THE SECURITY INSTITUTE

Respected, Recognised, Professional

DATE: September 2020
ISSUE NUMBER: 04
Through our expert industry knowledge, we help businesses solve their cyber security challenges. With our transparent approach, solution led services and unparalleled products we minimise risk and security threats ensuring your business is safe and secure for continued success. We specialise in:

- Cyber Security Strategy
- Cyber Security Consultancy
- Governance, Compliance & Risk
- GDPR & Privacy
- Security Awareness Training
- Cyber Essentials & IASME certified assessors

Visit www.macyberuk.com | contact mo@macyberuk.com
A Note from The Editors:

It has been a busy few months here at the Security Institute as we continue to adapt and support our members through the on-going Covid-19 pandemic. This period has emphasised the importance of continued professional development for security professionals, and we have strived to further improve our membership offering with the new addition of our Community Platform (Page 16) to support knowledge sharing amongst members as well as continuing our filled Webinar schedule. This will cumulate with our premier CPD event, our Annual Conference, which will take place virtually over the week commencing Monday 19th October (Page 8 – 9).

Other big news from the Institute in the last few months, is the launch of our Approved Training Provider (ATP) Scheme. The ATP Scheme provides a third-party assessment of quality for security-related training courses, which will assist security professionals that are searching for quality training opportunities (Page 40 – 41).

We have also launched a campaign alongside BSIA and the Security Commonwealth, to help ensure that the security professionals that continued their essential work during this pandemic are recognised by the wider public for their efforts (Page 10 – 11).

In addition, last month saw our first face-to-face since February with our August Members Lunch (Page 19). We have a full calendar of digital events that you can book to join here: https://event.bookitbee.com/security-institute

Jade Lapper and Ben Harding

Editor: Jade Lapper & Ben Harding
The Institute Quarterly is published 4 times a year.
For enquiries please contact: ben@security-institute.org
www.security-institute.org
Chief Executive’s Address

Rick Mounfield CSyP FSyI

I’ve been the Chief Executive of this incredible organisation for over three years and it has been my privilege to have the opportunity to engage with remarkable people in dozens of security disciplines, protecting people, property, information and the country in general, each professional displayed a selfless attitude and the mantra of “just doing my job” but so often, it’s a lot more than that!

It occurred to me that in each editorial I focus on those that have contributed to the development of the Institute but this month, I must make comment on the significant increase in activity, the majority of which is not widely reported. The projects where members are selected for specific skills and invited to contribute to the Institute’s part in National projects that will impact the security of society beyond our membership.

Our strategic aims are written for all to see and if you took time to review them, you would realise that the Board’s strategic aims born in 2017, are more advanced now than they have ever been. Specifically, I refer to the Institute’s Mission statement: “To Inspire, inform and influence professional excellence for the benefit of our members, the security community and wider society”.

I truly believe that now, the wider society is benefitting from the work our members conduct voluntarily behind the scenes, seeking no reward or recognition.

During a pandemic lockdown, every business is forced to reassess their priorities and capabilities. We did that, as did every other business. The result was a shift to digital content and knowledge transfer together with an enhanced portfolio of online resources. For the first time, I think we offered benefits to members globally in equal measure. Thankfully, our earlier transition to mobile and digital resources set a platform for further investment. The smartphone app usage increased. The professional development platform logins tripled and the mentoring volunteers flooded in. Behind the scenes, furloughed members had time to professionally develop and help others too.
In the Summer, we invested in the Community platform where all members have opportunity to connect with other Institute members, join special interest groups (SIGs) and seek knowledge. They also connected with other members, joined SIGs and continue to share knowledge. Like a Brain, the connections were firing and the community has taken on a life of its own. The SIGs have leadership and purpose. Members are starting new SIGs like the Inclusivity SIG, (Thanks to Anna-Liisa Tampuu ASyl/ Lisa Reilly) which attracted 44 people from all over the world onto a video conference and for once we saw what diversity truly looks like. Shane Green MSyl helped to convert his own concept of an information sharing platform into an Institute resource which is now very active with local intelligence and media sources posted relating to incidents all over the world, in real time. This is the community spirit that is impacting thought leadership, inspiring others to join and therefore influencing professional excellence, benefitting not only members, but the security community and wider society too.

Members have volunteered to contribute as the Institute in initiatives such as:

- Physical penetration testing register with the Cabinet Office.
- Created webinar presentations and given their time to present them.
- Frontline Security Skills Strategy Group with the SIA.
- Protect duty law consultation with Home Office OSCT.
- Development of the Cyber Security Council with DCMS & NCSC
- Improving the Perceptions of Frontline Security with The BSIA and Security Commonwealth
- The Next Gen and EY Foundation Secure Futures program

I continue to be inspired be each member and value every interaction. There are so many opportunities to get involved and many that will enhance you personally and your business too.

As you read through this edition, consider the opportunities you could engage with:

- Join the Membership Matters Advisory Group (MMAG)?
- Become an Approved Training Provider (ATP)?
- Join the Validation board (VB)?
- Present a webinar or write an article for the benefit of others. All count towards CPD and all add value.

As I draw to a close, I want to recognise and welcome the 30 Government Security Departments now registered as Group Members. This equates to about 800 individual members who have their membership paid for by the Civil Service as an investment in their development. I appreciate their input and professionalism that add to the collective capability. In the same vein, the Corporate Partnerships that keep us abreast of developments in Technology, intelligence and niche sectors without whom our offerings would be diminished.

Lastly, I must recognise my team who have weathered the lockdown changes without missing a step. Adapting to home working and now, back into a hybrid system of office & home without any reduction in output. In fact, digital output and engagement has never been higher and membership/ Chartered Security Professional applications continue to increase month on month so we employed Victoria Smith to help us cope. Welcome to the team Vicky! Already part of the furniture!

Enjoy reading this edition, I hope to see you in person soon.

Kindest Regards,
Rick
This summer we published our comprehensive annual report for 2019-20, detailing our significant achievements over the past year. Since the pandemic forced us to cancel this year’s AGM when we normally gain the opportunity to discuss our progress with members, after meeting our financial reporting requirements we decided to create a later, more extensive report that would serve a number of key objectives.

First, it is intended to help us affirm to our members, corporate partners, sponsors and other stakeholders that, in accordance with our corporate mission, we exist to inspire, inform and influence professional excellence in security, demonstrating good governance and the highest standards of ethics and integrity.

Secondly, it supports our management strategy and goal setting, enabling us to take a step back and consider our achievements over the past year to gain a big picture perspective, and inform our priority-setting for the year ahead.

Finally, it will serve as an important marketing and promotional tool for the Institute, to be shared with prospective members and key stakeholders in government, industry and academia to demonstrate our purpose, credibility, competence and influence.

The report was a considerable group effort involving many of the HQ team and directors, but special recognition is due to our Marketing and PR Officer Ben Harding who oversaw its development and production. We are next planning to have a limited print run of the report, and a pdf copy will also be available to enable it to be more easily shared. In this column, I want to draw attention to some of the highlights and encourage you to share the report, available here: https://security-institute.org/annual-report-2019-2020/mobile/index.html with prospective members and others who may find it interesting.

Strength in numbers

I hope readers will agree that there seems to be a real buzz around the Institute these days. Almost every time I log into LinkedIn, I see a new joiner celebrating their admittance, or a member displaying their annual continuing professional development (CPD) certificate of achievement. This is a wonderful illustration of the community of support and influence that we, as a collective, have created and we are grateful to those who share their accomplishments and convey their pride in the Institute.

As the annual report indicates, at the end of 2019 we had 3,404 members, a 20 per cent increase on our 2018 numbers. We are now recruiting an average of 113 new members per month, based on the average monthly figures for 2020, and are on track to reach around 4,000 members at the end of this year. The shortfall in these numbers is due to a data cleanse of student leavers earlier this year as board director Tony Aston mentions in the report.

Many of our new members are joining us through our government group membership and corporate partnership schemes, and we see scope to boost our student membership numbers again by building relationships with a wider range of universities as more security-related courses are created. I want to wish all of our new members a warm welcome into the Institute, and express my hope that you will both benefit from your participation and share your much appreciated expertise with us.

Growing activity

Rick’s column this month (p.4) puts a spotlight on the considerable breadth of Institute activity and the numerous volunteers behind all of these efforts. The pandemic lockdown led our HQ team to innovate and extend our online infrastructure to ensure there was no drop in activity. In fact, our activity has only increased, and extended its global reach as our online services and resources have expanded and regular, high quality webinars have become one of our core services. Having commenced in March, the webinar programme will be a feature of next year’s annual report.
As our latest report details, we ran 41 events in 2019, including numerous learning events, our annual conference, our awards dinner, workshops for prospective Chartered Security Professional applicants, the CSyPs’ annual dinner, a Remembrance event, our popular Christmas social, and specialist and regional meetings and events organised by our special interest groups.

The report also highlights other activities and benefits including our online community, mentoring and professional development platforms; our jobs board; our Membership Management Advisory Group, a forum that serves as a voice for our members; our corporate membership of London Chamber of Commerce and Industry and the wonderful facilities and events available free of charge to our members; and security updates from the Cross-sector Safety and Security Communications (CSSC) hub.

Educational excellence
Our educational offerings are going from strength to strength. A key dimension of this is detailed in the report is our CPD scheme, overseen by director Bob Martin CSyP FSyl and a mandatory requirement for Institute Fellows, Chartered Security Professionals and board directors. We would love to see the whole of the membership engage with this easily completed process and earn annual certificates for development activities that I am sure most already do. Annual CPD returns are a mandatory requirement in more established professions, and the trick is to claim close to the minimum requirement of 36 points and not labour for hours in competition for the highest score!

Alongside this service for members and around 65 CPD partner organisations, as the report details, we offer our popular Certificate, Diploma and Advanced Diploma courses in Security Management; and we enjoy close partnerships with a number of universities offering degree courses tailored to the needs of our members. Most recently, we have launched an Approved Training Provider scheme as a means of giving recognition to good quality short courses by means of a rigorous review process created by director Angela Vernon-Lawson FSyl, and helping members identify courses of quality.

Credibility and influence
All Institute members benefit from our well-recognised validation system, the peer review process on which member grades are based, delivered by our hard-working Validation Board. As Tony Aston FSyl explains in the report, they bring expertise from across a range of sectors and give the Institute its distinctive system of assessing professional competence and enhancing credibility through our post-nominals. We also manage the Register of Chartered Security Professionals, also discussed in the report, which continues to grow in size and influence, and actively encourage and support our members in working towards this prestigious certification.

The engine for thought leadership in the Institute is our special interest groups, co-ordinated by director Alex Yates FSyl, with brief reports on nine of these included in the report. We also engage in extensive external engagement across government, industry, academia and the security community. One of our most significant partnerships as the report outlines is our membership of the Cyber Security Alliance, on which we are represented by director Mahbubul Islam CSyP FSyl. The Alliance has the contract from the UK government to develop and deliver a national Cyber Security Council supporting the development of the cyber security profession in the UK.

In order to further enhance our credibility in government, we are in the process of appointing new Patrons who can represent us at the highest levels of influence. This will be another exciting update for next year’s report!

Good governance
It is essential that our members and other stakeholders have confidence that the Institute reflects the highest standards of corporate governance: that we are participatory, accountable, transparent, responsive, effective and efficient, equitable and inclusive. The report gives an overview of how the board functions and the roles that individual directors fulfil, as well as the roles undertaken by our HQ team.

As an organisation we have a strong commitment to being socially responsible, and the report also explains how we put those values into practice, under the headings of ‘community’, ‘people’ and ‘environment’. It showcases the Next Generation in Security initiative led by director Paul Barnard CSyP MSyl that lies at the heart of our CSR commitment, and provides another excellent opportunity for members to get involved in the Institute by helping us inspire young people to consider security careers.

Working together
What is so special about our achievements is that they represent a true collective effort, and a profession continuing to build its credibility and influence thanks to the efforts of every member in contributing to the growth of the Institute. Even a social media post is greatly appreciated: the visibility and reach of many of our member posts can be surprising, and add to the growing profile and recognition that the Institute is gaining. Thank you to all of you for your support and please continue to share the Institute’s successes, including this report. We hope to reward you with more great news this time next year ...
Our Virtual Conference: A Week of CPD Webinars

Following on from our very successful Annual Conference 2019, we are back again for our premier CPD event not only will we be extending our Annual Conference across an entire week. On the week commencing October 19th, we will be hosting 2 CPD webinars everyday that centre around the theme of: ‘The Science of Security’. The week will include industry thought leaders from all over the world tuning in to present, and we will also be running a virtual week-long exhibition, as well as a virtual charity auction.

Our conference week will begin daily at 9am, with our first presentation and 10am, meaning delegates will have one hour to enter our virtual exhibition centre and tune into the virtual delegate brochure and browse our online exhibition space. Delegates can then “take their seat” in our virtual conference centre. Conference presentations will be delivered at 10am and 3pm (BST) daily. That’s why we are calling it a 10-3 conference!

There will then be an afternoon break with further browsing opportunities across our exhibition hall and on our virtual auction stand, where bidding will commence on numerous items throughout the week.

The benefit of a 10-3 conference is that we can attract a wide range of expert speakers from time zones ahead of and behind the UK, which we would not have been able to do with a face-to-face conference.
The Science of Security

Science sits behind the majority of our Security Practices and capabilities. Some are obvious and some less so. The Security Institute Annual Conference 2020 will explore some of the benefits science brings to our ability to protect, influence and develop as security professionals.

Speakers will present on topics that will consider the importance of Science in all aspects of security, through:
- Engineering
- Psychology
- Technology
- The Human factors
- The impacts of connectivity via the Internet of Things (IoT)
- Forensic sciences
- Impact of space exploration

Along with a range of other fascinating topics, all of which fantastic learning opportunities about future threats and mitigating theories that will enhance your knowledge and hopefully make you think harder and research further.

Details of speakers will follow as timeslots are confirmed. Watch them all or watch only one, it’s up to you.

Bookings will close on 15th October at 12noon BST.

Charity Auction

This year we will also be hosting an online charity auction from 16th to 23rd October hoping to raise money for the Security Benevolent Fund who have assisted so many struggling security personnel during the pandemic. With prizes from holidays to memorabilia, paintballing to fine dining at venues all over the UK and abroad, we are sure there will be something you would enjoy winning whilst helping us build on the fund that continues to be available to all of you, should you ever need it.
The Security Institute has joined forces with the British Security Industry Association (BSIA) and the Security Commonwealth (SyCom) to run an awareness campaign to highlight the essential role that Security Officers play in public life and to increase respect and recognition for their capabilities.

The private security industry has developed vastly in the last 10 years and this campaign is designed to reset the public perception of the security professional. The campaign will showcase security professionals as a respected, valued, professional service provider contributing to and creating a safe and secure environment: critical to protecting people, places, and property – a key worker that is acknowledged and embedded in our daily lives.

Within the last few months, due to the onset of the Covid-19 pandemic, security officers have been working in critical settings playing key roles whilst remaining unheralded, such as; working at testing centres and the NHS Nightingale Hospitals, ensuring critical food deliveries from warehouses and managing queues and customers at supermarkets. They have also been involved in safeguarding the homeless in new sheltered accommodation, physical security at factories and premises, protecting industrial estates from illegal fly-tipping during lockdown; and supporting police patrols in London. These are just a few examples of roles the industry and their officers provide that the industry believes are rarely acknowledged by the public.

Rick Mounfield CSyP FSyI, Chief Executive, the Security Institute, said: “The security sector is vast with specialisms from Cyber and Engineering to protective services including both technical measures and security officers. The latter engages with society more than the rest but is often overlooked and unappreciated. Great effort has been invested in the professional standards and capabilities of frontline officers and they have proven their worth during the Coronavirus crisis in the UK. They, along with the wider security sector deserve to be recognised, respected and appreciated for the safety and security they provide across the UK.”
Mike Reddington, Chief Executive, BSIA, echoed Rick’s sentiments and said: “The recognition of security officers as key workers is the start of a re-appraisal of what service they provide to the community in keeping the public safe and secure. As we exit lockdown and have to navigate public spaces again, they will have a crucial role in supporting public confidence. We are working closely with the Police and all other public bodies to find the best way to achieve this.”

Guy Matthias MSyI, Chairman of SyCom, further added: “SyCom is comprised of some 40 organisations from across the security landscape all of whom share common objectives. These include building professionalism, raising standards and sharing best practice in order to help develop a more effective security response to keep people safe and secure. I hope that this campaign can make more people recognise the changes we have all made and continue to make.”

These achievements are celebrated across the industry which the public do not know about and part of the campaign aims to bring these examples of professionalism to a wider audience. The Institute and its partners are keen to work with the SIA as the industry regulator and are also encouraging the industry to engage with the #SIAHeroes campaign to recognise the great, and often unseen work that is being carried out by security officers.

The BSIA have also opened up a consultation on what to call the service that security officers provide, as Manned Guarding fails to reflect increasing numbers of women in the workforce and the scope of services provided. Today, the industry universally calls its staff ‘security officers’ to reflect a far wider safeguarding role than just guarding and reviewing other terminology is part of the overall campaign.

To respond to this please go to www.bsia.co.uk/hidden-workforce

The industry will be reaching out to all companies, professionals and organisations in the sector to participate in the campaign, and hope that over the coming challenging weeks as lockdown is eased, the industry can play its part in ensuring that the country emerges with confidence to start to recover and build for the future.
On July 30th, our new Inclusive Security Special Interest Group (ISSIG) hosted their inaugural event with a line-up of industry-leading speakers under the co-chairship of Anna-Liisa Tampuu ASyI and Lisa Reilly.

Our Special Interest Groups (SIGs) are at the centre of the Institute’s efforts to promote knowledge sharing across the security industry, and the launch of the ISSIG helps us continue this mission.

What is the ISSIG?

