

CORPS RELAY

Prepared by: Mike Bluestone & Neil Shanks

Date: January 2022

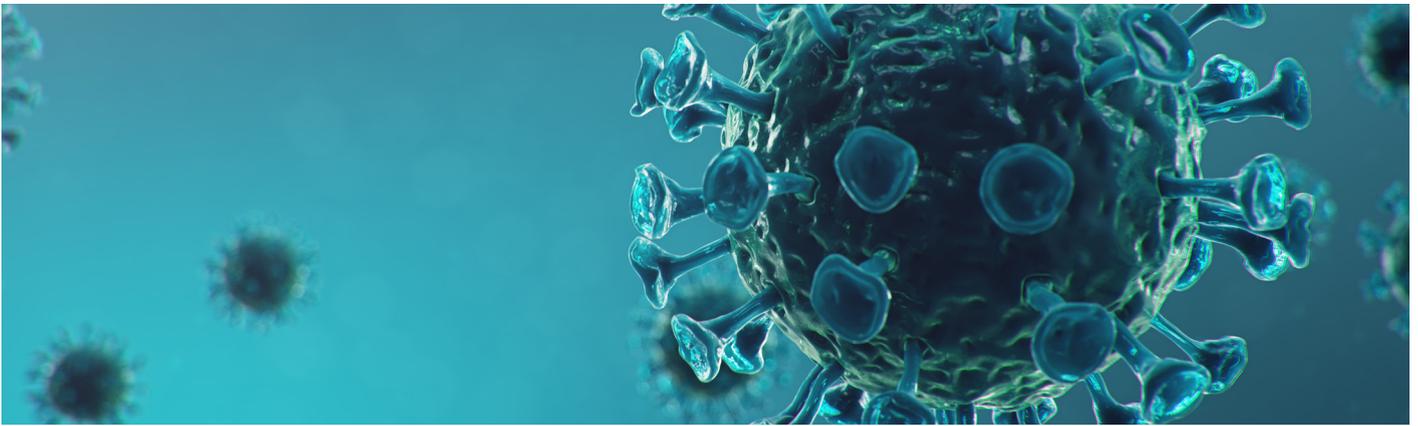
CORPS
SECURITY

COVID-19: UK still operating at different levels in COVID response

The UK continues to operate at different levels of COVID response. Details of the current COVID restrictions for each area are available from the associated .GOV website.

As restrictions are reintroduced or, in some cases, lifted, criminals continue to identify opportunities.

One of the latest developments involves [fraudsters that have been selling fake COVID test passes online](#). Companies and individuals should be mindful not to post images of their lateral flow tests.



Protect Duty Consultation Response Document

On Monday 10th November the Government published the [Protect Duty Consultation Government Response Document](#). The document contains an outline of why the consultation took place, a summary of the key themes within the responses (including statistical analysis), and an indication of how this will influence the Protect Duty considerations. The 40-page document explores the responses inline with four sections, namely: =who (or where) should legislation apply to; what should the requirements be; how should compliance work; and how should Government best support and work with partners. To follow on from the Protect Duty [Corps Relay Special Bulletin](#) published in December 2021, Corps Consult will also publish a Special Bulletin in January 2022 to provide an overview of the Protect Duty Consultation Response Document.



Log4shell – Vulnerability in widely-used logging tool Log4j

A [critical vulnerability in the Log4j](#), a widely used logging tool, was identified in late November, with a patch issued in December 2021. Log4j is used by organisations, governments and individuals worldwide when running online services. The National Cyber Security Centre (NCSC) have advised that although fixes have been issued, if they are not implemented “...attackers can break

into systems, steal passwords and logins, extract data, and infect networks with malicious software.”. Many groups have been taking advantage of the Log4Shell vulnerability and continue to do so on unpatched systems. The [Digital Security Team for the NHS](#) reported an active exploitation of Log4Shell vulnerabilities in unpatched VMware Horizon servers.

Google release Chrome patch to address Critical vulnerability

[37 security issues were identified affecting Google's Chrome web browser, with one being identified at a severity level of Critical.](#) The discovery of the vulnerability in November 2021 is credited to Yangkang, a Security Researcher of Qihoo 360 ATA, and is said to relate to a use-after-free bug in the Storage component. The impact of this could be used to either pass code to the victim's device or even allow the attacker to take control of it. Google have released the first of their updates for 2022 which addresses this issue.



