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

SERVICES
We offer a range of services to meet all your cyber security needs and budget.

TRAINING
Training solutions designed to ensure your staff are always up to date on the latest threats.

PRODUCTS
Our suite of products and expert knowledge make choosing the right solution easy.

Visit www.macyberuk.com | contact mo@macyberuk.com
In February this year, I asked our Office Manager Helen to identify a week in my diary that would allow me to work from home every day to catch up on the admin generated by a relentless stream of very productive meetings. Three weeks later, I got what I asked for and for longer than I anticipated. On 19 March 2020, we closed the office and all staff commenced working from home. Over the following weeks we developed a new routine and innovative ways of engaging with our members, whilst supporting their goals whether that be mentoring for job seekers or risk assessments and awareness of the new prevalent threats in cyber, homeworking and adapting to new ways of performing the business of security.

Physical events were cancelled and virtual events (Webinars) replaced them. All we had to do was deliver a reliable platform and production and the members and Corporate Partners have stepped up to provide the thought leadership. We are booked up 7 weeks ahead with 2 webinars per week! It’s remarkable, once again, the members volunteer their time to support their community…. The Security Institute membership.

If you have not engaged recently, take a look at the Professional Development Platform, it has 1000s of bitesize information to make you better at your job. We are about to launch the community platform which will give all our boards, project groups and Special Interest Groups (SIGs) a unique forum to collaborate in smaller groups. You will be able to request access to SIGs that interest you most. We will continue to develop new short courses and affordable CPD activity so that you, should you wish, can emerge from this lockdown as a more informed version of your professional self.

Thankyou for your continued support and feedback. We are here to serve you.
Chairman’s Update:
Becoming a ‘Virtual’ Institute
Professor Alison Wakefield CSyP FSyI

The Institute has long been proud to have members all over the world who gain benefit from membership without necessarily having the opportunity to attend our physical events, and we have continued to invest in member services that deliver value wherever one’s location. Yet the global pandemic has taken ‘virtual’ membership and the delivery of online services to a new level, in ways that are certain to continue long after the current challenges are over. It has been a period of great sacrifice for many of our members, staff and volunteers who have suffered illness or loss of loved ones, worked on the front line despite the increased health risks to themselves and their families, experienced job losses or a loss of income due to furlough, been separated from close family members, or had to postpone important events. Yet the efforts of Security Institute staff members and volunteers have helped maintain a degree of continuity and normality that I am sure has meant a lot to many. I want to start this column with a heartfelt thank you to Rick, Helen, Di, Paula, Jade, Becky, Lisa and Ben for not only keeping the Institute running so well and in difficult circumstances, but also for the incredible innovations they have made and the new skills they have taught themselves in order to do so.

I’m delighted to be able to report that new member applications are currently stronger than ever. Our partnership with the Government Security Profession, led by Dominic Fortescue, the Government Chief Security Officer and Head of the Government Security Function, is bringing us new members from across government and we warmly welcome them. We also continue to welcome a steady stream of new members joining us through our other routes. The size of the Institute membership matters since we gain strength through numbers, with an increased profile, a greater scope of expertise within our ranks, greater influence and a stronger income stream that builds our capacity and can be invested in new member services.

Our new online activities and services have ranged from one-off webinars, training sessions and social gatherings, to additional online professional resources, discounted courses, and our 12-week CPD challenge, promoting continuing professional development during the lockdown. One of the great successes has been our online Chartered Security Professional application workshops, demystifying the assessment process and introducing participants to the requirements of effective applications, which are well worth joining whether you feel ready to begin the process or just want to start thinking towards applying in the coming years. Having recently fulfilled my promise to the Board to make my application, and found that it took me a week to layout my activities and achievements in a way that sufficiently addressed the five competencies with the depth and coherence I wanted to convey, the rigour of the process...
ensured that I gained a great sense of accomplishment and pride from being admitted. I am sure that other new registrants would say the same, and want to strongly recommend the effort and experience to others. At the other end of the spectrum of new services, our informal Friday SyI Morning Features have brought people together over lighter themes such as book reviews, thanks to Rick and volunteers from among our membership. For both of these recurring events, the number of spaces is limited in order to ensure that all participants get the chance to contribute, so early booking is recommended. More informal still, our Member Engagement Director John Sephton FSyI is running popular online discussions on LinkedIn every Sunday, so watch out for his #SundayDebate if you have not already participated.

We have also been delighted to promote via our weekly eNews other online events that might interest our members, and supply guest panellists to partners’ events, with Rick and some of our directors contributing to a number of other webinar series’ including Professor Martin Gill’s popular OSPAs Thought Leadership Seminars, hosted by Perpetuity Research and the organisers of sector awards the OSPAs and the TECAs. The innovation across the security profession has been remarkable and provided numerous opportunities for professionals to expand their horizons and develop their learning amid the lockdown constraints. Other successful webinar series include those offered by CSARN, Resilience First, the SASIG (Security Awareness Special Interest Group), ASIS and the Royal United Services Institute.

