ASIS INTERNATIONAL™ United Kingdom Chapter

NEWSLETTER No.2 2020

Welcome to the second ASIS UK Newsletter of 2020

Most of us have faced significant challenges over the past few months with increased workloads, working from home, reduced pay, furloughing, redundancy, home schooling, isolation, shielding and (sadly, for some) sickness and bereavement. As we were coming to terms with the regular changes to social distancing rules, we now have more people returning to work as non-essential businesses open to reduce the financial burden. It has never been more vital for all security professionals to be on top of their game.

Having been the lead investigator in the UK for deaths in police custody and conducting investigations and training into deaths following police conduct internationally, I, like the majority of police officers past and present and any decent human being, was shocked by the callous conduct of police officers in Minneapolis that led to the avoidable death of George Floyd on 25 May. Many people around the world have voiced their anger at this savage act and have chosen to raise awareness of racism in all its ugly guises. Others, sadly, have chosen the appalling event as an excuse to attack police, culminating in many injuries. Please do all you can to support the police and our security officers who provide an essential service and often bear the brunt of criminal behaviour.

If you're aware of particular acts of heroism, please consider the City of London Sheriff's Bravery Awards. The act does't have to have taken place in London. Visit The Worshipful Company of Security Professionals' website for details.

My last role in policing was in a senior position in UK counter-terrorism. I was about to remind everyone that the threat from terrorism in the UK has not diminished when another act of savagery culminated in the death of three men in Reading on 20 June and the injury of several others. Please remind those for whom you have responsibility of the ever-present threat from terrorism and encourage them to complete the Action Counters Terrorism (ACT) training and to use the ACT app. You should all have it on your mobile devices. Further detail can be found on the NaCTSO website.

Your ASIS UK Board is implementing the change programme previously announced. Dave Marsh (Treasurer) and Nicola Thompson (Women in Security), due to work commitments, have resigned from the Board. We wish them well in their careers. I'm pleased to announce that Elizabeth Lewis (Vice-President of Operational Security at Deutsche Bank) has agreed to join the Board to lead for Women in Security. I have had to take on the additional role as Treasurer (temporarily). I'm also pleased to announce that we're now using a new accounting system and that the accounts are fully up-to-date. This will allow the Board, for the first time, to have detailed, accurate information about our financial position at each monthly Board meeting. Having put the accounts into a good position, I would like to hand this over at the earliest opportunity. If you have the skills and interest to serve your association as Treasurer, please do contact me.

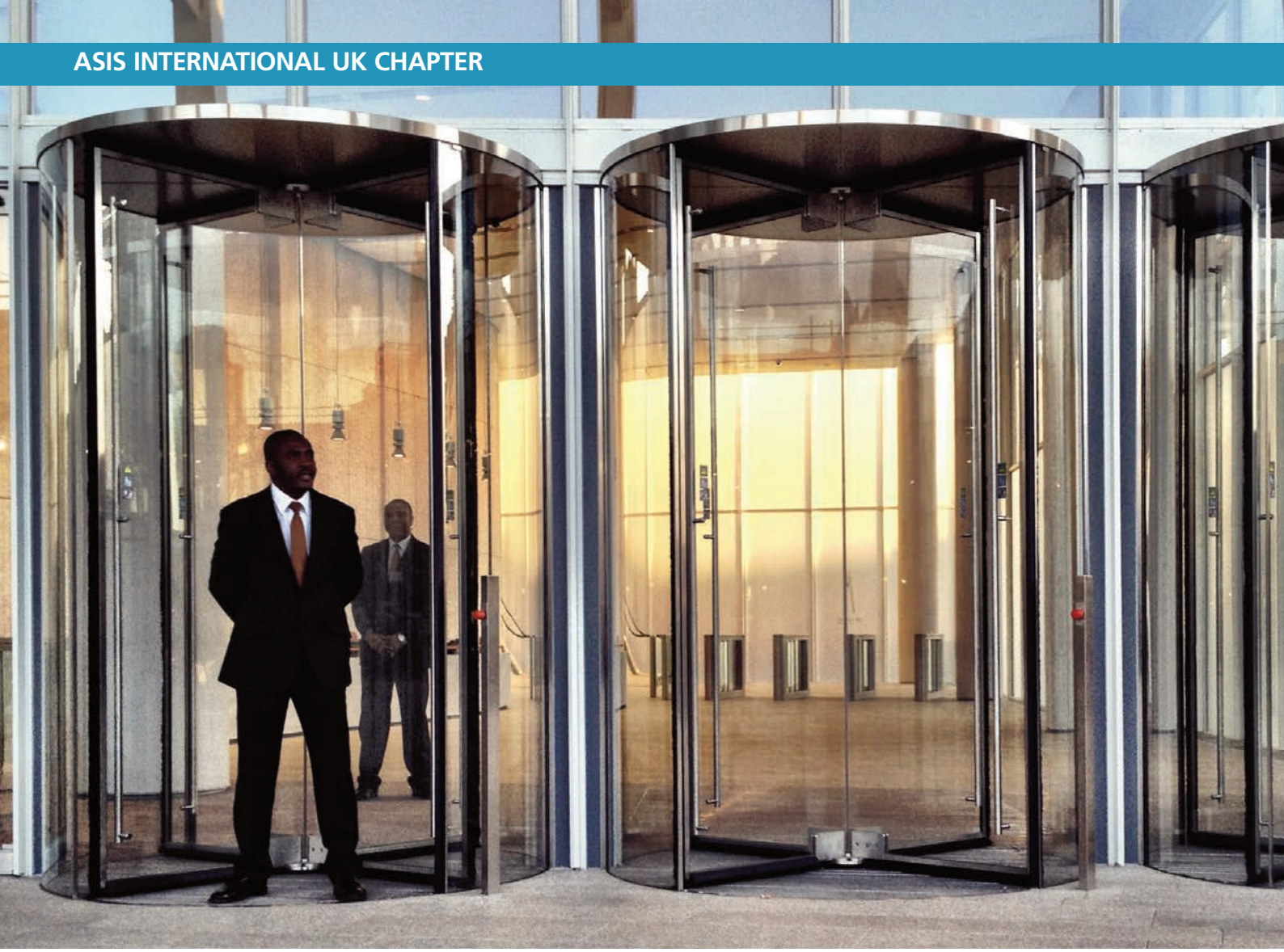
Rich Stevens is doing some great work to promote our own certifications as well as the Chartered Security Professional designation. Please consider these certifications as opportunities to further your own Continuing Professional Development going forward.

We will be unable to hold a seminar this summer, but are seeking a venue for our AGM and seminar in November. If you can assist, please contact Steve Emmins. We have been able to hold two well received webinars recently, one on the effects of COVID-19. The other, open to members only, was an excellent introduction to the Centre for the Protection of National Infrastructure (CPNI). I'm delighted to announce that the CPNI held a follow-up (again members only) webinar on Monday 13 July.

I would like to thank all of the Board members for their work and will be updating you as we make further progress. Many thanks to James Morris for pulling the ASIS UK Newsletter together on top of his many other commitments.

Please read on and stay safe. Don't hesitate to contact your Chapter Board members. We are here for you.

Russell Penny CPP
Chairman (ASIS UK)



Facing Up to Engagement: Unmasking Technology

By Darren Carter CPP MSyI FISRM

Technology continues to reach beyond known limits, exploring ever-renewed ways in which to manipulate the threat environment, enriching data and providing tooling that we would all once have marvelled at in comic books and feasted upon when seeing the latest 'Q' invention.

We're often very impressed by the scientific R&D initiatives of security manufacturers and the products they can bring to market.

It's also fair to recognise the truism that we often find ourselves over-reliant on technology. In our continual search for introducing efficiencies into our businesses, we're easily seduced by the latest, 'must-have' kit.

Over recent months, we've witnessed a small turnaround in the wider perception of key workers including security officers and the important and much-valued work they do. I would place any 'host'-type role within that description (ie a person being the first point of contact for visitors to a building). As many businesses return to work, the risks have shifted for those performing front line duties.

The continued presence of COVID-19 causes us to re-examine many ways in which we work, how we approach unknown individuals, conduct a bag search, a person search or detain a suspect, etc. Yes, there is technology out there that will transact one or two of those key tasks for you without you having to lift a finger.