Huawei accused of involvement in Australian Telecom Hack

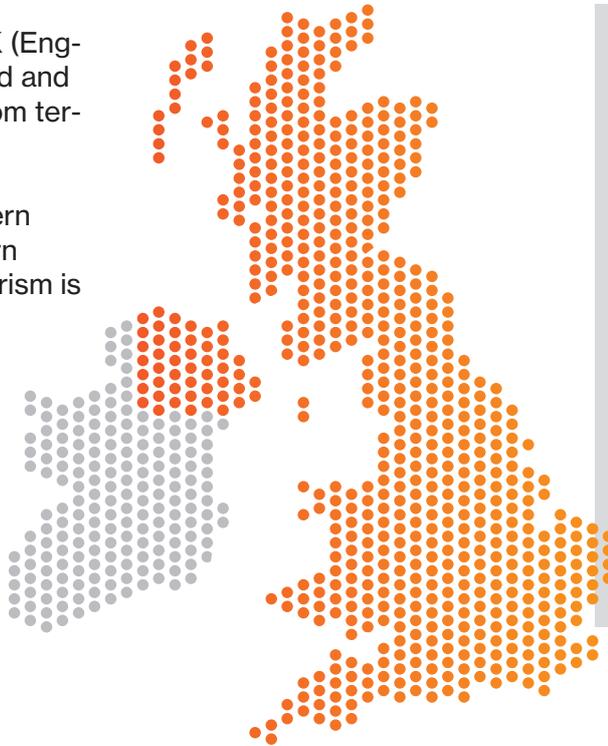
An investigation by Bloomberg News is reporting they have found evidence that a 2012 Australian telecom breach, which was previously unreported, has links to Huawei. Within the report it is stated that [Australian intelligence officials informed the US that a Huawei software update was “...loaded with malicious code”](#). Whilst the attack that this refers

to occurred nearly 10 years ago, this issue remains relevant due to the current questions raised regarding the security of various similar technology companies.

Current National Threat Level

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

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

Security Minister states COVID Lockdowns may have increased radicalisation

The Security Minister, Damian Hinds MP, has stated that he believes the effects of [lockdown secluding individuals may have led to a rise in radicalisation online](#). He stated "... more people who are spending more time in their bedrooms at their computer ... you are going to get a growth in that tiny proportion

of people for whom that is a dark journey...". The increase in online radicalisation was highlighted as part of a section in the [July 2021 Corps Relay](#) about the number of Terrorist Suspects that are under 18.

Alpha Men Assemble – Anti-Vaccination Group

Footage has emerged of a newly formed anti-vaccination group calling itself Alpha Men Assemble holding “boot camps” which included participants receiving training as part of their “global war”. Alpha Men Assemble was formed in December 2021 and have urged activists to target vaccine centres, schools, colleges, counsellors and directors of public health. The rhetoric being used is very combative, with phrases such as “take it to the Old Bill”, whilst others mocked the moderate practices used by other anti-vaccination groups.

Video footage taken from a park in Staffordshire shows approximately 100 volunteers being trained to march in formation and to use certain kickboxing techniques. Despite this group being very new there are already over 7,000 subscribers to their encrypted communications channel on Telegram. They plan to meet at Strathclyde Country Park (Motherwell, North Lanarkshire) at 11:00 on 29th January for another training session and may have other dates/locations planned.

