ISSUE 16: **DECEMBER 2022**

LEAD MEDIA PARTNER THE SECURITY EVENT

MEDIA PARTNER INTERNATIONAL SECURITY EXPO

www.securitymattersmagazine.com

Security MATTERS

The Independent Voice for Security and Risk Professionals

Surveillance reform

Government's proposals for legislation in focus
Read more on pages 20-22

From The Editor

Global Security in Challenging Times

In delivering the 2022 Royal United Services Institute Annual Security Lecture, Sir Jeremy Fleming (director of GCHQ) asserted that the Chinese Communist Party's (CCP) "fear" of losing its grip on power, its own people and the international rules-based system is threatening global security.

Fleming said that the Chinese leadership is using its financial and scientific muscle in a bid to dominate strategically important technologies, from digital currencies through to satellite systems. While the UK and its allies seek science and 'tech' advancement to enable prosperity, the CCP wield it as a "tool to gain advantage through control of their markets, of those in their sphere of influence and of their own citizens".

Fleming highlighted the paradox that China's "great strength combined with fear is driving the nation into actions that could represent a huge threat to us all". Warning of the immediacy of the threat, he said now is a "sliding door moment in history" that "will define our future". The science and 'tech' community in like-minded countries "must act to tackle it".

Addressing an invited audience at the Science Gallery in London, Sir Jeremy Fleming observed: "The Chinese leadership believes it draws its strength and authority from the closed one-party system. They seek to secure their advantage through scale and control. This means they see opportunities to control the Chinese people rather than looking for ways in which to support and unleash their citizens' potential. They see nations as either potential adversaries or potential client states to be threatened, bribed or coerced."

Sense of fear

Fleming continued: "The Party has bet its future on this approach, shutting off the many alternative futures for the Chinese people in the process. They hope that future success, based on this system, will be inevitable. I think underlying that belief is a sense of fear. Fear of its own citizens, freedom of speech, free trade, open technological standards and alliances: the whole open democratic order and the international rules-based system. It's no surprise that, while the Chinese nation has worked to build its advanced economy, the CCP has used its resources to implement draconian national security laws, a surveillance culture and an aggressive use of military might."

In addition, Fleming stated: "We're seeing that fear play out through the manipulation of the technological ecosystems which underpin our everyday lives, from monitoring its own citizens and restricting free speech through to influencing financial systems and new domains."

Further, Fleming warned how China is seeking to create "client economies and Governments" by exporting technology to countries around the world. According to Fleming, these countries risk "mortgaging the future" through buying in Chinese 'tech' with "hidden costs".

While highlighting the challenge, Fleming urged key players in the science and technology community to "think beyond the illusion of the inevitable" and "recognise the fact that creating an alternative, competitive and compelling offer for technology is an opportunity for wider society that we simply cannot afford to miss".

Sir Jeremy noted: "At GCHQ, there are times when it's our privilege and duty to see the sliding door moments of history. This feels like one of those moments. Our future strategic technology advantage rests on what we as a community do next. I'm confident that, together, we can tilt that in our nation's favour."

Conflict in Ukraine

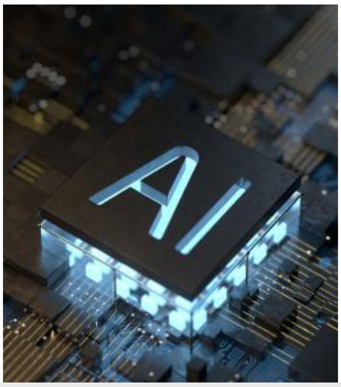
During the speech, Fleming touched on the war in Ukraine: "Far from the inevitable Russian military victory that its propaganda machine spouted, it's clear that Ukraine's brave action on the battlefield and in cyber space is turning the tide. Having failed in two military strategies already, Putin's plan has hit the courageous reality of Ukrainian defence."

Continuing this theme, Fleming asserted: "With little effective internal challenge, Putin's decision-making has proven to be flawed. It's a high stakes strategy that's leading to strategic errors in judgement. Their gains are being reversed. The costs to Russia – in both people and equipment – are staggering. We know – and Russian commanders on the ground know – that their supplies and munitions are running out. Russia's forces are exhausted. The use of prisoners to reinforce, and now the mobilisation of tens of thousands of inexperienced conscripts, speaks of desperation."

The Russian population has started to understand that. They're seeing just how badly Putin has misjudged the situation. What's more, they are now beginning to realise the extent of the dreadful human cost of their leader's 'war of choice'.

Brian Sims BA (Hons) Hon FSyi
Editor

China is seeking to create "client economies and Governments" by exporting technology to countries around the world. These countries risk "mortgaging the future" through buying in Chinese 'tech' with "hidden costs"



Features

Regulars

Editorial
Editor
Brian Sims BA (Hons) Hon FSyI
Telephone: 07500 606013
bsims@westernbusiness.media

Designer
Alex Romer

Advertising
Sales Manager
Leanne Velez
Telephone: 01342 333727
lvelez@westernbusiness.media

Production
Sharon Miller
Telephone: 01342 333741
smiller@westernbusiness.media

Circulation
circ@perception-sas.com

Directors
Mark Sennett
Keith Gabriel
Danny Kosifou

Company
Western Business Media Limited
Telephone: 01342 314300
admin@westernbusiness.media
www.securitymattersmagazine.com
Printed by Cliffe Enterprise

N1
NO
NGND
SHIELD
RS-485
OVERRIDE
TAMP
0V
INPUT; 12–24VDC; 0.18A
(CONTROLLER ONLY)
READER1
+V
LED
INPUT
RTE
DC
SIG A (D0)
(D1)
0V
pac®
511 DCi
ACCESS CONTROLLER
TCPIP
LOCK
NC
NO
COM
RELAY
NC
NO
COM
SECURITY SIGNALING
LISTED EQUIPMENT 4T99
UK CA
READER2
+V
LED
SIG B (D0)
(D1)
0V
https://pacgdx.com/support/pac-product-literature
LINK TO MANUALS AND HELP VIDEOS
VIN
0V
POWER
MSTAT
LOCK
0V
EARTH
ACCESS
ONE TOUCH
STATUS
BARCODE
LED DC RTE DOOR2

(ISC)² research reveals 3.4 million shortfall in cyber security workforce

(ISC)² – THE non-profit association of certified cyber security professionals – has highlighted a stark increase in the shortage of trained and qualified cyber security professionals.

The findings of its 2022 (ISC)² Cyber Security Workforce Study reveal that the global cyber security workforce is now at an all-time high, with an estimated 4.7 million professionals operational. However, despite adding 464,000 more cyber security professionals this year, the data suggests that 3.4 million more cyber security workers are needed going forward to secure assets on an effective basis.

70% of respondents report that their organisation does not have enough cyber security employees. More than 50% of respondents with workforce shortages feel that staff deficits put their organisation at a 'moderate' or 'extreme' risk of a cyber attack.

For those organisations looking to mitigate staff shortages, the research suggests that initiatives designed to train internal talent, rotate job assignments, encourage mentorship programmes and entice employees from outside of IT or the security team to join the field are the most effective.

At the same time, the report finds that 72% of respondents expect their cyber security staffing numbers to increase somewhat or significantly within the next 12 months. Indeed, this is the highest predicted growth rate when compared to the last two years (53% in 2021 and 41% in 2020).

"As a result of geopolitical tensions and macroeconomic instability, alongside high-profile data breaches and growing physical security challenges, there's now a greater focus on cyber security and, as a result, an increasing demand for professionals within the field," explained Clar Rosso, CEO at (ISC)², to Security Matters.

Government reviews CONTEST strategy in concerted bid to address emerging threats

THE GOVERNMENT is going to conduct a "wholesale refresh" of the UK's counter-terrorism strategy to protect citizens from new, emerging and persistent threats.

In the UK and overseas, there has been a shift towards self-initiated terrorists operating independently from organised groups with increasingly personal ideologies and warped views used to justify violence. The tactics and methodologies employed by terrorists are diversifying and becoming increasingly fragmented.

To meet those threats, the Government's counter-terrorism strategy (ie CONTEST) will be updated to reflect these new challenges. This will involve seeking a diverse range of views and engaging security experts from across the UK and overseas such that CONTEST continues to robustly protect the British public from terrorist threats.

Commitment to core values

Security Minister Tom Tugendhat noted: "Terrorists seek to divide us and sow hatred. We will not let them. Our commitment to the core values we cherish is too strong. As the nature of terrorism continues to evolve and endure, so must we. We will ensure our response to the terrorism threat continues to be world-leading and also that we have a strategy in place that allows people to go about their lives freely and with confidence."

The Government's timely update will take into account a series of important reviews, including the second volume of the Manchester Arena Inquiry. In addition, the findings from the Independent Review of Prevent, led by William Shawcross, will strengthen the Government's ability to stop individuals from being drawn into terrorism in the first place.

The Government will do everything possible to strengthen the UK's protection against terrorist attacks. This includes a renewed commitment to introduce the Protect Duty, which will enhance the safety of public venues, while also avoiding the placement of any additional burden on the shoulders of small businesses.

The UK's counter-terrorism system already encompasses the efforts of more than 20 separate Government departments and agencies.

Since 2017 alone, upwards of 200 recommendations have been implemented in response to terrorist

attacks, including the creation of the world's first multi-organisational Counter-Terrorism Operations Centre in London last year.

Enduring framework

Matt Jukes, head of Counter Terrorism Policing, observed: "Since its launch back in 2003, CONTEST has proven to be an enduring and effective strategic framework for the UK's counter-terrorism response, but it absolutely shouldn't stand still."

Dukes added: "Today's threat is dominated by increasingly fragmented ideologies, self-initiated terrorism and the reach of hateful online ideologies into the lives of young people. Any future strategy must reflect these learnings."

"Security managers lack influence over security budgets" reports Security Research Initiative

THE SECURITY Research Initiative (SRI) has just published its latest report. Entitled 'The Role of Security in Influencing the Budget', the aim of this study – sponsored by Axis Communications, Bidvest Noonan, interr, M&S, Mitie, OCS, PricewaterhouseCoopers, the Security Industry Authority and Sodexo – was to explore the extent to which security managers are able to influence the security budget, whether (and why) this matters and also examine how greater influence can be attained.

Results are based on the views of security professionals from both in-house and contract positions (predominantly those currently in a 'security manager/director'-type role) collected via an online survey and several interviews.

The survey outcomes make for particularly interesting reading. 76% of those security professionals surveyed agreed that being able to influence the budget is key to delivering good security.

Influence over the budget was considered important for several reasons. It's deemed to afford status to security in discussions with other departments, in turn enabling security advice and proposals to commonly be listened to, while also helping to direct the allocation of resources using relevant expertise.

A lack of influence here means that security managers cannot purchase basic and essential resources or plan effectively, duly resulting in security decisions being made by non-experts.

Levels of influence

Some 51% of respondents in a current security management role had a high level of influence on the budget. 10% were 'not involved'.

Further, 46% of security managers/directors thought that their current budget was 'insufficient' (whereas 42% believed that it was 'sufficient').

Unsurprisingly, those with the highest levels of influence over the budget were the least likely to view it to be insufficient in scope.

Half-year financial results posted by Mitie Group highlight "strong performance"

MITIE HAS released its half-year results for the six-month period ending 30 September 2022. Performance is "strong" with new contract wins and recent acquisitions more than replacing the short-term revenue boost from COVID-related contracts in the first half of 2022.

Guidance for the full year has been increased with operating profit before other items expected to be at least £145 million. Revenue of £1,923 million has been recorded.

A total contract value of £1.5 billion was added during H1, with renewal rates standing at over 90%. Operating profit before other items was £68.0 million.

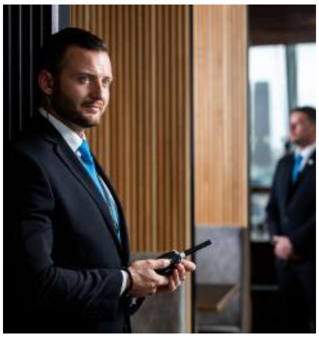
Commenting on the first six months of the year, Phil Bentley (Group CEO at Mitie) said: "Our strong performance in the first half of 2022 reflects good underlying momentum across all divisions. Our strategy is very much based on delivering underlying revenue growth and cost savings from our margin enhancement initiatives."

Business Services

Mitie's Business Services division delivers security solutions (among other services). For the last two years, Business Services was also primarily responsible for the delivery of Mitie's short-term COVID-related services across COVID-19 Testing Centres and quarantine services. These contracts ended early in Q1 FY23.

Revenue of £592.2 million was 24% lower than for the same period last year (H1 FY22: £775.0 million) due to the ending of the COVID-related contracts. Excluding the £12 million revenue from short-term COVID-related contracts in H1 FY23 (H1 FY22: £245 million), revenue increased by 9%.

Operating profit before other items of £32.9 million was 50% lower than for the same period last year (H1 FY22: £65.2 million). Excluding the £2.6 million contribution from short-term COVID-related contracts in H1 FY23 (H1 FY22: £40.8 million), operating profit before other items increased by 24%.



The total contract value of £616 million has been derived from new, renewed or extended contracts including renewals for Sainsbury's, Vodafone and Superdrug alongside the expansion of the Marks & Spencer contract and new wins involving Afghan Relocations and Assistance, Sky Studios and Netflix.

Business Services has mobilised three significant contracts in Q1 FY23 for BAE Systems, Hammerson and Poundland worth £27 million of annualised revenue.

Strong first half

In general, Business Services enjoyed a strong first half, winning new contracts and delivering margin enhancement initiatives to partially offset the loss of the prior year's revenue and profit from the short-term, higher margin COVID-related contracts. Excluding the COVID-related contracts, revenue, operating profit and margin all increased.

Business Services realised £425 million in total for contract renewals or extensions.

Professional Security Officer Live set for launch at Nineteen Group's The Security Event 2023

PROFESSIONAL SECURITY Officer Live is set to make its debut at The Security Event, which runs at the NEC in Birmingham from 25-27 April 2023.

This brand new 'show within a show' organised by the Nineteen Group will feature alongside the award-winning The Security Event (for which Security Matters serves as the Lead Media Partner), duly realising a dedicated concentration on front line security professionals.

Tristan Norman, Group director at the Nineteen Group, informed Security Matters: "Launching Professional Security Officer Live demonstrates our commitment to the security industry. It's a market we know very well. Our research has shown that there's a genuine demand from our exhibitors, partners and visitors to recognise the critical role that security personnel, operatives and front line professionals play in the security sector on a daily basis."

Never seen before and long overdue in the eyes of many commentators, Professional Security Officer Live will host major industry brands from the security guarding sector, all of whom will be showcasing the latest products, services, technologies, training and solutions that enable security personnel to perform their vital duties in protecting people, places and assets.

Supported by a comprehensive free-to-attend conference that will highlight and address key issues within the sector – among them training and certification, career pathways, the skills and talent shortage, standards, health and well-being and physical protection – Professional Security Officer Live is warmly welcomed and supported by leading industry stakeholders including the International Foundation for Protection Officers (IFPO), the International Professional Security Association, Skills for Security, The Security Institute and, in addition, ASIS UK.

Mike Hurst CPP MSyI, director and chair of the Advisory Board at the International Foundation for Protection Officers in the UK and Ireland, observed: "IFPO is dedicated to advancing the role of the security officer through education, certification, developing career pathways and supporting mental health and well-being. We are delighted to support Professional Security Officer Live and look forward to the show."

Register online now at ***www.thesecurityevent.co.uk***

FSM AWARDS
15 JUNE 2023 • CBS ARENA • COVENTRY
FIRE & SECURITY MATTERS AWARDS
ENTRIES NOW OPEN
Headline Sponsor
aico

Fire and Security Matters Awards 2023 open for entries

ENTRIES ARE now open for the Fire and Security Matters Awards 2023 organised by Security Matters and Fire Safety Matters – both of which are published by Western Business Media – in conjunction with the Fire Industry Association (FIA).

The inaugural Fire and Security Matters Awards generated more than 220 entries last year, while 450-plus guests attended the awards ceremony. The 2023 scheme is free to enter and designed to recognise excellence and innovation in the fire and security business sectors.

The winners of the Fire and Security Matters Awards will be revealed at a gala dinner and ceremony to be held at the CBS Arena in Coventry on Thursday 15 June 2023, which will be hosted by popular television comedian and Mock The Week captain Hugh Dennis.

It only takes a few minutes to enter the Fire and Security Matters Awards. It's the perfect way to gain much-deserved recognition for yourself, your team, your colleagues, a client, a product/service, a project/campaign or your organisation.

The list of security categories for 2023 is as follows:

- Security Manufacturer of the Year
- Security Guarding Company of the Year
- Security Installation Company of the Year (Sponsored by simPRO Software)
- Security/Risk Manager of the Year
- Security Company of the Year
- Security Team of the Year
- Security Project of the Year
- Security Industry Woman of the Year
- Security Innovation of the Year

The deadline for entries to be received is Tuesday 31 March 2023. Enter the Fire and Security Matters Awards 2023 for FREE at ***https://firesecurityawards.com/award-categories***

G4S awarded £12 million security contract by LLDC

THE LONDON Legacy Development Corporation has awarded G4S a four-year contract, worth in the region of £12 million, to provide security services for the Queen Elizabeth Olympic Park (including all of the open spaces, parklands and venues, among them The London Stadium – the home of West Ham United Football Club).

G4S will be operating under a framework agreement for the provision of security services at the location. That agreement will be used by the London Legacy Development Corporation, LS185 and Stratford Waterfront.

G4S is set to provide security services for the entire London Legacy Development Corporation land, as part of which the business will ensure the availability of key roles including security managers, security team leaders, security officers, CCTV specialists and also car park operators.

Further, G4S will monitor CCTV assets and systems located in the venues, the public realm and the wider Queen Elizabeth Olympic Park site via dedicated Security Control Suites.

As part of the agreement, G4S is going to deliver security services at Queen Elizabeth Olympic Park events, with those services including access control, ticket checking, search procedures and patrolling duties.

Chris Burr, managing director for G4S Events UK, informed Security Matters: "G4S is delighted to have been awarded the prestigious security contract for the iconic Queen Elizabeth Olympic Park and The London Stadium. We are now very much looking forward to working closely with the London Legacy Development Corporation."

**Photograph: Arne Müseler www.arne-mueseler.com CC-BY-SA-3.0 (Linked to https://creativecommons.org/licenses/by-sa/3.0/de/deed.de)*

Control Risks forecasts "historically broad and deep" set of risks for businesses in 2023

BUSINESSES WILL face an "historically broad and deep" set of risks in 2023, posing interconnected and existential threats across geographies and sectors. That's according to specialist risk consultancy Control Risks.

Launching its annual Risk Map forecast featuring the foremost risks for the business world, Control Risks has pointed towards a combination of fractious geopolitics, armed conflict, disrupted energy systems, economic strife and disarray in digital networks during the coming year, with cyber risk at the top of the agenda.

In 2023, the company suggests we can expect the emergence of a "fundamental breakdown" of global networks into distinct regional or even national architectures, caused by the 'weaponisation' of cyber space and a clash of national interests. The ambition of operating a single global network, suggests Control Risks, will be "significantly challenged".

Enabled by an expanded attack surface and a significant increase in automation across the entire spectrum of cyber threats, the cyber arms race will accelerate in 2023. In parallel with this 'weaponisation', nation states are looking to exert more control over what some have already defined as their national cyber space. The strongly held belief is that network and system resilience will be tested like never before.

Nick Allan, CEO at Control Risks, explained: "In the fragmenting world order, the 'weapons of choice' for many states will be found in the cyber sphere. This will either be through the spread of disinformation, aided by improving deepfake technology, or otherwise through cyber attacks or perhaps both."

Further, Allan explained: "2023 will see more geopolitical and economic volatility accompanied by operational challenges in energy and digital networks. The increasingly apparent effects of a changing climate will add additional stresses and strains. We feel that resilience, insight and courage will be the watchwords for business in the year ahead."

Operational risk

Operational risk is going to be all about managing while adapting to and surviving the energy disruption. Energy has returned as the main driver of global disruption and, states Control Risks, this will be a permanent and systemic change.

There will be no return to a pre-2022 stability and businesses should plan not only to survive the short-term price and supply shock, but also for how they can thrive in a new and comprehensively re-wired global energy system.

Royal United Services Institute signposts new projects designed to combat illicit financial flows

THE CENTRE for Financial Crime and Security Studies at Think Tank the Royal United Services Institute (RUSI) has welcomed ongoing co-operation with the National Endowment for Democracy, which builds upon previous work centred on empowering civil society and journalists to combat corruption.

A new grant supports three complementary workstreams: the continuation of the project entitled 'Restricting Kleptocracy: Strengthening Monitoring and Accountability in the First Mile', as well as two new initiatives entitled 'Countering Authoritarian Abuses of the Financial Action Task Force Standards' (FATF) and 'The European Sanctions and Illicit Finance Monitoring and Analysis Network' (SIFMANet).

The first phase of the 'Restricting Kleptocracy' project engaged civil society and investigative journalists in Latin America, East Africa and the Western Balkans with workshops on anti-financial crime standards. The discussions unveiled several areas that could further support grassroots communities in holding kleptocrats and corrupt actors in their countries to account.

The project will continue with a deeper focus on developing understanding of beneficial ownership transparency and asset recovery mechanisms and how this knowledge can be useful for investigative and advocacy work.

Countering abuses

The findings of the 'Restricting Kleptocracy' project demonstrate an interplay between the tactics of kleptocrats and autocrats: kleptocracy (and the laundering of its proceeds) erodes faith in public and democratic institutions, while autocracy serves to pave the way for leaders to engage in kleptocratic behaviours.

While appealing to recognised standards allows civil society to hold kleptocratic Governments to account, such norms have been 'weaponised' by authoritarian Governments to suppress critics.

National Audit Office document outlines Government's progress on combating fraud

GOVERNMENT DOES not know the full scale of the fraud threat posed to individuals and businesses and is not yet leading an effective cross-Government strategy to tackle it. That's the view of the National Audit Office (NAO) as outlined in its 50-page report entitled 'Progress Combating Fraud'.

The Home Office is responsible for preventing and reducing fraud. It does so in partnership with many bodies including the National Crime Agency (which, of course, hosts the National Economic Crime Centre), the City of London Police (the national lead force for fraud), other Government departments, the finance, technology and telecoms sectors and international partners.

Around 80% of fraud offences in the UK are enabled through computer technology, including by criminals who can operate remotely anywhere in the world.

In its 2017 report 'Online Fraud', the NAO concluded that fraud had been "overlooked" by the Government, law enforcement and industry, and demanded an urgent response. Since then, the threat from fraud has increased and evolved, but the number of fraud offences resulting in a charge or summons has fallen. Collated crime figures highlight that fraud was the largest category of crime in England and Wales in the year ending June 2022, amounting to 41% of all crimes against individuals compared to 30% in the year ending March 2017.

Number of incidents

The estimated number of incidents of actual and attempted fraud against individuals in England and Wales rose by 12% from 3.4 million in the year ending March 2017 to 3.8 million for the year ending June 2022. However, the number of fraud offences resulting in a charge or summons has dropped from 6,402 in 2017 to 4,816 in 2022.

According to the NAO, there are still "significant gaps" in the Home Office's understanding of the threat from fraud. Based on 2015-2016 data and on 2015-2016 prices, the Home Office estimates that the cost of fraud to individuals is £4.7 billion. It doesn't harbour any reliable estimate of the cost of fraud to businesses.

The Home Office also has what the NAO asserts to be a "limited understanding" of who actually commits fraud and those who enable it by their action (or inaction).