At least for now, it's mandatory to wear a face covering on all forms of public transport in much of the UK. Many will assume this 'new normal' behaviour for some time yet, I'm sure, and at least until their confidence is completely restored in being around mixed groups of people, particularly so within densely populated towns and cities. I have read several articles that speak around technology constraints with this in prospect, asking how technology will cope. I'm not so sure it needs to.

This focuses our thoughts back on to our front line colleagues who are now expected to engage daily with people they don't know and who are possibly a risk, and who are now, with some legitimacy, covering their face. Is it OK to ask a visitor

to remove their face covering during a public health emergency? Is it the right response to refuse entry to anyone who refuses to do so? At the very least, this may cause some distress to a person who holds a genuine anxiety about the prospect of removing their face covering. Worse still, it may well provoke an unwanted reaction, possibly aggressive or violent in nature. We've seen examples of this of late where serious assaults on security staff have resulted from their enforcement of face coverings.

This set of circumstances has propelled the subject of positive engagement metaphorically and practically to the front line. The ability of staff to be able to communicate in a natural and non-confrontational way that effectively enables them to assess risk, identify a potential threat and intervene with skilful communication is a highly valuable trait. This isn't a new phenomenon. It's by far the most effective tool we have within our own means. It's an essential skill, deeply embedded within the way many providers of hospitality operate. This isn't a space for tech'. Within my own business, we have for many years trained a 'Security Through Service' programme to all employees. At its core sits exemplary customer service: to host, engage, welcome and assist. Alternatively, to the customer with a more dishonest intent; to intervene, stop, question and suspect. This is a powerful deterrent and, when fully committed, will significantly reduce workplace risk, detect otherwise unseen circumstances and potentially prevent more significant events from happening.

Launched in 2019, the See Check and Notify (SCaN) training product from NaCTSO/CPNI recognises the 'Power of Hello' in its fantastic training package of six modules designed to help protect your workplace. Alongside behavioural detection methods, and when combined, it can be incredibly powerful and effective. No 'tech' required.

As for face coverings? This is where the art of vigilance, awareness and, most importantly, communication plays its ace card. It should not be a critical factor if someone is or isn't wearing a face covering. The interaction itself should feed the decision-making process sufficiently to understand the situation. Yes, there will always be sensitive buildings or environments that necessitate the need to remove face coverings even momentarily, but this will not be the case for the majority.

As we gear ourselves up for a much awaited return to business, we're mindful that the broad set of risks we faced before COVID-19 are still very much present today, as we were so tragically reminded with the recent murder of three innocent people in my home town of Reading.

There are always training needs to be met. A strong sense of customer service-based communication skills, I would suggest, must be up there among the most important to better protect our businesses and those on the front line.

Darren Carter CPP MSyI F.ISRM is the Head of Group Security at Edwardian Hotels and the Vice-Chair of the ASIS International UK Chapter

Planning and Building 'The Secure Smart City'

Steven Kenny (Industry Liaison for Architecture and Engineering at Axis Communications) discusses the challenges of the 'Smart' revolution and the innovation that's needed to create a smarter and safer world

The strange thing about smart homes, smart buildings, smart cities – indeed, smart environments as a whole – is that, despite the fact the technologies which make them possible seem to have been around forever, they're also still in their relative infancy. Many of us use devices and services which would have seemed like science fiction just a few years ago to order food, stream entertainment or work remotely. Our phones help us to navigate congested cities as efficiently as possible, while cities themselves rely on connected devices to collect data and improve public services.

At the same time, daily headlines about data breaches and cyber security incidents remind us all that there's a long way to go before 'smart' technologies are mature. Too many smart devices are vulnerable to known attacks, and too much data is stored on servers that are not properly secured by organisations which don't have the correct protocols in place for mitigating risk.

This is important because it has been clear for the best part of two decades that the data collected from smart environments will be essential to improving quality of life in the 21st Century. Humanity faces big challenges in the shape of population growth, urbanisation and climate change and technology will have an increasing role to play in order to make our cities more resource-efficient, safer, more secure and, ultimately, pleasant to live in. Real-time data analysis and automated decision-making will be the only way to ensure our traffic keeps moving, our power grids can adapt to new sources of energy and we reduce wastage in our food supply chains (to cite just a few examples from Axis' recently released White Paper on 'Smart Buildings and Smart Cities Security').

This White Paper has been produced in association with Virtually Informed and Unified Security in order to address important questions about the security implications of smart city technology. As the world in which we live and work becomes more digitally connected, so the potential grows for cyber security incidents to cause disruption or harm individuals and corporate brands. By understanding more fully the benefits and risks of smart technology, we can help to define Best Practice in security and deliver recommendations for stakeholders involved in its development/deployment.

Device interoperability: a pivotal moment in technology deployment

There are other promised benefits of the smart city. Faster, more affordable connectivity is directly linked to economic growth and can improve Health and Safety, too. Environmental monitoring can help influence policy decisions around green spaces, for example, or quickly alert officials to breaches of pollution law. Camera networks provide citizens with improved security and the same systems

About Axis Communications

Axis enables a smarter and safer world by creating network solutions that provide insights for improving security and new ways of doing business. As the industry leader in network video, Axis offers products and services for video surveillance and analytics, access control and audio systems. Axis has more than 3,000 dedicated employees in over 50 countries and collaborates with partners worldwide to deliver customer solutions. Founded in 1984, Axis is a Sweden-based company listed on the NASDAQ Stockholm under the ticker AXIS. For more information about Axis Communications please visit the company's website at **www.axis.com**

that help you avoid traffic jams can lead to faster response times for those all-important emergency vehicles.

On a more local level, smart buildings are delivering on the promise of being more energy efficient, providing safer working environments and – thanks to a proliferation of low cost sensors which can detect early signs of wear and tear – reducing the likelihood of systems failing thanks to Artificial Intelligence (AI) and predictive maintenance regimes.

What we identify in our White Paper is that, to fully realise the benefits of smart technology, we need to move beyond current deployments of individual systems and networks. Integrating data from multiple sources to create 'systems of systems' will lead to richer insights and optimisations than are currently being achieved. Today, the term 'smart' is used almost indiscriminately and largely to define systems which collect data, but mostly operate in silos. The terms 'smart buildings', 'smart cities' and 'smart environments' are ill-defined and watered down by overuse. As standards emerge to allow greater interoperability (ie systems talking to each other easily), we expect to see more strategic innovation.

We also expect this next phase of maturity to happen quickly. The basic technology is well understood by vendors, while the next generation mobile connectivity in the form of 5G will accelerate its proliferation. In particular, we expect to see the acceleration of the deployment of Internet of Things (IoT) devices as networks designed for Big Data and AI processing extend their reach.

This places us at a critical moment. The early years of smart city and building technology have been notable for the prioritisation of features and time to market over cyber security, which in turn has damaged public trust in smart systems. As we become more reliant on the technology, it's imperative that security is a primary design goal from the outset for any new implementation.

All stakeholders have a role to play in this, although one of the challenges highlighted in our White Paper is that the first step in risk mitigation is identifying who those stakeholders are. The use of frameworks, such as those developed by NIST, can help to bring together the right parties for security collaboration. From architects and landlords to security advisors and decommissioning consultants who can deal with data-rich systems at end of life, the future of cyber security is building layered defences at every step

of the design and implementation process for new products.

Security challenges and the trusted vendor

This collaboration is vital. The pace at which new technologies and advances in critical applications such as AI and data processing is happening make it difficult for any one stakeholder to be able to maintain an holistic view of security in a smart building or smart city. Each design decision made in the development of a new product carries its own implications for risk assessment.

The rise of 'edge computing', for example, which limits the amount of data transferred to centralised servers and processes data closer to the point of collection, brings with it a particular risk profile which is different to 'pure' cloud platforms. One critical challenge for the IoT is device management and ensuring that endpoints are kept up-to-date with new firmwares and software patches.

The blending of IT and 'operational technology' (OT) such as building management systems further complicates the security needs around implementation. Famously, a Las Vegas casino found itself the victim of a sophisticated cyber attack in which criminals breached its customer database records by first exploiting a weakness in an IP-connected fish tank thermometer.