Notable Dates/Events

Key Religious or National Celebrations

There are significant days for several religions and nations throughout January. 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 January include:

- 1st January – New Year’s Day – an international event
- 6th January – Storming of the Capitol – key event anniversary
- 6th January – The Baptism of Christ – a Christian celebration
- 7th January – Charlie Hebdo Attacks – key event anniversary
- 8th January – Thornton Heath Stabbing 3rd Anniversary – key event anniversary
- 9th January – Whitemoor Prison Attack 2nd Anniversary – key event anniversary
- 9th January – The Baptism of Christ – a Christian celebration (Roman Catholic)
- 14th January – Makar Sankranti – a Hindu celebration
- 25th January – Burns Night – a national event
- 27th January – Holocaust Memorial Day – an international event



Storming of the United States Capitol 06.01.2022 (2021)

A year on from the storming of the United States Capitol (as reported in the [February 2021 edition of Corps Relay](#)) and the topic remains live in international news. President Biden gave a speech on Capitol Hill condemning the actions of both the individuals that stormed the Capitol

Building and the then President, Donald Trump. This incident, whilst geographically removed from the UK, remains one requiring monitoring due to the influence it continues have on individuals and groups within the UK.

Charlie Hebdo Attacks 07.01.2022 (2015/16)

Friday 7th January 2021 marked the 7th anniversary of the attack on the Charlie Hebdo Offices in Paris, France, in 2015 and the 6th anniversary of the 2016 attack that took place on the first anniversary of the Charlie Hebdo attack.

2021 was a quieter year in regards to Charlie Hebdo following a troubled end to 2020 (see the 2020 [September](#), [October](#) and [November](#) editions of Corps Relay for more information).

2nd Anniversary of Whitemoor Prison Attack

On Thursday 9th January 2020 two serving [prisoners at HMP Whitemoor \(Cambridgeshire\)](#) stabbed [Prison Officer Neil Trundle](#). They were

using weapons they had made themselves and wore fake suicide vests.

Demonstrations

Kill the Bill

It should be noted that the Police, Crime, Sentencing, and Courts Bill is being debated and voted on in the House of Lords during January 2022 (between the 10th-17th). This Bill previously resulted in a number of protests and demonstrations around the country, with areas including Bristol, London, and Manchester seeing a number of arrests after some protestors became violent.

Whilst there are no events currently advertised under Kill the Bill, there are events associated with the Bill taking place. XR are planning a number of events although specific times and locations are currently unknown. The dates of the known events are:

- 15th January – National Day of Action
- 10th-17th January – Vote on the Bill in the Lords



Will 2022 be the year of integration and convergence?

Corps Focus: Security Issue of the Month

There is always a great deal of speculation of what a new year will bring, and with 2020 and 2021 offering arguably the biggest changes in workplace since the computer revolution in the 80's and 90's, the question is as poignant now as ever. Security must be proactive and either anticipate, or quickly react to, the changing demands of the environment it is being applied to. Therefore, as the workplace evolves, so must the security provision designed to protect it. To enable Corps Consult to do this affectively we actively engage with our Clients regarding the current and future nature of their workplace, as well as actively following the industry experts in workplace planning and the anticipated future use of the workplace.

2020 and 2021 saw the rise in popularity of hybrid working models where employees could work from both the office and home. These had previously existed in many sectors, albeit often for a select group of employees, and this provided advantageous for those companies when initially adapting to the COVID-19 lockdowns. The majority of employees did not have remote working capabilities requiring an investment in technology, both systems and devices, from companies to ensure they could continue to operate. The physical/digital requirements of this provision were business critical and at times the new regime was implemented before the necessary amendments to

the companies' policies and procedures were fully identified. This, along with less direct oversight and increased job insecurity, contributed to the rise in risk of insider threat.

Whilst many businesses have returned to an operating model similar to their pre-COVID-19 state, there remain a large number of businesses that have decided to continue with hybrid working practices. A full review of the risks and threats from the new working model should have been conducted by this point and it is likely that these will also identify a change in use of the physical premises occupied by businesses. These may include reducing the space required by the business or maintaining the same volume of office space but reducing the number of employees permitted to work in it (incorporating a degree of social distancing). Many businesses have either reduced their operating hours due to the reduction of staff on the premises or increased their operating hours to allow for revised shift times to reduce inter-departmental mixing.

In addition to the changes in employee access to sites, there may have also been large changes in the way visitors/customers access the site. Time and attendance has become more important than ever before, often requiring employees and visitors to identify when they will attend a site, and where



Will 2022 be the year of integration and convergence?

they will go. The use of digital systems can help with the administration of this process and, where this is taking place, there is a natural next step in incorporating this with the access control or time and attendance technology. The technology facilitating smart buildings are becoming more capable and this, in turn, allows for a greater level of detail to be applied to the buildings security systems e.g. only an employee that is registered to work has live access credentials, or, a building automatically sets the passive infrared sensor (PIR) to detect movement.