The Government has launched different strategies covering fraud and economic crime, but has not yet established what outcomes it wants to achieve. Strategies have covered a range of topics including cyber security, anti-corruption and serious and organised crime, making it somewhat challenging for the Home Office to focus and co-ordinate the activities of partners.

In April last year, the Home Office announced its desire for a Fraud Action Plan to set a national approach between 2022-2025. In March 2022, Government instead unveiled plans for a new Fraud Strategy in order to build on the initial development of the Fraud Action Plan.

Genetec issues alert on cyber security risks posed by legacy access control systems

GIVEN THE rise in cyber crime, unified security solutions developer Genetec is cautioning organisations of all sizes to be extremely vigilant about the cyber security risk posed by legacy access control systems.

"Many organisations are operating with access control systems that date back ten years or more," explained Christian Morin, vice-president of product engineering and chief security officer at Genetec. "While these older systems still allow employees to 'badge' in and out, there's a very high likelihood that they employ technologies which are now particularly vulnerable to modern cyber threats."

Vulnerabilities in legacy access control systems can introduce cyber security weaknesses that may put an entire organisation at risk. Cyber criminals can exploit weaknesses in access control system credentials, controllers, servers, readers or workstations connected to the network.

Once a cyber criminal has breached access control system credentials, they can then move on to an organisation's network and gain control of other building systems, view or steal confidential information from internal records or even launch attacks designed to take key systems offline.

Best Practice

To improve the cyber security of access control systems, Genetec recommends several key steps:

- Upgrade the system. Older systems were not built to address today's threats. When evaluating a new access control system or upgrading an existing system, make sure that cyber security is a key component of the vendor selection criteria
- Use advanced secure credentials and the latest communications protocols to secure data transmission since older credentials are easy to clone using readily available tools
- Educate employees and partners about cyber security Best Practice and ensure they are prompted to change passwords on a regular basis
- Regularly check for firmware and software updates and install them once available
- Use a centralised identity access management system in order to ensure virtual and physical authentication and the authorisation of employees for better control and, in addition, somewhat more effective maintenance of systems

CPNI launches "pioneering" course for security Control Room operators

IN ITS role as the national technical authority for physical and personnel protective security, the Centre for the Protection of National Infrastructure (CPNI) has launched a new training course aimed squarely at security Control Room operators.

The course and associated guidance produced by the CPNI enables businesses and organisations alike to plan and prepare for – as well as respond to – terrorist incidents, thereby increasing the capabilities of security Control Room operators and other security personnel.

Uniquely based around research undertaken since 2017, the course offers "world-first" immersive exercises that simulate multiple terrorist incident scenarios, enabling delegates to practice decision-making in real-time as if they were in a real Control Room environment.

The course is informed by the recently updated guidance, developed through detailed analysis of previous terrorist incidents, extensive research that has included live simulations of attacks and, further, detailed surveys of existing Command and Control capabilities.

Effective Command and Control is critical for mitigating the impact of terrorist incidents. Sites are unlikely to provide an effective response to a terrorist incident unless security Control Room personnel are provided with the appropriate equipment, policies and procedures and operators are given the necessary training and time to practice and exercise the response.

The course is specifically designed for operators who work in security Control Rooms within national infrastructure sites and crowded places. It's also valuable for those directly responsible for security Control Room operators

Spaces on the five-day training course will be available from January 2023 onwards.

Glencore to pay £280 million for "highly corrosive" and "endemic" corruption

GLENCORE ENERGY UK Ltd will pay £280,965,092.95 million (ie over 400 million US dollars) after a Serious Fraud Office (SFO) investigation revealed that the company paid US$29 million in bribes to gain preferential access to oil in Africa.

Sentencing at Southwark Crown Court on Thursday 3 November, Mr Justice Fraser stated: "The facts demonstrate not only significant criminality, but sophisticated devices to disguise it".

The Judge sentenced the commodities trading giant to pay a financial penalty in response to the seven charges of bribery representing "sophisticated offending sustained over prolonged periods of time".

Mr Justice Fraser also remarked on the culture that developed at Glencore "in which bribery was accepted as part of the West Africa desk's way of doing business... The corruption is of extended duration... It was endemic among traders on that particular desk... Bribery is a highly corrosive offence. It quite literally corrupts people and companies and spreads like a disease."

Commenting on the financial penalty – the largest ever for an SFO case following a conviction, in fact – Mr Justice Fraser noted: "This is a significant overall total. Other companies tempted to engage in similar corruption should be aware that similar sanctions lie ahead."

Guilty plea

Back in June this year, Glencore pleaded guilty to seven counts of bribery after an SFO investigation exposed that the organisation had paid bribes to maximise its oil trading profits in five African countries.

The conviction includes the first-ever use of substantive bribery offences for a company. Senior individuals at Glencore authorised the bribery instead of simply failing to prevent it from occurring.

The financial penalty ordered by the Judge includes a fine, a Confiscation Order for the profit Glencore obtained from bribes and the SFO's costs in full.

The Confiscation Order is not only the largest-ever for an SFO case, but the total amount the company will pay is the highest-ever ordered in a corporate criminal conviction.

The SFO opened an investigation into Glencore in 2019 focused on the activity of the London-based West Africa desk. This desk sourced and traded in crude oil.

The investigation uncovered a trail of text messages, large cash withdrawals and concealed payments that showed Glencore paid bribes worth a total of US$29 million to secure its access to oil in Cameroon, Equatorial Guinea, Ivory Coast, Nigeria and South Sudan.

£100 million-plus money laundering scam leads to multiple convictions

SIX DEFENDANTS – including a senior manager and two drivers of a road haulage business – have been found guilty of running a large-scale money laundering operation involving in excess of £100 million in cash.

Marcus Justin Hughes, the effective operator of road haulage business Genesis 2014 (UK) Ltd, has been convicted at Stoke Crown Court of one count of conspiracy to launder cash together with Leon Woolley, a transport planner at the firm.

Nicholas Fern and Damion Morgan, both drivers working for Hughes, were convicted of a single count of conspiracy to launder cash over a period of months.

Liam Bailey, another transport planner at the firm, and Simon Davies (a business associate of Hughes) were each convicted of one count of conspiracy to launder money.

The Regional Organised Crime Unit for the West Midlands became aware of a criminal operation to launder cash through a haulage company, namely Genesis 2014 (UK) Ltd. Hughes used an encrypted network phone, known as EncroChat, to communicate with a man in Dubai (specifically Craig Johnson, a convicted fraudster from Stoke-on-Trent).

They agreed that large sums of cash would be collected at various places in the UK and elsewhere on a regular basis with the intention of transporting it to London where it could then be transferred onwards and legitimised.

The scale of cash involved, the lack of any explanation for its provenance and the surrounding circumstances provided "an irresistible inference" that the cash was the proceeds of criminality.

The total amount of cash at issue was somewhere between £100 million and £150 million depending on the size of the loads for each journey.

ICO fines Interserve Group Ltd £4.4 million for data protection breach

THE INFORMATION Commissioner has warned that companies are "leaving themselves open to cyber attack" by ignoring crucial measures like updating software and training their staff.

The warning comes as the Information Commissioner's Office (ICO) issued a fine of £4,400,000 to the Interserve Group Ltd, the Berkshire-based construction company, for failing to keep the personal information of its staff secure.

The ICO found that the company had failed to put appropriate security measures in place in order to prevent a cyber attack, which enabled hackers to access the personal data of up to 113,000 employees through a phishing e-mail.

The compromised data included personal information such as contact details, National Insurance numbers and bank account details, as well as special category data including ethnic origin, religion, details of any disabilities, sexual orientation and, further, private health-related information.

John Edwards, the UK's Information Commissioner, said: "The biggest cyber risk businesses face is not from hackers outside of their four walls, but rather from complacency within their company. If any given business doesn't regularly monitor for suspicious activity in its systems and fails to act on warnings, or otherwise doesn't update software and fails to provide training for its members of staff, then it can expect a similar fine to be forthcoming from my office."

An Interserve Group Ltd employee forwarded a phishing e-mail, which was not quarantined or blocked by the company's system, to another employee who opened it and downloaded its content. This resulted in the installation of malware on the employee's workstation.

The anti-virus set-up quarantined the malware and sent an alert, but the business failed to thoroughly investigate the suspicious activity. If it had done so then it would have found that the attacker still benefited from access to the company's systems.

The attacker duly compromised 283 systems and 16 accounts, as well as uninstalling the company's anti-virus solution. The personal data of up to 113,000 current and former employees was encrypted and rendered unavailable.

For a globally free service of e-mail alerts, free conferences and access to our informative website:
JOIN free at www.tinyg.info and look our group up on LinkedIn

The World's Leading Counter Terrorist Intelligence & Information Sharing Platform For
15 years
TINYg

David Evans,
International Chairman &
Founder, TINYg

TINYg
Global Terrorism Information Network

TINYg (Global Terrorism Information Network) celebrated its 16th anniversary in 2022. Testimony to the value it has brought to its enormous membership in 150+ countries.

Why join TINYg?

The Benefits:

- Best practice driven by an esteemed group of global advisory council leaders drawn from law enforcement, academia, industry and blue chip organisations.
- Free to attend conferences Internationally with outstanding speakers.
- Free information alerts and information collated from our multiple partners on email.
- Access to a massive network with those who are interested in counter terrorism and closely related topics.
- An opportunity to communicate with TINYg and the membership, and the advice available.
- Remember, TINYg is the winner of the 2021 OSPA for The Outstanding Security Partnership and the largest Information Sharing Counter Terrorism Platform globally in 150 countries.

UK OSPAs
Outstanding Security Partnership
OSPA WINNER 2021

NEWS + NEWS + NEWS + NEWS + NEWS + NEWS + NEWS + NEWS

TiNYg on the road in 2022

It's been a very active 2022 so far for TiNYg taking its message on the road with presentations from leading experts in their fields and vibrant Q&A sessions through our programme of conferences. We have organised events in Stockholm in Sweden, BBC Media City in Manchester, at Barings and The Tate Modern in London and at the Disney Corporation in Burbank Los Angeles. The events created great networking opportunities for existing TiNYg members and extended our reach to new members. We have more events planned in Newcastle in September and at the US Embassy in London and even in Costa Rica in the fall.

A very busy 2023 is planned. Come and join us at one of our free to attend events.

Note:
Our NEW Level 5 Terrorism Management and Awareness courses are well worth a look at low cost and low time commitment.

INFORM

- **Providing high level physical and online events**
- **We share Best Practice**
- **Education and professional mentoring**
- **Certified Courses – Our L5 Counter Terrorism Management and Planning course, with full OFQUAL accreditation, will be available soon contact us for more information**
- **Provide articles, expert opinion and commentary on major incidents and other Counter Terrorism related issues**
- **Support the 'One to Many' messaging from key stakeholders**

INFLUENCE

- **Thought leadership**
- **Stakeholder facilitation**
- **A trusted partner on sensitive matters**
- **We provide tailor-made conferences.**

SO WHAT?

Get informed and stay ahead!

- **Members in over 150 countries**
- **Over 500,000 email alerts sent to members**
- **Over 60 International, free-to-attend, conferences**

TINYg's Premium Partners include:

The Institute's View

Through the passage of time, there's no doubt that globalisation has impacted security. Today, asserts Simon Donaldson, the security sector and the business realm in general seem to be at a tipping point of recoiling to a more nationalist agenda due to the enhanced strategic resilience challenges stemming from globalisation and the opportunities it first enabled

GLOBALISATION MAY be viewed as the integration of technology, economies and politics, regardless of geography and time. This entices security management into an environment no longer defined by local geography. Therefore, traditional approaches to security such as 'defence in depth' may no longer be wholly depended upon in order to achieve a state of 'security'. Potential risks now emanate from outside the immediate physical area and are manifested through non-kinetic means, such as IT connectivity, for instance.

This interconnectivity means that events thousands of miles away can have consequences locally. As such, it's now crucial for the security business sector to identify emerging risks and consider mitigations.

At present, there are several significant international strategic resilience challenges in play that have contested traditional security risk management approaches: COVID, cyber, the General Data Protection Regulation (GDPR), the Russia-Ukraine conflict, opportunity, supply chains, nationalism, climate change and terrorism.

Official UK statistics are reporting an increase in positive COVID cases as we enter the winter season. The frequency of sub-variants (with the World Health Organisation currently designating five COVID-19 variants of concern, in fact) also demonstrates precisely how the likelihood of such pandemics occurring is increasing.

For its part, COVID has become intrinsically linked with the risk of cyber attacks. This is due to working from home protocols expanding the surface area for such attacks and, in some reported cases, employees picking up bad cyber security habits along the way.

Managing attacks

Stemming from cyber risk is the challenge of managing the consequences of an attack that in, the UK, may constitute a breach of the GDPR. The probability of a cyber attack, as illustrated by the numerous official warnings from Governments around the world, has increased in the wake of the Russia-Ukraine conflict. While Critical National Infrastructure may be the primary target, businesses at large remain at risk.

Russia's invasion of Ukraine has resulted in a range of strategic resilience challenges and opportunities involving sanctions, significant global business decisions and supply chains being both affected and 'weaponised'. Companies including Jaguar Land Rover have suffered disruption and financial loss, while McDonalds withdrew from Russia citing the resulting humanitarian crisis.

The conflict has, however, highlighted the benefits of investing in security and how those businesses focused on security can prosper. Most NATO countries have agreed to increase defence spending since the war began. In Q1 2022, German-based firearms manufacturer Heckler and Koch reported a 22% increase in turnover to €77.5 million.

Global supply chains have been adversely affected by the Ukraine conflict, in turn realising international impacts. Russia's interference with Ukrainian grain exports caused disruption to global food supplies, with an estimated 1.7 billion individuals in more than 100 countries affected.

A nationalist view is now apparent around the world and appears to be the new dominant ideology, with politics becoming more important than economies demonstrated by Russia's invasion of Ukraine, China's relationship with Taiwan and America's withdrawal from Afghanistan.

Such nationalism in the western world – set against a backdrop of rising inflation, unstable energy markets and general cost-of-living increases in many nations – has the realistic potential to impact domestic security issues in some shape or form.

Climate change

New Delhi's decision to prioritise its own nation stems from an issue that's increasingly being accepted as a strategic resilience challenge: climate change. NATO has labelled climate change a 'threat multiplier' impacting security, with many NATO countries now declaring it a national security issue. This has the real potential to multiply existing threats, notably so in ungoverned states, in turn significantly enhancing the risk of terrorism.

Terrorism is an enduring threat to international security, with Islamist-inspired terrorism the most significant component. The rapid fall of Afghanistan to the Taliban risks the country once again becoming a safe haven for terrorists as it was considered to be pre-9/11. That's a prospect amplified by credible reports suggesting Al-Qaeda has increased freedom 'in-country' with 41 members of either the Taliban cabinet or other senior Government positions listed on the UN sanctions list for terrorism.

It has never been more timely to recognise the importance of intelligence and risk management, together with the changing nature of what constitutes security and resilience. The first steps in intelligence and risk management are the formulation of a requirement and risk identification. The modern security professional must ensure necessary intelligence is being obtained and used in decision-making and that risks are both identified and mitigated.

'Incidents' and 'emergencies' signposted within the UK Civil Contingencies Act 2004 may now last years and affect wider geography and business areas than initial business continuity plans were intended to address, forcing new ways of working within both the public and private sectors. This demands change from the security sector. ●

Andrew Donaldson CSyP FSyI is Head of Security for Real Estate Management (UK) Ltd and Co-Chair of The Security Institute's Counter-Terrorism Special Interest Group
www.security-institute.org

THE SECURITY INSTITUTE

SUNRAY
TIMBER DOOR DIVISION

Fire Door Inspections & Survey Services

Sunray Timber Door Division is a leading and accredited supplier of Fire Door Surveys and Fire Door Inspections in the UK.

- A thorough and finite detail of each and every door to determine compliance or non-compliance to passive fire protection
- Meticulous measuring and inspecting of each door to understand fire integrity and rating
- Comprehensive risk reporting
- Manufacture of bespoke Fire Rated Timber doors with fire ratings from 30 to 120 minutes including Fire Stop Partitioning and panels, Acoustic Doors, X-Ray Doors, Timber Security Doors and Flush Framed Doors.

For more details, call our specialised team
to discuss your particular project on:

01233 639039

sales@sunraytimberdoordivision.co.uk

SUNRAY
TIMBER DOOR DIVISION
www.sunraytimberdoors.co.uk

ASIS in the UK

The core subject of cyber security is high on the agenda of every organisation right across the UK and beyond. In what is now an increasingly connected world, highlights Steven Kenny, any device hooked up to the network presents a potential cyber security risk. On that basis, the development of a robust approach for reducing exposure to attack is absolutely essential

DEVICES WITH built-in cyber security controls are designed to decrease the risk of compromise and enable secure behaviours. It's important to look at the risks that exist throughout the lifecycle of any device, as well as explore the cyber security measures available and, importantly, the support provided to mitigate risk.

Ultimately, the key is to apply cyber security Best Practice in processes, policies and technologies from development all the way through to decommissioning.

Device security begins with a secure development process. This ensures that security considerations are taken into account from the outset and not addressed as an afterthought. Lack of secure development processes may lead to products being released with easily exploitable vulnerabilities.

Once that process is sorted out, cyber security should start at the most fundamental level: that of the microprocessor and the operating system, which provide the basis upon which secure products are fashioned.

An area that's often overlooked, but now acknowledged as a huge risk, is the supply chain. A lack of supply chain transparency can lead to compromised components in the final product. In the current climate of availability challenges, organisations must remain observant and maintain a robust approach towards supply chain due diligence.

Importantly, organisations should strive to keep information, systems, components, equipment, facilities, software and devices secure throughout supply. With this in mind, can your vendor ensure the authenticity of a device's firmware?

In addition, what physical security measures does the vendor have in place at their manufacturing facilities?

Distribution issues

One consideration often overlooked is the risk landscape during shipment. This risk is largely associated with the manipulation of a device's firmware or its configuration. Does the device offer features such as signed firmware and secure boot in combination with making a factory default on the device? If not, what protection is offered from malicious modification(s)?

Risks during implementation can arise from putting compromised or inadequately hardened products on the network. This may well result in unauthorised access to the network, the extraction of sensitive data or assets (such as private keys and certificates) for use in malicious attacks or otherwise enable altered data to be transferred between network endpoints. How does your vendor help you to address these issues?

While in service, a device can be exposed to threats from deliberate attacks or unintentional mistakes. Risks can arise from running firmware with known vulnerabilities that an adversary can exploit, updating devices with unauthenticated firmware or allowing secure configurations to lapse.

Today's organisations must work continuously to identify and limit the risks associated with discovered security vulnerabilities in their offerings.

To maintain the cyber security of a given device, ongoing support and making frequent OS updates are essential. Commonly, there are two ways of keeping an OS up-to-date: the active track and the long-term support (LTS) track. In the former, the OS is continually updated with new features and security patches. In the LTS track, only security patches are included in OS updates. This is an important consideration for maintaining potential third party integrations.

Efficient maintenance

For efficient maintenance while devices are in service, mature organisations offer device management tools (also known as asset management tools). The purpose of these tools is to provide an intuitive dashboard that allows all devices to be managed. Using such tools simplifies the scaling of crucial maintenance tasks, such as upgrading OS, defining, applying and enforcing security policies and managing applications.

Another important consideration is the approach to common vulnerabilities and exposures. Can the vendor demonstrate that they follow industry Best Practice in managing – and responding to – discovered vulnerabilities? An example of this is the ability to demonstrate the use of the Common Vulnerability Scoring System to rate vulnerabilities related to in-house developed code or third party open source code.

Does the organisation assess vulnerabilities in open source code according to how relevant they are for products when Best Practice recommendations are applied? Also, how does the company communicate important information about vulnerabilities and other security-related matters?

Having devices on the network that are no longer supported and have known, unpatched vulnerabilities poses a risk. Leaving sensitive data available on devices after disposal also presents a risk. What measures can be put in place to address these issues?

Staying 'cyber secure' is really all about managing risks. It's about understanding the risks, taking active decisions to manage those risks and ensuring Best Practice is implemented for active systems.

For their part, vendors should take responsibility by following Best Practice. They should also support the end user through guidance, technologies, tools and services that assist the latter in mitigating risks when using the vendor's products.

Speaking of the end user, they need to ensure that they ask the right questions and carry out thorough due diligence on vendors during the procurement process.

ASIS INTERNATIONAL™ UNITED KINGDOM

Steven Kenny is a Board Director of ASIS International's UK Chapter
www.asis.org.uk

On Inspection

In the latest instalment of his regular and exclusive series for Security Matters, Richard Jenkins explains how the National Security Inspectorate's appointment as a Transported Asset Protection Association (TAPA) Independent Audit Body for the EMEA region will help to increase resilience in the UK's supply chain, while also reducing transport-related cargo losses

THE UK is one of the most severely impacted countries for recorded cargo crime. On average, over £100,000 worth of goods are stolen from supply chains in Britain each and every day, yet this figure represents only a partial picture since the majority of cargo crimes go unreported.

According to TAPA – itself a global not-for-profit supply chain security and resilience association founded in 1997 to help supply chain operators address risk management – most reported losses do not include a loss value. In fact, during the 18-month period prior to 30 June this year, only 12.4% of the 11,332 cargo thefts across the EMEA region reported to TAPA stated the loss value; with the rest remaining unreported.

From 1 January 2020 to 30 June this year, 5,751 theft incidents from supply chains were reported to TAPA EMEA in the UK. Of those which did actually state a financial loss value, 50% of these acts of criminality involved a loss of over £100 million.

As measured by TAPA's latest survey, the most frequently stolen products included pharmaceuticals, tools and building materials as well as toys, tobacco, IT equipment, smart phones, empty trucks, car parts, metal and household appliances. These incidents occur through thefts of – and from – vehicles, trailers, containers and facilities in road, rail, aviation and maritime transportation.

Tackling the problem

Within this context, and effective from September 2022, the National Security Inspectorate (NSI) has been appointed as a TAPA regional Independent Audit Body, offering certification for TAPA EMEA's three primary standards, themselves focused on 'Facility Security', 'Trucking Security' and 'Parking Security'.

NSI Security.Improved

The NSI's fully trained auditors are now working with TAPA members, comprising manufacturers/shippers, logistics service providers, freight transport and security services companies, to support the adoption and growth of TAPA standards with a view towards minimising the number of high-value products stolen during storage in facilities or during the transportation process.

TAPA EMEA's Facility Security Requirements (FSR) protect high-value and theft-targeted products in environments such as warehouse operations, in-transit storage within supply chains and distribution centres. The FSR Standard specifies the minimum acceptable security standards and processes to be used in maintaining this standard, including specifications for service providers to follow to attain TAPA FSR Standard certification for one or more facilities.

The FSR Standard includes guidance on areas encompassing the facility's perimeter (including access points) and internal areas within warehouses and offices. FSR certification can be achieved through the NSI for both single site and multi-site operations.

There are three levels of certification as well as a self-certification option. Non-member companies may also achieve certification after completing the appropriate TAPA EMEA training course and paying the relevant training, auditing and certification fees.

Trucking security

Over 90% of cargo losses reported to the TAPA EMEA Intelligence System involve criminal attacks on vehicles. In the UK alone, upwards of 1,800 incidents of cargo crime were reported by TAPA members between August 2021 and August this year. That equates to over 23% of all incidents reported in the EMEA region, in fact.

The Trucking Security Requirements (TSR) Standard protects products transported by road with the aim of preventing criminal attacks and ensuring the safety of drivers, vehicles and cargoes alike. It's applicable to the operators of hard-sided trucks and trailers, rigid vans or fixed body trucks, sea container road transportations and soft-sided trucks and trailers. It includes guidance on management support and responsibilities, tracking and tracing, *en route* protocols, physical security and driver security training.