Vendors have long and complex supply chains which provide opportunities for vulnerabilities to slip in to product design. Buyers, on the other hand, often lack the skills to conduct a full security audit when making purchasing decisions.

In addition, there seems to be confusion even among vendors as to what Best Practice is and how to interpret standards. Against the decades-long culture of treating security as a secondary consideration to time to market and cost in the development process, the principle of 'secure by design and default' is still not applied widely enough.

The 'Smart' way forward

By identifying the challenges and threats, we can start to make recommendations about the way forward for the development and secure implementation of smart city and smart building systems and products. In the White Paper, we've made ten clear recommendations in order to assist stakeholders.

At the very beginning of the process, we encourage the adoption of the 'Secure by Design and Default' and 'Data Protection by Design and Default' mindset, a requirement of the NIS Directive, and how it applies to the purpose of the project in question. Developing a strategy to

implement those goals in a specific way may come over time, but having clarity around responsibility for project management and budgets for cyber security from the outset is essential.

Other recommendations cover issues such as standards, frameworks and compliance, and particularly how these differ to standards for physical security with which building and city managers may be more familiar. There are key recommendations for product strategy and full lifecycle support, including contingency plans for when suppliers may not be able to fulfil their obligations.

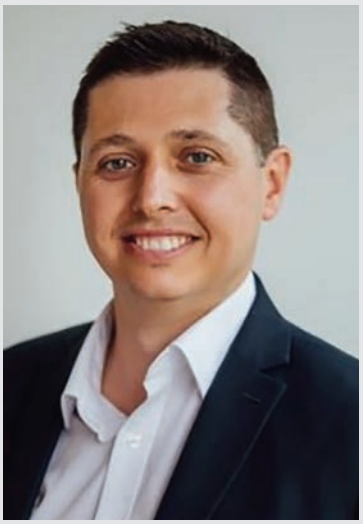
The White Paper also touches on the issue of data compliance, notably so as it relates to personal data and the European Union's General Data Protection Regulation. For vendors, there are recommendations around clarity when it comes to appropriate marketing terminology and they're actvely encouraged to fact-check their own claims as to the capabilities of their products. For buyers, there's much salient advice on vetting supply chains and how to run an effective Converged Security Operations Centre so as to achieve a single and unified view of their current risk profile.

What the authors of this White Paper don't do, however, is claim to have all the answers. Cyber security in the smart building or smart city is an ongoing and collaborative endeavour which is evolving as quickly as the technology itself. If we're to reap the benefits of the technology, and also maintain the trust of those who live and work in these buildings and cities, it's absolutely vital that we heed their advice.

Download the Axis Smart Buildings and Smart Cities Security White Paper:

https://www.axis-communications.com/Smart-buildings-and-smart-cities-security

Steven Kenny (Industry Liaison for Architecture and Engineering at Axis Communications)



Steven Kenny has spent 15 years in the security sector taking responsibility for key elements of mission-critical, high-profile projects across a number of different vertical markets. For the last five years, Steven has focused his attentions on how technology can best complement day-to-day business operations, specifically addressing operational issues and supporting the A&E consultant community across Northern Europe. Steven is the Director of Systems, Information and Cyber Security for ASIS International's UK Chapter and he sits on the Advisory Council for Emerging Technologies operaed by TINYg (the Global Terrorism Information Network Group).

ASIS International transitions GSX to become virtual event in 2020

ASIS International has taken the decision to transform its Global Security Exchange (GSX) 2020 event such that it becomes a fully-virtual experience entitled Global Security Exchange Plus (GSX+). The event will include more than 80 industry-leading education sessions and a robust exhibition marketplace and also realise unique peer-to-peer networking opportunities.

Following months of careful evaluation of the risks associated with convening an event of 20,000 professionals from across the globe during the COVID-19 pandemic, ASIS International's leadership concluded that transitioning GSX to a virtual-only environment for 2020v was the correct course of action n the best interests of its members, attendees, speakers, exhibitors and the public. Previously scheduled to take place from 21-23 September in Atlanta, Georgia, the new online GSX+ will bring together a global audience with many ive and on-demand features from 21-25 September.

Visit the event's website (www.gsx.org) for more details

GSX+ GLOBAL SECURITY EXCHANGE PLUS

ASIS Trauma Support: On the Phone and On the Internet

By Patrick Rea (ASIS Member and Security Marketing Specialist)

ASIS members can now benefit from free therapy for trauma, however it occurs, by phone or an Internet call with charity PTSD Resolution. The online service was developed to meet the need for help during the COVID-19 pandemic as a personal meeting with a therapist may not be possible because of social distancing.

In a survey before the pandemic, it was identified that thousands of security officers are traumatised because of verbal abuse and violence while on duty. In what is believed to be the biggest study of UK security personnel, University of Portsmouth researchers interviewed 750 workers and found almost 40% of them were showing symptoms of PTSD.

The incidence of trauma among security officers has increased significantly since the survey as a result of duties carried out during the pandemic. Staff are having to fulfil often long and unfamiliar shifts at a range of venues to control access to shops and other properties, while also dealing with their own fears regarding the risk of illness.

Many people working in the security industry are Armed Forces' veterans or reservists and may well be suffering from the effects of trauma from their time in service. Others might well be suffering because of a work-related incident, accident or some other kind of event that has transpired.

ASIS members are able to access free trauma treatment through PTSD Resolution. Therapy is provided confidentially and without the need for a referral so there's no record that may impact on the sufferer's employment situation. This can sometimes be a fear that inhibits people from seeking professional help.

Treatment is usually completed within an average of five sessions, when both the client and therapist agree that no further treatment is required. Treatments are followed up to ensure that the resolution of symptoms is sustained.

Trauma Awareness Training webinar

On 29 July, ASIS UK ran a free webinar

exclusively for members on Trauma Awareness Training for Employers (check the events page on the website).

The session introduced line managers and other staff to the issue of trauma: what it is, how to recognise it, why it affects performance and ways to resolve it.

Such training is intended for security line managers and counter-terror operatives, HR and learning and development staff.

The instruction enables learners to:

- Recognise post-traumatic symptoms
- Understand the effects of trauma on human behaviour
- Engage with traumatised individuals to explore practical options
- Identify clear routes towards resolving workplace difficulties caused by trauma

Even staff who are professionally trained to respond to and deal with security events have their own personal stress thresholds. Beyond a certain level of exposure to disturbing experiences, almost everyone is vulnerable to trauma.

PTSD Resolution is successfully resolving issues of military trauma, working with the employers of UK Armed Forces veterans and reservists with nearly 3,000 referrals to date.

Few employers can recognise the symptoms of trauma without support, far less assist employees and find out if they need help and then arrange appropriate treatment.

Tips on trauma

Piers Bishop, the Director of Therapy at PTSD Resolution, has stated that if, as a line manager, you have staff under your command who've been exposed to violent scenes, or otherwise encountered them in their current employment, you and they need to be prepared through proper training. Bishop makes these key points:

(1) If you experience the effects of trauma after an event, this isn't a sign of weakness. Rather, it's a normal reaction and can happen to anyone, even robust and apparently stable people. Everyone has a threshold beyond which they can be traumatised.

(2) It's OK to talk about the event and feelings of trauma, but it will not necessarily help to do so. Treatment is what you need. The sooner you access that treatment, the sooner you'll be able to return to normal life. If you broke your leg, you would endeavour to have that leg fixed professionally. It's not so different a scenario with mental health.

(3) Your doctor will likely not be a trauma specialist. In fact, you may know more about post-traumatic stress symptoms than they do because of the nature of your work and the people with whom you come into contact on a regular basis.

(4) The latest medical thinking is opposed to medication for post-traumatic symptoms, but many doctors still offer anti-depressants to new trauma cases. You should insist on seeing someone qualified in this subject area. There's a strong chance that, with the appropriate treatment being delivered, you will experience a good recovery.

PTSD Resolution has a network of 200 counsellors in the UK and bookings for training can be made centrally.

For further information visit www.ptsdresolution.org

PTSD Resolution
Counselling Forces' Veterans & Reservists
registered charity no. 1133188

ASIS | UNITED KINGDOM WOMEN IN SECURITY

The ASIS UK Chapter's Board is pleased to introduce Elizabeth Lewis (pictured, right) as the new lead for Women in Security for the ASIS UK Chapter.