As for most organisations, the lockdown has required us to change the way the Institute runs day-to-day, and some of the adaptations are transforming the way we do business. The Institute was already employing remote working strategies with increasing effectiveness, with the HQ team using videoconferencing software to facilitate more home working and enable our Membership Registrar Paula to join meetings from her south-west location; and directors and members using the facility for many of the meetings of the senior leadership team, board sub-committees, the Validation Board and our Special Interest Groups. Since the lockdown, the Institute has given all directors access to MS Teams, and the first online board meeting proved so effective that this approach will continue to be used for at least some of our meetings, saving time and reducing travelling expenses.

Having begun this column with a thank you to our HQ team, I want to end with a thank you to all those in the security sector continuing to go the extra mile to support the rest of us through these challenging times. Security professionals frequently provide the rock on which others rely, often at significant personal risk. The recently published data by the Office for National Statistics indicating that one of the highest occupational death rates from COVID-19 has been among front line security officers is deeply concerning and requires thorough investigation, raising numerous questions requiring answers in order to inform government policy and guidance, employer practices, and individuals to help them keep themselves safe. There is considerable variation in exposure to disease by job category, age and ethnicity, and we must be grateful to those who put themselves in harm’s way to protect others, and assist in the efforts to minimise the risk to them. The Security Institute contributed to the lobbying interventions that saw security officers recognised as key workers during the lockdown, and will continue to use its position to help make sense of challenges that affect our people, and engage with government where necessary in order to represent the sector, share knowledge and offer support. We are very pleased to promote the City Security Council’s #WeHaveYourBack campaign recognising the vital role that security professionals play in protecting the nation, and the Worshipful Company of Security Professionals charity the Security Benevolent Fund, which assists security professionals in times of great hardship with welfare support (See Peter French’s MBE FSyI Article p.54 -55).

Warm wishes to you and your families, and stay safe and well in these exceptional times.
Dear members,

In line with the Government guidance and the uncertain duration of the current lockdown, the Board of Directors decided to cancel the Annual General Meeting (AGM) this year but that did not negate the legal requirement to present key aspects of our AGM to you, the membership.

Specifically, we required the acceptance of a number of key actions:

• To vote to accept the nominees for Directorships on our Board.
• To accept the 2019 Statement of Accounts
• To appoint the auditors.
• To Approve the 2019 Annual General Meeting minutes

After being distributed on May 1st, the AGM voting survey is now complete and I am pleased to report that we exceeded by far the number of responses we needed in order to legitimise the results.

I am also delighted to be able to declare that both Peter Lavery FSyl and Andy Watkin Childs CSyP MSyl were unanimously elected to the Board of Directors for the next three years, and will continue to fulfil their respective roles as Deputy Chairman and Director of Standards Development.

The auditors were approved, as were the accounts. Three questions were raised by members have been addressed by the Deputy Chairman. These specifically related to the appearance of an overspend in the last financial year, which is the result of a change in the accounting process and relates to deferred income. Clarifications are provided in the boxes below and opposite, with the sections in italics taken from the last page of the 2020 Audit Committee report.

In accordance with Financial Report Standard 102 section 1a, Armstrongs have accounted for deferred income in the accounts. The principle is to “match” the correct income with the correct expenditure in the correct period. [NB: Deferred income consists of the money you have received during the year which relates to next year’s services. For instance, this could be a membership paid in December 2019 which relates to the 2020 year.]

In the normal run of things there would be a deferred income figure bought forward from last year. Unfortunately, our accounts were not prepared on this basis before and all income received in the year has been recognised as income in that particular year. This is not correct in accordance with Financial Reporting Standards. The result of deferring income in these accounts for the first-time results in a greater-than-usual deficit (due to the fact we had not accounted for deferred income bought forward).
However, whilst noting the increased budget deficit the Audit Committee expects this to decrease/fall in line with budget following the accountancy realignment and additional reserves to be built up as a percentage increase against revenue. The Institute remains in a strong fiscal position with total assets of £204,401.00 (as of 31st Dec 2019).

You will appreciate that the Institute is growing steadily and as such, revenue is increasing. As a “not for profit”, the Institute does not make profit, only surplus funds which we then invest into better membership benefits. At the time of writing, we have invested a considerable amount securing a new collaborative community platform from Higher Logic. This platform will give every Special Interest group its own workspace to enable their brilliant thought leadership to be captured and shared for all.