The third standard, covering Parking Security Requirements, is already the most adopted industry standard for secure truck parking, currently covering as it does sites in no fewer than 15 countries, but it must be stated that demand far exceeds supply.

The prevalence of crimes involving trucks in the UK is exacerbated by the severe lack of secure parking. This presents a significant business opportunity, of course, for 'Parking Place Operators' who meet the required levels of supply chain security.

Trucks parked in unclassified or unsecured parking places are involved in over 50% of the thousands of cargo losses experienced in the EMEA region and reported to TAPA. They actually account for the theft of products valued at tens of millions of Euros.

Over 95% of all recorded cargo thefts have involved attacks on trucks, while 50% of these crimes occur when trucks are brought to a halt in unsecured parking places.

Delivering a difference

The NSI's extensive expertise of auditing organisations against standards will undoubtedly help in delivering on TAPA's declared aim of driving more certifications and improving the security of transported supply chains right across the UK.

What's more, the NSI shares a common not-for-profit remit with TAPA. In bringing our experienced auditors' skill sets to bear in helping to cost-effectively tackle the unacceptable level and value of cargo thefts, we now very much look forward to playing a pivotal role in securing supply chain resilience within and across the UK. ●

Richard Jenkins is Chief Executive of the National Security Inspectorate
www.nsi.org.uk

FSM AWARDS

15 JUNE 2023 • CBS ARENA • COVENTRY

FIRE & SECURITY MATTERS AWARDS

Headline sponsor

aico

In conjunction with

FIA
Fire Industry Association
Leading Excellence in Fire Since 1916

Entries now open!

The Fire and Security Matters Awards return in 2023! Designed to honour and recognise industry professionals and teams from both the fire and security sectors, the awards promote the importance of innovation while also underlining the highest standards of excellence.

The winners will be revealed on the 15 June 2023 at The CBS Arena, Coventry. Ensure your achievements are recognised and celebrated by entering the 2023 awards.

You can enter the awards for free at:
www.firesecurityawards.com

If you are interested in sponsoring the awards, there are just a few sponsorships remaining.
Contact Leanne Velez via 01342 333727
lvelez@westernbusiness.media

Sponsors

aico · apollo · EMS · ffe Protecting Lives · THE FIRE SAFETY EVENT · Hyfire

NCAB GROUP · THE SECURITY EVENT · SIDERISE integrity in all we do · simPRO · tio connecting fire safety · UPTICK

Rule of Law

Figures issued only recently by the Department for Business, Energy and Industrial Strategy paint a stark picture of the amount of taxpayers' money lost to fraud through the Coronavirus-related Bounce Back Loan Scheme. Here, Niall Hearty assesses the gravity of the situation

THE DEPARTMENT for Business, Energy and Industrial Strategy launched the Bounce Back Loan Scheme on 4 May 2020, offering Bounce Back Loans of up to £50,000 – or a maximum of 25% of annual turnover – to support businesses during the height of the COVID-19 pandemic.

Banks, building societies and peer-to-peer lenders were accredited by the British Business Bank to pay Bounce Back Loans, which were guaranteed by Government. The scheme had limited verification, along with no credit checks being conducted on borrowers, which rendered it somewhat vulnerable to fraud and losses.

Around a quarter of all UK businesses applied to the scheme, and 1.5 million Bounce Back Loans worth £47 billion have been made. Over 90% of these – or £39.7 billion in monetary terms – went to micro-businesses with a turnover below £632,000.

When the scheme launched, the Department for Business, Energy and Industrial Strategy expected to support between 800,000 and 1.2 million businesses with somewhere in the region of £18 billion to £26 billion worth of loans.

As of March last year, the Department estimated that 11% of Bounce Back Loans worth £4.9 billion were fraudulent, although these figures were highly uncertain. The estimate excluded some types of fraud (for example, where a borrower overstates their turnover and receives a larger Bounce Back Loan). The Department also likely overestimated some losses by assuming that all fraudulent Bounce Back Loans are a loss when some funds should be recoverable.

The Department for Business, Energy and Industrial Strategy reports that, since September 2020, the National Investigation Service has opened investigations into possible Bounce Back Loan Scheme fraud totalling £160 million, even though the total amount of such suspected fraud is a staggering £1.1 billion.

Any positives?

If there are any positives to be taken from this situation, lenders have reported preventing more than £2.2 billion in fraudulent applications, meaning at least some of the fraud that was attempted never came to fruition. Yet the total amount of fraudulently-obtained funds that has been – or is set to be – recovered remains far from certain.

What's clear, unfortunately, is that a massive amount of money was lost to fraud due, at least in part, to a lack of adequate controls being in place at many banks with, in parallel, the Government prioritising rapid rather than properly thought-out action.

The fact that a large chunk of the previously quoted figure of £47 billion may never be accounted for – in the real-life rather than the book-keeping sense – reflects badly on those who drafted, approved and then rolled out the scheme.

The latest update from the Department for Business, Energy and Industrial Strategy states that up to 500,000 businesses could have permanently ceased trading in 2020 in the absence of the scheme. That being so, no-one could argue there was no need for the Bounce Back Loan Scheme.

That update observes: "It's unfortunate that some have made the decision to take advantage of this vital intervention by defrauding the scheme for their own financial gain. The Government has always been clear that anyone who sought to do so is at risk of prosecution. Checks were put in place from the outset to reduce the risk of fraudulent applications being successful. Lenders are the first line of defence and were required to make or maintain 'Know Your Customer' and anti-money laundering checks and use a reputable fraud bureau to screen applicants against potential or known fraudsters."

That quote contains the all-too-familiar noises about the Government cracking down on fraudsters. It emphasises that checks were in existence, but could be viewed as Westminster 'passing the buck' to the banks for letting so much money be lost to fraud.

Criminal planning

The Government is less inclined to emphasise its unwitting role in such fraud or explain in any detail exactly how much of the fraudulently-obtained money can – or will – be recovered and how that might be done.

Anecdotal evidence suggests that some of the proceeds of COVID-19 fraud were obtained without the need for any great degree of sophistication by the fraudsters. Many of those who set about gaining the largest amounts will have put a good deal of thought and planning into how they would go about it. That's likely to present a stern challenge to the authorities' bid for recovery.

This is a challenge that comes at a time when the Government has deemed Action Fraud unfit for purpose, with its replacement unlikely to take on any such investigation task until some point during 2024.

The Government seems unable to shake the symptoms of COVID-related fraud. The main ones appear to be large financial losses, no clear signs of a recovery in the near future and no prospect of a genuine remedy. The National Audit Office has been critical of what it sees as limited efforts to regain fraud losses and of the emphasis on speed of payments rather than anything else. ●

Niall Hearty is a Partner at Rahman Ravelli
www.rahmanravelli.co.uk

NATIONAL CYBER SECURITY SHOW

25-27 APRIL 2023
NEC BIRMINGHAM UK

UNITING THE UK APPROACH TO TACKLE CYBER THREATS AND PROTECT OUR DIGITAL WORLD

FIND OUT MORE:
www.nationalcybersecurityshow.com

Co-located with:

THE SECURITY EVENT

THE FIRE SAFETY EVENT

THE WORKPLACE EVENT

THE HEALTH & SAFETY EVENT

Media Partner:

Security MATTERS

Founding Partners:

3B DATA SECURITY · CyberSmart · Cyberfit security · CyberGuard Technologies · DARKTRACE · EQUILIBRIUM · protos NETWORKS · TecSec · Red flags from ThinkCyber

About face

Parliament is considering many pressing issues at present, among them energy price hikes, the cost-of-living crisis, the ongoing impact of the conflict in Ukraine and Brexit and strikes within the healthcare and transport sectors. Then there's the proposed legislation designed to reform public space surveillance by the police service. In this exclusive article for Security Matters, Fraser Sampson offers a personal perspective

AMONG THE less dramatic events ahead of Parliament's recess back in July was the quiet arrival of the Data Protection and Digital Information Bill in the House of Commons. Proposing many changes to our data protection regime, the Data Protection and Digital Information Bill will abolish the office of the Surveillance Camera Commissioner.

In my dual Commissioner role – one for surveillance cameras, the other for biometrics – I'm as much an exhibit for as I am a witness to the Government's recognition of the growing overlap between these areas. That they are to be split again so soon is not easily explained, but some of the key issues ahead can be readily understood.

How we understand anything depends heavily on perspective. There are three vantage points from which to view the proposals for reform in police surveillance: the technological (ie what can be done), the legal (ie what must/must not be done) and the societal (ie what people will support or even tolerate being done). Each perspective raises different questions and demands different answers in arriving at an understanding. All three converge most acutely at the point of facial recognition.

Set against that backdrop, then, let's examine each in turn and, subsequently, review the specific issues involved when it comes to facial recognition.

Technological issues

Biometric surveillance capability will revolutionise the investigation and prevention of crime and the prosecution of offenders, while the way in which that technology is used could jeopardise our very model of policing.

Public space surveillance is no longer about where you put a camera: it's about what you do with the millions of images and other biometric information captured by everyone's cameras. When it needs a human to analyse it, there is simply too much surveillance material out there, but the technology means that actors are now able to tap into an aggregated surveillance capability that's both vast and growing.

Of all the technological developments in terms of public space surveillance, that of facial recognition is by turns the most powerful and also the most sensitive.

As I mentioned at the Ada Lovelace event to launch the Ryder Review this summer, I'm often a lone voice in saying there's a case for facial recognition technology in policing. Yes, even live facial recognition in some extreme circumstances. The attack on the New York subway at 36th St Station, Sunset Park, Brooklyn on 12 April this year is, perhaps, an example and I've explained precisely why elsewhere.

The same technology can be used to frustrate policing, interfere with witness relocation or disrupt covert operations. We're now experiencing what one lawyer termed "omniveillance" a decade ago. Virtually everyone has access to biometric surveillance capabilities that were once the sole preserve of state intelligence agencies. What's more, they're using them as well.

Legal issues

The first thing to note about the legal framework covering biometric surveillance is that there are many different facets to it. Matthew Ryder QC's recent report summarises them very well. They span data protection, Human Rights, the common law and the concept of implied consent.

One element, namely the Surveillance Camera Code of Practice, emphasises the importance of any public space surveillance by the police service being 'legitimate' and carried out 'in a way that the public rightly expects and to a standard that maintains the public's trust and confidence'.

How do we know what the public 'rightly expects'? Have we asked the public? What are the standards that will maintain the public's trust and confidence in the surveillance technology? Where are they to be found and who sets them?

We know one thing that the public will rightly expect: that the police service is able to show how it has afforded due regard to the Code of Practice because the Code of Practice expressly states that it's a 'legitimate expectation'.

At the moment, the burden of proof rests very much with the police and this is why I've written to all chief officers in England and Wales asking for evidence of legitimacy and compliance. The Code of Practice is published by the Home Secretary, was approved by Parliament in January to cover facial recognition and is currently the only legal instrument specifically written for the police service's use of public space surveillance.

Along with the rest of the legal landscape, the Code is less the product of some 'eureka' policy moment and more a feature on the battleground of litigation by citizens and regulators asking proper and pertinent questions and receiving either what's deemed an unsatisfactory answer or no answer at all.

The aforementioned Ryder Review confirms that we are still dependent on litigation to set the boundaries and, further, serves to corroborate the view that we still don't understand where those boundaries reside.

Societal issues

The societal perspective of police surveillance is changing because the technology is changing. So too is our awareness of – and attitude towards – its use. If you're in the business of public space surveillance, it's important that you understand what level of public support you enjoy. If you're going to rely on the citizen's implied consent as a basis for your activity, it's pretty fundamental for you to gauge different public attitudes in the first instance.

Technology is also changing the surveillance relationship between the citizen and the state. The first police communication following an incident is often an appeal for any images that individuals may have captured on their GoPro digital camera, dashcam, shedcam or 'Ring' doorbell, none of which is specifically regulated. Increasingly, the police service depends not just on biometric information about the citizen, but also from the citizen – from their private devices as well as those belonging to their businesses and employers. This has profound implications for the 'biometric relationship' between the citizen and the state.

Users of facial recognition are now faced with statistics about algorithmic bias and unreliability from four years ago which, in technological terms, is from the Pleistocene period. In terms of legality, there has been surprisingly little legislation

If one part of the surveillance system has been winding up the citizen by issuing automated penalty notices to the wrong vehicle owner or misusing their Automatic Number Plate Recognition data, that citizen may well be less inclined to assist when the time comes for us to ask for their privately captured and unregulated information.

We should look after this surveillance relationship very carefully indeed because we're going to need each other.

Facial recognition

All three perspectives – technological, legal and societal – are brought into sharp relief in the areas of facial recognition and Artificial Intelligence. While the technology has raced ahead, early police service experimentation with the former generated some poor statistics and even poorer stories, in turn realising a somewhat negative image when it comes to the subject of public trust.

Users of facial recognition are now faced with statistics about algorithmic bias and unreliability from four years ago which, in technological terms, is from the Pleistocene period. In terms of legality, there has been surprisingly little legislation or litigation specifically around facial recognition, thereby creating an atmosphere of uncertainty and diffidence.

At the same time, Artificial Intelligence has excited a mixture of fascination and fear. I've heard people say their Artificial Intelligence-based surveillance technology is simply "too complicated" to explain and that even its designers don't really understand how it works.

Well, if you're demonstrating that you've met your Public Equality Duty, that you've avoided bias and are in no way perpetuating unlawful discrimination, that scenario simply will not do. If you're relying on automated decision-making, that will not do either and if, like the police service, you're putting ethics at the heart of your every action, the exact same can be said.

Transparency and 'explainability' are touchstones of public trust and confidence. Whether it's your technology or your company's ethical trading history, if it's too opaque to be understood by the citizen who's funding it – and purported to be benefiting from it – then, with the greatest respect, it's clear that the problem in this equation isn't the citizen.

Sheffield Hallam University has developed a practical accountability framework for the use of Artificial Intelligence in law enforcement. The methodology underpinning this included a citizen survey across 30 different countries in which over 80% of respondents ranked the need for a universal accountability framework governing the police service's use of Artificial Intelligence as being either important or extremely important.

Creating dependencies

Technological development in the biometrics realm has meant that our ability to prepare for, respond to and recover from critical incidents on a global level has increased beyond anything our forebears might have imagined. At the same time, though, it has also created dependencies and vulnerabilities on a similar scale.

If society is to derive the most return from biometric surveillance technology, it will need a systemic approach focusing on the integrity of both technology and practice, along with the standards of everything and everyone in it because, in a systemic setting, if you infect one part, you infect all of it.

In his valedictory report as Her Majesty's Chief Inspector of Constabulary and Fire and Rescue Services, Sir Tom Winsor stated that policing needs "a material intensification of partnership with the private sector, soundly and enduringly based on trust and common interest." That is certainly true, it must be said, of the police service's use of biometric surveillance.

In a world where almost all of our police surveillance capability resides in private ownership, we need to be very careful whose corporate company we keep. If our surveillance partnerships are not "soundly and enduringly based on trust and common interest" then we are going to be in trouble, not just as a sector, but as a society at large.

Looking to the future, Parliament may decide to treat police surveillance as simply a data protection matter. Of course, biometric surveillance uses individuals' personal data, but which public or private function doesn't? That's like saying it uses electricity. The fact of the matter is that biometric surveillance is no more 'just' data protection than DNA profiling is 'just' chemistry or facial recognition is 'just' photography.

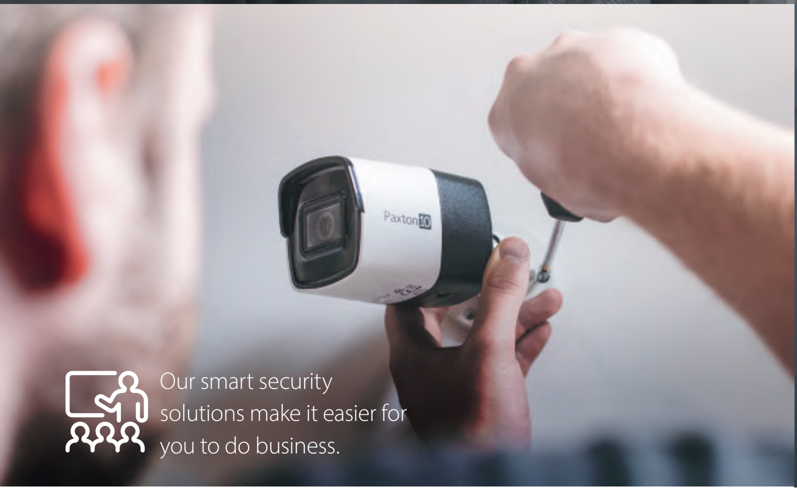
Legitimate role

The Data Protection and Digital Information Bill represents the Government's response to the public consultation orchestrated last year and will bring an opportunity – perhaps a necessity – to address for the first time the many pressing questions around the legitimate role for newly-intrusive technology (such as facial recognition systems) deployed by the police service. We now have an opportunity to do something momentous. Will we lead by thoughtful and courageous planning or wait to be slowly sued into shape, either by the citizen or the regulators?

Policy is for others and legislation is for Parliament, but practically speaking I believe we need a set of clear and indefeasible principles by which the police service can be held to account for its use of surveillance technology, both transparently and by way of audit.

There are many different models by which to achieve this end goal. Ultimately, though, the acid test for all of them will be whether they ensure that the technology (ie what is possible) is only being used for legitimate and authorised purposes (ie what is permissible) and also in a way that the citizen is prepared to support (ie what is acceptable). ●

Professor Fraser Sampson is Commissioner for the Retention and Use of Biometric Material and Surveillance Camera Commissioner
www.gov.uk



Continuity of process

Professor Fraser Sampson's insightful article for Security Matters that considers draft legislation designed to reform public space surveillance by the police service appears on pp20-22. In tandem, Laurie Clarke expands on the broader implications of proposed changes to the Office of the Biometrics and Surveillance Camera Commissioner, specifically in relation to the Surveillance Camera Code of Practice itself

THE SURVEILLANCE Camera Code of Practice, issued by the Home Office under the Protection of Freedoms Act 2012, was developed to provide both a coherent and comprehensive structure against which Best Practice in visual data processing and/or management could be reliably measured and assessed.

The Code of Practice duly sets out 12 guiding principles, which aim to strike a balance between protecting the public and upholding civil liberties, chiefly with regards to the data and privacy considerations absolutely central to surveillance operation.

Under Section 33(5) of the aforementioned Protection of Freedoms Act, local authorities, Police and Crime Commissioners and chief constables must pay due regard to the contents of the Code of Practice. Importantly, other organisations can voluntarily adhere to the latter as well.

The remit of the Code of Practice has expanded with evolving surveillance technology and currently includes all of the following: CCTV, body-worn video, unmanned aircraft systems (ie drones), Automatic Number Plate Recognition (ANPR) systems and also automatic facial recognition solutions.

The Protection of Freedoms Act 2012 also introduced a requirement for the Home Secretary to appoint a Surveillance Camera Commissioner – the present incumbent of that role being Professor Fraser Sampson – to report on compliance with the Code of Practice. This is achieved through a process of third party auditing, which is provided by a UKAS-accredited organisation, and certification via the Office of the Biometrics and Surveillance Camera Commissioner itself.

Formal verification

In many regards, certification against the Surveillance Camera Code of Practice is the only formal verification of surveillance data and privacy compliance available to both public and private sector bodies here in the UK. From the police service through to local authorities and from car parks to drone-focused companies, certification provides confirmation that an organisation's recording devices are used proportionately, effectively and in pursuit of a legitimate aim.

At the time of writing, upwards of 100 organisations have been certificated against the Code of Practice.

In our experience as an auditing body, the greatest area of growth by far has been within the private sector. This is perhaps because achieving third party certification of Code compliance presents additional operational and/or commercial advantages over simply having due regard for its principles.

Take, for example, the private parking sector. The current Private Parking Code of Practice specifically references alignment to the Best Practice requirements of the Surveillance Camera Code of Practice in two of its 16 designated sections. In the drones sector,

one of our more recently certificated clients has reported using its certification as evidence of data and privacy compliance in support of various bids and tender documents.

Alternatively, increased private sector uptake may well be a reflection of the exponential growth of that sector's usage of surveillance technology.

Continuing with the examples theme, if you attempt to count the number of ANPR systems and/or CCTV cameras in any standard car park, you will quickly find that you run out of fingers and toes. Likewise, just this year PwC published its updated assessment of the UK drone economy, duly predicting 900,000-plus commercial drones being in the air by 2030. Each of them presents a unique data and privacy challenge.

Most likely, both of the above factors are at play in varying degree.

What we can say with absolute certainty is that the Office of the Biometrics and Surveillance Camera Commissioner and its Code of Practice co-exist in order to both guide and highlight Best Practice, no matter the organisation and no matter the surveillance device. In this aim, they do appear to be extremely effective.

Draft Bill in Parliament

Back in September last year, the Government commenced a process of consultation on data protection reform, seeking views on simplifying the oversight framework for the police service's use of biometrics and the overt use of surveillance cameras by the police and, indeed, local authorities.

Having only recently appointed one individual to take on what were previously the part-time roles of Biometrics Commissioner and Surveillance Camera Commissioner, the Government wished to further explore the potential for absorbing these functions into the Information Commissioner's Office (ICO). Such a move, claimed the Government, would realise benefits for data controllers and the public alike by creating a single route for advice, guidance and redress.

In response to mixed feedback, the Government later revised that approach and said it would simplify the oversight framework for biometrics, but would not transfer the Biometrics Commissioner's functions to the ICO. It would instead consider transferring these functions to the Investigatory Powers Commissioner.

Fast-forward to 18 July this year. Three days before Parliament's summer recess, in fact. The draft Data Protection and Digital Information Bill was issued. At the time, the Government claimed the Bill would "seize the benefits of Brexit" to "reduce burdens on organisations, while maintaining high data protection standards". It's difficult to know where to begin with that particular word salad.

For the sake of collective sanity, let's glance across it and focus on the important elements.

Amid the usual rearranging of deck chairs, tucked away on page 115 of the draft Data Protection and Digital Information Bill (currently on its second reading in the House of Commons) is the following wording:

104. Removal of provision for regulation of CCTV, etc.

(1) The office of Surveillance Camera Commissioner is abolished.

(2) In the Protection of Freedoms Act 2012, omit Chapter 1 of Part 2 (regulation of CCTV and other surveillance technology).

Within the House of Commons Research Briefing, published on 31 August this year, it's further clarified that: Clause 104(1) would abolish the office of Surveillance Camera Commissioner. Clause 104(2) would repeal Part 2 Chapter 1 of the 2012 Act to remove the requirement for a Surveillance Camera Code. The Bill's Explanatory Notes state that the Information Commissioner would continue to provide independent oversight and regulation of this area, without duplication by the Surveillance Camera Code and Commissioner.

Early days

What does all of this mean, then, for those who rely upon the Surveillance Camera Code of Practice and/or those organisations who are currently certificated against it? First and foremost, it must be stressed that it's still early days for this draft Bill and it has yet to pass through even the Committee Stage in the House of Commons.

Safe to say it's extremely unlikely to go through the full passage – from the House of Commons to the House of Lords and on to Royal Assent – without amendments being made. Consider it a first draft of a Bill that, thus far, has entered the world largely without scrutiny from Parliament.

Nevertheless, it appears from this draft Bill that the Government may have underestimated the impact of the proposed removal of the Office of the Biometrics and Surveillance Camera Commissioner through focusing on Code simplification over the current scope of Code application.

While reference has been made to the merging of guidelines between the ICO and the Surveillance Camera Commissioner, issuing guidance is just one of the Commissioner's many roles and, at present, no consideration appears to have been given to formal certification and mechanisms designed to ensure continuity of this valuable process.