The ISSIG has been established to help us as the security community understand the challenges that many groups of society face whilst working within our industry, and the barriers of entry that can prevent different groups from joining the sector. The ISSIG will also address what can we collectively do to break down those barriers, and help promote a more inclusive security industry.

In addition, the ISSIG will also set out to explore how engagement with all groups of society can help pave the way for innovation and how a more inclusive security culture could lead to enhanced practices within the broader field of security.

The ISSIG aims to change the face of the field of security and risk management, by fostering more opportunities for all groups of society to gain access and thrive within the industry. By promoting a variety of perspectives, the ISSIG aims to help increase productivity, creativity and growth of the talent pool entering the security industry. The talent pool that the security industry attracts is vital as it will help advance new ideas and create positive disruption.

If you’d like to get involved with our ISSIG, members can join the ISSIG Community on our Community Platform: https://community.security-institute.org/

Inaugural Event

Anna-Liisa Tampuu hosted the event, and started by outlining the need within our industry for greater inclusivity and the key objectives that the ISSIG will be working towards.

The free-to-attend virtual event included talks from our Director of Cyber Convergence Mahbubul Islam CSyP FSyl, Laura Haynes, Mark Grant MSyI and Chairman of the Institute, Professor Alison Wakefield PhD CSyP FSyl.
Mahbubul Islam was the first speaker of the event, and spoke about his identity and the role that this has played within his career as a security professional. Mahbubul discussed how he identifies as a Muslim of Bangladeshi descent as well as a British Citizen, and described how this ‘triangle’ of identity can sometimes create a conflict of values and principles.

Mahbubul shared how after growing up in Tower Hamlets, he started his career as a Civil Servant in 2001 before moving into the security industry in 2007. He was introduced to the Security Institute by a colleague, but assumed at first due to his professional and BAME background he felt he would not fit in. He now identifies that this is an example of an unconscious bias, based on his learnt experience.

This led on to a discussion of the different types of learnt experiences which can lead to a range of biases, including unconscious bias, confirmation bias, selection bias and X type bias - which can all hinder the promotion of inclusivity within the industry.

Laura Haynes

Laura Haynes, the Chair Emeritus of the UN Women UK, then followed Mahbubul's talk by discussing her work within a number of sectors that have been trying to move the issue of greater inclusion forward and how it should be a priority within the security industry.

The efforts to achieve gender equality and reduce the ostracism of women in male-dominated sectors is a subject that Laura is an expert in. Laura discussed the necessity for a new inclusive approach, with those of all backgrounds working to help move industries forward and help close the gap between discussions of diversity and action. Through her work at UN Women, Laura has worked to have gender equality recognised not just as a women's issue but as a human right issue, an economic issue, a social issue and as a political imperative.

Laura defined equality as the aim to remove the social and cultural barriers to prevent people from achieving their potential, and thereby positively contributing to society. She went on to discuss how these barriers exist in public policy, educational opportunity, conscious or unconscious bias or economic opportunities.

Then, Laura spoke of the rise of a global movement to advocate for the advancement of women in the workplace and how this relates to the security industry. Citing a recent McKinsey report titled ‘Diversity Wins’, Laura discussed how the business case for inclusion remains robust in fact strengthening over time as the report highlighted a correlation between increased profitability and increased diversity.

To conclude her talk, Laura outlined a 5 point plan for tackling diversity within your organisation and creating strategic change:

- Establish your motivations through a mapping exercise
- Set measurable goals and clear objectives, to define what success looks like and relates it to the business plan
- Create an action plan that identifies key stakeholders
- Accountabilities need to be put in place that will allow transparency in all processes
- Engage with all employees to aid transformation, creating participants and advocates for diversity in your organisation
Mark Grant MSyI

Following Laura Haynes, Mark Grant MSyI then delivered a presentation titled ‘Diversity is not a dirty word’ that outlined the benefits of diversity and the measures that can be implemented in the security industry. Mark highlighted that diversity outperforms homogeneity, and without strong diversity, we run the risk of losing clients and falling behind other industries as we do not align with company cultures.

Within his talk, Mark emphasised that by seeking a diverse workplace we are not saying there is no room for white males in senior leadership roles or those from a military or police backgrounds.

Echoing the points made by Laura Haynes, Mark noted that not enough progress has been made in promoting women in the security sector. Despite it benefiting companies with increased varieties of perspective and increased problem-solving capabilities, with research from the Boston Consulting Group finding companies with a diverse workforce are 1.7 times more likely to be innovative leaders in their market.

Professor Alison Wakefield PhD CSyP FSyI

Our Chairman, Professor Alison Wakefield PhD CSyP FSyI was then the final speaker of the event. Alison outlined the steps being undertaken by the Institute to promote inclusion, and our agenda going forward.

Alison spoke of the Institute’s continued commitment to diversity and inclusion within the industry, and like Mark reinforced that inclusion is for everyone, not just those groups that are underrepresented.

The Institute’s Next Generation in Security (#NextGen) initiative has been at the heart of our commitment to promoting inclusion, under the leadership of Director Paul Barnard CSyP MSyI. This initiative has involved working with the Voluntary Police Cadets (VPC), an organisation with a 50/50 gender balance, to introduce young people across the UK to security career paths. In addition to this, our #NextGen initiative is now partnering with the EY Foundation to deliver a ‘Secure Futures’ employability programme for young people from disadvantaged backgrounds.

Alison highlighted several other initiatives being undertaken by the Security Institute, promoting opportunities and supporting everyone from all backgrounds. This has included hosting Young Member Group events, and a Women in Cyber event that was organised by Mahbubul Islam CSyP FSyI and held in March 2020. Also, the Security Institute have become signatories of the Armed Forces Covenant to help promote opportunities for members of the Armed Forces community.

In addition, Alison then went on to emphasise that diversity and inclusion extend to issues of social background and income, and that the Security Institute is committed to promoting career progression for security professionals on the front line. We are currently promoting the Hidden Workforce Campaign in conjunction with BSIA and the Security Commonwealth, which aims to ensure frontline security professionals that have been essential during the Covid-19 pandemic get their due recognition (p.10). Then, Alison also highlighted that at the time of the ISSIG launch event the Institute were pursuing accreditation as a Living Wage Employer, which has now at the time of publishing has been achieved and the Institute will continue to promote this to other organisations within the industry (p.36).

Looking into the future, Alison reaffirmed that the Institute will continue to monitor and promote diversity amongst the membership and across all of its Boards and committees at all levels. The formation of the ISSIG will play a key role in embedding these principles across all of the Institute’s decisions, as well as help open dialogue across the Institute. Finally, the Institute wants to help facilitate change across the sector. Alison reported that she is noticing an increased collective will to address diversity and inclusivity, and she hopes that sharing best practice will support those wanting to promote inclusivity.
ACCREDITED SECURITY MANAGEMENT QUALIFICATIONS

The Security Institute is the largest association in the UK for security professionals and offers news, networking, events and unique validation of experience highly valued by employers and clients.

We promote and encourage continued professional development through education. In collaboration with the Institute's education partner, PerpetuityARC, we offer an award winning accredited eLearning pathway from Level 3 through to Level 7 for those wishing to enhance their professional security management skills.

PerpetuityARC is at the forefront of security management training provision in the UK and has a unique background in security research and education. PerpetuityARC's trainers and management team are all highly qualified and recognised experts in their fields.

Our eLearning courses are recognised throughout the industry and offer you the opportunity to study at a time and place of your choice as you continue in your career. Each qualification is accredited through internationally recognised awarding bodies.

You will be eligible for FREE Student membership whilst you are studying.

CONTACT THE SECURITY INSTITUTE

024 7634 6464
info@security-institute.org
security-institute.org

BTEC LEVEL 3 CERTIFICATE
This qualification will benefit anyone seeking professional recognition and accreditation within the security sector.
Open to anyone who operates within the private or public security sectors.

BTEC LEVEL 5 DIPLOMA
This qualification is designed for practitioners who have experience in security management and now wish to achieve professional recognition and gain an accredited security qualification.
Suitable for those in middle and senior management level positions.

IQ LEVEL 7 ADVANCED DIPLOMA
In this ever-growing global market, linked with many other areas of development, this qualification will appeal to practitioners in international security and risk management who are striving to embrace modern approaches to their line of work.

MEMBERSHIP BENEFITS
Professional Credibility / Special Offers / Lobbying & Development / Mentoring / Member Discounts / LinkedIn Group / Career Development (CPD Scheme) / Networking / Newsletter / Special Interest Groups / Events & Masterclasses /
In mid-June, we proudly launched our latest member benefit: the Security Institute Community Platform. The Community Platform is an exclusive online network that allows members to make connections with other professionals within the Security Institute membership, ask questions as well as discuss the topics and issues that are important to them.

With the guidance of member feedback provided through the Membership Management Advisory Group (MMAG), our team are always looking for innovative ways to improve our membership experience, and the new Community Platform adds to our ever-expanding range of online benefits.

With the current challenges presented to us as a society and specifically the security industry, the necessity to remain well-informed and well-connected as professionals have become more evident than ever. A few months after launch, we are glad to have seen the Community Platform help strengthen the connections amongst Institute members and facilitate vital knowledge sharing within the industry.

This dedicated virtual space is designed to foster collaboration and engagement, allowing members to have meaningful interactions with each other and expand their network of security professionals across the UK and internationally. Since the initial launch of the platform, we have already expanded the number Communities on the platform to include a range of regional groups including those that cater to members in a specific area of the UK such as our North-West Members Group, as well as international groups including our Middle East Members Group.
Members can interact on the platform whenever and wherever they wish; whether that be on the commute to work, in the office or from the comfort of their own home.

There is also the option to customise their email preferences to receive updates of engagement on the platform as often as they wish, ensuring it is as easy as possible to stay up-to-date on the latest discussion topics and responses to their queries.

All members of the Institute are included in a membership wide community, if you haven’t already, we encourage you to post an introductory post.

In addition to the ‘All Members’ community, there are also communities established for each one of our Special Interest Groups (SIGs). As a member of the Security Institute, you are free to enjoy these knowledge-sharing opportunities by participating in one of the 11 SIG Communities by simply opting to ‘join’.

These SIG Communities will allow you to gain an insight into a specific security discipline and hear from other industry leaders within the field, our SIGs cover a broad spectrum and reflect the diversity of our membership and cover topics from Counter Terror (CTSIG) to Cyber Convergence (CCSIG), Built Environment (BESIG) and many more.

As the number of SIGs within the Institute expands, so will the number of online SIG Communities, creating further opportunities to learn about different areas of the security industry. Our newly launched Inclusive Security SIG (ISSIG) has established a new community on the platform for example, which is quickly growing and benefiting from the participation of members across the industry.

There are also communities exclusively for members of the Validation Board (VB) and the MMAG, to join these communities you must be an official member of each respective board.

Institute members can log onto the platform here: community.security-institute.org

If you experience any difficulties with the platform then please contact ben@security-institute.org
We are pleased to announce Malcolm Dawson BEM MSyI will be representing the Security Institute on ProtectED’s Advisory Board.

Malcolm is the Head of Security at the University of Leeds. With 44 years of police and higher education security experience, Malcolm brings a wealth of knowledge and expertise to this position.

ProtectED is an award-winning, not-for-profit membership and accreditation scheme — the ‘gold standard’ against which a university’s policies, processes and practice can be measured. The need for ProtectED is rooted in the recognition that universities have a wider role to play in supporting the safety, security, and wellbeing of their students — not only while they are on campus, but throughout their student experience. ProtectED is the result of four years’ research, design and development by academic researchers, professional services staff and security specialists, guided by an advisory board from the sector, which Malcolm will now serve on representing the Security Institute and our membership.

ProtectED accreditation is designed to assess the extent to which universities provide the services and structures that enable students to avoid problems and focus on their success.

Speaking of his appointment Malcolm stated:
“I am immensely proud to be appointed the Security Institute representative on the ProtectED Advisory Board. ProtectED is a quality Standard aimed at many issues that Higher Education Institutions are faced with today as we all continue to work to ensure that our campuses remain a safe and secure environment for academic study.

Our role has developed in recent years to become a much broader one, covering not only student safety but also student wellbeing — which amongst other aspects is covered in the ProtectED Code of Practice.”

Welcoming Malcolm to the ProtectED Advisory Board, ProtectED Director Brian Nuttall said:
“We are delighted to welcome Malcolm Dawson onto our Advisory Board as a representative for the Security Institute and appreciate that his values and priorities align with the student-centred ethos of ProtectED. We look forward to working with him on the growth and development of the ProtectED initiative.”
Our August Members Lunches

On August 11th, we were pleased to welcome back our Members Lunches and hosted our first Lunch since February.

Our Chief Executive Rick Mounfield CSyP FSyI and Engagement Manager Jade Lapper were on hand to welcome new members, and enjoyed the opportunity to catch up with some familiar faces at the Doggett’s Coat & Badge in London.

Fortunately, it was a lovely sunny day, which allowed all attendees to enjoy the buffet-style lunch with phenomenal views of the Thames. The event was filled with conversations reflecting on the past few unprecedented months, as well as looking forward to the future as we as an industry continue to adapt to the current challenges. It was a great opportunity to safely socialise and network with other security professionals, with the wide spectrum of security sectors represented amongst the attendees.

A big thank you to all those that attended this event, and a special thank you to our event sponsors Gallagher.

The Security Institute will continue to follow all government guidelines when running our events. All Institute events are currently limited to reduced numbers and will have extra measures in place to ensure the health and safety of all.

If you’d like to join one of our other upcoming events you can book here: https://event.bookitbee.com/security-institute
Effective Communications – Post Covid-19

We were joined by Anna Averkiou MCIoJ, the Security Institute Board’s Advisor on Media Engagement, to talk about the importance of communication in your return-to-work planning. This webinar addressed how the Covid-19 pandemic has revealed major shortfalls in the way organisations communicate. Through her presentation Anna also showed that it has brought about new and different levels of engagement which need to be harnessed to reassure staff, clients and visitors who will be understandably nervous about returning to the “new normal”.

Human Decision Making Under Stress

We partnered with Colin Morgan CSyP MSyI, who retired from the Metropolitan Police after over 30 years service in 2016, his last role was Chief Superintendent in charge of the Met’s Public Order Branch. The webinar focused on the role of critical decision makers charged with protecting the public and explore what constitutes “good” and “bad” decision making, including a “warts-and-all” insight into Colin’s own decision making over the years. The session also examined factors impacting on the stress levels of decision makers, including the traits of those charged with decision making in such environments and the theory behind why these traits manifest themselves.
Designing Out Crime and Secured by Design

Hosted by Emma Snow MSyl of Devon and Cornwall Police and Alfie Hosker MSyl, Technical Manager, Secured by Design, this webinar introduced the role of the Designing Out Crime Officer (DOCO) and its function within the police service as well as the role of the Police Crime Prevention Initiative (PCPI) Secured by Design (SBD) which works with the police to improve security in buildings and the environment. Amongst many other things, the webinar explored how the partnership approach to reducing crime by working with planners, developers, housing associations and other construction professionals provides people with safe and secure places to live, work and play.

The Science Behind Stopping Targeted Attacks

We were joined by Philip Grindell MSyl from Defuse Global who presented this insightful webinar. Having researched the best practices of stopping public figure attacks and been privileged to meet with and discuss the theories with the academics’ psychologists who developed them, Philip introduced these to Parliament in his role to stop another successful attack after the murder of Jo Cox MP. In order to ensure that these theories were operational applicable Philip mapped these theories against all the attacks on UK MPs since 2000, and published the evidence in his MSc dissertation titled ‘Targeted Violence Towards British Political Figures – Where should the Security Manager focus?’. In this webinar Philip discussed the research he conducted, and the methodology used to counter targeted attacks.

Security Culture - has Covid-19 Changed the Landscape

In this session, Sarah Austerberry CSyP FSyI looked at the importance of security culture, and how the current changes occurring within many organisations and their landscapes has impacted the effectiveness of their security culture. Sarah outlined how that staff that once fully understood their security responsibilities are facing a new range of threats that they may be unaware of, and offered some tips to help develop a strong security culture.
Introducing the newest member of our team

Victoria Smith, Membership Administrator

In July, our HQ Team expanded with the new addition of Victoria Smith. Victoria will be taking on the new role of ‘Membership Administrator’.

In this role, Victoria will be supporting two fastly expanding areas of the Institute. She will be supporting the work of our Membership Registrar, Paula Stanbridge, as our membership continues to grow more and more with greater numbers of security professionals seeing the value in Institute membership.

In addition, Victoria will be supporting our Project Manager, Di Thomas MSyI, with the Register of Chartered Security Professionals (CSyP) functions. Victoria is now administrating our CSyP Application Workshop Webinars, which you can book onto here:

Victoria brings a wealth of administrative knowledge and experience and will play a key role in the ever-expanding SyI membership and the growing CSyP Register.

Speaking on joining the Institute, Victoria stated:

“I’m very pleased to have joined the HQ team, and I am very much looking forward to learning more about the fascinating world of security.

It’s been unfortunate that due to the on-going circumstances I haven’t had the opportunity to have met as members as I would have wished to in person, but as we start to return to some form of normality with more upcoming events on the horizon I am sure I will have the pleasure to get acquainted with many of you shortly.”
Everyone is welcome to track their own personal development – why not launch the toolkit with your team? Of course if you are a Fellow or Chartered Security Professional, then making a submission is compulsory.

### CPD POINTS LOOK UP LIST

Here are some of the recent activity and the points to add to your 2020 CPD Record.

Download Certificates of Attendance for SyI events or download the 2020 CPD TOOLKIT from our website.

If you have any questions on CPD, please contact Di Thomas on 07879 330818 or email cpd@security-institute.org.

