threat, in addition to maintaining appropriate levels of physical security for their sites, assets, and personnel. Guidance around protecting against fraud and the insider threat can be found in the “Security Issue of the Month” section at the end of this document.

Manchester Arena Inquiry Report – Volume 2

Following on from the publication of the Manchester Arena Inquiry Volume 1 in June 2022, Volume 2 is now available to read. As stated in our July Corps Relay, Volume 2 focuses on the response to the emergency including the planning and preparedness of the responders to the attack. Corps Consult will be sharing a Special Bulletin in November that reviews the conclusions and recommendations from Volumes 1 & 2 of the Inquiry and what they mean for businesses and the UK. Figen Murray OBE, the driving force behind Martyn's Law which has developed into the Protect Duty, gave an incredibly powerful presentation at an event hosted by Corps Security and the Royal Opera House. Within her presentation she addressed the night of the Manchester Arena Bombing, the impact of the immediate aftermath, the lasting legacy of that night, and the importance of passing the Protect Duty legislation. Her presentation, which was a moving first person account of the impact of terrorism, was recorded and can be viewed here.

Christopher Middleton CSyP joins Corps Security

Corps Security welcomes Chris Middleton as a Director with responsibilities for Major Accounts & Strategic Development. Chris has over 19 years of proven and demonstrable leadership experience, having worked in, and consulted with, a wide range of clients in the security and facilities management sector. Chris joining Corps Security means Corps Security now have three Chartered Security Professionals, a professional certification that is recognised globally as certifying the holders as having achieved the gold standard in competence and commitment in protective security. Chris also won the Outstanding Security Contract/Director Award at the Outstanding Security Performance Award (OSPA) 2022. This appointment demonstrates Corps Security's continued commitment to supporting and enhancing the professionalism within the Security Sector.

Phone Security – TikTok, WhatsApp and Pegasus

In the digital age the smartphone is probably the most commonly used communications and entertainment device used on a daily basis. It is increasingly common for people to use the same device for their work and personal life, with applications such as Microsoft Office 365 and cloud-based storage allowing people to move seamlessly between these worlds. Whilst this appears, on the face of it, to be a logical approach, the likelihood and implications of breaches are not as obvious.

Unlike traditional computers (including laptops and desktops) mobile phones lack the processing power to include robust cybersecurity precautions without it impacting on the user experience. Which is more, it is possible to inadvertently download applications and software that compromise a mobile phone without the user being aware. Examples of this include:

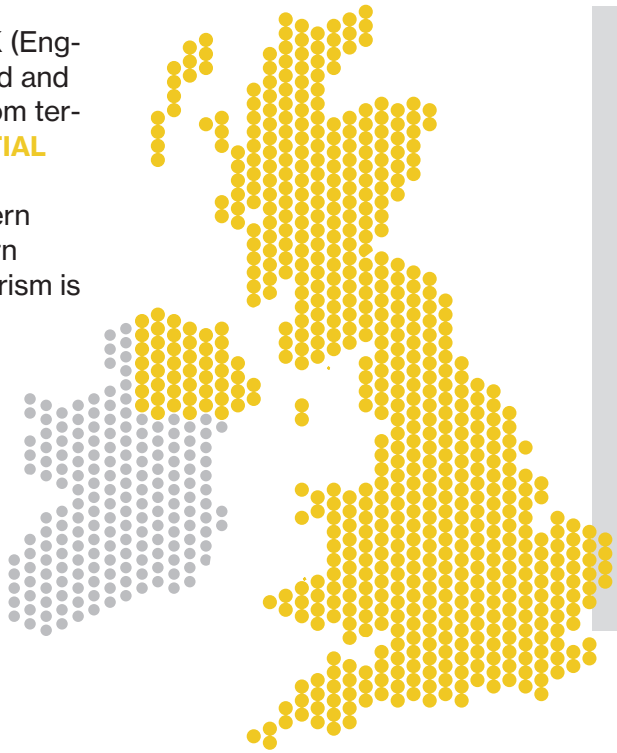
- **Pegasus Spyware** – Sitting at the upper-end of attack tools, Pegasus is a type of spyware that infiltrates a mobile phone and has the ability to collect personal and location data and control the devices features (including the microphones and cameras), all without the user's knowledge or permission. The most concerning thing about Pegasus spyware is that, unlike most malware and the earlier iterations of Pegasus, the latest version of Pegasus has "zero-click surveillance capabilities". This means it can infect devices without the victim having engaged in the process at all (no click required). Pegasus then passively collects data from the device, including an undetected keylogger and collecting the login credentials from the device.
- **TikTok** – A recent confirmation, which shocked many, is that TikTok users in the UK have consented to their devices data being accessible to TikTok employees in other continents. This includes being accessed in China, Brazil, Canada, Israel, the US, and Singapore. The transfer of data from the UK/EU to China has been the area which has caused the most controversy, not least because contracts between Chinese and European companies can't prevent access by the Chinese Government to that data. There has been an investigation into the "transfers by TikTok of personal data to China" opened by Ireland's data watchdog (who oversee TikTok across the EU.
- **WhatsApp** – The secure messaging App recently fixed a critical security vulnerability that had allowed cybercriminals to infect victims' devices with malware during video calls. This occurred through a vulnerability in the WhatsApp component "Video Call Handler" which permitted the cybercriminal to gain full control over their victims' device once triggered.