When we recall that this amendment was first proposed on the basis of simplifying the oversight framework for the police and local authorities – entities who are required to have due regard for these guidelines as opposed to the specific requirement for formal certification – and not the private sector, then perhaps we have some explanation for this apparent omission.

Seeking clarification

Concerned by the ramifications of the Government's proposals and what – on the surface, at least – appears to be a regulatory step backwards, IQ Verify reached out to its local MP for clarification. Specifically, the company asked the following questions:

Q1: What's the justification for such a change in light of the success of the Surveillance Camera Commissioner and the seemingly exponential growth of surveillance usage – both in the public and private sectors – across the UK?

Q2: What's being done to protect the interests of those countless organisations who rely upon – or, indeed, have achieved – certification against the Surveillance Camera Code of Practice?

A few weeks later we received a response direct from the Home Office and, more specifically, the Government minister with direct policy responsibility for this area. The minister duly explained that the change was being made with a view towards reducing duplication between the ICO and the Surveillance Camera Commissioner and to increase the regulatory powers available to investigate and fine data breach episodes.

Reference was also made to consolidating guidance and oversight in order to bring expertise into one place and ensure consistency, in turn making it easier for the police service and the public at large to understand.

Somewhat predictably, no reference was made within this explanation to organisations outside of the police service, nor indeed to those operating within the private sector.

The second question – the more critical of the two for the planning and continuity of those organisations who draw value from existing surveillance certification processes – was answered in the final lines of the letter.

The following is a direct quote from the response: "I recognise that some of the Surveillance Camera Commissioner's ancillary functions, such as the third party certification scheme, are aimed at encouraging Best Practice and consistency in operators' use of surveillance cameras, and I expect that there will continue to be a demand for similar assurance going forward. The Government is considering whether another existing body could support continuation of the scheme in some form and would welcome the chance to engage with key stakeholders, such as IQ Verify, in due course."

What springs to mind?

Two things leapt out of the page from these comments. The first is that insufficient consideration may indeed have been given to "ancillary functions" of the Office of the Biometrics and Surveillance Camera Commissioner, including third party certification, within the draft Data Protection and Digital Information Bill. The second is more reassuring in that it appears this potential oversight is now firmly on the Government's agenda to be addressed.

What happens next, then? For those organisations who rely upon the existing Code of Practice, be it for guidance or formal certification, the long and short of it is they don't need to panic. From the response provided above, the Government (now) appears to be in the process of developing a strategy to ensure continuity of third party certification services against the Surveillance Camera Code of Practice. While this process may – or may not – have different ownership in the future, at present there's no indication that there will be any change to the availability or recognition of formal organisational surveillance certification.

The updated Data Protection and Digital Information Bill will most likely contain the outline for these arrangements in due course.

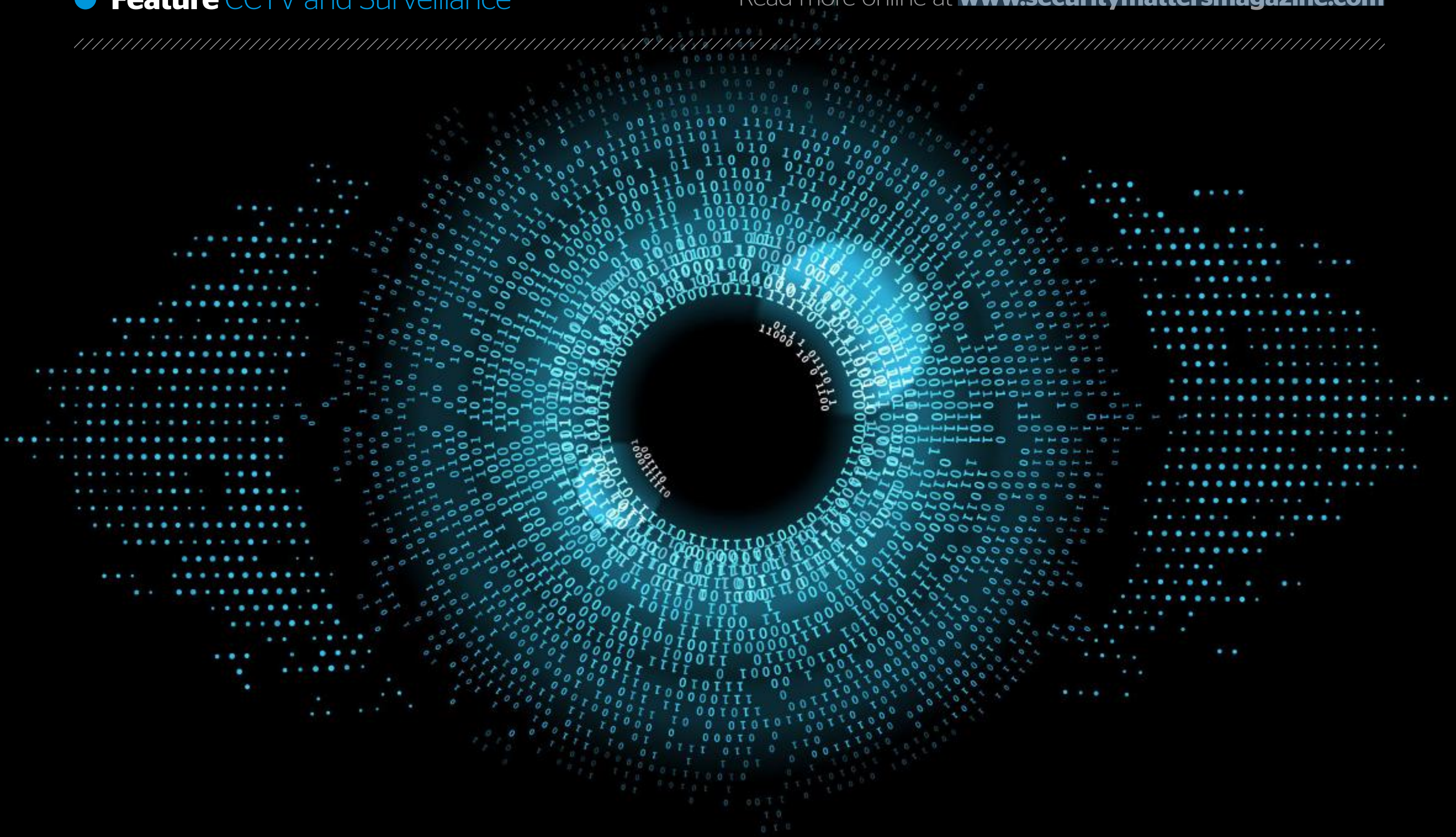
However, we would strongly recommend that all interested parties reach out to the Home Office and register their interest as a stakeholder in this project as soon as possible. In doing so, collectively we can help to ensure that surveillance standards – and the mechanisms by which these can be reliably assessed and, just as importantly, evidenced – remain in clear focus over the full passage of the Bill through the Houses of Parliament.

As for my own predictions? I have a sneaking suspicion the end result will be the continuation of existing certification activities with a renewed focus on the private sector and the introduction of a Commissioner 2.0. That individual may well be the same person. ●

Laurie Clarke is Certification Manager at IQ Verify Ltd
www.iqverify.org.uk

Cut costs over the whole
Cut the wires, cut the bill
ASSA ABLOY

simPRO



Keeping watch

In recent times, the use of CCTV has become increasingly widespread throughout the UK. With end users rightly seeking best value from their surveillance procurement spend, it's vitally important that system installers and integrators alike achieve the best outcome possible. Here, Pete Dowsett shares his thoughts on the common pitfalls to be avoided in today's CCTV projects

ORIGINALLY DEPLOYED to watch over larger establishments and monitor city centres, CCTV systems are now installed routinely within shops, schools and even individual vehicles on the public transport network. Through the passage of time, the surveillance market has undergone a rapid transition from analogue to digital recording technology and now data storage in the cloud, all of which has exerted a significant impact on the design and functionality of CCTV systems.

Ask almost any experienced video system integrator about surveillance projects they've worked on to date and they'll have at least one horror story to tell about a bad installation they've encountered and had to amend. It's something we see surprisingly often.

We'll be called to a site by a disappointed customer who isn't privy to the system performance they expected. This is usually because that system has been installed by engineers lacking the necessary experience in security. Engineers with no real appreciation of risk and no proper understanding of what it is they're doing.

Even before we arrive, we've already formed an idea of the typical problems we might encounter. On a regular basis, customers tell us they're disappointed by the grainy or otherwise indistinct images being generated by the cameras (often due to the wrong models having been selected and installed without due attention paid to lighting conditions).

We also witness end user customers struggling with the usability of their VMS, with problems including latency in real-time monitoring or cumbersome search tools that make it difficult to interrogate recorded footage. If you cannot easily search surveillance recordings, and then export them for evidential purposes, what's the point of storing them at all?

Monitoring operations may also be hampered by unreliable video transmission, which can have a range of common causes. One particular pitfall that's perhaps less obvious, but entirely worth avoiding, is the issue of OPEX costs (specifically storage costs, unexpected license fees and unaffordable maintenance, etc).

Put simply, there are many common traps into which an inexperienced system designer might fall and, in doing so, negatively impact the customer. That scenario must be avoided.

Surprising mistakes

Sometimes, we discover less common errors and installations that, to be frank, would shock even the most seasoned of integrators. One project that springs to mind featured cameras – conveniently out of view of the customer, by the way – that were held up by nothing more than duct tape. Absolutely shocking.

Bodged cabling work is surprisingly common, with shortcuts taken and inadequate temporary fixes (cables being wedged into 'convenient' gaps, for instance) that mean the system will inevitably fail sooner rather than later.

A problem we encountered at another site wasn't the fault of the original engineers. Cameras had been mounted above a building's main entrance in the perfect location for surveillance, and where a scissor lift could be deployed for easy maintenance. The only problem was that a porch and canopy had subsequently been added to the entrance, in turn obscuring the view and making camera access more than tricky.

In other instances, poor surveillance system design is simply the result of inexperience. For example, one project involved protruding bullet cameras being used alongside a roadway. Inevitably, they had been hit by a high sided vehicle. A low-profile dome would have been the right choice for this particular location.

The common occurrence that really sticks in my mind is cameras filled with rainwater because the installer didn't have the right mounting accessories and simply drilled a hole in the top of the unit. At one site, the dome camaras installed beneath an overhang porch at a smart new corporate headquarters had turned into goldfish bowls. All that was missing was the fish.

Bodged cabling work is surprisingly common, with shortcuts taken and inadequate temporary fixes (cables being wedged into 'convenient' gaps, for instance) that mean the system will inevitably fail sooner rather than later

Network infrastructure

Those are just some of the issues in play. How, then, do we ameliorate them? Let's run through some top tips for customers – as well as new engineers – such that the worst pitfalls can be avoided.

We've seen installations where the CCTV system has been bolted on to an existing corporate network, not a dedicated LAN, presumably because it seemed quicker and cheaper to do so. That's rarely a good idea. Aside from issues around cyber security and data safeguarding, the big problem is bandwidth. CCTV 'piggybacking' on the corporate network will be vulnerable to any maintenance work or changes undertaken by the IT Department (changes to routers or switches, for example). The surveillance view and recordings will be interrupted and the CCTV system wrongly blamed.

Over the life of the system, cheap brands rarely deliver best value. Much more important if you want to keep costs down are factors such as component interoperability (how easy is it to ensure all of the cameras, recorders and accessories are connected and working together without compatibility issues and glitches?). Then there's durability (ie do the cameras and NVRs come with extended manufacturer warranties?) and choosing the right camera for the project. Upgrading a system by simply replacing a cheap, but poorly performing camera with a dependable and quality product isn't the answer. It's far less costly to ensure the specification is right first time.

Look for ongoing manufacturer support for your chosen technology, with forward and backward compatibility for all devices. This means you'll avoid technology 'dead ends' and be able to easily extend or adapt the system if necessary. Ask for a transparent fee structure that you can easily understand (for example, one without high ongoing VMS licensing costs, hidden extras for functions you never use or punitive charges for adding more devices).

If you plan and install a CCTV system during the winter, remember that trees grow leaves. When foliage is thick, the vegetation doesn't only obscure camera views, but can also interfere with wireless links. The solution? You might need a few more cameras than you assumed to provide full site coverage. You may also need to design your transmission system differently. We've been asked to fix systems where this was a problem. Again, it's cheaper to make sure everything's right at the outset.

Planning stages

In the case of the aforementioned building where a porch was added, a failure of communication clearly occurred at some point. While some changes to building use or design cannot be predicted, often major projects are planned long enough in advance to allow them to be considered.

It helps if the manager who has ownership of the CCTV system (the security manager or head of IT, etc) enjoys a high enough profile within the organisation that they're consulted at an early stage before detrimental site modifications are signed-off.

Never underestimate the value of long-term support from your suppliers. If an experienced systems integrator has been trusted with the maintenance contract, as well as servicing the system itself, they should help you by keeping an eye on the site and giving timely advice if they do happen to see problems arising.

Always engage with an experienced systems integrator. The quality of the advice they provide will not just depend on the accreditations they have and the strength of relationships enjoyed with their trusted vendors, but also on their experience amassed from working on multiple projects. Look out for customer testimonials and never be afraid to ask for some recommendations.

It's worth referring to the Home Office Scientific Development Branch publication entitled the 'CCTV Operational Requirements Manual', which lists four key stages when planning the installation of a CCTV system.

The first step is to define the problem, be it a security threat, a public safety issue or other vulnerability. This is known as the Level 1 operational requirement (OR). Having developed a clear picture of the concerns that need to be addressed, attentions can then be turned to the specific issues relating to the CCTV system itself. This is known as the Level 2 OR and assists the CCTV end user/manager to further define the areas of concern, understand operational issues and responses, decide on the most suitable system requirements and then identify any managerial implications.

The third step is where a more detailed technical specification for the CCTV system is developed. This involves a consideration of camera selection, the effects of compression on image quality and estimating the storage capacity that should be included with the system.

The final stage in the process occurs when the surveillance system is installed and commissioned. At this point, it's important to check that it actually meets the ORs and also that system performance is deemed fit for purpose.

Bristol's Wild Place

An end-to-end IDIS video solution is helping the Bristol Zoological Society in the creation of a new Bristol Zoo at its 136-acre Wild Place Project site. This follows the closure of the Society's 186 year-old Bristol Zoo Gardens on 3 September as the charity pushes forward with what's undoubtedly an inspiring wildlife conservation agenda.

When the work is completed over the next few years, around 80% of the species at the new Bristol Zoo will be linked to conservation breeding and conservation programmes around the world – a higher percentage than for any other zoo in the UK, in fact. The Wild Place Project will remain open to visitors throughout the development phase.

Upgraded CCTV visibility across the site is a crucial part of the strategy and the installation, carried out by ourselves as an appointed IDIS integration partner, has already delivered welcome conservation benefits. For the first time, a wolverine cub has been born and raised in Bristol, with vets using remote video to avoid disturbing the notoriously skittish animals during the high-risk birth period (something that may result in newborns not surviving).

The powerful IDIS solution is also key for operations at the site as it affords members of staff 24/7 visibility over enclosures, perimeters and public areas, including the raised tree-top walkways.

2 MP 36x Lightmaster PTZs, which deliver crystal clear images in Full-HD resolution and can capture footage at distances of up to 350 metres in full darkness, are helping the maintenance team verify that fences are not compromised by storm damage and falling branches. The cameras feature 120 dB true Wide Dynamic Range, backlight compensation and advanced image control settings, which mean they cope perfectly with the continuous fluctuations in light and allow the well-camouflaged animals – including bears, wolves and lynxes – to be seen clearly.

Operating platform

The cost-free IDIS Center VMS delivers a powerful and flexible operating platform that makes the whole system easy to use, with the ability to seamlessly scale-up to Solution Suite as and when the site expands through time and necessity.

A transformed surveillance capability provides the Wild Place Project with a truly future-proof system. There are plans afoot to integrate it with Microsoft Active Directory, in turn making it easier to manage access rights and strengthen perimeter detection still further.

Adam Evans, head of IT at the Bristol Zoological Society, stated: "Our IDIS video solution, delivered by KIS Fire and Security, affords us the best long-term value for the Wild Place Project, with the flexibility to scale and adapt as we develop the new Bristol Zoo. The delivered solution also makes it easy for us to take advantage of Artificial Intelligence-powered analytics and integrate with wider systems." ●

> It's worth referring to the Home Office Scientific Development Branch publication entitled the 'CCTV Operational Requirements Manual', which lists four key stages when planning the installation of a CCTV system

Pete Dowsett is Installation Manager for KIS Fire and Security
www.kisfireandsecurity.co.uk

Sending the right signals

In a relatively short space of time, the world of alarm signalling has changed significantly. Only five years ago, the PSTN and 2G were seen as the ideal combination for dual path signalling systems of any grade. Today, as John Coleman affirms, dual 4G systems are the industry standard, while the clock's ticking for the PSTN

DUAL 4G systems provide the most reliable signalling ever thanks to network diverse roaming SIMs. Not only that, but the increased data usage offered by 4G also means there have been advancements in upload/download, remote diagnostics and other remote servicing tools. While 2G isn't going anywhere just yet and can still be accessed and used by 4G SIMs, the clock is most certainly ticking for the Public Switched Telephone Network (PSTN) and any services that depend upon it.

Why is the end of PSTN closer than you might think? We already know that the UK's PSTN is being switched off in December 2025 to make way for a new digital network that will provide a more reliable and future-proof broadband service for consumers. What many are less well aware of, though, is that a nationwide 'Stop-Sell' of PSTN lines is less than 12 months away.

In September next year, the whole of the UK will enter an intermediate 'Stop-Sell' stage designed by Openreach (the owner of the cables, cabinets and exchanges) to stop any new PSTN connections ahead of the full withdrawal of these services in 2025. In many areas, the sale of new PSTN connections has already halted because so many homes and businesses now receive – and benefit from – full fibre broadband. For those instances where this isn't the case, Openreach has developed a new product that 'bridges the copper gap' such that full withdrawal in 2025 isn't impacted. At the point of withdrawal, all analogue lines and products will stop working.

The areas where PSTN has already stopped include two exchange trials in Salisbury and Mildenhall, which have been underway since 2020 to find the best ways in which to migrate different types of PSTN services smoothly to All IP alternatives. The others where the level of 'full fibre' coverage is good and broadband is widely in use became 'priority' for 'Stop-Sells' and were announced in tranches.

Since the start of the network upgrade process, over 300 exchanges have been upgraded, in turn affecting 3.5 million premises. Between now and next September, an additional 279 exchanges will go into 'Stop-Sell' mode, duly bringing the total number of premises affected to no fewer than six million.

Out with the old

Currently, there are over one million alarm systems in the UK using the analogue network, with an estimated 800,000 being digital communicators. In general, the largest bases installers own are digital communicators and all of these will need to be swapped out for something compatible with the digital network. New orders and 'business as usual' will continue in normal volumes, which can be in the region of between five and 50 new units per month depending on the size of the installer.

From September 2023, these would all need to be All IP compatible as no new analogue lines will be available. If the swap-outs are left too late, installers could be seeing their workload double.

Finding out what's compatible with the digital network and choosing the right replacement isn't as complex a procedure as installers might think. It's 4G we must thank for the simplicity when it comes to upgrading older PSTN bases

Conversely, if they plan now, there's still time to build the swap-outs and new connections into a manageable schedule. Industry bodies are all in agreement that installers need to educate themselves on available solutions at this present time in order to remain compliant. It also makes sense that they familiarise themselves with the new equipment ahead of their businesses becoming very busy.

In terms of further information, there's a list of impacted areas available on the Openreach website, which can help Installers with their plans. Simply visit ***www.openreach.co.uk*** and search for the All IP programme.

The next tranche happens between now and Christmas and encompasses the involvement of another 51 exchanges throughout the country.

An example of what's going to happen here is as follows: Openreach announces the exchanges taking part in the latest tranche, giving 12 months' notice of the 'Stop-Sell' to telephone network providers such as BT, TalkTalk and Sky, etc. Those telephone network providers then send their customers in the affected areas a letter informing them that the local exchange is being upgraded to All IP (digital voice) and that they will be receiving a Smart Router, which should be plugged into their phone socket.

At this point, they should indicate a time frame in which this will happen in order for the consumer to be prepared. This is completely of the telephone networks' choosing and, in most cases, they are not giving the same amount of notice as Openreach.

Installers who act before the above process kicks in have had the most success with their upgrade programmes, with minimal disruption to their day-to-day business and, it must be said, happier customers. They simply need to identify which All IP compatible product is the most suitable upgrade for the PSTN-based product being replaced and then notify their customers.

Openreach has produced some collateral which can be branded to help installers explain what's happening. Additional detail is available online at ***www.openreach.co.uk*** Again, search for the All IP programme.

It's simple with 4G

Finding out what's compatible with the digital network and choosing the right replacement isn't as complex a procedure as installers might think. It's 4G we must thank for the simplicity when it comes to upgrading older PSTN bases and ensuring new connections work in harmony with the digital network.

Dual radio over 4G is now the industry standard for dual signalling systems and, similarly, there are affordable single-path 4G options available. These systems use network diverse roaming SIMs to send their signal to the Alarm Receiving Centre. The SIMs make use of independent networks and independent radio modules provide total resilience.

In order to determine precisely how installers are preparing for the UK's upgrade to All IP, it's worth taking a look at some recent Case Studies. Established in 1993, Atlas Fire & Security is a customer-focused organisation based in Birkenhead and the team members at the business are fully aware of the upcoming challenges posed by the UK's ongoing All IP upgrade project.

Recently, managing director John Piggott witnessed first-hand how end users will be impacted by these changes. "In the first week of October last year," noted Piggott, "I received a letter from BT to advise that they would be upgrading my home landline to the new digital service. I was also aware that my local exchange was going into its 'Stop-Sell' phase from 13 October, meaning that any changes to my service would automatically move to IP as older options would no longer be available."

Like many others, Piggott presumed the switchover would be transacted within the next 12 months following the 'Stop-Sell' phase beginning and that he would be given a good notice period of the upgrade date. This didn't happen.

"I then received an e-mail from BT on 19 October (ie six days after the 'Stop-Sell' phase began) to advise me that the upgrade to my service would happen just seven days later on 26 October. Sure enough, this all went ahead as planned. From this date, my PSTN service was switched off and replaced with an IP-centric solution."

Luckily for Piggott, he was aware of the implications of this switch and was able to plan for his own alarm system to be upgraded to the latest 4G solution. However, many end users will not be aware that this change impacts their alarm system and, consequently, may not notify their chosen installation business ahead of the change. This could cause lots of issues for installers, with emergency call-outs being requested as systems pass into failure mode.

"Having now seen for myself how home and business owners will be impacted by these changes," concluded Piggott, "we are proactively encouraging all of our customers to have their systems upgraded. Not only does this future-proof their system and allow us to provide them with a better service, but it also avoids any potential issues caused by the All IP switchover."

Preparing to transition

ESS is another trusted installation company with 47 years' worth of experience in the security industry. Thousands of commercial and domestic customers rely on the business to robustly protect their people and property.

As an established and accredited security provider, Belfast-based ESS has been proactive in preparing for the UK's transition to a fully digital service as part of the All IP project. These changes are extremely important to ESS as they will have a major impact on security systems, telecare systems and all things that customers need to use in the event of an emergency scenario occurring.

ESS has begun upgrading its legacy digital communicators to DigiAir Pro, a professional upgrade solution for any single-path system reliant on PSTN lines. DigiAir Pro, in fact, meets the latest European standards for SP levels (including SP2 for intruder and SP3 for fire) and is also compatible with CSL Live and the My Base app.