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Activity</th>
<th>Formal</th>
<th>Informal</th>
</tr>
</thead>
<tbody>
<tr>
<td>28 May</td>
<td>CSyP Application Workshop</td>
<td>Attend SyI and CPD Partner events</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4 June</td>
<td>(Webinar)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11 June</td>
<td>(Webinar)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18 June</td>
<td>(Webinar)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25 June</td>
<td>(Webinar)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 July</td>
<td>(Webinar)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9 July</td>
<td>(Webinar)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16 July</td>
<td>(Webinar)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23 July</td>
<td>(Webinar)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30 July</td>
<td>(Webinar)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6 August</td>
<td>(Webinar)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20 August</td>
<td>(Webinar)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16 June</td>
<td>Syl Validation Board Meeting</td>
<td>Committee work on a voluntary basis (per hour)</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>30 June</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14 July</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>28 July</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25 August</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26 August</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11 August</td>
<td>Members Lunch</td>
<td>Attend SyI and CPD Partner events (Whole event)</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>29 May</td>
<td>Syl Morning Feature Webinars:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 June</td>
<td>Your Member Benefits</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19 June</td>
<td>Welcome New Members</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26 June</td>
<td>Your Member Benefits - Mentoring</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 July</td>
<td>Our Qualification Pathway Explained</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 July</td>
<td>Welcome New Members</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24 July</td>
<td>New Member Benefit - Community Platform</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29 July</td>
<td>Professional Security Management: A Strategic Guide</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6 June</td>
<td>Syl CPD Webinars:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 June</td>
<td>Protecting Security Workforces From CV19 and Pandemic Risks</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17 June</td>
<td>Risk Mitigation in a COVID-Secure World with Gallagher</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>24 June</td>
<td>Human Decision Making Under Stress</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 July</td>
<td>Technologies for the New Normal with Avigilon</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8 July</td>
<td>Effective Communications – Post Covid-19</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15 July</td>
<td>Designing Out Crime and Secured by Design</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25 July</td>
<td>Security Technology as a Business Enhancer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29 July</td>
<td>The Insider Threat with CPNI</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19 August</td>
<td>The Science Behind Stopping Targeted Attacks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19 August</td>
<td>Security Culture - has COVID-19 Changed the Landscape</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 July</td>
<td>CSARN webinar series:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29 July</td>
<td>Are we fully prepared for the next biological event?</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>General Stan McChrystal ‘Leadership in times of crisis’</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Various Dates</td>
<td>OSPAS Thought Leadership webinar series</td>
<td>Attending Institute and CPD Partner organisational events (per hour)</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Various Dates</td>
<td>SASIG Webinar series</td>
<td>Attending Institute and CPD Partner organisational events (per hour)</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

Everyone is welcome to track their own personal development – why not launch the toolkit with your team? Of course if you are a Fellow or Chartered Security Professional, then making a submission is compulsory.

Fellow of the Security Institute, Jean Perois FSyl has won ASIS International’s 2020 Security Industry Book of the Year for his work ‘Strategic Security: Forward Thinking for Successful Executives’.

Now in its seventh year, the Security Industry Book of the Year is chosen by a committee of ASIS members who are established authors, editors, and reviewers. To be eligible for the prize a book had to be published in 2019 by an ASIS member. A total of 24 books were considered for this year’s prize, with ‘Strategic Security: Forward Thinking for Successful Executives’ being selected by the committee as the winner.

If you are interested in reading this book you can purchase your copy here: https://www.amazon.co.uk/Strategic-Security-Thinking-Successful-Executives/dp/0815357877
A few words about this book that shares a history with the Security Institute. It began as an idea after a course I prepared for the Institute quite some time ago for the SyI certificate. I thought that leaving this course at simply a course would be a waste, as I had worked hard to organise and develop my thinking about this topic. I decided to expand this course on security strategy and make it more palatable and pleasant to read, and mixed the technical aspects of the work with memories, advice and good or bad experiences I wanted to share with the readers. After all, the decades spent in security could benefit younger generations. I therefore used the frame of the course, and added some meat on the bone, the meat being mainly the result of my personal experience in the corporate environment. I also touched the topic of self-development always present in marketing books, but conspicuously absent in most security books. A career in security may not be only about skills, knowledge, certifications and degrees. They matter of course, but my point is that those may not be sufficient to climb the corporate ladder.

This book is my second book and aimed at security professionals in mid-careers who would like to improve their situation and improve some of their skills. It examines the idea of thinking strategically in a corporate environment, how to elaborate a strategy and how to implement it in a corporate structure. It then reflects about a problem that most senior managers have to face: how to sell your security programme to the top-management, “the upper crust”. I used my experience to try to make the security practitioner understand how other managers perceive them and how to circumvent these unfair prejudices. In the book I spend some time discussing the delicate issue of implementing the programme, since this is probably what will be of most practical value to the reader.

What gets measured gets done. Therefore, the next part of the book is about measuring the security programme to convince your management that what you are doing is worthwhile. To complete this, I added a chapter on awareness and programme maintenance.

In the following chapters I touched what I called personal strategy. Not being a psychologist, my approach what that of an amateur, fascinated by the topic, and supporter of self-development. This chapter is important, as I believe that many security practitioners are incredibly competent in their domain, but fail to sell themselves at their real value.

I hope this chapter will find some echo and help managers to be more self-confident in their relations with other managers and their hierarchy. The book closes on a chapter on creative security (CPTED and beyond), that some readers may find of interest, a topic I would like to develop further one day.
Unexpectedly Unemployed
Sharing how I got back to work after losing my role in a corporate restructure.

By Neil Shanks MSyl

I promised to write a short piece on my experience following a rather difficult time professionally over Christmas/New Year 2018/19, but regrettably, I never found the time. For those of you that were connected with me then, and many of you who became connections during that time, you likely saw a post where I reached out for help and support. This was because I suddenly found myself out of work, as the position I was due to start was cut during a restructure just before I joined the new company. I don’t mind admitting that the prospect of being out or work terrified me more than I could have imagined.

I was successful in getting my next job, a role I love with Corps Security, three weeks after the date I should have started with the company that “shall not be named”. I don’t mind admitting that the prospect of being out or work terrified me more than I could have imagined.

Why am I sharing this now? Following the events of Covid-19 and the ongoing impact on the economy, the impact of which will undoubtedly be felt for a long to come, I have seen an unfortunately high number of posts from people in a very similar boat to the one I was in. I should be clear that I was not made redundant, I left my previous position for a role that was then terminated before my start date. Regardless of this, I was still out of work.

So here is my story, as best as I can recall, and I hope some of the points that I think helped me may help others. You will have to excuse the slightly theatrical Step Zero, but when writing this I wanted to present a relatively accurate timeline of the process and I realised the foundations I laid over a few years before this played a big part in my journey.

Step Zero – Establish Yourself
I have worked in security-related fields for over a decade, with a large proportion of my career in custodial like settings. I had always wanted to join the Police so, like many people, I did a related degree (in my case Law), then sought relevant work before applying. This saw me working in Prisoner Custody for a time then, when I was ready to apply to the Police, the recession hit and unfortunately there were significant Police redundancies. I then moved into Healthcare Security within a large Mental Health Hospital group and began to learn a new side to security.

In the organisation, I moved from a Security Officer to the Head of Security within approximately 4 years. During this time I sought to immerse myself in the culture of the organisation and then look outwards to what the industry was doing. I found the microcosm I was working in was sadly devoid of much external influence and this was inhibiting both the organisation’s security approach and my development. Furthermore, as it was a privately owned business, whilst they did some great things their way, it was cut off from the security provisions of the NHS, which were better established.

I sought to improve my knowledge by completing the then NHS Protect Accredited Security Management Specialist qualification, and also an MSc in Security Management. I actively engaged with several healthcare industry-specific bodies. I worked with the Royal College of Psychiatrists, for whom I completed site reviews and contributed an article on technology and security in secure settings to one of their Quality Network publications. I also joined the National Association for Healthcare Security (NAHS), with whom I was a Non-Executive Director for during the time this article refers, but initially, I joined as a standard member. I was also a member of the Security Institute and was getting more involved in their activities, including working with some Special Interest Groups and helping with the Young Members Group.

In short, I have spent several years working in the industry and whilst I am not a well-known face or name, I have worked to take some of the further steps that many don’t. For a few years, I was reasonably insular, working on my academic achievements, rather than being active in the industry. Whilst my MSc, in addition to my Law degree, inevitably helped me secure my next role, I believe that the time spent on the extra-curricular activities really made a difference.

Always keep in mind that people hire people, and the more people you know, the better your chances of hearing about that job. The more credible and respectable people that can vouch for your abilities, the better your chance of securing that interview. The rest is up to you.

Now that I have established my prior status, here is my journey.
Step 1 – Managing Loss
Leaving my job of the best part of a decade had not been the hardest decision but what to do next had been difficult. The organisation had changed considerably, as had I, and I couldn’t see a place in the future where our journeys would converge again. I was ready to move on and I was relishing the new challenge. I was handing back various roles and thanking people for their help over the years when I received the call that rocked my world. I honestly think I will always remember being sat in the pub enjoying a farewell meal with one of my direct reports a week before my last day then taking that call.

Initially, I was more a little stunned by the news. To say I was devastated was an understatement. Like many people in that position, all I could foresee in that instance was prolonged unemployment and the damage it could do to my family after all the hard work we had put in.

I made the decision then that I would allow myself a couple of hours of self-sympathy whilst I break the news to my family and then I would work out my next move. It is to that end that I took Step 1 and posted what was to be the most influential LinkedIn post of my life to date.

I was not going to dwell on the negative and allow that to infect peoples’ opinions of my professionalism. Yes, something bad had happened but getting angry about it was not going to help me secure a new job and could hinder it.

What I could not have foreseen at this time was the impact this post would have. Not only did I receive an influx of well wishes and people offering numerous forms of support, but I also received a huge amount of shares on the post. The shares hugely influenced the number of views and although I cannot remember the exact numbers, I do recall that the shares were in the hundreds and views hit somewhere between 80k-120k. For someone that normally gets a couple of likes and the occasional comment that was huge.

Within the 80-odd comments, I had lots of people I had never heard of reaching out and offering support, as well as those I had known for years, which brings me to the next step, (re)connect.

Step 2 – (Re)Connect
In addition to all the online messages I received on my post, I also received calls/texts, most notably from two mentors I have been lucky enough to know over the years; one from Mike Bluestone CSyP FSyI whom I had known for several years, and one from Stuart Hughes FSyI, my mentor through the Security Institute. Both, as with some of the other fantastic colleagues I have had over the years, first reached out to offer me support and see that I was ok (relatively speaking) but also to offer help in planning my next steps. This was amazing and helped me start to think through my next big project, my employability.

One thing that you have on your hands when you are out of work is time and it is incredibly strange when you suddenly have all the time you would normally devote to work sat there empty. It is certainly daunting and one of the first things I did whilst formulating my plan, which I would advise be an early stage for anyone, is talk to people. Talk to as many people as you can that you may be able to help you, or you them. There will always be a number of people in your position and you only appreciate how hard it is when you are there yourself.

I connected with some great people whilst out of work, as well as reaffirmed some old standing professional friendships and this was a key to getting back on the waggon.

I knew I needed to get into job hunting mode and do everything I could to enhance my chances a.s.a.p. but before this, I needed to get my ducks in order and make sure me and my family were looked after. Which takes me to Step 3 – Keeping the Wolf from the Door.
Step 3 – Keeping the Wolf from the Door
Anyone that has been in this situation knows there are areas you need to think about that you would not ordinarily. For me, I wanted to ensure I could secure an income within a certain time period, even if it was not the dream job, to ensure that we would not lose a roof over our heads. This is survival at the end of the day and I gave myself a set period to find a role, after which I would lower my scopes and take something to keep the wolves from the door whilst I sought a more desirable career. Thankfully it did not come to this but I was ready in case it did.

My partner and I looked at all our outgoings, what income we would need and where we could cut back. We also looked at the potential to free up equity from our home to remove anything other than essential expenditure and even discussed moving into rental accommodation for a time to ensure we reduced our outgoings to meet the level of our reduced income.

These are big, life-changing decisions and they were not explored lightly, but at the end of the day, you are the only one that will look after yourself in this situation.

Step 4 – Be Seen to be Employable
As mentioned in Step 3, I needed to ensure I could move into any role as a.s.a.p., as well as plan for taking a lower-level role than I had been working in, if required. I had spent my time on the front line and I always enjoyed it, so this was not a daunting prospect, but I was missing one key thing due to my time as in-house security, an SIA licence. I knew I would need to get this in order to work at most places so the sooner I could get it the better. I also knew this would be an expenditure I could do without, however as it was necessary to allow me to earn, it was a no brainer. I booked the first available course within a commutable distance.

I was lucky in the sense that I already had an up to date, professional CV from the application to the job that was cancelled. Many people will not be as lucky so this is another area people may need to invest both time and money. Your CV is your potential employers first introduction to you so think about what you want it to say about you. They also need it to be written in the correct format for the level of job you are applying for. A list of duties in previous roles is fine for a front line role but a manager needs to evidence their capabilities and achievements, not that they processed their staffs holiday forms or did a roster.

I was also very lucky that a gentleman named Martin Garrity reached out to me and offered me some support. I had never had any previous interactions with Martin and he was a second-level connection on LinkedIn when he saw my post, commented and we connected. Martin is an expert in job seeking and is amazing at helping people put together their plans and get themselves ready to find that next role, as well as helping them secure it. Martin gave me an hour of his time, in which we discussed me, my plans, my goals and how I was trying to achieve them. His help on the call was great but also following him on linked in was invaluable.

I won’t share all of the information that Martin shared freely on LinkedIn during that time but with his permission, I have a few great tips to highlight:
1. Keep a spreadsheet of applications. Highlight prospective jobs, jobs you’ve applied for, interviewed for etc. If you can, include details of dates (applied for, heard back, closing date etc.), the progress of applications (stage), notes on interviews, questions etc. This is a database to help you keep your career search in order and help inform you when going for similar roles. It also really helps keep you sane as it is very easy to go “job blind” in these things and inadvertently waste time applying for the same job again, potentially via a different agency if the job is advertised multiple times.
2. Maintain a social media presence, and if possible, increase it. One or two pertinent posts a day, ideally an original one demonstrating your own professional knowledge and insight, with maybe a share or two goes to raise your profile and demonstrate your relevance in the field. Remember, people hire people.
3. Continual Professional Development is also valuable. You may never have this amount of time on your hands again so if you can upskill, you will be more favourable than your contemporary that hasn’t taken the time for personal development recently.
4. Don’t spend all day searching for jobs. An hour or so a day will show you what’s new as you have probably been looking for a while and seeing the same jobs repeatedly.

Step 5 – Give Yourself a Break
Knowing when to push and when to relax will be important. It is very hard to let go, believe me I know, but you have to. As I mentioned, my contract was due to start after New Year (02.01.2019 to be precise) so I was faced with Christmas and New Year as the beginning of my search. Not only does no-one really recruit for full-time employment over Christmas (especially 25th December – 1st January), it is also a time for celebration. This left me with a dilemma as I find it hard to sit back and let stuff go, preferring to take the bull by the horns, and I was understandably anxious about the future as well.

I did the only thing that I could do. I stepped outside myself and decided that, as it was largely out of my hands due to the seasonal lull in the job market, the best thing to do would be to enjoy a family Christmas as if nothing had happened. In truth, the rest was welcome. I managed to recharge my batteries and come out fighting after Christmas.

It is also important to know when to stop each day/week. It can consume your life, you can always do more or could have done more, to whatever gets thrown your way.
Step 6 – Stay Ready, Don’t Get Ready
I mentioned the CV earlier and this was one of the things that I had ready to fire off from day one. Any roles I discussed with people, I followed up with an updated version of my CV. I tailored it slightly depending on the exact nature of the role but had a generic one I could send in a minute or less if required. I also created a new, more professional email to send them from and used that only for business. That is also the email address I included on my business cards.

I had a few opportunities present themselves during my time searching for my next role. I put out a number of solid applications alongside some speculative ones. I also met with a couple of people to discuss prospective roles that never came to fruition but the experience was valuable. I maintained a state of readiness throughout the working week and I approached weekends more flexibly.

When I received a call regarding an opportunity at Corps Security I had previously discussed I was over the moon. As it transpired, in addition to maintaining a good professional relationship with Mike Bluestone, who I had the privilege to work on a project with 5 years previously, I had also previously met with one of the individuals involved in the role when representing NAHS and thankfully made a good impression. This then assisted me in applying for the position that I now hold.

I was lucky enough to reach the interview stage and so I made sure I did the necessary research. As someone that has conducted countless interviews, I have gained greater insight into the process, but nevertheless, the old adage that failure to prepare is preparing to fail remains true. I researched the company, the role, the sectors involved and everything else I could see as relevant. This is yet another time when the (re)connect phase helps as you can also speak to your network for any additional guidance and support you might need.

I secured the job and I was ready to start that day if required but obviously I needed to undergo the necessary employment checks. This gave me a little time to square away the inevitable loose threads of my search, thank the people that I needed to and retract/cancel any unnecessary applications, interviews or enquiries.

Step 7 - Reflection
The aim of this article was to share my experience with people in the hope that it might help in some way. If just one person finds it useful then it has been worth it. I am not saying that the way I approached it is the only way, or even the best way, but it was successful for me and within a relatively short period of times (3 weeks if you take Christmas out of the equation).

There are, hopefully, some valuable tools in here to help people that are experiencing the same challenges to organise their approach and overcome them. Additionally, I believe that Step Zero, though a little overly specific to me, also has some insight that may help people build some resilience in case they are in this position in the future. Look around you at what your peers are doing. If they aren’t doing anything, then you can do something to set yourself apart. If they are actively involved somewhere, you can do the same and either match or exceed their efforts.

I have mentioned several times how distressing this ordeal was for me but I have to also admit that I was charged with energy as well. There is nothing quite like adversity to get you into action mode. I was fortunate enough to have been able to face this situation and come out in a better position than I would have been. I can’t imagine that I would have been half as happy or worked with such a great team of colleagues and clients as I have since joining Corps Security.