Having spent 14 years within the security risk industry, Elizabeth has worked at leading consultancies, corporates and Government entities alike. Now responsible for the development of global operational security programmes at Deutsche Bank, Elizabeth has lived in and delivered projects across Africa, the Americas and the Middle East.

Passionate about encouraging, informing and connecting both aspiring and established female security professionals, Elizabeth also recognises the integral role that men have to play when it comes to the positive promotion of 'women in security'.

We would like to thank Nicola Thompson for her time leading the committee and please join us in welcoming Elizabeth. Any professionals eager to support the Women in Security Committee should contact the Chapter.

Crisis Management: Don't Lose Sight of the Horizon

By James Morris CPP

In late October 2014, protestors took to the streets in Ouagadougou, the capital of Burkina Faso, and several other cities in the country to protest efforts by the President Blaise Compaoré to extend his 27 years in power by enacting a constitutional amendment to lift term limits.

Over many days, the protestors blockaded streets and businesses, clashed with security forces and eventually attacked and looted several Government locations including the City Hall and the ruling Congress for Democracy and Progress (CDP) Party's headquarters. Protestors also stormed and set fire to the National Assembly Building. A curfew was imposed and flights into and out of the Ouagadougou International Airport were diverted as the airport was closed. President Compaoré dissolved the Government and declared a state of emergency before eventually fleeing to Côte d'Ivoire.

The People's Republic of Burkina Faso is a small landlocked country in West Africa, formerly named the Republic of Upper Volta. The Republic of Upper Volta was established on 11 December 1958 as a self-governing colony within the French Community and, on 5 August 1960, it gained full independence.

It's a poor nation. Around 80% of people are engaged in subsistence farming. Cotton and gold are Burkina Faso's key exports (the country is the fourth largest exporter of gold in Africa). As such, the nation has a large population of international organisations tied to the French Government and an expatriate community working in Government, development and the mining industry.

While the events of October 2014 were, of themselves, not particularly unusual, matching as they did political unrest seen in many parts of the developing world in the past decade, the events exacerbated the West Africa Ebola outbreak that had struck the region in late 2013. It was the most widespread outbreak of the Ebola virus in history, causing not only major loss of life, but also much socioeconomic disruption in the region.

As such, the unrest in Ouagadougou which led to the fall of the Government occurred while many regional Governments, international organisations and global companies were fully focused on another major crisis.

Parallels to the current situation

On 31 December 2019, the WHO's China office heard the first reports of a previously-unknown virus behind several pneumonia cases in Wuhan, a city in Eastern China with a population of over 11 million people. The WHO declared the outbreak a Public Health Emergency of International Concern on 30 January 2020 and a pandemic on 11 March. The virus, now commonly referred to as COVID-19, has hit most of the world and its effects remain widespread to this day.

While Ebola and COVID-19 are very different pandemics, the lessons from 2014 should be heeded by all: a crisis may not occur in isolation. Things can always become worse.

COVID-19 has severely impacted the operations of all companies around the world, challenging their crisis management and business continuity plans as well as their ability to manage supply chains, work from home protocols and many other aspects of their business. However, it's important to not lose focus on other events that could be building or on other threats on the horizon. Adversaries may still be looking for ways to target organisations, insider threats remain a concern and natural events may transpire to challenge an already stressed system. As security professionals, and in our role as both protectors and business enablers, we must maintain a focus on what else could go wrong.

Crisis on crisis

In recent months, this has proven to be the case on several occasions. COVID-19 has disrupted many industries and businesses, causing major job losses, the closure of firms and huge loss of revenues. However, there have been other prominent, non-COVID-19 events as well.

US Protests: On 25 May, George Floyd (a 46-year-old black man) was killed in Minneapolis, Minnesota during his arrest for allegedly using a counterfeit bill. While the events on the immediate arrival of the police are not widely known, footage from mobile phones distributed through social media show a police officer kneeling on a restrained Floyd's neck for almost nine minutes despite pleas from bystanders to stop and from paramedics to allow vital signs to be checked.

For the final three minutes, Floyd was totally unresponsive. The killing caused an explosion of protests in cities throughout the US and in major cities around the world. Peaceful protests were hijacked by anarchists and looters, while counter-protests were also launched, leading to clashes with security forces, widespread violence and significant damage. Many major cities imposed curfews, closed

down some areas and blocked protestors. Numerous businesses were targeted for damage and duly looted. Huge numbers of injuries were reported. The financial impact of the clashes is unknown as protests continue in many cities.

Super Cyclonic Storm Amphan: Amphan was a powerful and deadly tropical cyclone that caused widespread damage in Eastern India, specifically West Bengal and Bangladesh, in May. It was the strongest tropical cyclone to strike the Ganges Delta since the 2007 season and the first super cyclonic storm to occur in the Bay of Bengal since the 1999 Odisha cyclone. Approximately 4.2 million people were evacuated in coastal India and Bangladesh, with roughly 2 million from India and 2.2 million from Bangladesh. Amphan caused over US$13 billion of damage. Amphan is also the costliest cyclone ever recorded in the North Indian Ocean.

Attack on Amazon: In February, Amazon Web Services (Amazon's online cloud service which provides the infrastructure on which many websites rely) fended off the largest Distributed Denial of Service (DDoS) attack in history.

DDoS attacks are designed to knock a website offline by flooding it with huge amounts of requests until it crashes.

AWS said the February attack had fired 2.3 Tbps, which is a little under half of all traffic BT sees on its entire UK network during a normal working day. The prior record, set in 2018, was 1.7 Tbps.

James Morris CPP is Head of Security Services (EMEA) for Aon and a Board member for the ASIS UK Chapter

Lessons to be Learned

(1) Intelligence-led operations

While it's important to mitigate challenges to the business today, the best security programmes have an eye on the threats brewing on the horizon. These are intelligence-led programmes and they use information and analysis to consider risks and opportunities before they become full-blown problems.

While most companies will not dramatically respond to the initial reports of sickness in Wuhan, the rapid spread of a virus combined with the impact of travellers and on the extended supply chain of disruption in major Asian markets should trigger a review of contingency plans at the very least.

(2) Understand the business, its strengths and its weakest links

Understand the intricacies of the business. The supply chain is often the weakest link of any organisation due to its length and reliance on many other moving pieces, and it's most exposed to risks, so understand critical business functions and critical suppliers and understand their suppliers and onwards. The National Hockey League, itself a multi-billion-dollar sports and entertainment league in North America, faced problems early on in the pandemic when it suffered a major shortage of hockey sticks. This was because the main supplier of sticks – a critical tool, of course, for most players – was based in Eastern China. The impact of major events can be wide and surprising if you don't fully understand the loops in your chain.

(3) Realistic training

Test, test and test again and, above all else, make the testing realistic. As Mike Tyson once said: "Everyone has a plan until they're punched in the face." Expose your plans to realistic tests that make participants uncomfortable – give it a figurative punch in the face. It's only in this environment that true learning can happen and weak points may be identified and rectified. While it may not be necessary to use every exercise as an opportunity to make participants sweat – as the value of desk-top and small group discussions is also high – ensure that enough exercises are recreated with realistic scenarios and cadence. Similarly, when testing consider what would happen if things became worse (because they always can).

An incident being managed well allows you to develop your structure and response processes, enabling your business to take on better opportunities with the confidence that future threats will be spotted and addressed on a swift basis.

That's the key to sustainable competitive advantage, which in turn is the key to security functions becoming trusted advisors to the business leaders.

Has Your Professional Credibility Been Recognised?

The SSR Personnel and Executive Profiles 2020 Annual Salary Survey partners with ASIS International. Data is collated from more than 12,000 security professionals from across 40 business sectors including finance AND insurance, manufacturing, extractives, e-commerce, FMCG and logistics.

Average wage inflation was 3.1% and management increases were 5.1% from the SSR survey. Over 65% of respondents reported that they were underpaid, which is up from under 50% the year before.

The employment rate had remained high and then... COVID-19 emerged...