In essence, it's a wireless signalling device that uses a 4G radio path or a LAN path to signal an alarm. The device is provided with a standby SIM as a back-up to safeguard ESS' system if the active SIM should fail for any reason. Both SIMs operate independently for total resilience, while not forgetting that the device is also future-proofed.

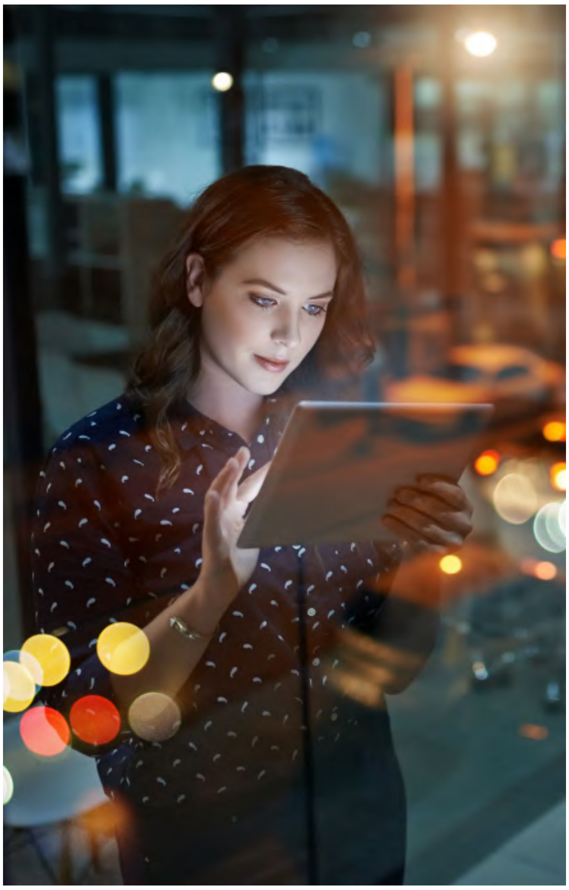
David McCullough, director at ESS (which specialises in intruder/fire alarms, CCTV and access control systems), observed: "DigiAir Pro has provided us with the latest technology to update our older systems reliant on PSTN. With many exchanges throughout the UK already moving towards digital voice – in some parts of Northern Ireland the migration is already completed – we knew it was important to act now in order to ensure that our customers retained their full monitoring services."

Better connected

Established in 1998 and based in Uxbridge, Ambush Security Systems has been proactive in preparing for the UK's transition to a fully digital service as part of the detailed All IP project. Many of the company's customers still had systems connected to – and signalling via – PSTN using digital communicators.

In order to ensure all customers could continue to receive the best service possible, not to mention a guaranteed police response, the company decided to upgrade all of its remaining PSTN customers to CSL Connected.

Ambush Security Systems has been upgrading systems to radio-only solutions for many years. The remaining systems in its portfolio connected to PSTN are often located in areas where mobile signals are somewhat limited. As a direct result, the business has taken the decision to use the All IP project as the optimum moment to upgrade the entire system to include a new panel and CSL Connected (radio only). CSL Connected is something of an ideal signalling solution for new installations as it uses the panel's communication hardware, providing connectivity directly to the Alarm Receiving Centre via the Gemini Global platform. This realises a quick installation for the installer and less disruption for the end user.



Additionally, CSL Connected provides the manufacturer's end user app as well as professional monitoring. This is important to Ambush Security Systems, as the app provides increased visibility for customers, while the professional monitoring allows for police response (which is something that Ambush Security Systems insists upon its customers having as standard).

It's only right to leave the last words to a satisfied customer. Georgia Riley, associate director at Ambush Security Systems, observed: "CSL Connected provides us with the ideal signalling solution for our recent systems upgrade programme. Our customers understand that their older systems will no longer work once All IP comes into effect. This solution enables us to continue to provide the highest level of service." ●

John Coleman is Head of Sales (UK and Ireland) at CSL
www.csl-group.com

For Queen and country

On Monday 19 September 2022, trained and licensed security personnel from Wilson James played an integral role at the State Funeral of Her Majesty Queen Elizabeth II. Here, Leonie Brumby and David Gregory offer their personal perspectives on preparing for such an important event and how the carefully planned security operation enacted on the day kept The Royal Family, invited dignitaries and members of the general public safe

THE STATE Funeral of Her Majesty Queen Elizabeth II that took place at Westminster Abbey on Monday 19 September at 11.00 am paid magnificent tribute to a reign spanning 70 years and 214 days and Her Majesty's remarkable life of dedicated service as Head of State, the nation and the Commonwealth. The State Funeral was broadcast live on television and radio, allowing people from around the world to take part in mourning The Queen.

Her Majesty The Queen's coffin had been Lying-in-State since the evening of Wednesday 14 September. At 6.30 am on the morning of the State Funeral, the Lying-in-State period officially ended. At 10.44 am, the coffin was borne in procession on the State Gun Carriage of the Royal Navy from the Palace of Westminster to Westminster Abbey for the State Funeral Service itself.

The State Funeral Service was conducted by the Dean of Westminster and the Sermon and Commendation given by the Archbishop of Canterbury. During the State Funeral Service, the Prime Minister and the Secretary General of the Commonwealth read lessons. The Archbishop of York, the Cardinal Archbishop of Westminster, the Moderator of the General Assembly of the Church of Scotland and the Free Churches Moderator all said prayers. To mark the end of the State Funeral Service, The Last Post was sounded followed by a two-minute silence being observed in the Abbey and throughout the United Kingdom. A rendition of the national anthem drew proceedings to a close.

The State Funeral Service was attended by Heads of State and overseas Government representatives, among them Foreign Royal Families, Governors General and realm Prime Ministers. Other representatives of the realms and the Commonwealth, the Orders of Chivalry (including recipients of the Victoria Cross and the George Cross), Government, Parliament, devolved Parliaments and Assemblies, the Church and Her Majesty's Patronages formed the congregation, along with numerous public representatives.

Almost 200 individuals recognised in Her Majesty The Queen's Birthday Honours List earlier this year joined the

congregation, including those who had made extraordinary contributions to the response to the COVID-19 pandemic and volunteers from local communities.

Royal salute

At the end of the State Funeral Service, Her Majesty's coffin was then borne to Wellington Arch via The Mall on the State Gun Carriage. Not seen on the streets of London since the funeral of Sir Winston Churchill back in 1965, the State Gun Carriage was pulled by 98 Royal Navy sailors, with a further 40 marching behind and acting as brakes.

His Majesty The King and members of the Royal Family followed The Queen's coffin in a procession which included detachments from the Armed Forces of the Commonwealth, as well as detachments of the British Armed Forces who, of course, held a special relationship with Her Majesty. The King's Guard gave a Royal Salute as the coffin passed by the Queen Victoria Memorial.

Once the coffin reached Wellington Arch, it was then placed in the State Hearse. The parade gave a Royal Salute and the national anthem was played as the State Hearse began its journey to Windsor, the final resting place of Her Majesty who has been buried alongside her late husband The Duke of Edinburgh at The King George VI Memorial Chapel.

Watched by millions of people all over the world and with thousands of individuals and families from across the country lining the streets of London and the route to Windsor in order to pay their final respects, the State Funeral Service for Her Majesty Queen Elizabeth II was a fitting farewell to a wonderful woman and the longest reigning British monarch, who died at Balmoral at the age of 96.

Building bridges

Behind the solemn ceremony of the occasion was a carefully orchestrated and brilliantly executed security operation that had been meticulously planned and refined over many years.

Planning for Queen Elizabeth II's State Funeral was codenamed Operation London Bridge. Senior members of the Royal Family are all given a bridge name as soon as they enter their role as heir or King or Queen: Prince Philip (The Duke of Edinburgh) was designated as Operation Forth Bridge, while King Charles III is Operation Menai Bridge.

Former UK counter-terrorism national co-ordinator Nick Aldworth described Operation London Bridge as follows: "Probably the biggest policing and protective security operation the UK has ever mounted. It just takes [the driver of] one car or one individual to do something abhorrent and not only have you disrupted a constitutional event, but people could be injured or killed."

On that basis, the security operation around the State Funeral needed to be honed such that the 20,000 security personnel involved throughout the day could be mobilised, deployed and organised at short notice.

As well as Operation London Bridge, smaller operations were initiated in the lead-up to the State Funeral. These included Operation Spring Tide, whereupon King Charles III toured each of the four nations visiting London, Edinburgh, Belfast and Cardiff. Meanwhile, Operation Unicorn saw the coffin of Queen Elizabeth II flown to London and taken by hearse to Buckingham Palace.

Operation Feather covered the logistics for Lying-in-State public visits. To that end, mourners who queued patiently in Londo across several days faced airport-style security checks before being allowed in the same room as the coffin, while extra policing patrols were enacted around the capital city.

Ask the experts

In the event of Queen Elizabeth II's passing, Wilson James' co-founder and chair Gary Sullivan had offered the company's services some years prior. The business was therefore honoured to receive a call from the Department for Digital, Culture, Media and Sport to initiate arrangements for providing support during the State Funeral as part of Operation London Bridge.

One of the largest ventures of its kind ever in the capital, only security services providers with proven track records of working on large-scale projects were trusted to take part and ensure the day ran smoothly. The ability to work with short timeframes and to a high standard is something that Wilson James has demonstrated on numerous occasions, including at the 2012 Olympic Games and the 2022 Commonwealth Games.

The company also played an integral role in the construction of the NHS Nightingale Hospital at London's ExCeL. As a key player in this massive collaborative feat, Wilson James used its logistics expertise to ensure that materials were met on delivery and then categorised, audited, inventoried, stored and delivered to where they were needed, when they were needed and, importantly, in the required quantities.

> One of the largest ventures of its kind ever in the capital, only security services providers with proven track records of working on large-scale projects were trusted to take part and ensure the day ran smoothly

Prior to Her Majesty The Queen's State Funeral, the police and security services had expressed concern about the possibility of terrorist threats or incidents. At the time of the event, the country's terrorism threat level stood at 'Substantial', meaning an attack was 'likely'. As Nick Aldworth alluded to, in a world now sadly accustomed to terrorist atrocities, there's a growing and disturbing trend whereby rather than working as part of a group or cell, radicalised individuals – or 'lone wolves' – are able to evade the 'radar' of the security services due to their willingness and determination to act alone.

While they hold views that go against the clear majority of others in society, these individuals are often what the security services reference as 'clean skins' (a term used to describe those who have a spotless criminal record, a history that doesn't arouse suspicion and no connection with the security services). With this type of background, it's incredibly difficult to identify and monitor 'lone wolves', a problem further compounded by the fact that they often have no communication with others.

Unfortunately, working alone makes it far more likely for those with malicious intent to succeed in their endeavours. The methods they use to carry out atrocities are usually basic, but deadly, often involving knives or vehicles.

Although the proliferation of 'lone wolves' poses an insidious and covert threat, it makes it all the more vital that security professionals work with the wider security services and the general public in a combined effort to increase vigilance and identify suspicious behaviour. To help mitigate all potential threats on the day, the Metropolitan Police Service put measures in place that included road closures and hostile vehicle mitigation solutions at crowded sites before and during the State Funeral.

With Wilson James' participation in safeguarding the event confirmed, director of solutions Marc Bannister set an incident response team in motion. Although there was limited detail at that stage about the exact part of the route requiring coverage, a company-wide call was immediately initiated to see how many colleagues would be prepared to make themselves available.

Over 200 Wilson James colleagues (including 19 senior management team members) volunteered their services for deployment along the procession route between London's Queens Gate and the Cromwell Road.

The security planning and execution on the day of the State Funeral was meticulous. Armed police, rooftop snipers, motorbike escort riders, officers carrying out patrols on horseback, dog teams and the marine unit were among the specialist teams involved.

Direction was provided and Wilson James' supervisors devised comprehensive briefing documents and a deployment plan for officers. Grouping pre-populated teams into dedicated locations gave personnel smaller areas of responsibility and, combined with the command structure on the day, facilitated simple, but absolutely effective operational management. Registered personnel were issued with their kit and instructions to expedite deployment. There was a need to make sure all roles and responsibilities were understood.

The planning process involved far more than simply deploying personnel on the day itself, though. Prior to the State Funeral, comprehensive risk assessments had to be conducted, while appropriate personal protective equipment – as well as radios, torches and even umbrellas – had to be ordered by the company's dedicated procurement team at short notice for use by deployed personnel.

Staff welfare also had to be a priority. Wilson James' senior managers used their extensive list of contacts to approach hospitality sites around Green Park. A dedicated operational Command Centre was established at the Brompton Oratory. A secondary break area at the Royal College of Arts provided facilities for rest, staff welfare and additional Command and Control functions.

Final journey

There were 12 teams with 15 colleagues in each including a supervisor and manager in regular radio contact with team members as well as the Wilson James Command Centre. The day began with a briefing at 5.30 am and personnel were sent to designated areas along the Queens Gate and Cromwell Road, with teams in position from 7.00 am.

As stated, following the State Funeral, The Last Post was aired before the procession to Wellington Arch made its way through the streets of the capital from noon to 1.00 pm. Colleagues were in place until demobilisation at 4.00 pm.

During the procession, team members were redeployed where necessary in high density areas to offer the most effective response possible and assist with escorting people across roads and administering First Aid if required.

Those viewing the State Funeral of Her Majesty Queen Elizabeth II would have had little idea of the size and scale of the security operation behind it. That's how it should be, as this indicates just how well it was carried out. The consensus affirmed a very successful operation. All Wilson James colleagues performed exceptionally well during a very long day.

Everyone involved, in fact, delivered the kind of professional and considered service that was needed for this 'once in a lifetime' event. For all of us, it was a tremendous honour and a great privilege to play our part in an unforgettable occasion that marked the end of the second Elizabethan era. ●

Leonie Brumby is Principal Consultant and David Gregory is Senior Lead for Operations at Wilson James
www.wilsonjames.co.uk

Chain of events

The potential theft of goods during storage and transportation, Health and Safety-centred issues, cyber security, the possibility of fire and flooding and bouts of civil disobedience or activism are just some of the issues facing security teams in the warehouse and distribution services sector. Noah Price delivers a timely overview of how those teams can stay one step ahead of the criminals thanks to implementing Best Practice techniques

IN TERMS of gross added value, the warehouse and distribution services sector contributes over £120 billion to the UK's economy each year. Indeed, this sector is the fifth largest employer, accounting for upwards of 2.5 million personnel. As a direct consequence, warehouse and distribution sites tend to be particularly busy locations. They contain high volumes of stock and are frequented by different groups of people (eg employees, contractors and visitors) during the day and also at night.

The effective operation of the sector plays a pivotal role in the smooth and successful running of supply chains. Indeed, disruption encountered at any single point in the process will exert an impact elsewhere. During the COVID-19 pandemic, for example, it's believed that 85% of global supply chains were negatively impacted in some way.

Traditional threats posed to the sector remain, while new ones emerge. Both demand a concerted response. It's fair to state that clients are now demanding more of their security solution providers. They want more than just a 'traditional' security service. Rather, they desire a security set-up that's innovative and encompasses issues including sustainability and Corporate Social Responsibility. Good security must not end with the warehouse. It now has to extend throughout the supply chain.

Threat landscape

The most common threat is focused on the potential for the loss of – or intentional damage to – goods and assets through criminal activities. This can happen at any juncture during the supply and distribution process, from the point of delivery of stock to warehouses and distribution centres, during storage or subsequently when goods are in transit to their next destination.

With online shopping now increasing in popularity – growing from 19.2% of all retail sales in 2019 to reach 28.1% just a year later – warehouses are burgeoning in size and, at the same time, hosting larger and larger volumes of high-value goods. It's not surprising, then, that this fuels the interest of (among others) serious organised crime gangs.

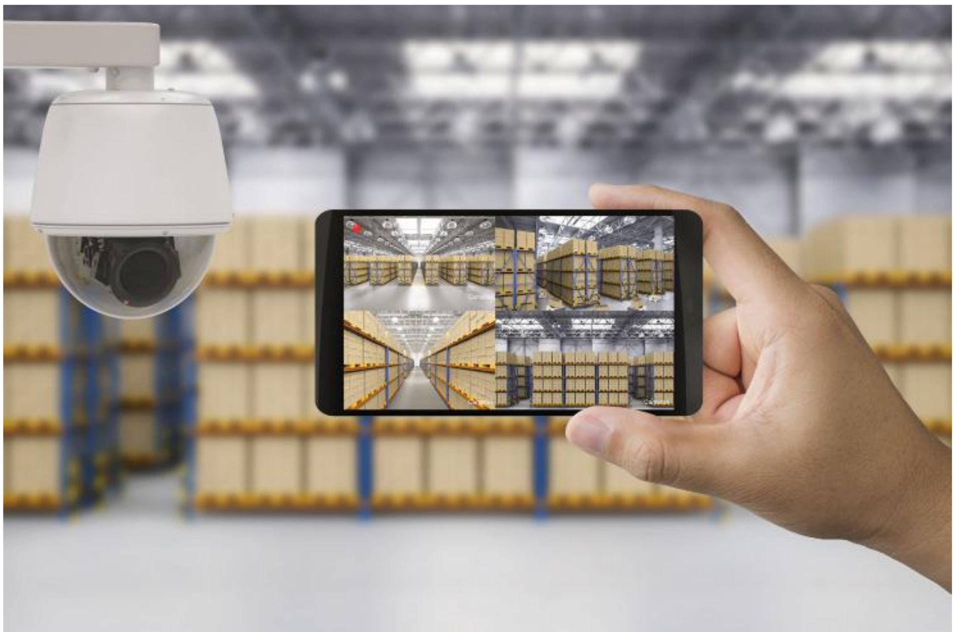
Although attractive high-value items (eg electronics, smart phones and cosmetics) will always be targeted, the portability of a given item and how easy it is to steal and then conceal will be the determining factor of what's illegally appropriated. Whether a particular site is targeted will depend on where it's situated and what it contains, as well as the security measures in place.

Beyond the attraction of valuable portable items, offenders may target other goods (such as works of art or products being held ahead of their release date).

To guard against external threats, organisations need to secure their sites and buildings by using a blend of detection and deterrence methods. This can include a mixture of CCTV cameras, intruder alarms and access control systems combined with a staff/visitor management system designed to ensure that only those individuals authorised are admitted to specific areas of the site.

All that said, the greatest threat to warehouse and distribution/delivery centre stock emanates from 'insiders'. Many of the staff will be on temporary

> To guard against external threats, organisations need to secure their sites and buildings by using a blend of detection and deterrence methods. This can include a mixture of CCTV cameras, intruder alarms and access control systems



contracts or supplied by agencies and often operating on low wages. Organisations can conduct checks to ensure that staff are *bona fide*, while management teams can implement random searches of bags and lockers.

Some areas can be restricted to authorised personnel only. Secure cages can be deployed for high-value items, and both can be monitored thanks to video surveillance systems. An anonymous reporting system is well worth consideration as this encourages suspicions involving co-workers to be reported without fear of reprisals.

During transportation

While being transported, security is a major concern as cargo can be stolen or tampered with in some way. According to the Transported Asset Protection Association, the number of incidents of cargo crime reported for the UK via its Incident Information Service in 2020 was 3,100 (representing a 250% uptick on 2019), with an estimated total loss to the industry of circa £77 million.

Although the *modus operandi* of criminals changes over time, most attacks on vehicles involve the driver having little time to respond. That being the case, it follows that security awareness for drivers is key. In Europe, there have been incidents where gangs have driven up to the backs of lorries, gained access to the trailer, 'surfed' into it and then stolen the goods without the driver being aware.

In the UK, attempts at deception are often used, with criminals stopping lorries by posing as police or Driver and Vehicle Standards Agency personnel. Once the driver has parked up, the vehicle then becomes an easy target.

Although routes are planned in advance to avoid risks, on occasion – for example due to delays or non-compliance – drivers may find themselves in a non-secure area. Here, vehicles are vulnerable to thieves or illegal immigrants. Thieves may simply slash open a soft-sided trailer with knives or gain entry through an unsecured door or a faulty padlock.

Methods of attack targeting cargo are becoming more sophisticated, but so too are the solutions, notably so those incorporating telematics to monitor vehicles and assets using GPS technology, remote immobilisers, sensors, on-board diagnostics and CCTV.

Organisations have a Duty of Care to attend to the Health and Safety of their employees, contractors, visitors and clients. If something should go wrong here, they may find themselves financially liable. Good security can enhance procedures to mitigate against such risks. On that basis, it's vitally important that regular and thorough security and safety risk assessments are conducted.

Cyber security

With many organisations relying heavily on automated processes and large amounts of data being exchanged between those operating within the supply chain, the risk of cyber attack has never been higher. Hackers will often find an entry point into the chain by attacking the less secure elements, enabling them to gain access to the systems and data of other organisations. Companies must work together to build resilience.

Fires in warehouses and distribution centres are not uncommon. The risk is not just centred on product loss, but also smoke or water damage, as well as employee injury, or even the loss of life, so too the resultant disruption to normal business activities.

The risk of flooding is increasing, which can lead to the damage of both stock and buildings and disruption to operations. There's also a risk from high winds. As well as taking the appropriate steps to minimise damage, organisations should document procedures and ensure that staff are 'security aware' and very clear about what to do in the event of an emergency (including an evacuation).

The use of campaigns and protests has significantly increased, creating a constantly evolving threat. On Black Friday last year, Extinction Rebellion activists targeted over a dozen Amazon distribution centres in the UK to highlight what they described as "exploitative and environmentally destructive business practices". Attacks may not be against the organisation directly, either. It could become a target because of the partners with whom it works or due to the nature or brand of goods stored or transported.

Protests can be extremely disruptive and, even when protestors issue a threat, this may cause people to change plans, shut a site or stop trading for the day. To guard against disruption through

activism or civil disobedience, it's important to plan for – and, in tandem, test – a range of scenarios.

Around three-quarters of supply chain organisations experienced some level of disruption and reduced operations due to the pandemic. The changes created new opportunities for criminals and organised criminal groups. There was a significant increase in theft, especially cargo freight, but also from warehouses as stocks built up due to transport backlogs. The effects of the pandemic continue to impact supply chains and security teams need to continuously review their systems.

Security fundamentals

In response to the threat landscape, a number of elements need to be in place in order to achieve good security and remain ahead of the evolving dangers.

With regular risk assessment and planning being the foundation of good security, it's worth taking time to consider whether your organisational and supply chain risk assessments and plans are up-to-date and whether you have a regular documented 'refresh' plan. Have there been any changes in the assets you need to protect (be they people, property, information or reputation)? Are there any new vulnerabilities? Are your assessments incorporating the latest good intelligence – in real-time – and, if so, are you building these into your plan and the way in which you respond?

In the same way that businesses use penetration testing to test cyber security, physical security should be tested against various scenarios. Table-top exercises can be an excellent way in which to identify possible weaknesses.

Organisations can benefit from thinking about training in a more holistic way. Security officers will receive training relevant to specific needs. However, it's also vital to encourage employees to take part in relevant security training. Joint sessions can be invaluable for all concerned and build rapport and understanding, which can then become particularly valuable in an emergency.

The best security solutions will be achieved where security providers and clients work closely together, whether that's on the planning of an integrated security solution or a small change in an existing plan. Collaboration can help to reach the best solutions more quickly. As an example, determine to work in partnership to extend the role of security from just the protection of the warehouse into supply chain transportation.

Strong culture

The development of a strong security culture will ensure that employees are security-conscious and aware of the most effective ways of protecting assets, including themselves. It's important to review the security culture on a regular basis in line with changes to the threat landscape, working practices and the technology being deployed.

Good security makes use of insights and shared information, while also employing Best Practice from first responders. In addition to providing an excellent security service, security officers working in the warehouse and distribution services sector must be proficient in customer service.