Whilst I hope to never be in the position I found myself in back in December 2018 again, if I were, I would be following the steps highlighted above and adapting them to any recent developments.

Remember, you can’t control what has or will happen to you, you can only control your response to it. You will get through this and you will be a stronger person having faced it. I am happy for anyone experiencing difficulties to contact me for a conversation and to offer any advice or help I can. I will endeavour to respond as soon as possible.

You can do this.
We can do this.
The electronic security industry, which is intruder alarm, CCTV, access control, and the installation of fire detection systems, requires no formal qualifications to either trade as, or to install of any of these systems. It remains an un-regulated part of the security industry.

Previously, as an owner of a security company, we gained accreditation from what was then the National Supervisory Council for Intruder Alarms (NSCIA), now known as the National Security Inspectorate (NSI). At that time the prerequisite for membership was of course you paid for membership, companies agreed to adhered to their rules and held the necessary insurance. Audits were conducted twice a year. The inspector may or may not be connected to the industry or indeed have any prior electronic experience, their primary function was the administration, auditing and compliance required to maintain membership. Obviously, this was an important function and I agree in principle with the process and part of the audit included visiting at least two recent installations. The choice of site is determined by the company and is not the auditor’s choice. The process defeated the aim of a site visit, allowing a company to ‘cherry-pick’ nice, neat, prime jobs for auditing. Poor installations remained unchecked.

Inspectors arrived to conduct an audit without tools or steps to carry out a physical inspection leaving the process to rely on a checklist of questions, i.e. “is that sensor in the correct location as per the specification? Yes/No”. Checks to ensure cables installed at ceiling level are actually correctly supported is omitted from the process. Yet this is a prerequisite of the BS 7671 Electrical Wiring Regulations as unsupported cables have proven to contribute to the death of fire fighters and people trying escape a burning building. Surely this evidence’s physical checks are more important than using a tick list to note a sensor is in the correct location?

I have also observed gaps in competency and knowledge particularly the lack of experience and wider knowledge of security installations. This means fundamental elements are overlooked during the audit process. If we as an industry is installing technical equipment and that equipment is installed incorrectly it could malfunction and not operate correctly when needed. The system may also provide a false alarm, and has the potential to electrocute, and ultimately cause death.

The following article is an observation of the electronic security industry by Richard Benyon. Richard currently volunteers as part of the SEATS SIG as the Security Technical Champion and shares his concerns about the sector.

By Richard Beynon MSyl
At least when I first started in the industry in 1981 at the tender age of 16, training was provided by at the time by the big 3 firms; Chubb, Thorn and Securicor and that was it. A few smaller companies surfaced but they were mainly run by engineers who had left the national companies to start their own businesses, but at least some training had been completed. Yet, I was never asked what qualifications or experience I had within the industry during the validation process with NSCIA, thereafter NSI or the Security System and Alarms Inspectorate Board (SSAIB) which I registered with at a later date. Although the SSAIB is more technical during site visits the process still lacks substance.

35-years after my career started the sector remains unregulated. There is no prerequisite for those in the Electronic Security Industry to have formal training and qualifications. An individual can start a security company without a background check and can purchase the same equipment as an NSI or SSAIB approved company from one of the many suppliers, including the Internet without any questions being asked. It is also possible to move membership from one inspectorate to another even if membership is withdrawn due to non-compliance. There is, however, credibility by being approved by either the NSI or the SSAIB as a commercial or industrial business. Insurance companies recognise the endorsement as approval of meeting a certain criterion, and police respond to intruder activations if systems are NSI or SSAIB approved.

For the sector, positive moves are afoot as in the last two years the Certified Technical Security Professional (CTSP) organisation has launched and currently working with SSAIB although the NSI does not recognise CTSP as they are allegedly “in bed with the enemy”. CTSP has introduced a level of regulation into the sector. Members are primarily vetted on their previous experience, time in the industry, formal qualifications and equipment specific qualifications. It is a great improvement but developments to meet the regulatory standards of other professions is still required. By reviewing other sectors, i.e. gas, electrical and security personnel a process can be developed to improve the credibility of the Electronic Security Sector.

- Gas Industry: Engineers are qualified and have a unique ID number. That number appears on all their certificates of completion and that number is traceable. It is illegal to work on gas supplies without the required qualifications, although it is not illegal to sell or purchase the parts and Gas safe companies are required to use qualified engineers in the field and engineers must be recognised as approved personnel.
- Electrical industry: Electricians do not require qualifications to carry out work, for example, in a hospital, but must have a Part P qualification to work in a domestic dwelling. The National Inspectorate Council for Electrical Installation Contracting (NICFEC) requires qualified “test and inspection” electricians who can sign off work carried out by unqualified people. This category of electrician is ultimately the “principal duty holder” who takes responsibility should any issues arise with the installation. NICEIC also have a customer insurance scheme whereby they will get the work rectified by another approved contractor should the original contractor refuse or stops trading.
- Security personnel: Front-line personnel are required to undergo a formal training process and obtain a recognised Security Industry Authority licence which should be worn or on the person during working hours.

The way forward - Regulation for the Electronic Security Industry. This can be achieved through qualifications, training and annual evidence of Continued Professional Development. Individuals and companies should be licenced to practice and more collaboration between the ‘inspectorates’ to avoid flipping between inspectorates is required. Inspections should consist of two parts; one being the administration of practice the other a physical check of one or more installations chosen by the Inspector and not the company or individual.

Pause for thought: Ask yourself this question- ‘What exactly is a security Manager and what does he or she do? The aims of the book are to examine what is required of the professional security manager in a demanding and fast-changing business-orientated sector, and in order for him or her to be able to do this, they need to understand risk and strategic business awareness, and they should have a good working knowledge of a number of skills required to carry out their roles professionally in the eyes of their peers and employers. One of a number of problems for the security manager today is that in certain corporate environments the security manager is often seen as, and there is no disrespect here, a security officer wearing a suit; the person who mans the ‘no desk’, someone who is believed to be a business disabler as opposed to being capable of supporting business growth. A worrying perception.

Business risk
I suspect that if I were to ask a group of security managers what exactly is their role in an organisation, they would probably say that they were expected to protect and secure the assets of the company; and that of course is correct. However, it is also correct to argue that such professionals are required to assist in business development and understand the business risks that their organization faces on a daily basis, and in order to do that they must have a professional recognition and understanding of security risk management.

Risk is the likelihood of a negative occurrence that can impact an individual or organisation, negatively or positively, and that is another twist, as most security managers I have spoken to, having carried out a risk assessment, tend to view risk negatively. The risk assessment of course identifies, and then multiplies likelihood by impact, and that is a pejorative process, as it infers a negative result; arguing that the organisation is going to suffer from a particular threat, such as cybercrime or terrorism. Referring to the original answer that security managers exist to protect the assets of the organisation, then of course such a risk assessment is constantly required, referred to as a dynamic risk assessment.

However, this is an extremely sensitive area, because whilst we must be seen to be protecting the company from a range of risks, the security function must also be aware of the importance of understanding business development, and although it may be uncomfortable for the old and bold security managers in the industry, in order for a company to grow, it must take risks. This is known as the risk appetite or acceptance by the owner of the risk, generally the Board of Directors, and it is part of the overall risk management strategy that must be adopted by the organisation.
Technology and thinking like a criminal

Pause for thought: Ask yourself this question- ‘What exactly is a security Manager and what does he or she do?’

This is such a contentious question for which there is no black and white answer, as it generally depends on how technology is seen by the user. However, in my opinion a balance has to be struck and todays security manager should neither be over dependent on technology, nor should he or she be in denial, as technology is with us to stay; the genie is out of the bottle!

Technology, and indeed manned guarding is critical to the risk management strategy of an organization, as both are imperative in terms of security company assets but must be deployed only when it can be proven that they will reduce the risk. There is insufficient scope within this article for me to detail particular types of technology being used, nor is there space to describe how a manned guarding contract is effectively managed, but there are two concepts that I would like to highlight.

The first concept is that of the Operational Requirement (OR), which describes how and why particular security hardware and technology should be deployed. The OR is part of the risk assessment process and it is a means of understanding how deployed systems can manage risk. An extremely useful website to visit is https://www.cpni.gov.uk/operational-requirements.

The second concept, and I would argue the most important piece of advice I can offer any security professional, no matter how experienced he or she may be, or indeed what professional and academic qualifications they possess, is to always think like a criminal. Heresy, I hear you shout. Logic I would reply.

I have, on too many occasions witnessed security technology being deployed on a whim, or perhaps reflecting the vanity of the security manager who is trying to impress the CEO with the new glass batwing electronic access control system, that is designed to accept a Radio Frequency Identification (RFID) proximity card and bio metric scanning applications. It looks fabulous and the Board cannot be anything other than excited when they see how their 1.5 million pounds has been invested. That is of course until the twelve-year-old boy takes a run and slides under the sparkling batwings that are eighteen inches above the ground. Or the burglar who is watching the security officer, recently issued with a new patrol management system consisting of a number of RFID points spread around the perimeter that must be interfaced by the officer as part of her patrol. The criminal knows that once the security officer has struck point one, she is intent on moving to point two which is five hundred meters away, paying little attention to what is happening between points one and two. The fact that the poorly designed and installed CCTV system has not operated since the day it was hastily procured by facilities, without consulting the security function, only helps the burglars cause.

Think like a criminal.
Stay professional, stay focused and stay safe.
Our Membership

Member Insight: Is Privacy Dead?

by Marc Smith, Security Institute Student Member

Everyday we willingly share every detail of our lives. Who we are, where we are, our likes and dislikes, the list goes on. For years we have been told of the dangers of oversharing on the internet but it has done little to prevent widespread narcissistic behaviour. The naïve of us may think the worst outcome is an embarrassing overshare or worry that a misjudged tweet will come back to haunt us. God forbid our internet search history is exposed for all to see! Unfortunately, the truth is much scarier. The modern social engineer and OSINT (OpenSource Intelligence) investigator can utilise your information to identify attack vectors and target not only you but your employer/ company as well.

Within industry there is a buzz around OSINT with everyone from criminals, journalists, law enforcement and even HR departments deciding to utilise the information people have decided to share online. Buzz words like penetration testing, security operation centres, phishing, pretexting, smishing, baiting and tailgating are commonplace. What is less commonly discussed are the steps an individual should take to best protect themselves (and by association their company) from a social engineering/ OSINT attack.

In order to educate and help protect members of the institute, this article outlines a simple step by step guide to regaining some of your online privacy. By increasing your privacy, it will hopefully prevent you from being the ‘low hanging fruit’ that attackers are most likely to target. The advice below will not only make you more aware of the personal information you have exposed on the internet, it will also help you to remove information that will make it much more difficult - but not impossible - for a third person to locate you.

Which category are you?

Currently there are four main categories that prompt an individual to examine their own online footprint:

Identity theft victims – Sources now estimate that one in three of us will be impacted by identity theft in our lifetimes. Most people make it extremely easy for fraudsters to gain the personal information necessary to acquire credit in their name. The guidance contained below will make it more difficult to collect.

Targeted subjects – History informs us that certain professions are more likely to be targeted online. Do you work in the criminal justice system, work in a senior position for a well-known brand, or have involvement in controversial environmental decisions? If you or your clients fall into this category you should not wait until you face a personal threat to begin securing your online footprint.

Special operations and the intelligence community – Those with access to sensitive information or who hold SC or DV security clearance could be of interest to foreign state actors who may attempt a social engineering attack.

Celebrities / ultra high net worth individuals (UHNWI) – This group tend to be victims of stalking, trolling, extortion, scams and violence. The guidance below will make it more difficult for a would-be attacker.
Background Checks
The aim of a background check is to identify what the internet already knows about you. By following the specific search instructions below you will be able to identify your personal information in a fast and efficient way.

Before conducting any searches, it is advisable to use private browsing and to ensure you are not logged into any online accounts such as Gmail, Hotmail, Facebook etc. Searches should then be completed on each of the following websites: Google.com, Bing.com, Groups.google.com, News.google.com, Google.com/images, Bing.com/images, Yandex.com and Exalead.com

Initially conduct your search as if the details below were yours:

Boris Johnson
10 Downing Street
Westminster
SW1A 2AB
077 11223344
Boris.johnson@email.com

Next, conduct the following searches including quotation marks. The quotation marks are essential as they direct the search engine to only search that exact phrase.

“Boris Johnson” “SW1A 2AB”

This search will produce all pages on the internet which contain both name Boris Johnson and the full postcode SW1A 2AB. Try the following variations with your own details across all the search engines and document what you find. Try including your interests or hobbies to give a full picture of what information you have exposed.

“Boris Johnson” “10 Downing”
“Boris Johnson” “07711223344”
“Boris Johnson” “077” “1122”
“07711223344”
“Boris Johnson” “Prime Minister”
“Boris Johnson” “Member of Parliament”
“Boris Johnson” “MP”
“Johnson” “MP”
“Boris” “Westminster”
“Boris.johnson@email.com”

There may be additional search variations that you can come up with.

Once you have completed all searches, you want to contact each company that holds details on you in order to have your details removed. Go to the privacy section of each website and there is usually an email address that you need to request removal from.

Further websites that need to be checked
In addition to conducting your checks across the search engines listed above, you should also visit the following websites:

Haveibeenpwned.com - This website will identify if any of your emails have been found in a data breach. Check all your emails and those of your family. If your email is in a data breach change your password if you have not already. Also remember to change the password of any accounts that also use that password.

192.com - In my experience 99% of the UK population have their home address listed on this website.

Again, you want to contact these companies to make sure that your details are removed.

Social Media
Whether you are on Facebook, Instagram, Twitter or LinkedIn you need to review your privacy settings. Ensure that you are not giving them your personal preferences, your location and your contacts. Try to only fill out the required fields and avoid giving a telephone number if possible as this is the easiest way of tracking you. Ensure that you log out of Facebook after use as they are able to track every website that you visit while you are connected to it.

When you download a social media app onto your phone you are giving it access to your contacts, your photos, your microphone and your camera. Remove these apps and instead use your phones web browser to connect to your social media accounts.

A safer future
By implementing the above steps you will be able to locate and remove your personal details from the internet. This will give you better privacy and will better protect you from being found through open-source techniques.

Now that content has been removed you need to ensure you do not repopulate the internet with your details. In the next edition I will discuss techniques that can be used to ensure companies are not able to track you across multiple platforms and that all of your communications (private and professional) are secure.
New Member Introduction: Satia Rai MSyl

I have over 25 years’ experience in risk management and security services within the public and private sector at both operational and strategic levels. I have played a significant role at director level in various key organisations, managing a diverse range of hard and soft FM services and has a strong track record of leading transformational change within the security sector. I joined Woodwill Security Services in 2020 and have ultimate responsibility for the development and growth of the company.

In February 2020 I decided to apply for membership with the Security Institute. I am proud to have achieved the Security Institute member status in March 2020. It’s been by far the best decision I have made this year in terms of my own personal development. Subsequently I have completed my CPD activity for 2020 & Cyber Security for home users/workers course. In addition to this I have participated in over 100 webinars which have been very informative, beneficial and relevant. I have connected with security professionals from all over the globe.

My learnings have enabled me to improve our business continuity plan and our people framework model at Woodwill Security Services. It has also been a great platform for me to raise the profile of our organisation Woodwill Security Services. There are many more benefits to add.

A special thanks to Rick Mounfield CSyP FSyl and the Security Institute for making this possible. I am looking forward to a long term affiliation and association with the institute.
Our mission at North Star is to enable you to conduct business globally, no matter where the opportunities are taking you.

We ensure this by providing global access to reliable and affordable journey management services in the most complex environments.
The Security Institute is proud to be part of the Living Wage movement as an accredited Living Wage Employer. This means that every member of staff in our organisation earns not just the minimum wage but the Real Living Wage. The Real Living Wage is an hourly rate set independently and updated annually, based on the cost of living in the UK.

The Real Living Wage is £9.30 for the majority of the UK, and £10.75 for London, is calculated based on the cost of living and determined by independent public consultation. The real Living Wage provides a robust benchmark for responsible employers who voluntarily choose to ensure their employees earn enough to meet their basic everyday needs.

The real Living Wage goes beyond the Government’s statutory National Living Wage, which was introduced in 2016 for those aged 25 and above and is based on a percentage of median earnings. Currently, full-time workers paid the real Living Wage earn approximately £40 more a week than those on the Government’s National Living Wage, which equates to £95 a week in London.

The Security Institute now joins over 6,500 accredited Living Wage Employers. To become a Living Wage Employer an organisation must voluntarily pay all their directly employed staff and their regular third-party contracted staff the real Living Wage, such as cleaners, caterers and security staff.

Currently, the list of Living Wage Employers includes a wide range of sectors and workplace environments, directly employing over 2.6 million people. They include major brands such as HSBC, IKEA and KPMG; Combined Authorities and Local Councils; the NHS; retail; and many hundreds of SMEs. Altogether, these employers have put over £1 billion of extra money into the pockets of low-paid workers across the UK since the Living Wage campaign began.

Speaking on the Institute’s recent accreditation, our Chairman Professor Alison Wakefield PhD CSyP FSyI stated: “Taking good care of our employees must be a priority for a socially responsible organisation and becoming accredited as a Living Wage Employer is one of the many ways in which we actively put this into practice.”

You can find out more about the Real Living Wage and how you can get involved by visiting www.livingwage.org.uk
How can the Real Living Wage benefit the Security Industry?

Over 1.3 million key workers in the UK are paid less than the Living Wage, and are in insecure work according to research conducted by the New Economics Foundation. The Security Institute believes it is crucial to thank the key workers that have continued working during this period of extended lockdown and will be essential to us returning to ‘normal’, many of which are security professionals. We want to harness the public support for these key workers by celebrating them and highlighting the importance of paying them a Real Living Wage.