Up to February 2020, a record 33 million people were in employment. This was mainly driven by an increase of women in employment and self-employed workers. By June, advertised jobs had dropped to 75% of the pre-COVID levels, with at least 8.4 million workers covered by the Government's Coronavirus Job Retention Scheme, according to the Office for National Statistics.

We're seeing a gradual return to work, but the tech giants that have prospered during this period have in general told office-based members of staff not to return to work until the New Year. Twitter has said that its own 'business as usual' model may become remote working.

Physical security growth

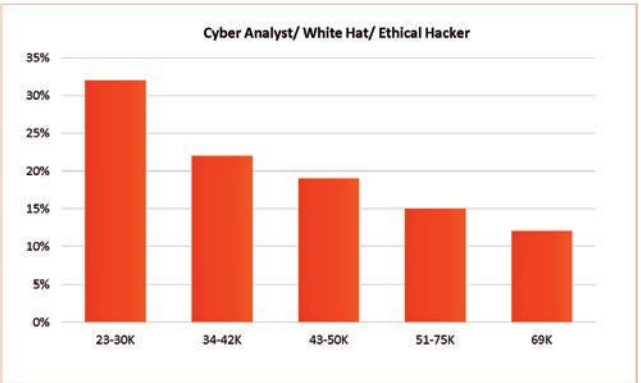
The total value of world production of physical security products at factory gate prices in 2019 was $34.3 billion. According to a report from Research and Markets, it forecasts that global market sales will reach $56.76 billion in 2024. These figures are robust and not deflected by the pause in economic growth, but most probably will be accelerated through insecurity.

In 2019, Artificial Intelligence-centric technology applied to video surveillance data was just being trialled. In 2020, it will become a key component in identifying COVID carriers' behaviours when added to thermal imaging. Significant improvements in AI video analytics software is making this possible and, over the next ten years, it will become a standard requirement across surveillance solutions. There's a critical need to make full use of the massive amounts of data being generated by video surveillance cameras and AI-based solutions are the only practical answer.

Cyber security still booming

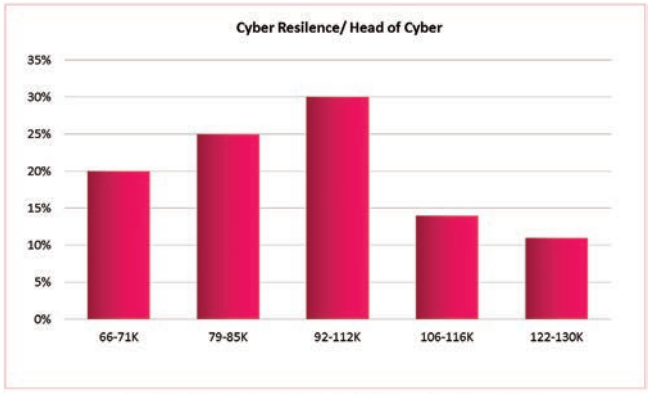
The SSR Middle East 2020 Annual Workforce Survey estimates cyber security vacancies globally are approximately 3.5 million, which is increasing in this COVID environment as remote working will become the norm. Most offices can only operate at 50% capacity within a one-metre distancing rule. You must then factor-in a capacity of 2-to-3 people per lift for accessing their desks.

Computer sciences and programming degrees have not been the first choice for many graduates. This is changing as more women are attracted to cyber security. That would significantly rebalance the estimated female under-representation in IT of just under 20%.



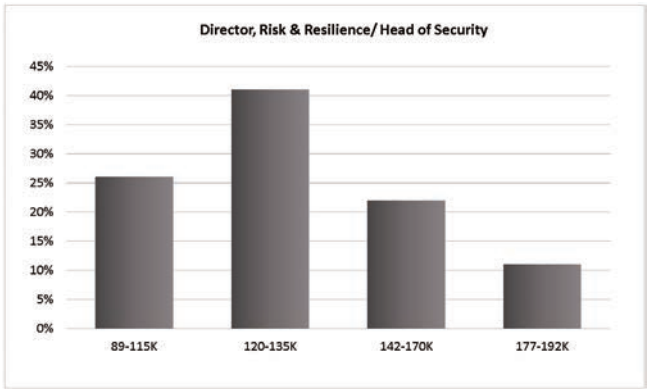
Cyber Analyst/ White Hat/ Ethical Hacker

As organisations go on the attack against Cyber resistant intruders, the skills for this role are streched across the United Kingdom and Europe. Certification will not help, like law enforcement you are seeking technicians who have an exploring nature, 'in hamrony with machine code'



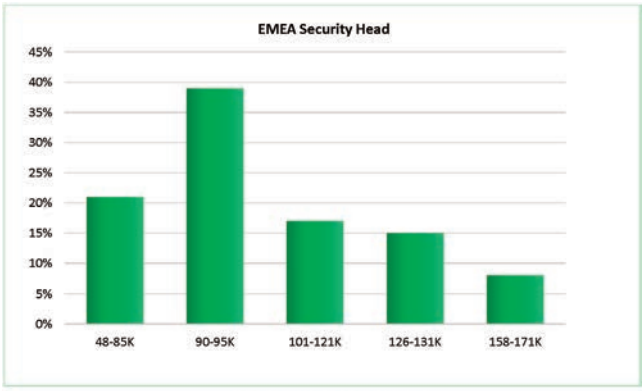
Cyber Resilience Manager/ Head of Cyber

A role that is developing across a range of sectors as organisations elevate their response to cyber attacks. The rapid controls of insider users that organisations need to have requires a robust Cyber policy against perennial and growing risk.



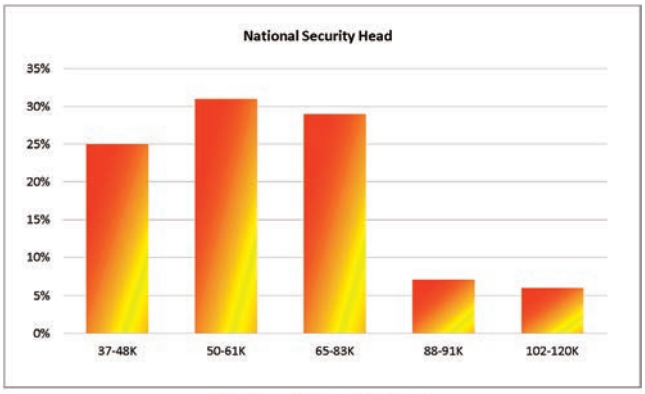
Director, Risk & Resilience/ Head of Security

Responsible for delivering localised policy and executive board briefings. They are a driver for change and service expansion. Responsibility for Cyber Hunting, Risk Alert programmes, Business Continuity and Crisis Management should have increased basic salary by 20-30%



EMEA Security Head

Regional policy development, executive reporting, promulgating corporate policy overview of physical and intellectual protection. Taking responsibility for cyber hunting ,risk alert programmes, business continuity and crisis management should have increased basic salary by 20-30%

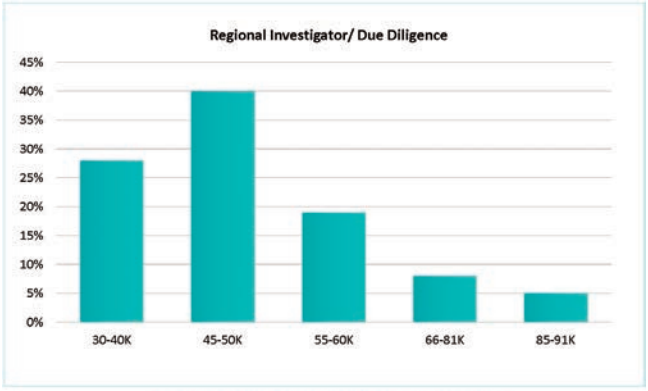


National Security Head

Responsible for all aspects of corporate security and maintaining standards across an estate. Developing an estate programme for internet connected devices and plant what has been overlooked by I.T departements. GDPR has been and remains a major part of this role oversight.

Main HQ Site Security Manager

Physical and information protection, proactive, local policy implementation and development. Budget responsibility £2m - £5m+.



Regional Investigator/ Due Diligence

Supply chain management, implementing corporate procedures. Compliance and audit functions within supply chain, 3rd party manufacturing.