Security that's integrated and planned holistically is likely to be far better, precisely because it has been designed to ensure that there are no gaps to be exploited. Physical security, for example, is best when security professionals work in harmony with good technology and when it's integrated with personnel security (ie protecting from the insider threat) and cyber security (ie protecting digital data and systems).

The security world is changing in response to ever-evolving threats. Those intending harm – by whatever means – are adjusting their own outlook in a bid to circumvent security measures as soon as the latter are put in place. Going forward, it's essential that security teams integrate technologies, build a good degree of focused intelligence and evolve practices to suit numerous scenarios. ●

Noah Price is International Director of the G4S Academy
www.g4s.com

Future worlds

Over the next two decades, the world – and with it the future operating environment for policing and security – is forecast to experience dramatic change. This will impact the public and private sectors in the form of threats to business and operating models. However, as David Lydon asserts, it also provides new opportunities for those with the prescience to prepare and plan ahead

NEW CRIME types that emerge are invariably linked to changes and developments in wider society. When new technologies appear, their policing and security implications are often overlooked or otherwise afforded inadequate amounts of attention, which can lead to their exploitation by way of a 'crime harvest' until such time that solutions are forthcoming.

We see many potentials for criminal activity which law enforcement in particular are sometimes unaware of, or slow to predict, identify and respond to in the real world. Most recently, these have included complex digital connectivity through the Internet of Things, nanotechnology, biotechnology, Artificial Intelligence, machine learning, augmented and virtual reality, robotics and cybernetics in addition to developments in transhumanism (itself a philosophical and scientific movement that advocates the use of current and emerging technologies to augment human capabilities and improve the human condition).

While in some quarters the global growth and proliferation of the private security sector is sometimes viewed with suspicion or as being in some way problematic, it's often better placed and equipped to respond to these new threat vectors and capitalise on the opportunities they provide.

Moreover, there's a demonstrable record of the sector driving important innovation and stimulating partnerships and collaborations with public sector bodies, industry and academia towards smarter policing and security provision and outcomes.

As uncomfortable and perhaps unpalatable as it might be for some commentators, the public sector is – and, what's more, will become – increasingly dependent on this crucial and symbiotic relationship as time progresses.

State decline

That relationship – and the threats and opportunities arising in the future – needs to be seen in the context of geopolitics, commercial enterprise and state power and authority. On a global scale, the capacity of nation states to support, maintain and deliver public services is receding. Notably, the remit of public policing is shrinking. In re-visiting the core mission and functions of the police service in England and Wales, the stark realisation is emerging that policing's traditional role in public safety and security and its capabilities and organisational structures are not fit for purpose in the 21st Century. It's an analogue model in a digital world.

Recently, there have been proposals for the strategic reform of policing in

In an increasingly fragmented and less co-operative world, crime and disorder will weaken the state's ability to govern effectively and public policing will be overwhelmed by efforts expended to cope with a chaotic and conflictual society

England and Wales. There's ongoing talk of force amalgamations, a legal duty for larger businesses to incorporate crime prevention into their products and activities, a narrowed focus on emergency response, the issue of safeguarding vulnerability, preventing and detecting crime and harms and community-based policing initiatives. Taking all of this into account, the police service lacks the entrepreneurialism, skill sets and thought leadership to fully meet future safety and security demands on its own.

One way of looking at this is that public sector funding limitations, structural and resource re-organisation and internal learning and development programmes (both academic and vocational) are unlikely to provide the gamut of relational and specialist investigatory and digital skills necessary for the future of public policing. This paves the way for the private security sector to move into these capacity and capability gaps and contribute to public safety and security on an expansive level.

Realistically, any future system of safety and security provision can only consist of an ever-evolving network of private and public sector actors.

Future worlds

The world in which policing and security will operate can be viewed along a continuum of possibilities: one which is based on the configuration of power and levels of co-operation at both the state and non-state levels.

At one end of the spectrum, states will remain all powerful and be able to rely on their existing structures and frameworks for good governance and social control, largely based upon co-operation between the state and the general public and the state and other nation states. This multilateral condition will witness instability through tension and conflict between countries reduced by access to formal frameworks and legal processes.

Going forward, the middle ground will be occupied by a network of public and private actors. However, non-state actors such as large commercial enterprises will increasingly adopt a lead role in identifying and delivering diverse security solutions on behalf of the state. Speaking from the geopolitical standpoint, the rise of private 'mega cities' may see them operating outside the direct control of state authorities altogether.

At the other extreme, the context for policing and security will be seriously fragmented, wherein state and non-state actors (both *bona fide* and criminal in form and intent) compete for power and control. Co-operation will be scarce and self-serving. All parties jostle for the control of resources and space, using any means necessary to advance their goals. With areas of the world unfit for human habitation, communities will become somewhat congested and, that being so, vulnerable to exploitation.

The impact of these potential future worlds on security is likely to reflect the level of co-operation between the various parties. For example, where states have a legitimate commitment to maintaining the status quo, they will be disinclined to conflict with each other and seek to ameliorate societal unrest to stabilise society. Measures aimed at doing so will by no means be the sole preserve of the public-facing police. As stated, there's a recognition that public policing cannot effectively and efficiently deliver crucial safety and security outcomes alone.

This is particularly so where investment in technology, digital skills and managed services is necessary. Historically, the police service has been poor in developing, implementing and applying technology for operational use. Transitioning from a model of reactive crime detection to an initiative-taking and preventive one will place even greater reliance on the service.

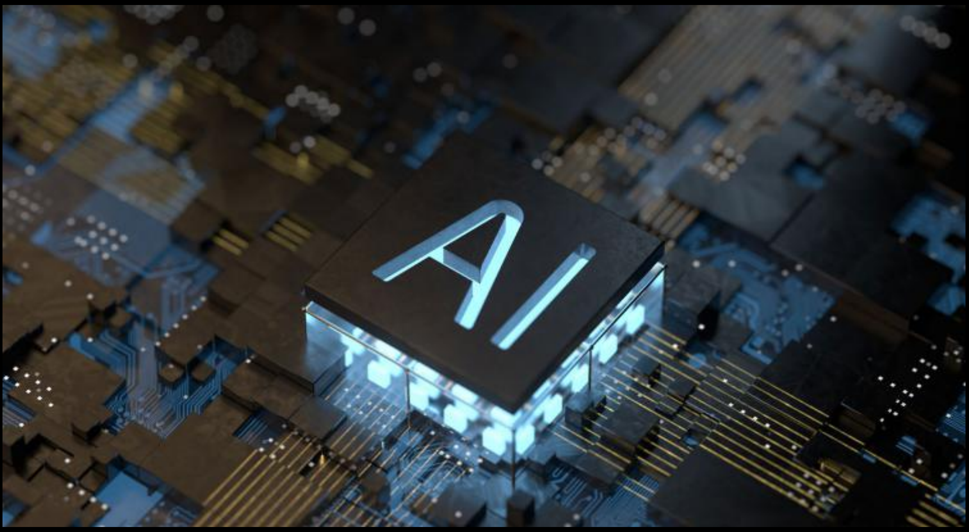
Good governance

In an increasingly fragmented and less co-operative world, crime and disorder will weaken the state's ability to govern effectively and public policing will be overwhelmed by efforts expended to cope with a chaotic and conflictual society that's fuelled by civil unrest and criminality. Effectively, this will bring about the breakdown of good governance and civilised society.

It's worth noting here that none of the potential worlds outlined are fixed. Both state authorities and non-state actors strive to mould the future to their own ends for good or ill. They do, however, provide scenarios to be considered, planned and prepared for as far in advance as possible.

Elements of these future worlds may combine into a complex operating environment. Further, they may well be dictated by influences beyond human control and the unintended consequences of human activities. For example, greater inequality and social unrest could well lead to gross deprivation and increased levels of violence with unregulated online (mis)information polarising communities and fomenting hate.

There could be technology-related unrest generated by the dependence on Artificial Intelligence and automation, an increased vulnerability in an elderly and diverse population, a chaotic global economy and a state of climate emergency leading to competition for food, fuel and other resources deemed essential. The intersection of these



influences, in as yet unforeseen ways, is likely to create uncertainty for policing and security provision. All the more reason, then, to plan and prepare for their occurrence in the present moment.

Predictable implications

According to global strategic trends analyses, there are predictable implications for policing and security in these future worlds that require careful consideration and the planning of responses. The implications themselves represent many opportunities for the private security sector.

Rising inequality (engendered, for example, by income disparity), increasing inflation, lack of opportunity and social deprivation are likely to lead to a more polarised society. There's research evidence to suggest that such developments contribute to increased levels of acquisitive and violent crime. Not only will this damage social cohesion, but the police will become more involved in combating that crime on a much larger scale. If the scale of violence reaches critical levels, then it may well stretch policing resources beyond their capacity. At that juncture, other ways in which to manage crime problems will be necessary.

Advances in digital technology and a perceived lack of regulation make the creation and distribution of information and misinformation much easier. Two developments in this area are the problems arising from fake news and so-called 'deep fake' technology.

The former can be used to incite societal tensions, in turn leading to extremism and hostility. While states can and do use this technology for their own means, malign state actors also do so to attack other countries and undermine trust and confidence in the authorities. Diligent fact checking and the controlling of narratives will be vital tools in countering misinformation.

'Deep fake' technology is exploited by criminals for the purposes of extortion, fraud, bribery and corruption. These are areas in which the police service has been reluctant to engage, particularly without having the specialist resources and legal frameworks to do so. However, all are spheres of operation where the private sector is well versed and capable.

Beyond digital technology in the form of social media looms the convergence of technologies, such as (*inter alia*) the Internet of Things, Artificial Intelligence, augmented and virtual reality, automation, robotics, nanotechnology, biotechnology and transhumanism. This convergence will provide new ways for criminals to operate in terms of designing and 'selling' the means to commit crime as well as using it themselves.

It will be somewhat difficult for the police service to equip itself with the means and resources to respond to this crime model. The police service might also be reluctant to engage due to the ethical concerns involved in doing so.

Extensive engagement

Where the police service itself employs cognate technologies for crime prevention and detection, it will face challenges in identifying, procuring, operating and supporting such technologies internally. There's a requirement for extensive engagement with the private sector within an appropriate governance structure.

With the economic and societal impacts of 'climate emergency' increasing, policing is likely to operate within a legislated 'green' agenda aimed at decarbonisation. This will require investigation, enforcement and prosecution of 'carbon' criminals.

Organised criminals may exploit opportunities to commit 'green' fraud or seek ways of circumventing regulation. Responding represents a paradigm shift in public policing. Should the police be the primary agency involved in that response? This remains in question.

Private security providers will not be immune to the impacts and consequences described. Indeed, those impacts and consequences may well pose existential threats to business models and commercial interests on a global scale.

The potential future worlds and their implications raise two significant challenges for security providers. One is all about planning and preparing for threats and their implications. The second is focused on planning and preparing for the opportunities they present.

How 'future fit' is the security sector? Developing thought leadership and adopting a futures-centred mindset will be absolutely critical in the future world of policing and security. ●

Dr David Lydon is Senior Lecturer in Professional Policing at Canterbury Christ Church University
www.canterbury.ac.uk

Streamlining with software

Advances in technology are increasing the number of tasks we can automate on a daily basis. Machines magically brew the perfect cup of coffee before you leave the comfort of your own bed. The lights are on when you arrive home from a long day at the office. The list is seemingly endless, but what about automation when it comes to your security installation business? Simon Tushingham Jones has the inside track

THE INTERNATIONAL Society of Automation (ISA) outlines that the dictionary definition of 'automation' is the technique of making an apparatus, a process or a system operate automatically. The ISA itself defines automation as the creation and application of technology to monitor and control the production and delivery of products and services. Whichever definition you choose to adopt, automation describes a wide range of technologies that, in essence, reduce human intervention in processes.

Importantly, automation encompasses many vital elements and systems and duly delivers benefits to so many key industry sectors. Think of the utilities (eg oil and gas, water and wastewater, telecommunications and electric power), manufacturing (eg chemical and petroleum production, food and pharmaceuticals) and transportation (eg railways, aviation and automotive).

Drilling down a layer or two, process automation manages business processes for uniformity and transparency. Typically, this form of automation is handled by business apps and dedicated software. It has been demonstrated that the use of process automation can increase productivity and efficiency within a given organisation.

Further, it can deliver new insights into everyday business challenges and, what's more, suggest solutions. Workflow automation, for example, is a specific type of process automation.

The increasing trend towards using field service software to help organise business procedures and provide more insight into what's working – and, equally importantly, what's not – can only be seen as a positive development. That said, moving a security installation business towards software and harbouring the goal of 'going paperless' is just the beginning. Even more can be done to make work easier, faster and more profitable. Field service software is the 'power-up' mechanism that, if used correctly, can elevate a business to the next level.

> The increasing trend towards using field service software to help organise business procedures and provide more insight into what's working - and, equally importantly, what's not - can only be seen as a positive development

Technology in the trades

Technology has come a long way in the trades. Armed with the right software, members of staff in a security installation business are able to communicate with convenience and ease. Rather than having to call the office, engineers out on site can use their mobile devices or tablets to relay important information in an instant. In addition, if the end customer wants an update on a particular job, this is deliverable with one central tool.

The transparency that today's technology provides builds trust and positively reinforces the security installation business' name in the market. It can also assist in building long-lasting relationships with customers, duly encouraging repeat business and word of mouth referrals.

Field service automation is the use of software and other management tools to automate what might otherwise be deemed tedious and time-consuming everyday tasks and processes. The main goals of automating processes and procedures are to improve the overall efficiency of the workforce, increase productivity and free up some more valuable time for high-value tasks.

Administrative tasks such as organising incoming data from e-mails and scheduling and creating work orders can drain time from the working day. Automating workflows, though, can increase the efficiency of your team.

Scheduling staff is a necessary and everyday job, so why not look to make it an easier and faster procedure? Scheduling efficiently is crucial to a smooth-running trade business such as a security system installation company

Whether it's a last-minute job or scheduling security maintenance projects on a monthly basis, data, customer information and business processes need to be considered. The good news is that software helps take the 'juggling act' out of scheduling and can often automate the different processes that go into creating job orders and delivering staff to site as soon as possible.

Software with mobile apps can also speed up communication to make reacting to job changes faster by eliminating phone calls back and forth from the site to the office. Importantly, this type of functionality alerts field engineers to changes in their schedule in real-time. It even allows them to clock in and out from each job from their mobile device. That being so, billable hours are tracked with absolute accuracy.

Reduce billing errors

Using one form of software for the management of a security business is a great way in which to collect data and keep track of jobs, communication and billing. With an app, teams of on-site engineers can track time on the job, equipment and stock used. They can also invoice and collect payment while on site. This minimises the risk of making a mistake during any part of the job workflow that will impact the invoice.

Think how much easier it would be to have one centralised tool where you can manage jobs for staff, re-arrange schedules, invoice customers and send purchase orders to your suppliers. With electronic invoicing, you have the ability to send an invoice by e-mail and receive payment at a speed with which paper-based methods simply cannot compete.

Planning and making sure security service jobs are booked ahead of time saves any future confusion and serves to build credibility with the customer base. These jobs can be based around contracts which are easy to manage with maintenance planning software. However, there's more than one way in which to manage maintenance work.

Managing a team around the work that's coming up, and notably so repeat visits to sites for preventative maintenance tasks, is a process that needs to run smoothly. Investing in the process and offering this type of service for your customers will add another string to your bow, build brand credibility and encourage customers to procure your services going forward. Software eliminates the tedious nature of asset management. Use it to manage work orders, capture asset readings and quote asset defects on a swift footing. Field apps can also be used to update asset statuses in real-time and streamline maintenance workflows for faster service.

Additionally, most software can support the management of recurring maintenance schedules and even set up automatic recurring invoices, thereby eliminating the need to manually create new paperwork every time a maintenance check occurs.

Further, innovation through the Internet of Things, for example, continues to simplify asset management. With the implementation of remote monitoring through sensors, businesses can now move away from regular maintenance and instead be alerted to faults in real-time by the assets themselves.

Faster service

Security installation business owners are very busy people. Their customers are busy people as well. All of the businesses working in the supply chain for equipment and materials are busy. Quite often, it's the businesses that work fast and provide great service while doing so that reap the rewards.

Field service automation enables businesses to complete tasks that once took a long time on a far quicker basis. This means that every workflow benefits: the booking of an emergency job, payment collection, route optimisation to a job site. Everything is faster.

Nobody likes to be kept waiting, and particularly so when making enquiries about a given service that an installation business can provide. The faster you can respond to your customers, the faster you can encourage business contracts through the front door. When you're able to focus on delivering prompt responses, you can then complete jobs much faster and generate more revenue.

If the last few years have taught us anything, it's that agility is key for future-proofing and succeeding in the trades. Automatic data collection is one of the most important aspects of maintaining an agile company. Running a security business using software enables the automatic collection of data from every aspect of the business. For example, reporting can showcase where a business is making and losing money, which jobs are most profitable, if projects are running on time and whether stock is running low. All at the click of a button.

Often, necessarily detailed reports can even be customised to pull out specific information of key interest or otherwise be set to publish every month such that even more time is saved. Goodbye and good riddance to spreadsheets.

Ever lost a job card? Not sure why a whole heap of stock is missing? Frustrated that one of your field engineers forgot to track his time on jobs today? Manually tracking data and shuffling paper is the cause of unenviable amounts of headaches. With many security system installers at the mercy of changing schedules, the situation can quickly develop into chaos. With automation and software, not only is time saved, but errors are proactively reduced and, importantly, customers are happier.

End-to-end solution

One company that has secured its future with software is US-based SL Security Pros Inc. Like many security businesses, SL Security Pros Inc started out without any technology to help support daily operations. Owner and CEO Joseph Kasenchak and his team mostly used pen

and paper to manage the business before bringing software solutions on board in the early part of the 1990s.

Fast forward to more recent years and the SL Security Pros Inc team – which has grown to encompass 25 employees taking care of intruder alarms, CCTV, access control and home automation solutions – had kick-started the process of using multiple software platforms to manage jobs and projects from start to finish as well as invoice recurring service clients. However, this caused significant inefficiencies that severely hindered cash flow and, further, hampered the ongoing growth of the business.

With so many steps and the manual entry of data needed to keep jobs on track, the room for error was high, but that wasn't the only issue. The jobs took longer to invoice because of these inefficiencies and errors began to creep in. Inconsistencies in billing practices prevented proper cash flow, making it more difficult for Kasenchak and his colleagues to manage profit and loss.

Without a complete view of overall performance, growing the business became a daunting task. The demand for SL Security Pros Inc's security expertise and offer was increasing exponentially, but in the background the company's back office software and business practices were antiquated and could not keep up with company growth.

In short, SL Security Pros Inc needed to upgrade to better software that would streamline processes and allow the organisation to manage jobs from start to finish in one end-to-end solution.

> The enhanced visibility that's actively delivered by an end-to-end software solution assists in collecting, tracking and analysing vital data such as notes added at the customer's site and job completion times

Having evaluated different field service management software solutions over a five-year period, the business decided to select an end-to-end, cloud-based solution developed by simPRO.

The next level

If you firmly believe it's time for your security business to move to the next level, then look no further than field service automation. The benefits can be life-changing. An investment in field service management software can realise substantial benefits including the co-ordination and monitoring of employee schedules, customer appointments and timelines. Optimising those appointments saves valuable time, while the ability to automate central tasks including dispatch, scheduling and invoicing procedures reduces the opportunity for errors creeping in.

One key – and often overlooked – benefit to be realised is that engineers on site are given more time with customers because repetitive and manual administration processes are removed. The enhanced visibility delivered by an end-to-end software solution assists in collecting, tracking and analysing vital data such as notes added at the customer's site and job completion times.

Increased communication and transparency between on-site engineers, the security systems installation business' management and that company's customers is hugely beneficial, leading to greater levels of operational efficiency and productivity among the workforce. ●

Simon Tushingham Jones is Vice-President of UK Sales at simPRO
www.simprogroup.com

Meeting the challenge

Thousands of security professionals representing more than 70 countries descended on London's Olympia from 27-28 September as the Nineteen Group-organised International Security Expo – for which Security Matters served as Lead Media Partner – returned to showcase the very latest technological innovations designed to protect people, businesses and the UK's Critical National Infrastructure. Brian Sims reports

WITH MORE than 300 companies demonstrating thousands of the most cutting-edge products and solutions available in the sector, attendees were treated to an unmissable opportunity for in-person demonstrations and insights, in turn helping them to understand how today's technology can meet both current and future challenges.

Demonstrating the event's invaluable role in facilitating new product launches, many exhibitors took the opportunity to unveil their latest innovations, sharing all-new technologies and refreshed solutions to a packed audience of buyers from the UK and international territories.

Among them, **Apstec Systems** announced the launch of a new version of its Human Security Radar. Version 4 of the innovative system provides high-throughput, low-contact security screening and ensures a "seamless" security experience for people being screened. It delivers "proven and effective" functionality in an attractive, smaller and more mobile unit that's perfectly suited for deployments at prestigious locations.

Elsewhere on the show floor, **Apex Vanguard** demonstrated its Hecate ruggedised tactical camera system – a specialised IP67-rated multi-platform camera system featuring a wide view day camera, IR night camera and a **FLIR** thermal imaging camera all-in-one system. It's supported by an integrated COFDM microwave transmission module with all the video and data transmitted to a fully functional ergonomic hand-held receiver unit.

Demonstrating two new product launches, **LINEV Systems UK** revealed its PROTEUS range of baggage X-ray security systems. The range is fully equipped with the latest Artificial Intelligence features to help detect pyrotechnics, flares and smoke bombs.

The company also showcased Clearpass C.I., itself an X-ray scanner designed for smaller spaces. With a footprint of just 0.85 m², the technology offers "exceptional" mobility and "the fastest scan acquisition time available on the market". It's available with advanced contraband detection software and designed to detect contraband 'on' or 'in' the human body. By allowing selective area-focused screening, this solution also reduces screening and overexposure to other parts of the body.

> The International Security Expo also played host to the National Crime Agency, Counter Terrorism Policing and representatives from the Home Office, who held a behind closed doors event for Project Interknow

Analytics and investigations

X-ray capabilities were also the focus of the **Videray** stand, where the company announced its new PX Ultra – the “most powerful” handheld backscatter X-ray imager on the market. After nearly three years of development and testing, the PX Ultra uses the first 160 keV X-ray source, enabling operators to see through up to 10 mm of steel. It features the same ergonomic form factor and intuitive software used by the popular PX1, reducing its scatter and leakage measurements by a factor of two.

Meanwhile, Canadian defence and security start-up **Patagona Technologies** demonstrated its THREATDESK analytics and investigations platform. This solution provides OSINT analysts with the tools to combat co-ordinated information operations by state and non-state actors. It allows analysts to gain deep insights into online threats such as co-ordinated influence operations, online radicalisation and information security threats by dint of leveraging hundreds of online data sources from news, forums and social media platforms.

Across the show floor, product demonstrations helped to bring the latest security technologies and solutions to life. In the Loss Prevention Certification Board Live Testing Lab, crowds gathered to witness a team of professional forced entry specialists put a range of physical security products through their paces.

Located in the show’s Perimeter Protection Zone, supported by the Perimeter Security Suppliers Association and sponsored by **Barkers Fencing**, the line-up for the Testing Lab included products from exhibitors including **Eagle Automation**, **CLD Fencing**, the **Bradbury Group**, **Jacksons Fencing**, **Lochrin Bain** and **Surelock McGill**.