A Living Wage Employer Survey conducted by the Cardiff Business School in 2017, found that 75% respondents reported increased staff motivation and better employee retention rates since paying the Real Living Wage. In addition, 86% said the reputation of their business as an employer and corporate entity had improved as a result.

Recognised Service Providers

Although the Living Wage Employer mark is the final aspirational target for many Employers, service providers aren't always able to immediately attain this goal due to their clients having the final say on contract pricing. It is with this in mind that the Living Wage Foundation introduced the Recognised Service Provider scheme.

Recognised Service Providers guarantee the Real Living Wage to their directly employed staff and to regular third-party contracted staff who are, crucially, not tied to client contracts. Where Recognised Service Providers differ from Living Wage Employers is in relation to staff and the third party contracted staff who are tied to client contracts.

Recognised Service Providers pledge to champion the real Living Wage by always offering a Real Living Wage option to prospective and current clients alongside every market rate tender bid, giving the client the opportunity to implement the Real Living Wage through their contracts where possible. Since the Real Living Wage rates increase annually (in November), Recognised Service Providers and Living Wage Employers must uplift their minimum wage payments each year (by May the following year at the latest) to continue to qualify for this status.

There are currently over 140 Recognised Service Providers, such as Mitie, Sodexo, Carlile Support Services and Corps Security, who collectively operate over 10,000 Living Wage contracts and employ close 100,000 workers on the real Living Wage.

Speaking on the Real Living Wage, Emma Pearman-Wilson, Contract Supervisor working for Carlisle Support Services on a contract with East and North Hertfordshire NHS Trust said:
“Receiving the Real Living Wage rate of pay has supported me and work colleagues to be happier both inside and outside of work. It has helped to improve morale and motivation between our team – the mood is upbeat and we’re engaged to do the very best job that we can”
Our new Approved Training Provider (ATP) scheme: How we are assuring quality in security training courses

The Security Institute strongly believes that everyone who is committed to their personal and professional development should have access to credible training. However, as many members have expressed, identifying credible learning and development opportunities often requires a leap of faith to navigate the myriad of training providers.

In response, the Security Institute is launching an Approved Training Provider (ATP) scheme. The Institute’s ATP scheme provides a third-party assessment of quality for security-related training courses that are not already accredited by existing qualification bodies such as BTEC.

All of the Institute’s ATPs must demonstrate that their course is delivered to a recognised standard, and that the material is up-to-date and meets the course’s stated purpose. The ATP scheme will thus help provide assurance for learners across the sector that are seeking training opportunities to continue their professional development, and give employers confidence when funding employee training that has gained ATP status.

The launch of our ATP expands on the Institute’s existing efforts as a not-for-profit organisation to enhance professional standards across the security sector, and support the professional development of all security practitioners. It will ensure that those seeking training can easily identify quality providers, as well as providing a greater incentive for training providers to deliver quality courses.

The scheme will include two different ATP endorsements:

---

**Approved Training Provider: Continuing Professional Development (ATP CPD)**

- The ATP CPD endorsement is for workshop or online events endorsed by the Institute’s CPD scheme.
- Participants will receive a training provider CPD certificate (or similar) endorsed with the SyI ATP CPD logo
- CPD points will be allocated by Institute representative
- The duration for an ATP CPD programme will not extend beyond 1 working day.

---

**Approved Training Provider: Professional Certification (ATP PC)**

- The ATP PC endorsement is for short courses which are more informed than a CPD workshop or event
- The course will include a form of assessment, i.e. Q&A, multiple choice questionnaire, scenarios or practical participation
- Participants will receive a Professional Certificate endorsed by The Security Institute
- The duration is unlimited but must be more than one working day

---
How can I tell which Training Courses are approved by the Security Institute?

Our ATPs will be issued exclusive ATP logos to use on their promotional material and certificates awarded to learners, which will contain the same orange colour as seen in the logo below as well as the year the logo was issued. There will be one logo for ATP CPD courses and another for ATP PC courses.

In addition, all ATPs will be listed on the Security Institute website: www.security-institute.org/atp/

What does the Security Institute assess during the ATP application process?

ATP applicants will be required to complete a comprehensive due diligence process to ensure instructors are appropriately qualified and experienced, that training is relevant and current, and assessment is fair (ATP PC only). Insurance documents, policies and procedures will also be reviewed as part of the process.

All ATP applicants will also need to satisfy the Institute’s requirements for quality and ethical practice as laid out in the Institute’s ATP Terms and Conditions. A successful applicant will receive the appropriate ATP endorsement and then be listed on the Institute’s website.

If you are interested in finding out more or joining the ATP scheme, please contact the Security Institute’s Engagement Manager Jade Lapper: jade@security-institute.org.

Speaking on our new ATP Scheme Rick Mounfield CSyP FSyl, Chief Executive at the Security Institute stated;

“The Institute recognises that those working in the sector have a demanding job; therefore, the quality of the training provider and content must undergo a due diligence process. This way, the SyI ATP scheme removes the guesswork for those seeking relevant and affordable training opportunities. The ATP logo will be an endorsement of quality, enhancing the decision-making process. In short, the Security Institute has taken away the risk of wasting money. And with the significant training expertise in the Institute, the end-user will have access to upskilling opportunities that are time savvy and financially affordable. There is no doubt, Angela Vernon-Lawson FSyl, supported by Carl Dakin CsyP FSyl, has created a scheme that many professionals will value well into the future.”

What do Security Trainers gain from participating in this ATP Scheme?

Gaining ATP status is a mark of high-quality security training, which can be displayed using the Institute’s ATP on any promotional material and any certification awarded to learners upon completion of the course. The ATP logo will be reissued annually, indicating to learners and employers that a training course remains up to date. All ATP approved courses will be eligible to double points in the Institute’s Continuing Professional Development (CPD) scheme, with 2 points for every hour of formal learning. This will be an additional draw for those participating in the scheme, which is now been adopted by four other organisations.

The Institute will also display all ATP courses on their website, as well as help highlight these quality training opportunities to members in their various communications.
Strengthen your Leadership Pipeline with the Business and Strategic Leadership MSc

The Security Institute proudly supports the Business and Strategic Leadership MSc for the security sector being offered by Cranfield University, as a unique opportunity to sponsor your high-potential managers through a highly regarded programme developed specifically for the security services sector.

The delivery of the course is designed to ensure all content is relevant and directly applicable to the role of a security professional, with all material being applied to the learner’s organisational context and assignments will focus on progressing their organisation’s strategic agenda with the opportunity for group projects that address the strategic agenda of their organisation. As working security professionals, a key strength of the course is that it is a practical one. It requires participants to possess the ability to apply theory to live issues, helping the taught material effectively translate to real challenges that are faced within the security workplace.

In addition to directly applying the content of the participant’s organisation, the learning experience has been personalised for the Security Institute with two industry-focussed modules that ensure that course provides sector-specific insight and aligns with organisational development. The industry-focussed modules for this programme are ‘Global Security: Emerging Challenges’ delivered by module leader Dr Anastasia Filippidou, and ‘Global Security: Culture & Complexity’ delivered by module leader Dr Bryan Watters.

From a business perspective, the course will help strengthen the leadership pipeline within an organisation by allowing ambitious security professionals to focus on their personal development to lead in an organisational setting. Empowering learners to become leaders not just managers, with the capability to set strategy and provide direction within an organisation.
Furthermore, a unique feature of this course is that the programme will consist of a consortium of the Security Institute members, which will enhance the learning experience for all with other security professionals offering their insights on issues and this will also provide great networking opportunities for all participants.

Speaking on the programme, the Security Institute’s Chief Executive Rick Mounfield CSyP FSyI stated:

“It is well recognised that Security leaders today must be able to articulate the value security can offer to business. Global and strategic security concerns taught alongside business administration in a Masters level degree is revolutionary. The Institute is delighted to partner with MBA-triple-accredited Cranfield University to support strategic Security Leaders in their professional development”

Cranfield’s Director of Practice Development David Deegan shared:

“At Cranfield, all of our faculty have deep connections with industry and understand the challenges businesses face. Our programmes are therefore pragmatic, tightly aligned to industry problems, and therefore have a direct impact on industry success. We are committed to transforming knowledge into action. Effective security professionals work more on the business, rather than just in the business, and this programme enables them to elevate their business practice to that level.”

The programme normally costs £18,000, However, for this cohort commencing in early December 2020 only, eligible organisations in the UK will be able to utilise the Apprentice Levy scheme to fund all £18,000 for the programme. After the end of 2020 this opportunity will not be available as a fully-funded programme. So this presents a unique opportunity to obtain impactful development using the Levy monies. Non-levy funded delegates are also able to attend at the cost of £18,000 plus expenses.

For further details on this course and to join our December 2020 cohort please email Kim Bibby by September 27th kim.bibby@cranfield.ac.uk

You can also recap a webinar discussing the programme that features Rick Mounfield CSyP FSyI here: https://blog.som.cranfield.ac.uk/bsl-in-the-security-sector#findoutmore
We have recently launched 2 new Covid-19 Back-To-Work Training Courses to help our members and the wider community develop their essential skills and adapt to the current challenges that we are all currently facing. These two courses are:

• ‘Standard Operating Procedure for returning to work COVID-19: Induction’ Course
• ‘COVID-19 Compliance Officer’ Course

These courses have been created to help organisations train their staff according to the public health requirements, addressing the current COVID-19 associated risks.

As lockdown measures start to be eased across the country, on-site work can now recommence for many organisations. Navigating the work environment post-lockdown presents an array of new challenges for organisations to consider in order to ensure the health and safety of their employees, customers and the wider general public.

There have already been several instances of COVID-19 outbreaks that have been traced back to a specific workplace reported in the national news, take many outbreaks traced back to specific factories as a recent example. Organisations have a duty of care to their employees, customers and the wider community to ensure that any return to the workplace is conducted safely, and strictly follows the current government guidelines.

These two courses address the need for organisations to make their teams aware of best practices that need to be followed. The ‘Standard Operating Procedure for returning to work COVID-19: Induction’ Course has been designed for the general training of your team, whereas the ‘COVID-19 Compliance Officer’ Course contains additional information for managers or the assigned Covid-19 Compliance Officer within your organisation (see further details on the right hand page).

We are currently offering a discounted bundle package on these two courses, which can be purchased by individuals or in bulk for employers.

You can purchase our Covid-19 Back-To-Work Training Courses here: https://security-institute.org/online-training-courses/
Completing these courses will also earn you double formal CPD points in the Security Institute’s CPD Scheme, helping you continue your professional development and gain a competitive edge over other practitioners.

‘Standard Operating Procedure for returning to work COVID-19: Induction’ Course

This course takes you through the processes to follow during recommencement of work at your organisation, ensuring you are prepared for the challenges your organisation faces as we exit national lockdown.

It outlines the essential considerations and procedures that need to be in place to ensure the safety of your team and the general public, including:

• how to prevent cross-contamination, rules on social distancing and administering First Aid
• best practices to ensure your site is always employee-friendly to combat infectious diseases
• how to deal with suspected and confirmed cases of Covid-19

‘COVID-19 Compliance Officer’ Course

This course focuses on the roles and responsibilities of a Covid-19 Compliance Officer, an essential role within all organisations as we start to create safe working spaces post COVID-19.

The best workplace management approaches to follow will be specifically addressed. You will gain insights on the various strategies and best practices used by the Officer to ensure a safe and sanitary working environment that is free from Covid-19 and prioritises employee wellbeing.

Expanding on the ‘Standard Operating Procedure for returning to work COVID-19: Induction’ Course the ‘COVID-19 Compliance Offer’ Course contains an additional two modules:
Our online Professional Development Platform brings a vast range of eLearning resources to the fingertips of our members, helping discover and develop essential career skills. Members have access to interactive courses on a broad spectrum of topics, as well as expert-advice videos and articles. The constantly updated material ensures that all of our members are up to date with the latest employment trends, and are the best equipped to achieve their career aspirations.

It is also important to note that using the platform is a great way to acquire valuable free CPD Points.

Returning to work after Furlough

Transitioning back into what now may be an unfamiliar workplace can be extremely daunting, and this is a challenge being faced by many professionals now as lockdown measures are beginning to ease and they are taken off the Government’s Furlough Scheme.

This new course that has just been added to our Professional Development Platform for all of our members, helps you prepare for your return to work and offers advice on what you can do in the initial stages of your return to feel as happy, productive and supported as possible.

Members of the Institute can find this course here: https://security-institute.careercentre.me/u/91dkok9u
The Dos and Don’ts during a Video Interview

Given the current circumstances most companies are opting to conduct video interviews, when trying to find the ideal candidate.

To be successful in a video interview, should you treat it just as you would a ‘normal’ face-to-face interview? Or are there any key differences you need to be aware of? We’ve compiled a handy checklist of what you should and shouldn’t do during a video interview to help ensure success.

Members of the Institute can find this article here: https://security-institute.careercentre.me/u/6h9l0etr

Our Professional Development Platform also contains a range of other interview and job-hunting related resources including: ‘Answering Common Interview Questions’, ‘Curveball Interview Questions’ and ‘What type of CV do I need?’ to name a few.

What is Cultural Intelligence?

A new short course called ‘What is Cultural Intelligence?’ has recently been added to the Professional Development Platform, explaining how diversity can be embraced within your organisation and create fruitful collaborations.

As professionals we need to ensure that we don’t let our differences hamper opportunities for beneficial collaboration and new working relationships. This is where cultural intelligence comes in. It is clear, that being culturally intelligent is key in helping you achieve success at work. This course explains what cultural intelligence is, why it’s so important and how you can develop yours.

Members of the Institute can find this course here: https://security-institute.careercentre.me/u/m3lmjnlt
Having a professional mentor could mean the difference between finally achieving resolutions and giving up on them for another year. By entering a mentoring relationship as a mentee you will be encouraged to set time aside to work with your mentor to work on developing yourself: analysing where you currently are, identifying strengths and opportunities that can be built on, overcoming weaknesses and threats, setting clear goals and planning a route to achieve those goals.

Especially, during this difficult time in the midst of the global COVID-19 pandemic, security professionals at the early stages of their career could benefit from an experienced mentor to help navigate the unprecedented challenges that they are presented with.

Although, security professionals can benefit from a mentor during all stages of their professional development. The Security Institute offers an online Mentoring Platform, which is accessible through the Members Area of the Security Institute website: https://security-institute.org/members-area/. This resource is designed to support professional development for all levels of experience with categories that provide guidance for those currently in education, applying to become a Chartered Security Professional and many other areas of expertise. The platform can match mentors and mentees according to their sector, skills, meeting preferences and regions.
For example, Mark Bramwell MSyI had a successful career within the British Army and wanted to draw on the experience of a mentor as he transitioned into a management role within the security industry.

Speaking on his mentoring relationship, Mark stated:

“I have a mentor who is a Head of Security, who has all the right experience to be able to provide and guidance. He is a very senior head of security in a large Multinational and has all the right experience and exposure that I wish to tap into.

“Having a mentor to bounce ideas off and ask for advice is priceless. Sometimes you just need to be able to speak to someone who is outside your chain of command who is non-judgmental. I would encourage everyone to have a mentor, even if it’s just for a short term issue.”

It is important to also stress, that mentoring is not a one-way street with just the mentee benefiting. Becoming a mentor can be a valuable experience for the mentor too. Firstly, being a mentor feels rewarding. Knowing that your skills and experience has helped someone else to succeed is a great feeling. But you will also gain insight into how others approach challenges and in turn may learn new things in the process. Your mentee may have a different perspective, as well as knowledge and skills that you don’t.

Offering yourself as a mentor will give you the opportunity to develop your own learning, and potentially improve your knowledge of the security industry.

Speaking on his experience as a Mentor on the Security Institute’s Mentoring Platform Darryn Robbins MSyI stated:

“I felt satisfaction that although it may have only been a few hours per month, my support and guidance has helped an individual promote and raise their standards within the industry, which in turn will rub off on someone else.

“If I am really honest, anyone in our industry who doesn’t want to gain further knowledge, use the experience and skills of others or look for CPD through mentoring, shouldn’t be in our industry. We have a vast range of skills, attributes, experiences within the SyI and all of us as members, whatever our level, should be looking to learn from others.”

Likewise our Director of Educational Development, Angela Vernon-Lawson FSyI, is also a big advocate for the platform and has been using it to provide support to other security professionals. Speaking on Mentoring, Angela stated:

‘Through the mentoring programme, I have assisted mentees to return to the workplace, change careers, identify transferable skills, improve confidence, move into a leadership or management position or study. Mentoring has proved particularly useful for those transiting from a military or police career’.

Through the mentoring programme, Angela was able to offer Maitseo Pelaelo MSyI advice based on her years of industry experience and to assist with professional connections to support his personal and professional journey from within her network.

Speaking on our mentoring relationship, Maitseo stated:

“The mentorship programme exceeded my expectations. In 3 months, I achieved my objective - to gain promotion. As if this was not enough, the mentorship resulted in building an international relationship between my employer (CAAB) and another organisation (CAA) - something I did not see coming. I continue to engage with Angela as a colleague outside of the mentorship programme - this is a positive indicator of successful professional relationships.”

To reflect the positive impact that participating in a mentoring relationship can have on your professional development, for every hour of time spent mentoring or being mentored will earn 1 informal CPD point.
In the mission of discovering how Covid-19 has affected UK large organisations and their readiness to limit the negative impact of the pandemic, SASIG (Security Awareness Special Interest Group, a cybersecurity industry networking forum), and one of their Supporters, ESET (a cybersecurity technology provider) ran a poll of online security leaders.

The SASIG membership, exclusively made up of cybersecurity front-liners with direct responsibility for online security at their organisations, were asked a series of questions focussed on:
How Covid-19 has impacted their business
Their readiness to deal with the challenges it has created
How they feel the changes made will impact the business going forward

Martin Smith MBE, Chairman and Founder of SASIG, said: “I am delighted that SASIG and ESET UK have come together to conduct this important research within the UK cybersecurity community. Our members have told us their many stories of how organisations have transitioned to remote working and the challenges they have faced in adapting their business continuity measures.”