The global cyber security market is booming, having grown by 30 times in the last 13 years. The cyber security sector was valued at US$161.07 billion in 2019 by Mordor Intelligence and is expected to reach US$363.05 billion in value by 2025.

Increasing cyber security incidents and regulations requiring their reporting are driving the human and technology growth. The USA Center for Strategic and International Studies and McAfee reported that cyber crimes currently cost the world almost US$600 billion each year. That's 0.8% of global GDP.

The cyber security sector requires diversity to thrive. The field is wide open for people across generations, races and gender identities. Creativity and collaboration are as important as technical acumen so there's no 'stereotypical' cyber security professional. The 2020 Tessian Report stated that if women earned as much as their male counterparts, the sector cost would increase by £4.4 billion in the UK alone.

While slowing trade, the pandemic has not slowed the growth of cyber criminality. Ransomware-wielding criminals are also growing increasingly ruthless based on the size of their extortion demands and their increasing propensity to leak data in an attempt to force victims to pay up. That's according to BakerHostetler's investigations into hacking breaches.

Based on more than 1,000 incidents investigated in 2018, the average ransom paid was, in fact, $28,920 and the largest payment masde was actually $250,000. In 2019, the average ransom paid jumped to a total of $302,539, while the largest single payment was $5.6 million.

What of the world post-COVID and Brexit?

More than a billion workers around the world could suffer financial hardship as the Coronavirus destroys jobs, cuts working hours and slashes pay. One-third of the global workforce is expected to feel the effects directly, according to the International Labour Organisation (ILO), with those in the retail, manufacturing, accommodation, food and transport industries hardest hit.

The ILO said: "Workers who are engaged in activities deemed essential – for example food distribution – continue to work, but they face greater occupational health risks. Workers in non-essential businesses face widespread closures and sharp reductions in employment and hours."

Essex University research predicts that 6.5 milion jobs in the UK could be lost post-October after the furlough scheme ends.

A common thread in the SSR study was that Brexit will affect respondents' future options, with many commenting that upward travel in a security career is hard. Has the appetite for confrontation diminished on either the UK or EU negotiation sides with a recession three times worse that that of 2009 and the worst recession in 300 years predicted? The smart money would appear to be on a 'No Deal'. We are all wounded by a virus, the Euro will be under pressure and Turkey has many millions of refugees to send to Europe and the UK. Life is not going to be normal. We will have economic uncertainty for years, but we must also bear in mind that the UK's security business sector will have opportunities to thrive.

SSR Personnel
the face of recruitment

ASIS | UNITED KINGDOM EDUCATION

By Richard Stevens (ASIS UK Chapter Director for Education)

As security professionals navigate these uncertain times, it's worth outlining the temporary changes which have been made to the ASIS certification process due to the impact of COVID-19, the pathway for those looking to apply for an ASIS Certification and the UK Chapter's position as a licence holder for the Register of Chartered Security Professionals (CSyP).

Security professionals have been at the heart of the global response to COVID-19, helping their communities and organisations keep people and businesses safe. The COVID-19 pandemic has touched all aspects of our professional lives, and this includes those who are part of the ASIS certification process. As a result, ASIS International has made short-term adjustments to its certification policies for members who are planning to sit the certification examination or, indeed, those who need to re-certify.

In many locations, the Prometric Test Centres remain closed, or are otherwise operating with greatly reduced capacity to accommodate social distancing measures. These operational changes mean that many members who have booked a certification exam have had to re-schedule their appointment. In response, ASIS is temporarily suspending all cancellation and rescheduling fees for ASIS certifications for any member unable to sit their exam or who are uncomfortable sitting the exam due to COVID-19 concerns. Once you've cancelled/re-scheduled your exam with Prometric, please contact ASIS hq such that your records can be updated.

If you're not quite ready to take your exam, you do have two years to take your exam from the point at which you were approved, so for many there is time to wait until the current situation subsides before sitting an exam. If you're close to your two-year point, and have not taken the exam, then please contact ASIS hq to discuss extending your deadline.

For members who need to re-certify, many of the traditional options for collecting CPE credits have been cancelled or postponed. ASIS has a range of online learning offerings which already qualify for re-certification credits, including low cost and free webinars. Full details can be found on the professional development tab on the ASIS international website.

Useful contact information
Prometric: www.prometric.com/asis
ASIS hq: certification@asisonline.org

Are you thinking about taking a certification?

Although Testing Centres are currently closed, or operating at reduced capacity, applications for study can still be made: you have two years to take your exam. One question regularly asked is: "Which Qualification is right for me?" ASIS offers four security certifications and a member can hold three qualifications (this is because the APP certification is subsumed by the CPP when you achieve the latter).

The Certified Protection Professional (CPP) program is designed for those who've demonstrated competency in all areas of security management, including nine years of security experience, at least three years of which shall have been spent in responsible charge of a security function. The 'Gold Standard' for more than 40 years, the CPP credential provides demonstrable proof of knowledge and management skills in seven key-critical domains of security.

The Professional Certified Investigator (PCI) program is designed for those whose responsibilities include case management, evidence collections and the preparation of reports and testimony to substantiate findings. Earning a PCI certification

provides independent confirmation of specialised skills in security investigations, including case evaluation and review of options for case management strategies. It validates your ability to collect information through the effective use of surveillance, interviews and interrogations. To be eligible for the PCI requires five years of investigations experience, including at least two years in case management.

The Physical Security Professional (PSP) program is designed for those whose primary responsibility is to conduct threat surveys, design integrated security systems that include equipment, procedures and people or install, operate and maintain those systems. Earning a PSP demonstrates expertise in conducting physical security surveys to identify vulnerabilities and performing cost analysis for the selection of integrated physical security measures. In addition, it confirms specialist knowledge in systems procurement, final acceptance testing and also implementation procedures.

The Associate Protection Professional (APP) program is designed for those with one-to-four years of experience in the fundamentals of security management. This certification measures the professional's knowledge of security management fundamentals, business operations, risk management and response management.

Overview of the certification process

Step 1: Baseline your knowledge

The Self-Assessment Study Guide allows you to test your professional knowledge against the syllabus of your preferred ASIS certification. For those who have not studied formally for a while, the guide also contains help with creating and implementing a study plan. The Self-Assessment Guide is a free resource available to download from the ASIS International website.

Step 2: Application

All applications for certifications are made online via the ASIS International portal. Once an application is reviewed and approved, you will receive an 'Authorisation to Test' e-mail. ASIS exams are offered at Prometric Test Centres.

Application Fees: 2020 Application fees for CPP, PCI and PSP are $335. The fee for the APP is $200.

Step 3: Studying

Your personal learning style will determine which is the best route for success when studying for an ASIS certification. The benefit of the ASIS certifications is that there are a variety of study routes which you can mix and match.

Certification reference material is available for members to purchase directly from ASIS International. The documents are hard copy versions of reference materials, standards, guidelines and manuals. The latest reference material can be found at the following link www.asisonline.org/commerce/store/

CPP and PSP Online Learning: ASIS International offers online reviews for the CPP and PSP certifications. Enrolment provides you with round-the-clock course content, allowing you to study at your own pace and convenience.

Intensive classroom study courses: Several specialist education providers run classroom-based intensive study packages which members can purchase. The packages are a supplement to self-study and some also include the exam on the last day.

UK Study groups and 'bootcamps': Chapter members who are studying for ASIS International certifications are also involved in organising informal study groups in order to support collaborative and collective learning.

Final Step: Examination

Within your two-year window, book and sit your chosen exam.

Register of Chartered Security Professionals

For those ASIS members who hold senior security appointments, the UK Chapter (along with The Security Institute) is a licence holder for the Register of Chartered Security Professionals. The Register of Chartered Security Professionals was established under a Royal Charter issued to The Worshipful Company of Security Professionals in the UK and launched in 2011. Registrants use CSyP as a post-nominal and are called Chartered Security Professionals.

Becoming a Chartered Security Professional is a means of being recognised and continuing to represent the highest standards and ongoing proficiency. It's 'The Gold Standard; of competence in security. The Register of Chartered Security Professionals is recognised across the UK, including by the Security Industry Authority, the Centre for the Protection of National Infrastructure and membership organisations, among them the Association of Security Consultants and the International Professional Security Association.