Product innovation

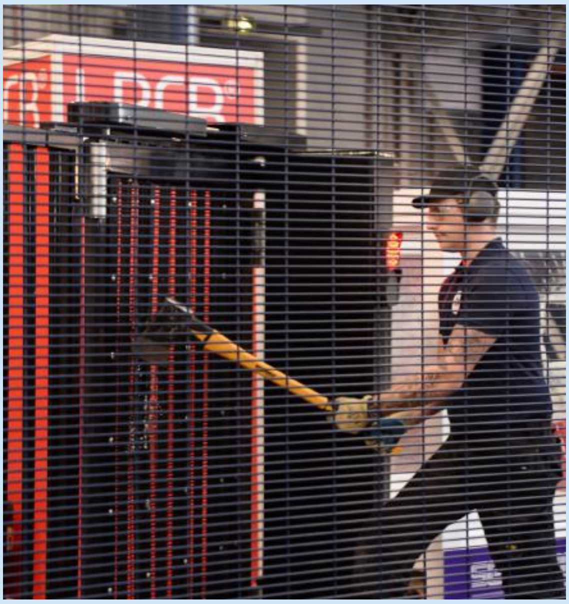
The Product Innovation Theatre provided a vital platform for the likes of **QinetiQ**, **Greyscan Australia**, **T3K.AI**, **Pimloc Limited**, **Everbridge** and **Global Security Solutions** to share the rationale behind their latest innovations and the challenges they’re designed to meet.

For example, **Smiths Detection** showcased its Canary Biological Detection Technology, which uses a genetically engineered immune cell called a ‘biosensor’ to identify and then bind to a specific target. When a pathogen is found, a reaction starts causing the biosensor to luminesce. By measuring light output from the cell, it can determine if the target biological is present in the sample.

Returning to the Product Innovation Theatre on Day Two, members of the Defence and Security Accelerator team introduced suppliers funded under the Innovative Research Cell 2020 for Explosives and Weapons Detection. The suppliers – **Iconal Technology**, **Fraunhofer UK** and **IRsweep and Metrasens** – shared insights on the projects funded through this competition and the opportunities for like-minded businesses to become involved.

Among the sector-specific zones helping attendees target the suppliers specialising in the products or solutions most relevant to their challenges, the updated International Risk and Resilience Zone highlighted the fundamental aspects of ‘Resilience’, ‘Prevention’, ‘Response’ and ‘Recovery’. It united specialist manufacturers and service providers of products that businesses need to remain resilient during a crisis.

Speaking about the increased focus on resilience, Chad Simpson (resilience and security lead at the Science Museum Group) said: “The show extensively covers both the security and resilience sectors, which makes it a ‘no brainer’ to attend for somebody like myself who needs to be clued up on industry and market trends for both. It really is the place to be for new product innovation. There’s a wealth of expertise.”



Meanwhile, the Government Zone returned to demonstrate the continued support the event receives from central Government. With attendees joining from Border Force, the British Transport Police, the Joint Security and Resilience Centre, the Home Office Publicly Accessible Locations policy team, UK Defence and Security Exports, the National Counter-Terrorism Security Office and FCDO Services, this area of the show served as a one-stop shop for the latest insights into Government initiatives and tactics designed to respond to current threats and challenges.

The International Security Expo also played host to the National Crime Agency, Counter Terrorism Policing and representatives from the Home Office, who held a behind closed doors ‘invitation-only’ event for Project Interknow (the UK’s response to the emerging threat of privately manufactured and 3D-printed firearms).

Guest speakers representing Europol, the ATF, the Dutch Police, Kings College London and Armament Research Services covered the history of 3D-printed firearms. Together, they explored the threat, sharing Case Studies and the investigative opportunities and intelligence requirements in place to enhance law enforcement and private industry’s collective response.

Industry experts

This year’s hotly anticipated conference programme witnessed record crowds gather to hear from myriad industry leaders. Three streams ran over the course of the two days: the Global Counter Terror and Serious and Organised Crime Summit, the International Security Conference and the International Risk and Resilience Conference.

In the Global Counter Terror and Serious and Organised Crime Summit, Tom Tugendhat MP (the newly appointed Minister of State for Security) joined attendees to deliver an address. Tugendhat duly recognised the importance of transparency and freedom for long-lasting democracy and duly reflected on the success of Operation London Bridge, with the seamless delivery of Her Majesty Queen Elizabeth II’s State Funeral being its focal point.

Sharing unique insights into the collective efforts behind Operation London Bridge, Assistant Commissioner Matt Twist (representing Counter Terrorism Policing) spoke about the breadth of the operation from the integrated counter-terror package right through to the 'biggest ever deployment' of law enforcement and supporting Government agencies. Twist also revealed that the counter UAV response investigated 80 flights. Those behind four of these flights are now facing prosecution for their intended actions.

Among the other topics under the spotlight at the Global Counter Terror and Serious and Organised Crime Summit, the 'chronic and corrosive threat' of serious and organised crime was addressed by Matt Horne, deputy director of investigations at the National Crime Agency. Horne detailed the alarming scale and complexity of the evolving threat, which is costing more than £37 billion every year to defend against.

Further, Horne revealed that serious and organised crime rates are climbing and now exceeding pre-pandemic levels, with many offenders increasingly taking advantage of technology, which has witnessed a huge upsurge in adoption over the course of the COVID-19 pandemic. Describing it as a "technological arms race with criminals", Horne stressed the importance of updating legislation, collaborating with industry and academia and adopting "innovative" protection measures.

One of the other topics dominating the agenda was the pending Protect Duty legislation. Among the speakers joining to discuss this topic was Shaun Hipgrave (director of Protect and Prepare within the Homeland Security Group at the Home Office). Hipgrave reminded attendees that terrorism doesn't abide by conventional boundaries and stressed the importance of an adaptable 'whole community' approach. He reflected on the progress made to date on the Protect Duty legislation, citing it as a "once in a generation opportunity" and suggesting that a change of culture is required for security precautions to be normalised.

International views

The International Security Conference featured a series of sessions examining the pending Protect Duty. Adam Thomson (head of the National Counter-Terrorism Security Office) revealed how the Publicly Accessible Locations Programme and policing response is designed to make the public safer from terrorist attacks. Thomson ran through ideas for a future operating model, indicating which processes will be used to tackle the growing diversification of terrorist attacks.

In addition, Julian Platt (deputy national co-ordinator for Protect and Prepare within Counter Terrorism Policing) provided a snapshot of Protect and Prepare – how it's changing and what organisations need to be aware of. He stressed the importance of bringing like-minded individuals together and encouraged attendees to visit ProtectUK, an information sharing platform designed to make the UK the safest place in which to live and work for all its citizens.

The platform, which was launched this year, is a new central hub for counter-terrorism and security advice. It's designed to help business owners, security professionals and members of the public alike gain access to the latest news and online courses that will enable everyone to be better prepared.

In one of many panel sessions taking place over the course of the two-day event, five industry experts joined forces to explore the impact of diversity on the provision of a secure environment. They included Satia Rai (CEO at the International Professional Security Association), Rick Mounfield CSyP (director at the Optimal Risk Group), Seetan Varsani (director of major accounts and strategic development for Corps Security), Anna-Liisa Tampuu (co-chair of the Inclusive Security Special Interest Group at The Security Institute) and Chris Middleton of Corps Security representing IFPO UK.

Together, the panel members agreed that it's only when there are role models in the industry standing for equality and diversity that significant change will happen. They encouraged business owners to overcome their fear of political correctness and tackle the issues, encouraging conversation to increase equality and diversity in the workplace. Here, it was stressed that a two-way discussion that's consultative and constructive is key.

The International Risk and Resilience Conference welcomed influential industry leaders who offered attendees actionable insights to survive a crisis and rebuild. Among them, security consultant Mike Croll spoke about the risk of terrorism in the UK and the impact of the proposed Protect Duty legislation. Croll discussed the practical challenges of implementing the Protect Duty, which is anticipated to cost more than £825 million per annum on inspections alone.

Attendees at the International Security Expo also benefited from its co-location with the industry's newest cyber security event: the International Cyber Expo. Bringing together cyber security veterans and newcomers, its debut as a stand-alone show saw exhibitors welcome the crowds as they searched for the latest cutting-edge technologies.

From CISO Round Tables and informative talks through to immersive demonstrations, the Expo served as the ideal networking hub for myriad practitioners, among them software developers and Government officials.

International Security Expo returns to London's Olympia on 26-27 September 2023. Visit the event's website at *www.internationalsecurityexpo.com*

Topics of conversation

Wednesday 9 November witnessed the Security Matters Digital Conference 2022 being broadcast live online, duly affording delegates no fewer than 12 detailed presentations of Continuing Professional Development-approved content covering a plethora of key subjects. In the first instalment of a two-part review, Brian Sims (chair for the one-day event) looks back on the morning sessions

THE SECURITY Matters Digital Conference enabled delegates – all of whom could register for free – to view the excellent content delivered on the day as well as network with each other and sponsor Heras via the live chat function.

Pleasingly, the Security Matters Digital Conference was supported by many of the sector's leading organisations, among them ASIS UK, the Business Continuity Institute, the IASME Consortium, the International Foundation for Protection Officers (IFPO), the Institute of Risk Management, the Institute of Strategic Risk Management, the International Professional Security Association, the Internet of Things Security Foundation, the National Security Inspectorate, the Security Systems and Alarms Inspection Board and TINYg.

Generous and welcome support was also kindly provided by the Nineteen Group – through The Security Event (for which Security Matters serves as the Lead Media Partner) and the International Cyber Expo – and, of course, The Security Institute.

The day began at 9.00 am with another superb delivery courtesy of David Rubens CSyP FISRM, executive director at the Institute of Strategic Risk Management, who chose to talk about the security lessons learned in 2022.

It was Churchill who once said of the Balkans: "Their problem is that they have too much history." It was one of Churchill's successors, namely Harold Macmillan who, when asked what the biggest challenge was in politics, replied: "Events, dear chap, events."

It seems each year that passes becomes increasingly full of major events that will make it on to the pages of history books due to their magnitude. The question is no longer whether our world is changing, but whether we're being agile enough in identifying the challenges and adopting appropriate strategies to prepare ourselves for the high-level and potentially existential impacts that change will bring.

Pandemics were on the Risk Register, but the Russian invasion of Ukraine wasn't. Once unthinkable, the frightening prospect of nuclear conflict is now back with us

Rubens recounted that, 12 months ago, there was a general consensus we were emerging from bad times. We were dealing with COVID-19 and 2022 would be a year of recovery. How has it panned out in the real world, though?

Rubens referenced the great academic Patrick Lagadec who once talked of "unthinkable events in inconceivable context". "Pandemics were on the Risk Register," asserted Rubens, "but the Russian invasion of Ukraine wasn't. Once unthinkable, the frightening prospect of nuclear conflict is now back with us."

What can security professionals do to engage with such issues and bring their insight, wisdom and capabilities to bear? The planetary system is becoming unstable. Events driven by this are now higher impact. Economic impacts are being felt. "Leadership can exert an impact in terms of trust, vision and methodology," observed Rubens, "but we are certainly in tough times."

Rubens quoted from a House of Lords document prepared by the Select Committee on Risk Assessment and Risk Planning. That document asserts: "We found a dangerous level of self-confidence in a risk assessment system which is, in many ways, deficient. Before the pandemic, the UK's approach had been internationally commended and was generally viewed as rigorous. Afterwards, not so much."

There's a widely held belief that many of the bodies primarily responsible for coping with risks feel ill-informed and under-involved. "Security and risk managers can make a difference," stated Rubens. "They just need to be given the opportunity to do so. Structure and methodology is what we do."

Professionally protected

At 9.40 am, Mike Reddington (CEO at the British Security Industry Association) began to outline the 'People, Property, Places: Professionally Protected' campaign focused on promoting security officer services. The soft launch took place on 24 July (ie International Security Officer Day), with the official full launch taking place on 31 October.

The national campaign seeks to raise awareness about security officers and their work, improve recruitment and retention in the sector and promote the benefits of purchasing professional security services among the client base.

It follows on, of course, from 'key worker' status for security personnel having been secured during the height of the pandemic. "We want to build on that," affirmed Reddington, "as this sector, and those operating diligently within it, still have a relatively low profile."

Multiple themes frame the campaign: training and apprenticeships, the Living Wage, reputation, equality, diversity and inclusion, Corporate Social Responsibility, client satisfaction and the strengthening of partnerships.

"We want to promote security as a career of choice," continued Reddington. "A career for anyone from any background that's underpinned by a good salary and genuine progression opportunities. It's a job of service embracing technology and aspirations. Security is a valuable asset to society and a benefit for all."

Readers of Security Matters who would like to learn more about the campaign should visit the British Security Industry Association's website at ***www.bsia.co.uk/professionally-protected*** and also determine to search for #SecurityCareerofChoice on Twitter.

Perimeter protection

From 10.20 am-10.50 am, Daniel Fryer (account manager for perimeter intrusion detection systems – ie PIDS – at Security Matters Digital Conference sponsor Heras) offered his considered perspectives on perimeter protection.

As a business, Heras designs, manufactures, supplies, installs and services permanent and temporary perimeter protection solutions for customers across numerous business and industry sectors. Solutions focus on demarcation, entrance control, detection and integrated systems.

Fryer commented that a fence line where systems (such as CCTV cameras and alarms) have been fitted becomes a smart fence. "There are several benefits

to be realised with PIDS," reasoned Fryer. "Security staff will be notified of an alarm event as the would-be intruders are attempting to gain entry. The host organisation can cut down on damage and theft, thereby resulting in lowered insurance claims. These systems are also very stable and require only low levels of maintenance and support."

Not every client needs a PIDS installed. They may be fine with some fencing and additional CCTV. There will be a security audit to determine the requirement. Fryer referenced a Case Study of a warehouse from which an average of £10,000 worth of tobacco was being stolen every month. Using the Heras Security Model, PIDS and CCTV were subsequently integrated to eliminate blind spots. Any potential intruders are now flagged and the police notified.

Mental health

Unfortunately, Chris Middleton CSyP MSyI – a member of the Advisory Board for IFPO UK and due to present at 11.00 am – was caught up in traffic on the M25 due to a Just Stop Oil protest. Thankfully, Mike Hurst CPP MSyI – chair of the Advisory Board – was able to step in at the last minute and deliver a succinct round-up of the hugely important Security Minds Matter campaign.

IFPO was established over three decades ago, with the UK Advisory Board active since 2020. The organisation exists to promote, educate and certificate front line security personnel, assist in realising career pathways for them and also focus on issues pertaining to their mental health and well-being. The latter objective is really where the Security Minds Matter campaign – itself an industry-wide project supported and championed by the Security Industry Authority (SIA) – comes into the equation.

Last year, UK workers took over 319 million days off due to illness at an estimated cost to employers of circa £43 billion, while mental health issues were the prime cause for absence from the workplace in 2021.

Many employees experiencing poor mental health will struggle in their job roles, coping by working longer hours (sometimes even when they're unwell) or on their days off when they should be resting. This is known as presenteeism.

A recent study conducted by researchers at the University of Portsmouth investigated the impact of violence, verbal abuse and physical abuse perpetrated on security officers. 750 officers were interviewed. 40% of them exhibited tendencies towards Post-Traumatic Stress Disorder.

Mark Button (Professor of Criminology at the University of Portsmouth and an IFPO UK Advisory Board member) suggests that mental ill-health is not being taken seriously enough by security managers. "There's an emerging picture of a failure by the industry to address this issue."

What, then, can be done to help? "Management needs to be about empathy," affirmed Hurst. "There has to be a culture of treating people as people and not as symptoms. It's a good idea to appoint 'Mental Health Champions' in the business and share useful links and resources among members of staff."

Security Minds Matter was launched in 2021. There are roughly 360,000 individuals holding around 400,000 SIA licences, plus in-house security personnel. This is the target audience. Objectives encompass amendments to BS 7499, including an element of mental health within the Approved Contractor Scheme assessments (Health and Safety's listed, but not well-being) and a desire to partner with a mental health charity and/or support group.

> Not every client needs a PIDS installed. They may be fine with some fencing and additional CCTV. There will be a security audit to determine the requirement

Further detail on the Security Minds Matter campaign is available online at ***www.securitymindsmatter.org***

Security convergence

ASIS International has put a great deal of effort into analysing the relationship between physical security, cyber security and business continuity in modern organisations with a view towards determining Best Practice for creating more effective and cost-efficient security in tandem with risk-focused operations.

Despite years of predictions about the inevitability of security convergence, however, it remains the case that relatively few organisations have converged their physical and cyber security functions.

From 11.40 am until 12.10 pm, that subject was aired by four specialists in this domain, namely James Willison (project and engagement manager at the Internet of Things Security Foundation), Sarb Sembhi (CEO of Virtually Informed), Nigel Stanley (director of cyber security at Jacobs) and Allan Dickinson (technical director for Advancis, the specialist in open architecture Command and Control system software for integrated security and building management).

Willison began by outlining convergence, which is the bringing together of different security functions and other departments within an organisation – such as Human Resources, legal and finance – to identify, prevent and respond to all security risks across the business.

"We need to do this if we're to have any chance of countering cyber-physical threats," stressed Willison. "Ultimately, it's all about focusing on effective real-time response."

In 2021, ASIS International conducted a Security Convergence and Business Continuity Survey. The results suggest there has been an increase in convergence being applied. Of the 40% of respondents who are not presently looking at a convergence model, 20% of them do feel it will happen across the next two years. 60% of companies are converged with business continuity.

"At Advancis," commented Allan Dickinson, "we are certainly starting to witness an increase in clients talking about the subject of convergence, but perhaps the manufacturing side needs to do more in order to help them along this route."

Conversely, Nigel Stanley isn't seeing an uptick. "Budget, politics and lack of leadership are coming into play," suggested Stanley. "The converged approach makes complete sense."

Sarb Sembhi observed: "Physical security people are now having to be involved with the cyber realm. There is a perception that there's convergence, but it's more of a 'dipping the toe in the water' exercise. It's a start, though."

As Nigel Stanley correctly pointed out, practitioners' involvement in the cyber realm is something of a natural segue into the convergence model.

Integrated delivery

The scramble for 'tech' advancement and adoption is only quickening in the current global crisis. The latest GDP figures for the UK point towards a sharp and deep recession and one that may take some time to ameliorate. The loss of jobs in the economy is going to take its toll on the Government's spending and investment plans. In a similar vein, plans for companies in terms of new investment could well take a hit.

Set against that backdrop, service delivery must lead from the front and adapt to what's now an ever-changing world and business environment.

Bob Forsyth (CEO at Kings Secure Technologies) joined conference at 12.20 pm. Focusing on 'Integrated Service Delivery: Differentiation and the Role of Technology', Forsyth proceeded to explain that such delivery is concentrated on being ready to invest time and collateral in new technologies that will make a valuable difference to a client's estate and/or benefit that company's overall productivity.

Forsyth began his first-class delivery by outlining some of the key economic issues that are driving the need for change and innovation within the security business sector. COVID-19 has cost the UK's economy circa £167 billion. The Russian invasion of Ukraine has realised huge issues. The Real Living Wage has increased. The National Minimum Wage will ramp up in April. Interest rates are rising. Recession is upon us in tandem with political turbulence.

"For me," observed Forsyth, "technology should lead to increased productivity and cost prevention or reduction. Deep analyses of spend and outcomes are now considered a key component when you're talking about investment data driving decision-making. Earlier adoption is becoming aggressive due to the drivers of ratcheting costs and recruitment challenges. What's more, risk is being scaled back by the pace of opportunity."

In simple terms, the Kings Secure Technologies model is about data capture, subsequent data analysis, monitoring trends and then deploying against the outputs for the benefit of the customer. This has been a common theme for some time now, in fact, and has been taken on board by more and more customers. Decision-making with the facts to hand is very much the core theme these days.

"There's no doubt that differentiation is critical for success," explained Forsyth. "It's the space where price becomes less relevant or is taken into wider consideration. We must strive to achieve positive change otherwise our sector is in a 'no win, low margin' scenario where, ultimately, there's no investment and, put simply, no more road to tread." ●

On Demand Service

Watch the Security Matters Digital Conference 2022 on demand by visiting the event's website at **www.smdigitalconference.com**

Part Two of our detailed review of the Security Matters Digital Conference 2022 will appear in the April 2023 edition of the magazine

Better connected

In this third instalment of a four-part exclusive series for Security Matters, Jane Waterfall examines the latest Internet-connected technology that's bringing cutting-edge solutions to the security business sector. How is that technology actively serving to increase the attack surface and threaten security and, in parallel, what can be done to mitigate the risks currently being presented?

THE SECURITY sector provides and monitors an increasing amount of Internet-connected devices. Smart security cameras, lighting systems, intruder detection and fire alarms, physical access control systems and drone-centric surveillance are all prime examples of technologies used to identify threats on a faster basis and subsequently conduct investigations more easily. The installation – and resulting upkeep – of such technologies is rendered an easier task by remote configuration.

As you can imagine, such Internet of Things (IoT) devices and connected sensors collect and process an enormous amount of information, much of which needs to be analysed and stored using distributed information technology. This means the data is processed and stored in locations other than on the device itself.

The location of that computing will depend on what the data is needed for and how fast it's required. The security of the data involved may not be under your control, yet it remains your responsibility. That being so, it's time to read the small print and find out a little bit more about what's behind today's connected devices.

Before examining that small print, though, it's worth bearing a few points in mind. As things stand today, there are an estimated 7.74 billion IoT connected devices in existence worldwide. Further, that number is forecast to burgeon and attain a figure of circa 29 billion come the advent of 2030.

That being so, and perhaps not surprisingly, there have been several major announcements of late in relation to the drive for connected devices to be made more resilient in the face of ongoing cyber criminality.

For instance, there's the all-new global standard devised by the Connectivity Standards Alliance (the US-based organisation whose stated mission is to "ignite creativity and collaboration" in respect of the IoT by developing, evolving and promoting universal standards that enable all objects to securely connect and interact) and the European Commission's own proposals for a Cyber Resilience Act.

Cyber Resilience Act

The ideas underpinning the latter were made public by the European Union only a few months ago – at the midpoint of September, in fact – with the main objective being to proactively harden existing rules pertaining on cyber security so as to ensure the European marketplace for hardware and software products is that much more secure.

It's common knowledge that those hardware and software products are now increasingly prone to malicious cyber episodes estimated (in 2021) to be costing a cool €5.5 trillion globally. At present, the legal framework in the European Union fails to address the cyber security of non-embedded software.

As a result, there's a core desire to place hardware and software products on the market that have fewer vulnerabilities. This will be realised by fashioning the right conditions for the development of secure products with digital elements, while putting in place mechanisms to ensure manufacturers take security seriously from the inception of a product to end of life. On top of that, the European Union wants a mechanism that facilitates end users taking cyber security into full account when the time comes for them to select, procure and deploy products harbouring digital elements.

The proposed Cyber Resilience Act – which, incidentally, is the very first European Union legislation of its kind – is firmly focused on bringing forward cyber security requirements that are mandatory for those products, whether they reside in the business/industrial or consumer realms. Interestingly, the proposed measures encompass a framework that takes in planning, design and development and continues on to maintenance and support regimes.

Cloud computing is a huge and highly scalable resource for processing and storing data. The Data Centres operated

> As things stand today, there are an estimated 7.74 billion IoT connected devices in existence worldwide. Further, that number is forecast to burgeon and attain a figure of circa 29 billion come the advent of 2030

by cloud service providers could be in any one of the many distributed global locations. Even the closest Data Centre could still be hundreds of miles from the device or sensor where the data is actively being collected.

Communication between the device and the cloud relies on a good Internet connection, but that connection can be disrupted by bandwidth limitations and unpredictable network disruptions themselves. Disconnection and latency (ie lagging) issues may be problematic and frustrating if you are trying to operate a lighting system on a remote basis, for example, but could actually turn out to be catastrophic if you're relying on a connection for real-time analytics of a crucial security camera or a driverless car.