Research Findings
How prepared were we for Covid-19?
Almost half of the companies had some “pandemic business continuity measures” (or equivalent) in place before the Covid-19 outbreak, and more than 80% of the UK companies had a version of a “remote working strategy and operations” plan in place. These were deemed effective (3 in 4 respondents believe they were) and made them partially prepared for the pandemic.

A vast majority (72%) of the IT decision-makers in the surveyed UK companies rate the general readiness of their organisation to respond to crises and black Swan events as “prepared”.

What is the biggest security challenge of migrating to a remote workforce?
Three-quarters of respondents have more than half of their workforce working remotely, with half of all respondents having transferred over three-quarters of their current workforce to a remote work environment due to Covid-19 (who were not working remotely before).

The biggest challenge associated with employees working from home was identified as the increase of cybersecurity risk caused by the human factor. This was followed by an increased risk of cyber crime, which was also identified as a key challenge.

Martin Smith MBE of SASIG, continued: “The human factor in cybersecurity has long been discussed at our meetings as one of the main issues facing businesses across the UK, This research reinforces the point that human error, ignorance, omission and occasional malicious behaviour are the root concerns of many organisations.”

How has the pandemic affected IT security budgets?
The impact of the pandemic on companies’ IT security budgets this year varies. The biggest group of companies state the crisis will not affect their IT security budgets. The second biggest group (32%) state it will increase their IT security budget this year by up to a half, compared with the planned budget. A smaller group (21%) thinks it will decrease their budgets by up to a half.
Overall, for most organisations the impact on their budget was minimal: three-quarters of the responses are between +25% and -25% impact on their budget.

Will the changes being made become the new standard in a post-Covid-19 world
Most IT decision-makers say that their organisation has adapted to the crisis efficiently and adequately. They indicate that their transition to the online environment was not complicated and did not involve significant change or impact on projects they had planned before the crisis. The vast majority (77%) of companies indicated they had to cancel less than a quarter of their projects because they were unable to move them to a remote working set-up.
Still, companies do not plan to keep all the changes mandated by Covid-19 in the future. The views and perspectives differ regarding the lasting impact of the pandemic, but from our findings, we can generalise that two-thirds of companies plan to keep 25%-75% of the installed changes as they go forward

The IT decision-makers surveyed think the changes to the ways their company operates due to the crisis, both from a short and long-term perspective, will be:
- Internal workflows and processes
- Automation and digital transformation
On the other hand, they do not expect a significant change in the balance between in-house and outsourced expertise.

Malcolm Tuck, MD of ESET UK, commented: “It is clear that there is some post-Covid economic uncertainty, with analysts predicting Enterprises in some sectors to weather any European recession but with more challenging times for SMB’s. Overall, the security market should remain more or less unaffected albeit with IT spending predicted to grow more slowly from original forecasts.”

About the researchers
SASIG’s membership represents 2,000+ organisations of all sizes from across the world and from all sectors, public and private, with its 4,500+ membership is responsible for cybersecurity within their organisations. The SASIG currently presents a daily showcase of online presentations, panel sessions and networking events to its membership.

Are you a cybersecurity professional? Did you find this useful? Find out more about joining the SASIG to get more information like this at thesasig.com
Do you need security software? Find out more about ESET at eset.com

About the research
97 respondents completed the survey 28 May - 15 June. 2 out of 3 respondents are from enterprise organisations of more than 1,000 employees, with more than half from large enterprises of more than 3,000 employees.
With veterans already nearly twice as likely to be unemployed as civilians, and the impact of the Covid-19 pandemic already hitting many hard, it will be unsurprising if we see many veterans looking for employability and employment support over the coming months. However, it’s not all doom and gloom. Employers who hire veterans praise their reliability, resourcefulness and self-discipline.

So why the mismatch? There’s two parts to this answer – firstly, employers who haven’t hired veterans before often focus on stereotypes regarding mental health – those unhelpful ‘mad, bad, or sad’ labels that have been cultivated by some. And secondly, whilst veterans have amazing transferable skills, they can struggle to effectively communicate these skills to civilian employers in a way they understand.

Luckily, there are organisations out there who can help bridge the gap. One such organisation is Royal British Legion Industries. Founded back in 1919 to help retrain wounded soldiers after the First World War, this charity has become an expert in all things employment. They run two social enterprises where the majority of staff are either veterans or civilians with disabilities – there are not many places you’d find a production line of ex-Gurkhas!

They also provide housing, care and welfare support to veterans in a state of the art village in the heart of Kent. However, it’s their unique LifeWorks programme which has been changing the lives of veterans for the past 9 years, helping them showcase their talent to employers and find sustainable work. Delivered across the UK, it has supported over 1,500 unemployed or underemployed veterans to date.

The programme, which was designed by veterans and is delivered by a team of veterans and former emergency services personnel, involves a period of concentrated face-to-face support via a 5-day course, followed by 12 months of formal ongoing contact – called ReachBack. However, veterans who have attended are able to call back at any time following the course, with no limit on the amount of support provided. RBLI’s Head of LifeWorks Garrath Williams, a British and Australian Army veteran is a firm believer in the positivity veterans can bring to any organisation and is committed to changing perceptions that all former Service personnel can be a liability.

“The experience many veterans have mustered over a career in the military is recognised by some industries more than others. If you can work on an Aircraft carrier can you work in the hospitality sector? If you can drive and maintain an Armoured Personnel Carrier you can work in agriculture? If you are an experienced and adaptable planner – you can work in the security sector? I think so.”

Unlike other programmes, LifeWorks has been developed to offer a truly personal experience. Each veteran who gets in touch is offered what the team call a ‘vocational assessment’. This powerful tool is at the heart of what LifeWorks offers and provides essential career direction advice.

“The vocational assessment basically helps the veteran and our team better understand what career pathway a veteran might take to ensure they are able to find meaningful employment. It’s not just about their wants and interests, although that’s important, it’s about where their skills lie and how they can be used in civilian industries.

Sometimes the assessment opens the door to a realistic conversation about the future. For example, a veteran who has been injured may be keen to enter a specific industry, but their injury would make particular jobs very frustrating for them – this may be the case with a brain injury for instance. On other occasions, it’s a really positive opportunity to discuss options a veteran thought wasn’t a possibility for them, or they hadn’t even considered before. There are careers out there that not everyone has heard of, but the team are able to shed light on those and
also instil that confidence to give it a go. At the end of the day, you don’t get anywhere if you don’t take a chance.

Following the assessment, LifeWorks’ trainers work with individuals and groups on employability skills to ensure veterans can really sell themselves to civilian employers. This includes working on building a CV, filling out tricky application forms and practising interview technique. LifeWorks even offers veterans mock interviews, matching individuals with employers or professionals from their chosen industry wherever possible.

But Garrath says whilst all these skills are important, he’s noticed the one thing that veterans always talk about following contact with the LifeWorks team is an increase in confidence.

“It’s amazing really because you get veterans who’ve done incredible things whilst serving. They’ve travelled the world, they’ve been in really high-pressure situations... but when it comes to thinking about civvy careers they really struggle to see themselves achieving.”

“The results speak for themselves, nearly 90% of veterans who attend the course have found sustainable employment within 12 months – most of those within the first 6 months after making contact with the LifeWorks team.”

“Every veteran we help get closer to achieving their goals is a win for the team as well. As many are veterans themselves, they really feel that connection and are so pleased when a fellow veteran finds stability and success on civvy street.”

Whilst supporting veterans has always been the primary goal of the LifeWorks team, the prevalence of employment issues faced by members of the broader military community has led them to adapt the programme for different audiences. They now also deliver courses to the spouses and partners of serving personnel and veterans through a ‘LifeWorks-Families’ programme.

“Military families can have a hard time of it. Again they have so many inherent skills from the life they lead – not least resilience and adaptability – yet when it comes to finding work, they often struggle. Sometimes it’s a lack of confidence, sometimes its that employers are reticent to employ people they think won’t be around for long. In reality, the stats show that the average person doesn’t stay in a job longer than 3 years, and the average military posting is a similar length of time.”

Like many businesses, LifeWorks has had to adapt due to the impact of Covid-19. Since April 2020, all of their support has been delivered online, with 1-2-1 calls scheduled with individual veterans, and group video sessions to address common problems.

“It’s really important to us to make sure we are delivering safely – many veterans we support have long term health condition or anxiety, so we need to know that what we are doing won’t have a potentially negative effect on their health. That said, we’re really looking forward to delivering face-to-face again – there is something special about the connection you get when there’s a group of veterans in the room. We even had a couple who meet on LifeWorks get married recently!”

So what’s the first step if you are, or you know, a veteran who is out of work or struggling to adapt to the civilian workplace? Luckily it’s very simple. No forms, no pressure. The team have a dedicated free phone line which is manned on weekdays 8am – 5pm – just call 0800 319 6844 and have a chat! If phones aren’t your thing, then you can also email them on lifeworks@rbli.co.uk. Additionally, you can get in touch with the RBLI LifeWorks team and keep up with our regular communication via Facebook, Twitter or LinkedIn.

It could change your life. It has saved some, we know that.
In August, a new dedicated Peer Support Network for Front Line Security Workers was conceived with the launch of the ‘Guild of Security Industry Professionals’ (GoSIP).

The people behind the ground breaking security industry publication, ‘The Professional Security Officer Magazine’ (TPSO), are launching an initiative that will finally provide a voice for an estimated 400,000 front line professionals.

The new GoSIP will not only be giving a say to the legions of hard-working men and women, in ‘the shop window’ of one of the U.K.’s largest industries, it is a peer support network providing:

- massively discounted training opportunities from some of the most respected companies in the business
- career guidance
- a conduit for the views and opinions of its members
- free CPD resources
- campaigning to promote good news and stories of security industry excellence, to counter negative media and public misconceptions, in support of the Security industry initiative to change perceptions of security officers in the public domain: https://www.bsia.co.uk/blogs/81/security-industry-to-reset-perceptions-o
- a way to raise concerns at Govt and Legislative levels about the unacceptable levels of violence and aggression that security staff regularly suffer in the course of their duties
- all verified front line security operatives will be given their first 12 month’s membership free – ongoing annual registration fees will be on a sliding scale, including ongoing free memberships for colleagues in financial hardship.

The Guild is already working closely with numerous industry stakeholders, to help change perceptions, improve training standards and make a career in physical security a desirable, respected and justly rewarded vocation.

For more information visit: https://gsip.co.uk/
I am really excited to be chairing Behavioural Analysis Week Online 2020. The transition of the conference to its new online format, for this year only (hopefully!), enables more people around the globe to benefit from the content. With no quarantine periods to worry about, visas to apply for, flights or hotels to book or travel expenses to incur, the programme is now accessible to all those interested in identifying people with negative or hostile intent — through behavioural analysis.

No need to worry about which time zone you are in, whilst most sessions are scheduled within the UK’s working day, presentations will be recorded and viewable, on a password-protected platform, for a period of two weeks. Obviously delegates will have to be ‘live’ online to participate in the panel Q&A sessions, but some of these are early in the day in the UK (in order for Australasian and Asian delegates to join ‘live’ before bedtime) and others late in the UK afternoon (so those in The Americas can join ‘live’).

The original two-day conference has been spread out over four days as, however exciting the conference content is (and it is very exciting!), delegates will not wish to be glued to their computer screens all day.

So, what’s in store?
Day One: A keynote address by Prof. Paul Gill from University College London will provide a scene-setter outlining the emotional responses of hostiles when planning and preparing a hostile act. The UK government’s Defence Science and Technology Laboratory (DSTL) will then explain how the British government has been researching how behavioural analysis can contribute to the security of different environments.

Three different sectors will set out how they have utilised behavioural analysis techniques to protect their patrons and infrastructure, including Senedd Cymru (Welsh Parliament) and the former Head of Security for the European Broadcasting Union considering it from a major events perspective — notably the Eurovision Song Contest.

After lunch we’ll put behavioural analysis in the spotlight and provide a scientific panorama of non-verbal behaviour and explore what we can really identify in people’s non-verbal communication and set out what science can tell us about the link between non-verbal behaviours and the security threat a person might pose. We will then ask, and answer, the question whether Pinocchio’s nose actually exists; there are, after all, a multitude of myths that need to be dispelled in the area of deception detection.
We end day one with one of our conference highlights and a keynote address from Dr. David Matsumoto, Professor of Psychology at San Francisco State University & CEO of Humintell. Dr. Matsumoto is one of the most highly regarded experts in the fields of emotion, non-verbal behaviour, deception, and culture, having produced over 400 academic works, including books, articles, book chapters, and conference presentations on the subject.

Day Two: We address the subject of the ‘halo effect’, blending theory with an operational perspective by considering the challenges faced in training border guards to avoid stereotyping and appreciate that good looking people and women can also be threats! The conversation then moves on to discuss deviant behaviour, highlighting cultural-, gender-, and age-based perceptions and how they are addressed in the operational context of the Metro in Russia. And we explain the development of intelligence-based human profiling, the importance of memory, observation and recognition.

The day concludes tackling the challenging subject of suicidal terrorism. Our speakers will attempt to take us inside the mind of a suicide bomber and consider what behaviours they might exhibit, as well as the minds of those trying to understand the motivations and mindsets of suicidal terrorists. But it’s all very well considering suicidal terrorism from an academic viewpoint; in any security operation, staff need to know how to respond should they suspect a suicide bomber be about to attack. That action requires management buy-in and our final speaker presents his thoughts on drafting the requisite operational protocols and countermeasures and how staff should be supported when they make the decision to intervene.

Day Three: Airports have been at the forefront of discussions regarding the use of behavioural analysis as a tool for passenger screening. So, we have a one-off presentation entitled Towards Unpredictability in Airport Screening; should we all be treated the same?

Thereafter, we move away from the world of counterterrorism and into the sphere of mental health. After all, security is about preventing any unlawful act, whatever the motivation or cause. With mental health-related problems increasing, security professionals need to have a much better understanding of the types of behaviours which might be exhibited and know how to protect both the operational environment and the suspect themselves from harm.

Security is therefore not just an issue for the densely populated conurbations of the world; it’s a challenge at every venue in every state. With this in mind, we are thrilled and privileged to welcome Greenland’s Minister of Finance, Vittus Qujaukitsoq, to outline Greenland’s security dilemmas in our third keynote address. Greenland, despite its relative isolation, and only having a population of 55,000, is not immune to security challenges, many of which can be addressed by the implementation of behavioural analysis. As baseline expectations are much easier to quantify in smaller communities, it’s an ideal environment to trust humans more than machines.
Minister Qujaukitsoq’s keynote precedes three presentations examining mental health-related challenges, starting by considering suicide, specifically identifying those with suicidal intent in public places. We then go on to discuss stalkers and the associated behavioural indicators of the fixated. After all, sports stadia, concert venues, red carpet event theatres, beauty pageants, political rallies and all locations which attract celebrity visitors, politicians and performers have to protect themselves not only from the actions of those who wish to enter without a ticket, but also from those individuals who have the right of entry but who have negative intent due to excessive adulation for an individual or, worse still, a desire to target somebody in particular. And we conclude with an operational perspective on responding to the increasing frequency of ‘upskirting’. Our speaker from the British Transport Police’s VISOR Unit, looks at such sexually deviant behaviour, along with the activities of frotteurs who are active on mass transportation networks around the world.

Behavioural analysis is usually left to humans, but technology is likely to play an increasingly important role in automating hostile intent detection. We end the day with a session on technology and how we might use technology to decrease risk in crowded places. Academic presentations include one looking at the way CCTV can be used to identify shoplifters, and another explaining how head vibration analysis is already enhancing airport security. But behavioural analysis need not just be on the day of the attack. Before their attacks, many perpetrators have published their intentions, justifications, or ideology in writing either via letters, online diaries, forum posts, or manifestos, hence we conclude with a demonstration of a profile risk assessment tool that can be used to analyse and assess the risk in written communication.

Day Four: The final day covers insider threats, online threats and creating the right operational mindset to facilitate effective threat detection through behavioural analysis. Presentations cover holistic insider threat management, insider threat detection within the airport community, and the ways in which linguistic indicators can also aid in the detection of insider deception.

The online behavioural analysis session examines online radicalisation and how such people behave in their online communication. The second paper looks at online addictive behaviours, and offline suspicious signs that might indicate somebody has become addicted. As society becomes ever more interconnected online, so do the risks to vulnerable individuals increase. Those who have addictions, such as to online betting/gambling, pornography and webcam-based sex or even to the ‘excessive’ use of social media platforms or online shopping, can end up in financial debt, let alone suffer from mental health-related problems. Those who end up being trafficked into domestic servitude, slavery, organ donation or the sex industry often commence their journeys online. Isolation can lead to radicalisation, sexting can lead to cyberbullying and online imagery can impact self-esteem.

Security is usually about prevention, but an ability to respond effectively in the aftermath of an attack is equally important. All contingency plans include sections on liaising with the press and media, but we must also develop competency in managing ‘fake news’ which can be rife in the aftermath of an attack. We explore contingency planning and the use of behavioural analysis to distinguish between fact and fiction should an event occur.

Behavioural Analysis Week Online 2020 ends with three operational perspectives: the project manager for the behaviour detection programme at Belgium’s Federal Judicial Police focusing on their programme’s history, structure, selection of trainers, training approach and course content, specifically addressing how they ensure objectivity and prevent discrimination on grounds of ethnicity, gender or age.

Human trafficking is the third most lucrative criminal activity in the world and a subject the hospitality industry is keen to address. Our presenter explains how Hilton hotels ensure security buy-in from personnel whose primary role is customer service or safety. Hotel receptionists are now being trained to identify victims of trafficking, and the traffickers themselves, whilst room cleaners and taxi drivers are also being encouraged to report unusual activity. And, finally, Virgin Atlantic explain how their aircrew are trained to use behavioural detection techniques during boarding to identify not only intoxicated revellers but also victims of human trafficking and, in the worst-case scenario, potential terrorists.
Global MSC Security has announced that entries are now being accepted for the 2021 Gordon McLanaghan Award, which recognises an individual, project team or organisation that has gone above and beyond, to achieve a technical security solution.