The vulnerabilities highlighted in the three scenarios above demonstrate the necessity for companies to have tight security controls in place for all their employees' digital devices as their companies' data can be at risk if they do not. A network is only as good as its weakest entry point, which may well be an employee's personal mobile device.

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 **SUBSTANTIAL**



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

Terror Attack at Immigration Centre

There have been two incidents at immigration centres in England, the first of which showed signs of extreme right-wing terrorist ideology. Andrew Leak, a man who has been banned from multiple social media platforms for sharing his extreme right-wing views, committed suicide in a petrol station after attacking an immigration facility in Dover with homemade incendiary devices. The attack on October 30th 2022 has now been classified as a terrorist attack due to evidence collected post incident from key witnesses and digital media devices.

The second incident occurred at approximately 02:00 on Saturday 5th November, when riot police were called to respond to violence at the Harmondsworth immigration removal centre. The incident occurred during a power outage and involved a group of detainees leaving their rooms and entering the courtyard of the facility armed with makeshift weapons. The result was resolved without any injuries to anyone and the reason for the disturbance remains unclear. The location has been the subject of a government report last year which raised concerns with the living conditions of the detainees, deeming them as below acceptable standards and high levels of vulnerability amongst detainees, although there is no suggestion this was the reason for the unrest on the 5th.

There is nothing to suggest any link between the two incidents.

Notable Dates/Events

Key Religious Events, National Celebrations, and Anniversaries
There are significant days for several religions and nations throughout November. 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.

Notable dates in November include:

- 1st November – All Saints Day – a Christian celebration
- 1st November – Day of the Dead/Dia de los Muertos – an international celebration
- 8th November – Birthday of Guru Nanak Ji – a day honouring the founder of Sikhism
- 11th November – Remembrance Day – an international event
- 13th November – Remembrance Sunday – a national event
- 14th November – Birthday of His Royal Highness King Charles III – an international event
- 14th -20th November – Road Safety Week – a national campaign
- 18th November – Children in Need – a national event
- 21st November-18th December – FIFA World Cup – an international sporting event
- 20th November – AJEX Jewish Military Association Parade – Whitehall
- 24th November – Jain New Year – a Jain celebration
- 24th November – Thanksgiving – a US celebration
- 30th November – St Andrew's Day/Feast of St Andrew – Scottish national celebration and Christian celebration

Prevention of Fraud and the Insider Threat

Corps Focus: Security Issue of the Month

Fraud
The Metropolitan Police have provided these Ten Golden Rules to prevent fraud:

Remember these ten golden rules to help you prevent fraud and beat the scammers:

- Be suspicious of all 'too good to be true' offers and deals. There are no guaranteed get-rich-quick schemes.
- Don't agree to offers or deals immediately. Insist on time to get independent or legal advice before making a decision.
- Don't hand over money or sign anything until you've checked someone's credentials and their company's.
- Never send money to anyone you don't know or trust, whether in the UK or abroad, or use methods of payment you're not comfortable with.
- Never give banking or personal details to anyone you don't know or trust. This information is valuable so make sure you protect it.
- Always log on to a website directly rather than clicking on links in an email.
- Don't just rely on glowing testimonials. Find solid, independent evidence of a company's success.
- Always get independent or legal advice if an offer involves money, time or commitment.
- If you spot a scam or have been scammed, report it and get help.
- Don't be embarrassed about reporting a scam. Because the scammers are cunning and clever there's no shame in being deceived. By reporting it, you'll make it more difficult for them to deceive others.

Another really useful tool is "The Little Book of Big Scams" by the Metropolitan Police. This booklet provides an overview of many of the current types of fraud being used and the techniques favoured by criminals. As always, forewarned is forearmed.

Insider Threat
The Cybersecurity & Infrastructure Security Agency (CISA) have provided a useful set of tools around mitigating the insider threat, based on the principles of:

- **Define**
  - What is an Insider
  - What is Threat
  - Types of Insider Threat
  - How does the threat manifest
- **Detect & Identify**
  - Threat Detection
  - Threat Indicators
  - Progression to Malicious Intent
- **Assess**
  - Threat Management Team
  - Threat Assessment Process
  - Assessment Criteria
- **Manage**
  - Management Strategies
  - Intervention and Prevention Considerations
  - Law Enforcement

More information on Insider Threat Mitigation from CISA is available here.

Market House
85 Cowcross St
London
EC1M 6PF

07890 590352
Neil Shanks

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