For its part, edge computing is a distributed information technology that moves some portion of storage and computing resources out of the core Data Centre such that it's as close to the source of data as possible. This solution relieves many of the issues caused by the sheer volume of data generated by the tens of billions of IoT devices which can overwhelm the Internet.

What's more, edge technology can help solve the problem of data sovereignty as sensitive data may be kept in the country where it originated, which might then assist with compliance obligations.

Examples of edge technology could be a small server on a factory floor, in a retail outlet or at a railway station allowing the collection and processing of specific sensor data. The end results of that processing (eg real-time business insights or equipment maintenance predictions) can be sent back to another Data Centre for human review, storage and broader analytics.

Somewhere in the middle

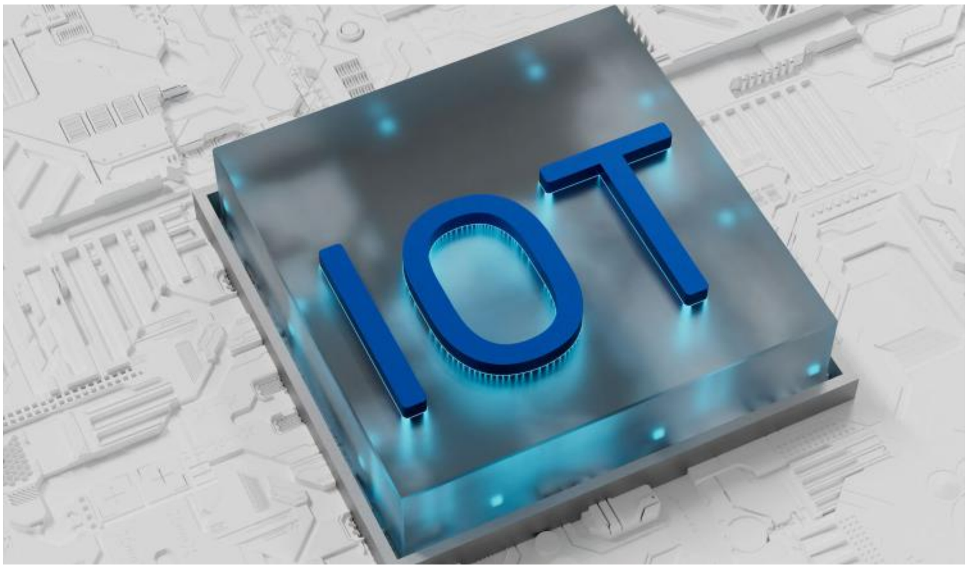
IoT applications that require real-time decisions with minimal latency – among them facial recognition and traffic management systems – need real-time analysis at the edge. However, most edge technology doesn't have the computing resource for this level of analysis, while relying on servers in the cloud raises the ugly problems of congestion and the aforementioned latency.

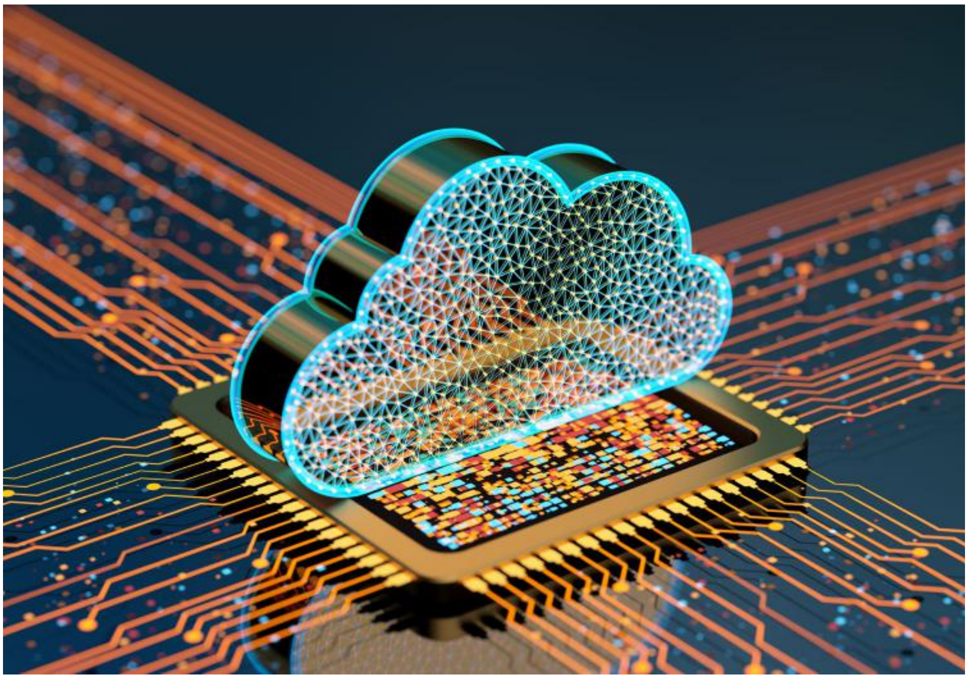
The fog node is the architectural answer to this problem. A fog node is a physical server located between the cloud and the device, close to the network edge, but not actually at the edge. Fog computing brings real-time analytical processing to the IoT, above and beyond the routing and messaging functionality of simple edge nodes.

If you don't have physical control over the servers communicating with your IoT devices and connected sensors, how do you know if they're really secure?

IoT devices are notoriously insecure, in fact, so it's absolutely vital to do your research and choose devices that are designed with security as a priority.

Best Practice IoT security is based upon the thirteen ETSI security requirements (as referenced in the article entitled 'Consumer conscious' that ran on pp50-52 of the September 2022 edition of Security Matters). The ETSI 303 645 standard was created by





experts across Europe emanating from industry, academia and Government with the aim of preventing large-scale commodity attacks against smart devices. Released in 2020, the standard establishes a security baseline for connected consumer products provisioning a set of 13 recommendations and provides a basis for IoT certification schemes.

Many organisations have already based their products and certification schemes around the ETSI standard, while several countries have underpinned their IoT security legislation by using some or all of the aforementioned 13 requirements.

Interestingly, new legislation coming into UK law specifies three mandated security features, which are themselves aligned with the Top Three requirements of the ETSI standard.

No default passwords

At present, passwords are still the main method for securing access to almost all of our different accounts and devices. It's a good idea to devise, hold and employ policies about secure configuration, including a clear password policy that applies to everyone in the organisation (with contractors part of the mix).

Each device should use a uniquely generated password, a user chosen password or – deemed to be the best option of all – another method entirely that doesn't employ passwords at all.

Further, each device must be able to keep passwords, keys and other security parameters safe at all times.

It's recommended that users enable two-factor authentication on connected devices to ensure that other individuals cannot access the device from the Internet with just a password. Put simply, two-factor authentication is a process whereby the user must request and is then sent (typically via the medium of a text message) a code for their mobile phone that needs to be entered. The alternative is using an authenticator app in addition to a password.

Manufacturers need to implement a vulnerability disclosure policy that clearly specifies the process by which security researchers (ie ethical hackers) and others are able to report security issues.

If you harbour software, it's essential to have the ability to update it. A manufacturer must specify for how long their device will receive software updates and, further, deploy the necessary security updates in a timely manner.

It's recommended that software is verified using secure boot mechanisms. This ensures that software updates are both genuine and safe.

IoT devices should use Best Practice encryption of data when at rest and in flight (ie when communicating with the hub or cloud). This will help to protect the confidentiality of personal data when in transitioning between devices

Have you checked the security features of the devices you're using? Does a specific device ask you to set up a unique password? Does it tell you how to update the software? Does it give you a link to the vulnerability disclosure policy?

Cyber expertise

In the last three years, the cyber security sector has grown exponentially and, in consequence, skilled and trained IT and cyber security employees are in short supply. There are particular shortfalls when it comes to cloud computing security, security analysis and investigations and application security.

The full extent of the problem can be ascertained by reviewing the 98-page Government report entitled 'Cyber Security Skills in the UK Labour Market 2022', which is freely available to view online at GOV.UK.

In-house or outsourced expertise applied to your specific business set up is a crucial security factor. Organisations can use internal experts, external consultants and third party providers. It's worth noting here that accredited and listed companies offering IT solutions may not always be well versed in cyber security practises. A cyber security consultant is often needed in addition to a degree of bespoke IT support.

The IASME IoT Cyber Assurance certification scheme affords manufacturers (and those individuals responsible for purchasing connected products) a way in which to show due diligence in the selection of secure products. The IoT Security Assured scheme badge is displayed on a device to reassure the end user that their device has the most important security features included.

The IoT Cyber Assurance scheme, itself launched only last year, is aligned with the leading global technical standard in IoT security, namely the aforementioned ETSI EN 303 645, as well as with imminent UK IoT security legislation and guidance. In point of fact, the Level 2 audited scheme provides an additional level of certification above the managed self-assessment level, duly delivering third party testing and independent certification. ●

Jane Waterfall is Business Development Manager at IASME
www.iasme.co.uk

Command Centre v8.80 and Command Centre Web introduced by Gallagher

COMMAND CENTRE v8.80, the latest iteration of **Gallagher Security's** own security management software, has been introduced in order to enable organisations to "make security easier, faster and more efficient". Further, the new version of the software is supplied with Command Centre Web, itself described as "an invaluable tool" for managing sites anywhere with an Internet connection.

The release of Command Centre v8.80 brings to the fore features that allow for greater flexibility and efficiencies, including site plan enhancements, SIP integration and a new bulk configuration tool.

Command Centre v8.80 enables customers to navigate and visualise complex site plans. The site plan enhancements reduce the number of items that need to be visible on a constant basis, thereby affording the ability to easily answer intercom calls from within a site plan, not to mention the chance to rotate that plan for better situational awareness.

Further, Command Centre v8.80 delivers access to the aforementioned bulk configuration tool, which saves significant time and data entry procedures when setting up new sites or loading large amounts of hardware to an existing one.

"Command Centre Web will prove to be an invaluable tool for managing sites anywhere," commented Andrew Scothern, chief systems architect at Gallagher. "Through interfacing with Gallagher Command Centre via the Gallagher API Gateway, it allows safe and secure access to Command Centre Web from anywhere there's an Internet connection."

The first component introduced in Command Centre Web focuses on cardholder management and allows administrators to view cardholder history, see the activity of the cardholder, manage cards and credentials (excluding printing/encoding cards) and manage cardholder access/assign access.

www.security.gallagher.com

SoloProtect launches new range of intuitive touchscreen devices

SOLOPROTECT HAS launched a new range of intuitive touchscreen devices developed specifically to bring an enhanced level of technology and design to the lone worker security and safety market. The touchscreen range consists of three devices: SoloProtect ID Touch, SoloProtect Shield and SoloProtect Curve. Each is feature-rich, instinctive to use, water and dust-proof (to the IP67 rating) and accesses 4G networks for "comprehensive" cellular connectivity.

All of the new devices benefit from SoloProtect's core safety features including Red Alert, Incapacitation Alert (sometimes known as a 'Man Down Alarm') and Check-In, along with 24/7 monitoring from SoloProtect's Alarm Receiving Centre.

They also feature Ready2Talk, a popular new service launched in 2021 and designed to 'chaperone' workers in those situations where there's a clear safety risk (eg walking to a car at night and, in doing so, passing a group of people acting suspiciously).

The SoloProtect ID Touch combines a personal safety device with an ID badge. It's extremely discreet, allowing end users to raise an alarm without breaking eye contact, and is also deemed ideal for those workers who wear an ID badge as part of their role or to gain access to a given premises.

The SoloProtect Shield is a versatile pocket-sized device that doesn't compromise an active or outdoor role, providing comprehensive protection off-road or on-site.

The SoloProtect Curve is a contemporary device that's ideal for a work scenario, but every bit as appropriate in a personal setting.

www.soloprotect.com/uk/

3xLOGIC heralds launch of VIGIL CLOUD system in Europe

INTEGRATED AND intelligent security solutions provider **3xLOGIC** has announced the availability of its innovative VIGIL CLOUD system across Europe.

Originally launched in the US in 2020, VIGIL CLOUD extends the scope of 3xLOGIC's award-winning VIGIL video management system (VMS) into the cloud and has proven popular among those organisations looking for a powerful, scalable and easy-to-use platform.

"We are incredibly excited that VIGIL CLOUD is now part of our European product ecosystem and look forward to building on its incredible success in the States," explained Alex Buckle, business development manager for 3xLOGIC here in the UK.

VIGIL CLOUD can be accessed via desktop or mobile app. Users can view live and playback video from cloud cameras, bookmark cameras for quick and easy access from the main dashboard, check camera heath status and collect and package related video events together.

www.3xLOGIC.com

OPTEX unveils FlipX Advanced sensors for high-security environments

FOLLOWING THE successful EMEA roll-out of its FlipX Standard indoor sensors back in September, sensor developer **OPTEX** has now announced the launch of its Grade 3 FlipX Advanced series.

OPTEX FlipX sensors feature a bespoke pyroelectric sensor for increased performance that adapts to the human shape, in addition to a lens that can be 'flipped' to provide both wide and narrow detection in a single sensor.

Rotating the lens through 180° means the sensor can be used to protect narrow or long areas such as a corridor or warehouse aisles up to 24 metres, or otherwise a wide, open area like a lobby or a high-value retail store to 15 metres at 85°.

In addition, and to provide a higher level of security, the Advanced models feature intelligent IR anti-masking, which protects both the PIR and microwave sensors, in turn generating an alert if they're covered.

www.optex.net

RISCO Group supports security installers' expansion into commercial sector

RISCO GROUP – THE manufacturer and distributor of security solutions for the commercial and residential markets – is helping accredited security installers to cost-effectively grow their business in the lucrative SME market by expanding its commercial product portfolio.

NSI and SSAIB accredited installers form a rapidly increasing share of RISCO's customer base. On that note, the company has announced the arrival in the UK and Ireland of the first stock of its new integrated alarm, access control and video verification solution for commercial and high-end residential projects sought by those installers.

Large-scale commercial end users – including those in the office, logistics, retail, hospitality and manufacturing sectors – are increasingly stipulating access control as part of many installations. By adding integrated access control to the LightSYS+ scalable hybrid intruder alarm system launched back in January, LightSYS+ Access Control precludes the complexity of combining two standalone solutions.

www.riscogroup.com

Videcon named inaugural distribution partner for Siemens fire safety products

TECHNOLOGY COMPANY **Siemens** has named **Videcon** as its new strategic partner for the Cerberus FIT range of fire detection and alarm products. As a result, Videcon becomes Siemens' first-ever distribution partner for fire safety products in the UK and Ireland.

Products in the Cerberus FIT range have been designed specifically to provide a cost-effective option for those end users who are looking to move from conventional to addressable systems for small through to medium-sized applications.

Videcon will now be adding Cerberus FIT to its existing portfolio of fire and security products and services through its dedicated fire safety division, which is headed up by sales director Alan Fowlie.

Commenting on the new partnership, Fowlie informed Security Matters: "I knew Siemens from the work I had done before my business became part of Videcon back in 2020. Cerberus FIT offers the ideal solution. It affords us an engineer-friendly system with brand values."

www.siemens.com

Chubb celebrates four decades of partnership working with fashion retailer

CHUBB – THE provider of security and fire safety solutions – is currently celebrating an impressive 40-plus year partnership with Ireland's largest discount fashion retailer, all the while delivering expert security systems to minimise loss prevention.

Founded back in 1969, this Irish fast-fashion retailer operates more than 380 stores worldwide, providing quality fashion products.

One major challenge the retailer faces is the management of loss prevention, as none of its products are tagged so its stores are an easy target for petty theft. In-store security is an essential part of the retailer's loss prevention strategy, but this is not sufficient on its own to satisfy the necessary security regime.

As a business, Chubb has been delivering expert security solutions to the retailer since the early 1980s. Today, provision consists of a combination of CCTV surveillance, access control and alarm monitoring for all 37 stores in Ireland and all 188 stores in the UK, as well as a large number of stores across Europe.

www.chubbfiresecurity.com

Qognify VMS 7.2 supports investigation and adds cloud capabilities

QOGNIFY HAS launched the second release of its video management software Qognify VMS. The latest software version – designated Qognify VMS 7.2 – comes with extended support for body-worn cameras, additional functionalities to support investigations and also a new web client architecture.

Qognify VMS 7.2 addresses the increasing use of body-worn cameras across many sectors, ranging from police and security applications to customer service and quality control.

The need to integrate footage into a fully featured VMS environment for investigation purposes has become increasingly apparent. In this particular context, it's crucial that the integration framework is able to maintain the chain of custody of captured footage for law enforcement applications.

Qognify has worked closely alongside system manufacturers to ensure that the chain of custody protocols is observed, and notably so when devices are used in multiple shifts by different users.

In addition to supporting further video sources, Qognify VMS 7.2 offers new enterprise-class capabilities for investigations.

www.qognify.com

Ajax Systems holds fourth Special Event under 'Comfort Zone' branding

TUESDAY 11 October witnessed **Ajax Systems** holding its fourth Special Event, this time around under the 'Comfort Zone' banner. The company has entered a new niche area by unveiling a fire-focused product line, while at the same time adding comfort-centric devices to its security systems portfolio.

This year's online presentation was broadcast in no fewer than 19 languages and viewed by Ajax users and partners from upwards of 130 countries worldwide. The main offline event was held in Paris, while over 3,000 security professionals attended local screenings in the UK (where Security Matters was in attendance), the Ukraine, Spain, Italy, the Netherlands, Germany, Romania, Turkey and Canada in addition to several other nations.

The London gathering at the Curson Bloomsbury within The Brunswick Centre witnessed UK country manager Steve Proctor and his colleague Sam Griffiths (the company's dedicated training and support manager) preside over a Q&A session orchestrated to highlight the various new products and also how they add several options for end users on top of their basic security-focused requirements.

In all, the business showcased four new solution lines, namely LifeQuality, LightSwitch, WaterStop and FireProtect 2.

LifeQuality is a professional indoor air quality monitor designed to measure carbon dioxide, temperature and humidity levels. Packed with Swiss and Swedish sensors used in medical equipment, LifeQuality provides highly reliable data.

With LightSwitch, system users can control a wide range of illumination devices, both on-site and remotely, through Ajax Systems' apps. LightSwitch features a large touch-sensitive panel that's responsive to a contactless activation.

For its part, WaterStop is a water shut-off valve with remote control.

www.ajax.systems

"Energy savings achievable through access control systems" states Paxton

CHANGES IN the global energy supply, coupled with the expected winter demand uptick, have realised energy price increases for businesses and households across the UK.

In looking for ways in which to save energy usage, access control can be a helpful solution. With this backdrop in mind, security technology manufacturer **Paxton** has just issued guidance notes on how to efficiently manage building activity and save energy through the use of access control systems.

Back in August, Ofgem announced that the energy price cap could rise by 80% to an average of £3,549 per household per year starting from October. The Government has since introduced an energy price guarantee to freeze prices at £2,500 per year for a typical household.

Businesses will have their energy costs capped at around £211 per MWh for electricity and £75 per MWh for gas, which is less than half the prices anticipated this winter.

Even though the average energy bills are now lower than originally expected, there's still a substantial increase with which households and businesses alike must contend for the foreseeable future.

Businesses can reduce their bills by using smart security systems that integrate with their current infrastructure to control building activity and limit energy usage. Paxton has developed two award-winning systems – namely Net2 and Paxton10 – that provide features specifically designed to support a reduction in energy usage.

Chris Hodge, functional architect at Paxton, stated: "Using the standard events within the access control software, the systems can also be employed to shut off power to equipment that's not in use. As such, they can help in saving energy."

www.paxton-access.com

The Last Word

Mike Reddington outlines precisely why the British Security Industry Association is an extremely keen supporter of the sector's ongoing focus in relation to the subject of 'Women in Security' and, as a result, plays a continual and active role in ensuring that practising professionals determine to encourage more talented females into its ranks

RECENTLY, THE British Security Industry Association (BSIA) officially launched the security officer services awareness campaign entitled 'People, Property, Places: Professionally Protected', which includes a national recruitment drive – dubbed 'Security: a career of choice' – at its heart. The message is that a career in security is for everyone and anyone.

While we see a clear improvement in the recruitment and promotion of women in our industry, there's still much work to be done here. Year-on-year, the gender balance in the industry is improving, but not at the pace required. Today, estimates suggest that only 12% of the front line security officer cohort is female, although that figure is up from 2016 (when it stood at only 9%).

The new campaign highlights the career opportunities available in the sector, and we believe this will attract a larger number of female applicants for the roles available. We know from working with our members that there are many roles within the sector being filled by women, most encouragingly at a senior level. There are many great and inspirational female business leaders who have worked their way through the ranks and are actively promoting equality, diversity and inclusion campaigns – both in their own companies and through trade bodies – to ensure this low percentage rate increases.

Recruitment challenge

Recruitment in our sector is currently posing many challenges due to the ongoing effects of COVID-19, Brexit and retirement. This challenge is further compounded by the legacy view of who traditionally takes on roles within the security business sector.

Historically, our industry began as a role aimed primarily at males, either from the Armed Forces or manual labour backgrounds (many roles in security evolved from nightwatchmen) and was seen as a dangerous and risky job only attractive to males from a stereotypical standpoint.

It wasn't until the 1950s that women began to work in the industry, but only outside of specific 'guarding' roles. They would make up wage packets for Cash and Valuables in Transit companies, for example.

Though some businesses did start to employ females, initially they were positioned in roles described as 'the gentle touch' (ie searching women's handbags in department stores). Otherwise, females were (sadly) relatively invisible as security was perceived as 'a man's world'.

Of course, this is a terribly outdated and archaic perception of the modern industry in which we all work. By employing more women, we are bringing into play a breadth of different skills and dynamics. Companies are seeing the advantages that a diverse team can realise for clients and the wider industry.

Such a move can also improve the culture of the workplace environment, offering broader thinking and viewpoints and potentially improving financial performance. Recent research conducted by Deloitte concluded that a diverse workforce improves innovation by circa 20%.

Changing perceptions

Over time, the perception of the security industry as an attractive home for females has been gaining momentum for the better. The 2019 report sponsored by ICTS UK and Ireland and produced by Perpetuity Research – itself entitled 'Women in Security' – highlighted the fact that those females who work in the sector indicated their perception was more positive now than when they began their journey.

The most common reason given was that those females now have a greater understanding of the realities of the sector, finding the work to be more interesting and varied than their original perception of what security work involved and, in addition, feeling that they had benefited from lots of different opportunities to learn more about security as a discipline.

Others had expected to battle negative experiences such as violence or sexism, but found that these were less commonplace than their original expectations. Similarly, some had expected to encounter low levels of professionalism and low standards, but in reality found the opposite to be true.

Female security professionals are regularly making significant contributions in keeping 'People, Property and Places: Professionally Protected'. As a direct consequence of their diligent work and achievements, they're also highlighting that this is an industry for everyone. In short, security is a career of choice, regardless of gender.

Removing misconceptions

We must still look to remove the misconception that security is a 'pale, male and stale' industry that hasn't evolved to 'reflect who we protect' in our modern society. Over the last few years, that misconception has been changing steadily. Our industry now harbours representation from many backgrounds, while our constituent security companies work tirelessly on their focused equality, diversity and inclusion programmes.

This is the exact message we hope our 'People, Property, Places: Professionally Protected' campaign will convey – and that the work of our equality, diversity and inclusion champions and senior leaders can impart – to correct the gender imbalance and negative stereotypes often referenced in relation to the security industry. ●

Mike Reddington is CEO of the British Security Industry Association
www.bsia.co.uk

bsia
british security industry association

IN CASE OF FIRE
LIFT COVER - BREAK GLASS