Now in its eigth year, the free-to-enter award is managed by Global MSC Security and is judged by an independent panel of respected UK security practitioners. The panel look for compelling evidence of innovation and the impact that a technical security solution has had in solving a specific issue. The prestigious award is presented in memory of Gordon McLanaghan, an innovator within the Bristol City Council CCTV and Emergency Control Centre, who sadly passed away in 2014. The previous winners of the Gordon McLanaghan award are:

2019 - Dyfed Powys Police
2018 - Cornwall Fire and Rescue
2017 - Cumbria Constabulary
2016 - Gloucester City Council
2015 - Jim Guiton, Dacorum Borough Council
2014 - Safer Communities Glasgow

The Managing Director of Global MSC Security, Derek Maltby, states: “The Gordon McLanaghan Award is open to any organisation in the UK, that has implemented a truly innovative technical security solution in the past 12 months. Since we launched the award in 2014, it has been dominated by some truly inspiring and successful projects undertaken in the UK public sector.” Maltby adds: “The award is truly agnostic, so if you have a solution that has set a benchmark, or has been delivered in a new and creative way in the private or public arena, we encourage you to enter this year.”

The Gordon McLanaghan Award 2021 is free to enter and more information including how to submit can be found here. The deadline for entries is Friday 29th January 2021.

About Global MSC Security
Global MSC Security's independent advice, knowledge of security technology, deployment, funding and audit is trusted by public bodies, like Thames Valley, Dorset and Dyfed Powys Police, Sutton Safer Partnership Service, Barnet and Merton Councils, Traffic Wales, Bristol City and Dorset Council, Wycombe, Chiltern and Aylesbury Vale District Councils, the Universities of Queen Mary's, Bristol and the West of England and by private companies, such as DAS Insurers and The Prudential, as well as by private individuals with valuable properties to protect.

MSC delivers the best possible results for an organisations security investment. The combination of its law enforcement, architectural, engineering and IT backgrounds and many years of working with organisations, means MSC provides the right integrated security solutions at the most effective possible price.
A Reliable Security Process: The CARVER Methodology
by Luke Bencie

As the father of modern-day automotive processes and measurement standards, W. Edwards Deming (the American management consultant who helped build Japan’s auto industry after World War II) famously stated, “If you can’t describe what you are doing as a process, you don’t know what you’re doing.” In the security industry, there are many processes which contribute to an effective security strategy. One of the most trusted of them is the CARVER Target Analysis and Vulnerability Assessment Methodology.

Developed during World War II, CARVER (then one letter shorter and known as CARVE) was originally used by analysts to determine where bomber pilots could most effectively drop their munitions on enemy targets. During the early 1970’s, the Central Intelligence Agency (CIA) repackaged CARVE into CARVER, as a means for predicting where terrorists might strike against American targets overseas. Following the events of September 11th, 2001, CARVER has entered the mainstream private security market, as the go-to critical infrastructure protection assessment model.

One of the many beautiful things about CARVER is its ability to lay concepts out in a logical sequence. The CARVER Target Analysis and Vulnerability Assessment Methodology is a system which uses specific procedures, that are both qualitative and quantitative in nature, to interpret and determine the Probability of Attack (Pa) from an adversary against critical infrastructure assets and/or key resources. It can be both offensive and defensive, meaning it can be used for identifying your competitors’ weaknesses and for internal auditing.

To clarify, CARVER is an acronym, which stands for:

- **Criticality** – identify critical systems and points of failure
- **Accessibility** – determine the ease of access
- **Recoverability** – the time and effort taken to recover from an adverse event
- **Vulnerability** – system effectiveness vs. adversary capability
- **Effect** – scope and magnitude of adverse consequences that would result from malicious actions and responses to them
- **Recognizability** – evaluate likelihood that potential adversaries would recognize the asset as a critical or valuable target

To use CARVER — whether you’re assessing a system, a facility, or some other component of a critical infrastructure — you assign scores from 1 to 5 (with 5 being “most essential,” “most likely,” and so on) for each of the six criteria above. The sum of the six scores is the total score for whatever you’re assessing. Once you’ve calculated the total scores for various assets, you can compare them. For example, you could use CARVER to compare two vulnerable assets within an organization to determine which is more susceptible to attack. Whichever has the higher score is probably where you would want to divert resources and offer protection.

The important thing to remember is that this exercise is conducted to identify, categorize, and prioritize high-risk assets; to assess vulnerabilities; and to make recommendations around risk.

Once a CARVER assessment has been completed, and material risks and threats have been identified, security and risk management professionals can determine the best approach to take. Even the smallest difference in CARVER scores could influence whether an organization opens up a facility in a certain “hostile” region of the world, or how they might allocate their security budget for the coming year. Because it is based upon common sense, as well as numeric values, it serves as an excellent decision-making tool for managers.

Let’s face it, subjectivity regarding threats are all too common in today’s security environment. Opinions — which are determined in large-part by the individual assessor’s personal experience — can complicate a threat analysis matrix more than actual fact. By implementing a time-tested process like the CARVER Methodology, security professionals can more easily explain threats and how to mitigate them.

To learn more about the CARVER methodology and become a Certified CARVER Assessment Professional (CCAP), please visit www.smiconsultancy.com.
With what could be argued as the most important enabler of wider society, the word Security by definition and in practice, is one of the most rewarding fields to be involved in.

If women in security is still a rarity, what changes need to be done? Security is a broad concept containing strength and physical capabilities, but it also involves and requires leadership, strategic thinking, courage, commitment, trust, networking and more. Of course, these qualities and skills can be found in any gender and apply to many other industries - growth and development can be best achieved by eliminating gender-based limitations and differentiations.

The two authors, Alessandra and Anas, started with a genuine aspiration to protect society, understand crime, its origins and how to tackle it. They decided to pursue their education, professionalising their position and truly testing how the learned theories can be put into practice.

Despite different backgrounds, upbringing and histories, their paths met at some point, they shared workplace for a short while, they uniquely managed to gain and build relationships with the same mentors along the way. Great male role models [who] have always supported them, pushing them to become better, giving the conviction to go the extra mile, but naturally, have never fully understood why and when, they were underestimated purely from just being women.

Benefits of Women in Security
Women have a greater ability to multitask, which of course assists in any sector (Stoet et al, 2013). Indeed, we believe that the bigger advantage is women's problem-solving skills in the world of security, when real-time performances must be greater than in other fields. The on-the-spot decisions, agility in changing resources and managing expectations can solve some of the most difficult situations. A woman will rely on her ability to defuse a situation, rather than strength as a first response.

The ‘natural instinct’ or ‘having a feeling’ are simply intangible benefits that come with hiring a woman, they simply are able to sense when a colleague is not happy or is feeling uncomfortable, or unable to speak up. This is not saying men don’t hold emotional intelligence, but this is a trait that is more embedded in the makeup of a woman. Differences should be celebrated, but be treated as equals. Since the quality of strength is often related to men and celebrated in security, the feminine touch needs to be taken into consideration as part of the business growth strategy and the needed change in the industry.

Society as a whole is experiencing uncertainty and unpreparedness when facing the COVID-19 crisis. In no other situation has mental strength, support and empathy been so necessary. It is through this willingness to communicate (in the day and age of increased technological advancement, a skill still lacking) and receiving feedback, contributing to problem solving and risk management, that productivity can be improved. Women possess greater purchasing power based on the uniqueness they add to this industry.

Empowering women in the industry can lead to a better organisation that benefits from women's skill-based differences and embraces women’s unique drive to achieve in the workforce.
Leadership

Diversity in the workplace continues to be the forefront discussion for many industries. Gender equality does not only mean a level playing field and equal pay but inspiring a future generation by showing women in senior positions. Whilst admittedly more women are moving into the field, particularly within cyber security, physical security still lacks women leaders.

Until this day, the feeling of imposter syndrome is ingrained in many women in security, having heard often, many who find it difficult to either explain their jobs, roles or even having to justify their C-suite position. Both women have experienced this within their roles, through both leading male dominated teams and managing projects. They have both learnt that they are enough and more, where in fact it's more about becoming a dedicated leader (rather than a man or woman). In doing this you can lead successful teams with no fear or regret. Many women use the fact that people underestimate them, purely for being a woman, as a chance to shine and to not only prove equality but to showcase that gender doesn't play a role. Leadership is about bringing and keeping people together through trust and conviction.

The great thing about the security industry is that professionals are not competing with each other, aiming to build a new landscape together in order to deliver the best service, inclusive of all genders and differences, creating a community of professionals who are always aspiring to shape the industry to make it relevant to all agendas.

Future

It is great to see that security is now being recognised through professional bodies including the ISRM, and qualifications are increasing amongst some of the world’s top universities.

Anas and Alessandra hope to see an understanding for the genuine positive change that women can bring to security industry board rooms, raising standards and professionalising the field so that it is desirable to all future generations.

Women in security is still a rarity and there is the need to rebalance the scales shaping the industry in a way that can benefit from different approaches, skills, qualities and differences between the genders. The rebalance of gender inequality will bring a real reflection of society into the industry and will allow both men and women, to work together to protect and inspire. Only through a balanced combination of all gender identities in the security industry a better organisation can be achieved.
Introducing the newest Corporate Partners

Carlisle Security Services

With over thirty years’ successful trading history, Carlisle Support Services are very proud to be one of the UK’s leading specialist suppliers of value-added solutions. From our central headquarters based in Luton, Bedfordshire, we deploy more than 3,500 operatives weekly to perform Security, Stewarding, Cleaning and Merchandising services. It is with great pride that we work with some of the UK’s leading businesses and recognise wholly the role we play in supporting and enhancing their operations and brands.

Find out more about our Corporate Partner Carlisle Support Services on their website: www.carlislesupportservices.com

Fastline

Fastline Steel Services UK Ltd are proud to offer a unique service in the perimeter security market. They have year after year, consistently implemented procedural improvements which have helped them grow organically and become the UK’s leading manufacturer of steel perimeter systems. Their current annual turnover is quickly approaching £15,000,000 and they continually invest in their processes, equipment and their team. Operating from their manufacturing facility in Wolverhampton, they have their Head Office in the same location and 3 other regional offices, ensuring good National coverage.

Find out more about our Corporate Partner Fastline Steel Services on their website: www.fastlinesteel.co.uk
Minimal Risk Consultancy

Minimal Risk Consultancy (MRC) are specialists in risk consultancy and project management within the security sector. MRC focuses on personal service, sound analysis and implementation, together with rapid, cost-effective delivery. Their support clients ranging from government and corporate bodies through to small businesses and high net worth individuals. MRC's consultancy services include reviews and advice on the protection of organisations' people and assets with the generation of effective business solutions through; analysis, audits, surveys and operational procedures. The company offers pre-entry studies, geo-political analysis and independent reviews of existing services and systems including design and planning.

Read more about our Corporate Partner, Minimal Risk Consultancy Limited on their website: www.minimalrisk.co.uk

Zitko Consulting

Zitko Consulting are a fire and security specialist dedicated to creating long-lasting relationships through high quality recruitment. They believe that the best way to recruit is an approach based on strong foundations, and principles that are transparent and honest. Zitko aim for quality and deliver excellence. They strive to build partnerships, co-dependence and trust.

They're confident that our customers benefit from a highly tailored service that saves time and money and greatly improves the hiring process. Zitko Consulting is a growing, ambitious business striving to be the number one recruiter in its field - their consultants are trained to understand every aspect of the security and fire sectors.

Read more about our Corporate Partner, Zitko on their website: www.zitko.co.uk
Our Corporate Partners
BECOME A CORPORATE PARTNER OF BRITAIN’S LEADING ORGANISATION FOR SECURITY PROFESSIONALS

Help us in our work to deliver quality to the sector, value to organisations and confidence to society

IF YOU AGREE WITH THESE STATEMENTS THEN CORPORATE PARTNERSHIP IS FOR YOUR ORGANISATION

- We support the Professional Security Community
- We are committed to professional excellence in Security Practice
- We stand committed to Continuing Professional Development for all our security personnel
- We support the development and implementation of professional standards across the security sector
- We support the mission of the Security Institute to ensure that security professionals are recognised as being of equal standing to professionals in all other categories within modern organisations

BENEFITS OF BECOMING A CORPORATE PARTNER OF THE SECURITY INSTITUTE

- Use of the exclusive Corporate Partner logo on your website and company stationary
- Presentation of Corporate Partner certificate
- Confirmation of your Corporate Partner status added to the SyI membership and wider network
- Inclusion in the Corporate Partner Showcase on the SyI website, including dedicated space in the Virtual Exhibition Area
- Affiliate memberships and further discounts on additional applications
- Exclusive opportunity to take part in knowledge-generation and sharing activities and projects
- Promotion at Security Institute events, and discounts for bookings
- Discounts on Security Institute Qualifications
- Copies of bulletins, newsletters and press information from the Security Institute
- Advanced access to sponsorship and exhibition opportunities

THE SECURITY INSTITUTE
1 The Courtyard, Caldecote, Warks, CV10 0AS
024 7634 6464
info@security-institute.org
www.security-institute.org

security-institute.org

I WANT TO BECOME A CORPORATE PARTNER, WHAT NEXT?

A Corporate Partnership application comprises;

- Completed Corporate Partnership Application Form
- Details of the proposed Affiliate Members
- Payment of the appropriate fee – an invoice can be requested

The Security Institute will complete company checks and take up references, and may request further supporting information depending on the outcome of the background checks.

Once completed, the Security Institute will confirm the Date of Appointment as a Corporate Partner, prepare a Certificate of Appointment and complete appointment activity.

It is anticipated that the application process will take 6 – 8 weeks.

The proposed Affiliate Members will be reviewed by the Validation Board in line with standard operating procedure, and receive individual confirmation of membership.

WHAT CATEGORY OF CORPORATE PARTNERSHIP IS RIGHT FOR YOUR ORGANISATION?

There are three different levels of Partnership - Large, Medium and Small, determined by the number of employees working in Security within your organisation. All will receive the same benefits from Corporate Partnership.

Corporate Partners have bundles of memberships included in their agreement with us. If a Corporate Partner already employs Security Institute Members of any grade, these can be included as part of the CP bundle – members will retain their existing grade of membership. Every new person joining the Security Institute as part of a Corporate Partner bundle will be processed at the Affiliate level of individual membership. Each will receive correspondence confirming their Affiliate membership and access to a large range of member benefits offered by the Security Institute.
At the beginning of lockdown a group of IT and cyber security specialists decided it would be good idea to put something together to keep children being freshly homeschooled busy for a while and help parents. The result was a weeklong (plus a bit) project of rapidly assembling YouTube content, learning lessons as they went, and some interesting discoveries about engaging children in security.

While we all worked together to design and produce the content, it was largely independent in different topic areas, with sessions covering encryption, threat modelling, OSINT, and basic ethical hacking tools. We learned very quickly that targeting content at age groups simply did not work – initially I was told by a wide range of people that encryption was too tough for the younger children, an argument that lasted until a ten year old recorded a video of her own demonstrating how the original Engima machine worked and started encrypting and decrypting messages with it.

A social engineering class for a fictional chocolate factory led to a vast number of chocolate chip cookies being baked and shared on Twitter after some social media analysis and lateral thinking to get to secret recipes.

Ethical hacking sessions were predictably popular, but what surprised me was the popularity of stay safe online, threat modelling, and smart cities sessions being comparable.

Responses were fascinating – often around the idea that none of these were things students were exposed to in school. It was mentioned that the cryptography lessons covered material most people didn't encounter until university, while ten year olds were eager and able to not only learn and use it, but to learn more.

More interestingly, many adults were enthusiastic about the content and excited to be watching with their kids (or in some cases on their own) and learning about areas they had never been exposed to before.

As well as learning various technologies to help build this sort of content, and about general pedagogical principles (I picked the brains of a large number of teacher acquaintances to help), the key takeaway for me was that children are genuinely interested in and enthused by security when given the chance to explore it. I've seen this before when doing lockpicking workshops in schools, presentations on cyber security to college students, and others, but this was the largest audience I've come across for this type of learning and by far one of the most enthusiastic.

The question then is whether there is a way to make use of this and keep that enthusiasm going – there are a lot of programmes to do similar with STEM subjects, and in security we should look at and learn from these to allow children to understand that it is a career path that is open and available to them, and begin cultivating their curiosity and skillset as early as possible.

The project has not come to an end, as it did take up a lot of time and there's content being put out by much better resourced full-time bodies such as the BBC. Sadly none of this content really covers the same subjects, instead being focused on the classical curriculum, and from what I learned in the Cyber School project this is a massive missed opportunity.
In Greek Mythology, Soteria was the Goddess of Intelligence and Safety... today, a new “virtual” SOTERIA is protecting critical infrastructure and key assets...

**INTRODUCING:**


**PROBLEM:**

Security vulnerability assessments are tedious, utilize time-consuming paper checklists, provide non-standardization, subjectivity to the assessor’s experience level, and only provide a snap-shot in time for the asset or facility being threatened.

**SOLUTION:**

In 2020, the SOTERIA mobile collection device and data management platform will finally resolve these decades-long vulnerability assessment challenges.

**SOTERIA** is an innovative risk and vulnerability assessment software system for security and intelligence organizations that uses an iOS and Android based mobile app for security assessors. Mobile app provides a step by step process for performing a vulnerability assessment using the CARVER Methodology. Web-based program management platform provides Chief Security Officers with the ability to track/monitor their organization’s critical assets vulnerabilities and global facilities in real-time via one dashboard.