Every Chartered Security Professional has demonstrated advanced competence in five key areas. These are :

- **Security Knowledge**
- **Practical Application**
- **Communication**
- **Leadership**
- **Personal Commitment**

ASIS' UK Chapter has extensive expertise in advising and guiding applications wishing to join the Register. Anyone interested in applying for the CSyP Register can access more detail online at http://www.asis.org.uk/CSyP.shtml or, alternatively, contact Mike O'Neill or Rich Stevens.

CSyP

ASIS UK Chapter Member Profile

Matt Dixon CPP PCI PSP CSMP FISMI (Director, Comperimus Consulting Limited)

Tell us about yourself

I'm currently the director of my security consultancy firm, Comperimus Consulting. The company is based in Reading and specialises in providing security and risk management consultancy to the SME sector. My passion is security surveying and the design of physical security systems for clients. I enjoy the detective work of surveying a building to identify the vulnerabilities and then working with a client to devise cost-effective solutions. I'm a self-confessed physical security 'geek'. My wife once told me off at a wedding reception for paying more attention to the security cameras' layout than the other guests at our table.

What's your current role and how did you come to be in this position?

I worked within the corporate security world for 15 years, but decided in early 2019 that I wanted to make the break and set up my own business. Long days commuting to London had lost their appeal. I had worked my way up the career ladder, having started as a regional security manager and moving through the ranks to become head of security for one of the world's most famous jewellers and luxury goods companies.

I'm a former police officer, and I think that many of the skills I learned in the police service have served me well throughout my time in security. Immediately after leaving the police, I worked as a close protection officer for a diamond dealer. That was an interesting role demanding quick thinking and the ability to be flexible at the drop of a hat.

What does a typical day look like in your current role?

One of the great pleasures of being self-employed is the flexibility that comes with it. I take my children to school and then settle down at my desk with a good cup of coffee. Unlike the corporate world, no-one gives you work when you're self-employed. You have to go and find it yourself. If I'm not working on a project for a client, I spend my time generating new leads and new business through networking, social media and marketing. It's challenging and sometimes disheartening, but when you successfully engage a new client, it's worth it. One day, I could be writing a security policy and strategy for a client, and the next I can be surveying the proposed fence line for a new development. No two days are ever the same.

What changes have you seen during your time in the industry? What do you think the future of the industry looks like? Where do you think the industry is going?

I think the most significant change I've seen over the past 15 or so years is the shift of mindset in the corporate world that security is not just about 'guards, gates and guns'. The clichéd image of the security professional being a sort of nightclub doorman has thankfully given way to the understanding that security is in itself a highly professional discipline.

There has also been a shift in the perception of what value security brings to an organisation. Limited budgets have always focused on those business areas that generate revenue. With challenging economic times, businesses understand the value of protecting their assets more than ever and are seeing how security actively assists this process.

The convergence of traditional security and IT is the way forward. However, there will always be a need for more traditional security and risk management disciplines. Technology is a force multiplier for security operations and that will only increase as our world becomes more cyber-focused.

There's now a much more defined career progression in the security industry and the wide range of qualifications out there demonstrates the industry's commitment to helping people develop professionally.

Tell us about your ASIS experience

It's like the world's most mammoth little black book of security contacts. I joined ASIS when I was working in my last corporate role, primarily to be able to network with a global audience of fellow security professionals and to have access to the most up-to-date literature and thinking in the industry. I'm a massive fan of the message board forums. Generally, security professionals are a friendly bunch, and it's great to bounce ideas off people and to receive input from various countries and cultures. I was working on a project and couldn't see a solution to a problem. I posted a question on the message forum and, within 24 hours, had responses from Australia, the US, South Africa and Europe. All the contributors freely offered advice and opinion and my problem was solved. Like every organisation, you derive from ASIS what you put into it. I highly recommend attending an event and speaking to as many people as possible.

Can you talk us through your journey to achieve The Triple Crown? Why did you decide to take it on? Any tips for others thinking of doing the same?

When I started my own business, I had some time on my hands and decided that I would use the opportunity for professional development. I sat the PCI first of all as I've always had an interest in the science and psychology of investigations and interviews. I was also drawn to the fact that there are not many PCI holders in the UK. Having done this, I attended an intensive classroom training course and duly passed my PSP exam. Having obtained these, I wanted to 'go for the full set' and participated in a subsequent intensive classroom course for

the CPP. I had previously studied large parts of the CPP exam doing PCI and PSP, so it felt like a natural continuation of the study process. There's no doubt that CPP is the global 'Gold Standard' for security, and I hope that its credibility gives my clients confidence in my ability and knowledge. I completed all three in eight months (which is not something I would necessarily recommend!) while also sitting a challenging Level 6 security qualification. I was delighted to pass my CPP exam on the first attempt and have a few weeks off studying. It was hard work, but I'm hugely proud to be a Triple Crown holder.

For anyone thinking of going for the certification I would say: "Do it". There are many ways to study, and while it's a significant commitment in terms of time and effort, every time you open the POA you're increasing your security knowledge. I would be very happy to chat with anyone considering taking the ASIS exams. JDrop me a line through LinkedIn.

What are the benefits of holding ASIS certifications?

As a consultant, it affords me credibility and provides my clients with reassurance that they're making an investment in someone who has knowledge and demonstrable expertise in the field.

As I said, CPP in particular holds a global status as 'The Gold Standard'. Obtaining certifications makes a statement about your commitment to self-development and your ability to commit to a study regime. The need for re-certification ensures that you stay on top of your CPD. Passing the certification is really the first step on the journey.

I think the new APP certification is a very good step as it provides for those at the earlier stages of their security career the opportunity to gain CPD. It seems to be a good stepping stone to the next stage of certifications such as CPP or PSP.

What piece of advice would you give professionals who are at the beginning of their careers?

Take every opportunity to develop yourself professionally and build as wide a network of contacts as you possibly can. Visit events and seminars, complete CPD, partake of webinars and training and, above all, talk to (and network with) as many fellow professionals as you can. Every challenge you face will have been faced by your peers at some point in their careers, and I've not yet met a security professional who hasn't been willing to share their time and expertise.

Data Centres: Securing More With Less – Lessons From The Pandemic

By Terry King (Regional Director for EMEA/APAC, Guidepost Solutions Limited)

In the weeks following the spread of COVID-19, countries and businesses were abruptly forced into critical decisions relative to reducing or ceasing operations, defining essential operations and manoeuvring multiple mandates. The resulting questions include: 'How are we going to do more with less?' and 'How can we ensure the safety of our people and the security of our business?' Some had no choice. Emergency and primary healthcare are always essential, while businesses directly serving the public (such as delivery services, supermarkets and drug stores) are, by default, essential to maintain a healthy public.

By the end of March, regulated geographies impacted nearly half of the global population. Most workers moved to remote home offices and students switched to online learning. As people locked down, quietly the cloud had become more than essential and the Data Centres that provide an actual physical home to cloud and computing services were clearly (even if not designated as such) essential to our pandemic mode of operation. Industry-leading Data Centre operators faced key questions about how to continue operations, mitigate the risk of employees contracting COVID-19 and secure their facilities with less.

How does your business continuity plan measure up?

The speed at which the virus moved across the globe caught many business experts off guard. A variety of business operations were caught on their heels working through outdated business continuity/disaster recovery plans – plans that didn't properly account for a global pandemic, nor the re-routing of all business operations to remote locations.

Data Centres, however, have spent the last decade fine-tuning how to ensure the required uptime of their facilities with remote monitoring, maintenance and operations. Data Centre operators

implemented technologies to secure facilities, including improved access control to deter incursions and video capabilities to monitor critical operations such as air-cooling units, PDUs and back-up power systems.

Much like a consumer's phone or fitness 'watch', Data Centre operators could ascertain issues with any number of systems remotely and in real-time prior to the system or component failing. This ever-increasing advance in technology allowed Data Centres to quickly reduce on-site operational capabilities, augment staff scheduling and determine which components of their business were essential to ensure unimpeded operation of their mission-critical facilities. Business leaders can glean some valuable lessons from the approach taken by Data Centres.

Ironically, the efficiency of operating and maintaining the mechanical components of a Data Centre have improved as a result of the same digital technology in which they host. Securing these facilities during the pandemic has taken on an even greater level of urgency as staffing evels were reduced and the public became more reliant on digital business being hosted within the walls of the largest Data Centres in the world.