The changes in the buildings' use, and the technologies that have been adopted, will undoubtedly have an impact on the requirement for physical security on site. It may be that increased opening hours now require an increased security presence on site, or conversely, the reduction of staffing in the building could require additional physical presence outside of core hours as part of the buildings fire regulations. There have been a number of businesses that have utilised Security Officers to monitor vacant premises, providing not only security for those premises, but often also monitoring key functions on behalf of facilities or maintenance colleagues.

Where buildings have had a significant reduction in occupation this has, at times, resulted in the reduction of physical security personnel. This was achievable through reviewing the options of alternatives to those functions, which include: automation of certain functions (e.g. access control); providing remote operation of functions via a Control Room or Monitoring Centre (e.g. CCTV, Access Control, Alarm Monitoring);

implementing mobile patrols; and implementing a physical or remote lock/unlock service for the building. Whatever the case, it is imperative that the impact of any changes is assessed prior to making them, with policy and procedure adjusted accordingly. There may be new/additional security considerations resulting from a change in service/staffing and these must be fully risk assessed.

Many businesses that outsource their security provision either have, or will, ask their security providers "is the security provision for the site still fit for purpose?". This is a very reasonable question and needs to take into account the multifaceted make up of a site's security provision in relation to its operational requirements. This encompasses areas including the physical security provision on site (e.g. Security Officers), the security systems (e.g. access control system, building alarms, CCTV), non-security systems (e.g. visitor management, HR systems), the site's operational requirements, and potentially associated roles/fields (e.g. H&S, Front of House, Facilities). There are many examples of diversification, convergence, and system integration being adopted in response to changes in the workplace and Corps Security can assist with ensuring these are not only fit for purpose but optimised.

The use of convergence here represents both the bringing together of multiple functions under one role and the standardisation of practices to allow this to work effectively. The convergence of multiple functions under the umbrella of the Security Officer is not new. There is long standing precedence for additional non-security roles, responsibilities and duties being reassigned to



Will 2022 be the year of integration and convergence?

security teams.

Diversifying the role of the Security Officer is often a popular way of consolidating roles/duties with certain areas proving to be highly successful. There is a lot of scope for Security Officers to provide additional support with evidence shown in functions such as H&S and front of house customer service and support roles. Corps Security have had great success with Security Officers taking greater roles in supporting Facilities Managers with various site checks, as well as Officers taking greater responsibilities in the customer facing front-of-house roles and switchboard.

The key to effective role convergence is establishing how to complete these duties without it preventing the Security Officer from fulfilling their primary function of protecting the site. Corps Security and Corps Consult regularly conduct reviews to identify areas for increased efficiency for Clients, often identifying new technology or processes that can achieve additional functionality without leaving the site vulnerable e.g. where Security Officers are required to provide a mailroom function, franking letters on site is preferable to taking them to a local Post Office as this does not remove them from site. Integration of a site's technical systems is another method that is being widely adopted. The basic principle of integration is to combine separate systems together in order to create a whole (system) that is greater than the sum of its individual parts. Systems all contain different information that, if combined, can provide a far greater understanding of what is happening, in turn providing vastly improved functionality. Common

systems that can be integrated to improve performance include access control, CCTV, building/fire alarms, building management systems (BMS), reporting systems, visitor management systems, HR databases, and communication systems. The combination of these allows systems to respond automatically to information provided by other systems, collecting data and taking necessary action, whilst also reducing the amount of duplicated work significantly.

It is likely that many reviews into the optimum security provision for a site will have a certain financial focus. Whilst this is undoubtedly important, it is vital that this is balanced against the risks that are being mitigated. Businesses should remain conscious of the impact of the Protect Duty that is expected to be brought into law in 2022 (more information can be found in the Protect Duty section above and the [Corps Relay Special Bulletin](#)) as this is likely to contain a number of requirements for businesses in relation to their security provision.



Market House
85 Cowcross St
London
EC1M 6PF



07890 590352
Neil Shanks



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