Based upon the CIA’s **CARVER Target Analysis and Vulnerability Assessment Methodology**, SOTERIA provides both practical qualitative and quantitative results, allowing for greater accuracy and consistency across assets and facilities.

FOR MORE INFORMATION, VISIT: [WWW.SOTERIAPRO.COM](http://WWW.SOTERIAPRO.COM) The Security Institute Members will be provided SOTERIA discounted rates.
Security Convergence – A Cybersecurity Viewpoint
by Andy Smith CSyP FSyI

Across the Security Institute and indeed across the wider security communities, one concept keeps popping up; that of Security Convergence. This is something I have been dealing with for a while. In some ways its a paradigm shift in the way we work.

When everyone worked in the office and Information and Communications Technology (ICT) was the realm of the IT department, it was easy to draw a boundary around the ICT and the company information. You did not need to trust your people that much (though most did), physical security was with facilities or corporate security and consisted of badges and gates to get into the building. Even some aspects of IT security were with facilities, such as printers and photocopiers. Personnel security was with HR and nothing the CISO need concern themself with.

Only 20 years ago, you sat in front of a desktop in the office, did your work and went home. All the data was nicely squirreled away in servers in your corporate data centre or back office. To get at the data, miscreants had to physically enter your building and take copies.

Enter the modern world. Cloud computing, outsourcing everything, working from home, the Internet of Things; the result being, your data everywhere. Now you have to trust your people completely, the physical security is with the cloud providers and with your users with their various computer devices. No longer are computers desktops in the office, they range from workstations through laptops, tablets, phones, et cetera; including Bring Your Own Devices (BYOD), where staff can use their own phones and tablets for work. Your data can be anywhere on any device.

So what does this mean. Well it means you cannot draw a nice neat line around the company ICT, you may not even own all the ICT with Cloud and BYOD becoming commonplace. It may not just be BYOD, it may be a corporate laptop from KPMG, Accenture, Deloitte et al, doing work for your company but using their corporate devices.

Convergence is where everything comes together; the personnel security, physical security and technical security. You have to trust your people and not treat them like sheep. This means ensuring you can trust them in the first place, so you have to corroborate that trust at the outset more effectively with background checks and identity checks. Without that foundation of trust, all bets are off.

Access to company data is then not about where you are, but who you are. Access Control becomes the new boundary and therefore passwords and other static credentials have to become a thing of the past, with multi-factor authentication such as biometrics, tokens and one-time passwords becoming critical. In many cases, the access control is your only line of defence. Now you are not trusting the IT to protect the data, you are trusting the User, thus technical and personnel security has converged.

The physical security actually morphs into protecting the data wherever it travels, using concepts such as encryption rather than tin and string. For example, you can encrypt the data as a blob, so you do not care where it goes or where it is stored, you just have to protect the encryption keys, which you control and which are linked to access control.
The data is stored in the cloud and on various devices. With people working at home, in hotels and generally anywhere, the physical security of the devices is also with the User, so physical security has also converged with the technical and personnel.

It's all with the User and security suddenly becomes a matter of trust rather than walls and doors. Hence with a converged paradigm of security there is a need to trust your users, but in doing so, use the well-known principles of ‘need to know’ and ‘least privilege’ to help retain some semblance of control.

However relying on access control mechanisms has advantages, it means that when someone leaves the company, you can revoke the credentials and encryption keys and any company data they have on their phone or other devices is effectively rendered useless. No more physical boundary, now it's a virtual boundary but you still have control.

Looking from a different perspective, physical security is still very much a critical aspect, but now it is about protecting the offices and cloud data centres as physical assets, more than the information. However in the case of cloud computing, all of the servers have to be stored somewhere and these can be massive, highly critical data centres, supporting thousands of customers, hence availability becomes much more of a requirement than confidentiality and that comes down to preventing denial of service attacks on the data centres.

But even in the realms of physical security, staff now have to use computers for most things. CCTV, alarms, intrusion detection systems (IDS) all use Internet Protocol (IP) networks. Gone are the separate coax and phone networks. Welcome to the Internet of Things (IoT), where everything is connected to the Internet, be it your phone or the corporate CCTV.

Now you can sit in your SOC in London and watch real-time the CCTV in your Dublin data centre in high-quality HD. The video may no longer be stored on-site either, but entrusted to a large cloud provider such as Amazon Web Services where it's really cheap to store data for a long time and you can get at it from anywhere, anytime. It also stops miscreants stealing the tapes.

It does not matter what sort of company you are, even if your an accountant or recycling firm, the chances are your IT is outsourced or you use Internet-based services for your office work. That maybe email and Internet browsing or may even extend to providing services via your website. The chances are your security and risk management is converging and you just have not noticed.

There is no getting away from the fact that there is no longer a physical boundary around any company, staff are not assets they are a trusted part of the ecosystem and ICT is pervasive both in business life and home life.

Convergence will mean those who are specialists in specific areas will need to at least understand the basics of the others. It will also see the separate aspects of security gradually merge in larger companies, usually under the CISO. One of the key benefits of the Security Institute is that peers across a whole spectrum of specialised skills can learn from each other and support our journey to converged security.
Alongside the five core competency skills required for Chartered Security Professionals (security knowledge, practical application, communications, leadership and professional commitment) there is an over-arching requirement to be acting in a strategic manner. We are often asked what we mean by strategic impact, that “magic ingredient” we are looking for in all of our chartered security professionals. What is it and how do you prove it?

The dictionary definition of strategic is: Adjective - relating to the identification of long-term or overall aims and interests and the means of achieving them.
“the company should take strategic actions to cope with fundamental changes in the environment”
Synonyms: planned, calculated, deliberate, tactical, politic, judicious, prudent, clever, shrewd, well thought out

It seems clear therefore that the qualities we are looking for in an applicant is the ability to understand the current issues/situation and effectively plan for dealing with the challenges ahead. A Chartered Security Professional is someone who has ideas, can turn them into well thought-out and developed solutions, and will be at the forefront of driving those solutions forward. They are people who search out their own solutions, not just implementing instructions from their line manager. So do you have to be a Director or Head of a business to be working strategically? Not at all. We’re looking for people who within the role that they have can demonstrate they bring strategic thinking and delivery to the work that they do.
We are looking for leaders, not followers. And when we say leaders, we don’t necessarily mean those who have teams under them, but people who are thought leaders, influencers, someone you would trust to give you the right solution.

This doesn’t necessarily come with age, but it certainly comes with experience, which is why all Chartered Security Professionals need to show they have been working strategically for at least two years before they apply (for graduates) or for at least five years (for non-graduates).
If you are that person who is driving security forward in your day job, then surely you should be aiming to apply to the Register of Chartered Security Professionals.

Chartered Security Professionals - Leaders not Followers. This is why so many of the Security Institute’s Boards, Committees and Special Interest Groups are led by CSyPs.

Chartered Security Professionals ~ making a difference.
CSyP Application Workshop Webinars

We are running our CSyP Application Workshops as webinars that prospective CSyPs could attend from the safety and comfort of their own home. Now due to exceptional demand, we have opened booking until the end of the year with Workshop webinars every two weeks.

Joining one of these webinar workshops will help you learn the best way to complete and submit your application so that the admittance process is as easy as possible for you and us.
- Learn about the steps your application will follow
- Gain a good understanding of the competencies we are looking for
- What you should and shouldn’t put on your Application Form
- Meet Interview Assessors and hear practice questions

These are all interactive workshops, where you will be able to receive one to one advice on making a successful application to the Register. Applicants are encouraged to bring copies of qualification and training certificates / letters of support / examples of work etc. to discuss with the assessors and administrators. After attending one of these webinar workshops you should feel confident to complete your application, and have a better understanding of the application process and timescales, and what CSyP can do for you.

To allow for a detailed discussion with each attendee, places for each webinar workshop are limited to 12 people.

Attendees of these CSyP webinar workshops will also earn 3 formal CPD points.

You can book your space and find further details here:

We have also launched two special International CSyP Application Workshop Webinars, see details below.

**CSyP Workshop Webinar: The Americas**

September 17th at 17:00 - 18:30 BST
Due to exceptional demand, we are happy to present a special CSyP International Application Workshop Webinar for security professionals based in America, Canada and the wider geographical region. Book here: https://event.bookitbee.com/28746/170920-csyp-application-workshop

**CSyP Workshop Webinar: The Middle East, Asia & Australasia**

October 15th at 08:00 - 09:30 BST
Due to exceptional demand, we are happy to present a special CSyP International Application Workshop Webinar for security professionals based in the Middle East, Asia and Australasia region. We ask if you are able to attend one of our usual sessions at 14:30 that you please allow this opportunity for International security professionals to find out about Chartership. Book here: https://event.bookitbee.com/28748/151020-csyp-application-workshop
Jennifer Ciolfi CSyP
Regional Physical Security Manager

I never planned to make a career out of being a security officer. As a matter of fact, I tried to become almost anything else. I tried nursing and psychology and even pursued a college diploma in Emergency Telecommunications, however nothing seemed to fit right and during all this time I kept working in the Security field, and I kept enjoying it.

Much to my personal chagrin, not only did I find that I significantly enjoyed the work, but also that I was fairly successful at it. I was granted the promotions that I applied for and I was lucky enough to encounter some very instrumental people who became mentors to me in different fields of Security. I was given the opportunity to train to become a trainer and instructor, a job which I still enjoy immensely whenever I get the opportunity to engage. I was taught security systems by a manager who insisted that you could never learn to create a security system strategy without understanding the hardware, the software, the programming and how it all tied together. And I grew to learn from an excellent branch manager the importance of business, business strategy, financial planning and management, and large-scale organizational strategies.

These mentors played the largest role in my growth within the security field. Beyond supporting and encouraging me, they nurtured my love for the industry by allowing me to continue to grow and explore new and excitingly different fields in the industry.

I’ve had the opportunity to build and grown my own program at different organizations. I’ve been a part of large-scale multi-million dollar construction and redevelopment projects and have been able to work in several different countries and visit several more through work. But the single most amazing experience of my security experience to date has been the opportunity to provide guidance and mentorship to others.

I have recently completed a Master’s degree in International Security and Risk Management and am now pursuing a second Master’s degree in Terrorism and Political Violence. This formal education has helped professionalize all the experiential education that I spent the last 20 years accumulating.

The pursuit and achievement of the Chartered Security Professional certification marks a significant point of recognition of the hard work and effort that I have invested in the Security industry. More than just a recognition of achievement, this is an announcement of rededication. One of the most appealing aspects of this credential is the requirement for continuous learning and growth. As the CSyP designation becomes more popular and recognized globally, the appeal of the designation to employers should be, most importantly, the understanding of the dedication and commitment of the Chartered Security Professional to not only be aware of and experienced in best industry practices but also an inclusion in the creation of those standards and a requirement to stay on the leading edge of the industry.

The Register of Chartered Security Professionals will hopefully give me access to a whole new suite of peers and potential mentors. As an advocate for continual growth and learning, I’m excited about the opportunity to learn from new people. I’d like to believe I’m only half-way through my career with a large cache of undiscovered opportunities ahead of me. I’d like to see myself as the Head of a Global program. I’d like to see myself advising National and International policy makers who can impact safety and security worldwide. I’d like to believe that I’ve only just begun to make my mark on the global security industry.
Obtaining Chartered Security status has been a real achievement. Having spent almost 20 years in the security sector I was keen to quantify my experience in some way. The CSyP is a credible and prestigious standard and once achieved, ensures that individuals continue to represent the highest standards and ongoing proficiency within the security industry. The career that has led me to the CSyP has been varied; the majority of which has been based outside of the UK.

During a 9-year military career as an officer in the Light Infantry/Rifles, I took part in military operations in Iraq and Kosovo and also served in the UK, Central America, the Falklands, Africa and South East Asia. On retiring from the military, I embarked on developing my security knowledge and broadening my communication skills by spending a year in Yemen as a security manager for a mining company, operating in a complex tribal environment. Subsequent to this, I moved to the corporate setting of Etihad Airways in Abu Dhabi where I took on the role of Senior Manager for Corporate Security before moving on to be part of Etihad’s Senior Management Team; there I was responsible for airline operations and security in Abu Dhabi Airport – a role which offered a plethora of hands on practice of corporate security and particularly allowed for developing leadership in others. In this latter role I led, managed and developed a team operating the Middle East region’s first US Pre-Clearance Immigration Facility, working closely with US Department of Homeland Security and local UAE customs and law enforcement.

I joined my current company, Boeing, in July 2016 as a Regional Security Advisor for the India, Middle East & Africa Region based in Abu Dhabi, United Arab Emirates. This role allowed me to pull together the skills of leadership, security knowledge and communication within this varied and dynamic region. Additionally, I became the focal for Boeing’s High Risk Travel program, working on a global scale and at all levels, enabling me to further develop communication skills and look for new opportunities for efficiency and streamlining. I was also selected to be on the steering committee of the OSAC African Regional Council – a post that I still hold. I have recently relocated back to the UK from the UAE and now work within a small core team for Boeing International Security where I am responsible for global governance and operations.

My decision to embark on reaching Chartered status was ignited by a desire to pull together the different strands from my career and to quantify and recognize the experience that I have. Continued Professional Development is something that all of us should focus on. Becoming a Chartered Security Professional is a huge step, particularly in an industry where compliance, qualifications and standards are becoming ever-more important. The application process, although slightly daunting at the start, was an excellent opportunity to go through my career to date and to calibrate my achievements with the core competencies required for membership. I felt a great sense of achievement in gaining my CSyP and I look forward to helping others to become accredited. I strongly advocate the process and encourage fellow security professionals, either UK or internationally based, to apply.
Upcoming Events

**Syl Golf Day**  
**Thursday 24th September 2020**  
Time: 10am - 6pm  
Venue: Pine Ridge Golf Club, Old Bisley Road, Frimley, Camberley, Surrey, GU16 9NX

A perfect way to meet other members for a relaxed (if not competitive) day of golf, feel free to book your own team of 4 but don’t worry if you don’t know anyone we will create the teams. Pine Ridge Golf Club has 18-holes and was opened in 1993, the course winds through gently undulating pine forest, on sandy soil that drains superbly, enabling us to keep the course in excellent playing condition all year round.

Book here: https://event.bookitbee.com/29300/240920-syi-golf-day

---

**Syl Virtual Annual Conference Week**  
**Monday 19th October - Friday 23rd October**  
Time: Webinars everyday at 10:00 and 15:00  
Venue: Online

A perfect way to meet other members for a relaxed (if not competitive) day of golf, feel free to book your own team of 4 but don’t worry if you don’t know anyone we will create the teams. Pine Ridge Golf Club has 18-holes and was opened in 1993, the course winds through gently undulating pine forest, on sandy soil that drains superbly, enabling us to keep the course in excellent playing condition all year round.

Book here: https://event.bookitbee.com/29300/240920-syi-golf-day
## Other Upcoming Events

Industry events, exhibitions and conferences to keep noted

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Place</th>
</tr>
</thead>
<tbody>
<tr>
<td>5th November</td>
<td>ST20</td>
<td>London</td>
</tr>
<tr>
<td>24th November</td>
<td>ST20</td>
<td>Glasgow</td>
</tr>
<tr>
<td>25th November</td>
<td>Security and Fire Excellence Awards</td>
<td>London</td>
</tr>
<tr>
<td>19th January</td>
<td>ST20</td>
<td>Manchester</td>
</tr>
<tr>
<td>24th - 26th January</td>
<td>Intersec</td>
<td>Dubai</td>
</tr>
<tr>
<td>10th February</td>
<td>Women in Security Awards</td>
<td>London</td>
</tr>
<tr>
<td>18th February</td>
<td>ST21</td>
<td>Birmingham</td>
</tr>
<tr>
<td>9th March</td>
<td>CyberCon</td>
<td>London</td>
</tr>
<tr>
<td>9th - 11th March</td>
<td>Security and Policing</td>
<td>Farnborough</td>
</tr>
<tr>
<td>15th - 16th March</td>
<td>Global MSc</td>
<td>Bristol</td>
</tr>
<tr>
<td>15th - 17th March</td>
<td>Intersec Saudi Arabia</td>
<td>Saudi Arabia</td>
</tr>
<tr>
<td>18th April</td>
<td>ST21</td>
<td>Glasgow</td>
</tr>
<tr>
<td>27th - 29th April</td>
<td>The Security Event</td>
<td>Birmingham</td>
</tr>
<tr>
<td>10th - 11th May</td>
<td>CyberUK</td>
<td>Newport</td>
</tr>
<tr>
<td>18th - 20th May</td>
<td>CTX</td>
<td>London</td>
</tr>
<tr>
<td>18th - 20th May</td>
<td>IFSEC</td>
<td>London</td>
</tr>
<tr>
<td>13th July</td>
<td>ST21</td>
<td>Manchester</td>
</tr>
</tbody>
</table>
The Security Institute is the largest membership organisation for security professionals in the UK, with members from all over the world. We promote standards, develop and endorse education across the sector and provide a rich membership experience.

**WHAT WE CAN DO FOR YOU**

Membership of the Security Institute bestows credibility, enhances career prospects, provides a valuable network of excellent contacts, offers mentoring, runs a comprehensive continuing professional development (CPD) scheme to recognise your efforts in maintaining and adding to your skills base; and fantastic networking opportunities.

**KEY BENEFITS OF YOUR MEMBERSHIP**

- Benchmark your training qualifications and leverage your experience
- The value of your membership is recognised by employers and universities
- Exchange experience with other members at our networking events
- Enjoy access to job opportunities and our online careers services
- Gain valuable insights by being involved in our mentoring programme, whatever your career stage
- Enjoy member-only discounts
- Bi-Monthly newsletter with exclusive offers and weekly eNews update
- Members-only Linked-In Group
- Continuing Professional Development that evidences your professionalism
- Access to accredited and employer-recognised security related qualifications
- Participation in a genuinely supportive community
- Membership to the London Chamber of Commerce and access to their facilities, events and resources.

security-institute.org