With operations minimised, some providers significantly reduced their internal operations and closed European operations to customers needing access to their sites. Many operators adjusted and reduced staffing globally. Some augmented internal operational guidelines for site access to include temperature scanning and the pre-access screening of visitors at sites. Site security workers, already essential to maintaining both a secure and hospitable environment for Data Centre customers, were now on the front line of ensuring the facility would be secured from standard external threats and an unseen, highly contagious virus.

Data Centres would be forced to use all aspects of their enterprise access control and video solutions to accommodate a variety of variables including a reduction in staffing, augmented site access requirements and physical tours throughout the facility. While some eliminated customer access in Europe, most commercial Data Centres could not simply close their doors. Mitigating customer access could potentially disrupt critical services provided by a variety of companies and public sector entities. These mission-critical tasks would lead to newly updated Standard Operating Procedures to allow operators to properly manage their reduced and remote teams. Companies implemented temperature screening and site disinfection requirements with other Data Centre operators across the globe, evaluating solutions such as Enterprise Voice Over Internet Protocol (to allow for remote communication) video analytics, thermal imaging, facial recognition, the capabilties of Remote Global Security Operations Centres (GSOCs), managed concierge services and virtual credentials.

Currently employed enterprise-level systems allow for the management and operation of remote security. However, in some scenarios these capabilities fall short. For example, localised intercom communications, the manual issuance of access credentials and integrated visitor management platforms lack remote security options.

In other cases, the highest level of securing access points within the Data Centre itself became a 'flash point' for viral concern (such as with the use of contact biometrics). Highly secured areas within the Data Centre may require the use of a card reader and fingerprint reader for dual authentication access. In January, this level of access was considered critical. Come April, facial recognition found itself as the top priority.

Other emerging technologies, such as thermal screening, require a greater level of on-site personnel to operate effectively.

Even with new technologies and a quick pivot by most in the industry, securing more with less was still a challenge and one that evolved as the COVID-19 pandemic spread.

The post-Coronavirus context

In my 25-plus years in the security industry, I've had the pleasure of designing, co-ordinating and implementing high-level security systems for the Data Centre environment. As security is a critical feature to the Data Centre operator, most locations have been thoughtfully planned and designed for the highest level of security systems implementation. Local operational staff and supporting security team members are reliant on complex and integrated security solutions and security workflows that dovetail the technology and the operational management.

Facilities have been located areas that are remote from central business traffic to better ensure a cost-effective and more controlled environment, but with the proper level of accessibility to power and infrastructure. Buildings have been hardened with perimeter fencing, facility-wide video coverage and blast-resistant materials, all designed to protect against potential threats to the digital economy that drives most of our business today.

However, in what seemed like a moment's notice, today's threat became one that was not only unseen, but had the ability to mitigate the very systems and processes that have protected Data Centres. In many industries, the terms 'security' and 'safety' have now taken on a new context as organisations move to protect their people, while also remaining flexible to the ever-changing global environment.

Terry King (Regional Director, Guidepost Solutions)

Terry King is an expert in the design, consultation and implementation of electronic security solutions. He has more than 25 years of experience in both security consulting services and systems integration. Terry specialises in large, new commercial construction projects placing an emphasis on effective communication between critical stakeholders and all associated trades and partners. Further, he has significant experience in the development of design standards for electronic solutions in both the commercial and public sectors covering a wide range of vertical markets. In addition to his design and engineering experience, Terry has a significant background in the assessment and analysis of existing facilities, including security systems, operational security and standard operating procedures. His expertise extends to the programme/project management of large-scale implementation projects and the administration of standardised systems.

The 'New Normal': Increasing the Range of Risks to Business

By Ioannis Choulakis

Facebook recently joined the list of companies including Twitter, Mondelez, Nationwide, Barclays and others that have announced remote working will become the 'new normal' way of working for many employees. While the shift is clearly driven by the COVID-19 pandemic, as security professionals our role is to identify risks to the business and assist in mitigating them. One risk that this shift in the way of working could accentuate is 'The Insider Threat'. With millions of employees working remotely, cyber security and IT teams subjected to new and heightened demands, supply-to-demand volatility and escalating psychological stress, cyber criminals have begun to actively exploit this crisis.

'The Insider Threat'

There are several definitions of insider threats. Here, let's consider 'The Insider Threat' as an employee with malicious intentions (ie a deliberate act) or an employee with non-malicious intentions (ie an accidental act).

Signpost Six, a cyber security consultancy, states that: "An insider threat is posed by an individual who has or had authorised access to an organisation's network, system or data and who, wittingly or unwittingly, potentially causes harm to the organisation. The problem is that the insider threat impacts organisations across all industries. Although the attack methods vary, the primary types of insider acts – ie the theft of Intellectual Property, sabotage, fraud and espionage – continue to hold true and are increasing with the expanding reliance on digital technology."

'The Insider Threat' and COVID-19

The insider threat risk has increased because of mass remote working during the COVID-19 quarantine. In a recent COVID-19 Cyber Security Pulse Survey conducted by (ISC)2, it was shown that cybers ecurity incidents have increased by 23% since the beginning of the pandemic. This demonstrates the difficulty that businesses have in safeguarding their information assets while their employees are in different locations and can access business-related information just as if they were in the central working environment.

The problem is the result of three ingredients wherein each has a knock-on

effect, consequently increasing the risk of the insider threat.

The first is the lack of Human Resources in information security teams. This is depicted by the ISACA's State of Cyber Security 2020 Survey Part 2 report which states that 62% of organisations' security teams are understaffed. This has decreased the ability of the security team to monitor good cyber security behaviours at a time when, arguably, they're needed more than ever before.

Second is the lack (or bypassing) of control measures designed to minimise the risk. This is the end result of several factors, such as the lack of Human Resources in the Security Department as described previously and the willingness of employees to cut corners to make their jobs easier. In recent research, 52% of respondents believe that they can 'get away' with riskier behaviour by working from home. A rogue employee may feel that security is not the organisation's priority and will think that the risk of being caught while committing a crime is low. This, along with the employee's appetite and the availability of resources, are factors that, according to routine activity theory, increase the possibility of someone committing a crime.

Meanwhile, employees with non-malicious intentions are an increased threat because they're not aware of the risks they pose and have less natural oversight in place because of being away from colleagues and in a much more relaxed (ie far less cautious) state.

While business continuity, and even survival, has become the key business priority, companies and employees alike are now exposing themselves to significantly increased cyber risk which, in turn, heightens the exposure to a range of other risks.

Proposed mitigations

For organisations to minimise the risks, they should identify and manage them by adopting an holistic approach to them. A useful risk management framework in this regard is the Enterprise Security Risk Management (ESRM) framework created by ASIS International.

This will have, in effect, several layers of the security strategy. First, the Security Department will take into consideration all the threats that the organisation faces. For example, why invest heavily in an awareness campaign on identifying phishing attempts, but not mention that employees shouldn't be leaving company laptops and sensitive information unprotected at home?

Similarly, the implementation of ESRM across organisations will help to create a strong security culture. In conjunction with security awareness campaigns, this increases ownership of risks and mitigations. Ownership of risks and responsibilities for mitigations ensures that investment in security is not wasted due to the small loopholes or negligent behaviour. It increases the likelihood that employees are aware of their own behaviour and that of their colleagues (be that rogue or simply negligent) and, as well as the likelihood that malicious acts are spotted or otherwise thwarted early.

There are also a range of technological solutions available that can support mitigation effort. These increasingly include decentralised peer-to-peer blockchain networks on which the organisational data can be stored and a multifactor authentication based on machine learning technology that will verify the identity of the users. The range of technological solutions now available benefits organisations if the fundamental security measures supporting them are also in place.

One threat of many

The approach described here is based on one very limited risk: 'The Insider Threat'. However, adopting an holistic approach around the concept of ESRM allows companies to mitigate a broader spectrum of risks. That's increasingly important during these challenging times.

Ioannis Choulakis is a Cyprus-based experienced security professional, having worked for the Hellenic Police and the European Asylum Support Office (EASO), with post-graduate studies undertaken in the subjects of security and risk management