The annual report would, ordinarily, have been available to you at the time of the AGM but, due to the current crisis and the commitments of the directors and other contributors, we extended the deadline for their contributions with a view to circulating the report a little later. The report will be completed and distributed next month and will detail our achievements as well as our future plans. I thank all of the contributors for giving their time and effort when so many other priorities in their working and personal lives must take precedence in the present circumstances.

Thanks very much to you all for your assistance with the survey, and your continued support for and faith in the Security Institute. I hope it will not be too long before I have an opportunity to catch up with you in person. I would also like to convey my gratitude to the HQ team for designing and implementing the survey in order to enable us to meet our obligations, and our Company Secretary Nigel Churton MBE FSyI for his invaluable advice and assistance to the HQ team and myself.

Best wishes,

Professor Alison Wakefield PhD CSyP FSyI
We are proud to have a full calendar of webinars, allowing our members to complete their CPD from the comfort and safety of their own home during this prolonged period of national lockdown.

The recent COVID-19 outbreak has resulted in unprecedented social change and uncertainty. We recognise that the security industry has been presented with unique challenges that make it particularly hard for security professionals to undertake networking, career and professional development at this time.

Leveraging the vast knowledge of our Corporate Partners and members, we have been able to and will continue to deliver a diverse range of topics in half-day CPD workshops and shorter webinar presentations. These events can be booked via the Security Institute website and the smartphone App, with new webinars being announced continually. Please find our current lineup here: https://event.bookitbee.com/security-institute

All webinars are presented live with interactive features that allow attendees to ask questions, ensuring that everyone can gain an in-depth understanding of the topic. Also, all previous webinars and seminars have been recorded so that members can download and watch all webinars at their convenience, these can be found here: https://security-institute.org/members-area/
Speaking on the subject of professional development, our Chief Executive Rick Mounfield CSyP FSyI stated:

“During these challenging times, it is paramount that we continue to understand emerging threats and how our community is collectively mitigating them. Being well-informed and well-connected as a security professional in a community such as the Institute has never been more important. We received overwhelmingly positive feedback following our first webinar which was attended by over 60 people, and several others since have had an attendance exceeding 100 members. This illustrates to me that digital learning using technology and remote platforms is the new norm and that will resonate after this crisis is over. We will continue with a programme of web-based learning from now on”.

So far our lineup has included a range of webinars that provide an insight into the current COVID-19 pandemic from a security professional’s perspective. We held a talk from the SIA’s Chief Executive Ian Todd on the regulator’s response to the on-going crisis, as well as collaborating with our Corporate Partner’s TrackTik to produce a webinar that explored how this crisis will change the way that security professionals operate. Pantelis Angelides MSyI, one of our overseas members, also led a webinar that covered the COVID-19 pandemic from an international perspective by analysing the response of Cyprus as a nation.

In addition to topical webinars, we have produced webinars that spotlight other important developments within the security sector. We worked with our Corporate Partner Aviligon to hold a webinar that focused on the use of security surveillance, particularly focusing on the way in which emerging technologies are changing the capabilities of security professionals. Nedap, another one of our Corporate Partners, lead a half-day digital seminar for us alongside their partners Indigo Vision and Ievo. Together speakers from the three organisations outlined the importance of employing integrated technologies for secure, scalable systems.

This is on top of regular webinars that explore our digital member benefits, such as the Professional Development Platform, giving members to ask any questions they may have and ensure that they are making the most of their Institute membership.

These free-to-attend webinars present an opportunity to participate in the Institute’s Continuous Professional Development (CPD) Scheme from the comfort and safety of your own home. Attending a Security Institute webinar will acquire 2 formal CPD points for each hour of learning. All attendees are sent a certificate of attendance, to support their future 2020 CPD submission.

If you would like to share your expertise with your fellow members, then please email jade@security-institute.org to discuss organising a future webinar.
Security for Life-Integrated Technologies for Secure, Scalable systems

We collaborated with our Corporate Partner Nedap to bring you this interactive online CPD Seminar exploring the important considerations for security professionals when aiming to implement a secure and scalable integrated security system, primarily focusing on the significance of establishing a close and effective working relationship with technology partners. Nedap works very closely with Indigo Vision (CCTV) and Ievo (biometrics) to provide their integrated security system. Security professionals from all 3 of the organisations discussed in this webinar how their strong working relationship has helped produce an effective security system, explaining the important topics within their respective areas of expertise.

COVID-19: The Cyprus State of Play

This informative webinar offered a unique international perspective on the current global COVID-19 pandemic. Pantelis Angelides MSyl presented an in-depth analysis of Cyprus’ response to the escalating crisis, examining the various risk factors that influenced the country’s response and its effectiveness. Pantelis Angelides MSyl evaluated the state of readiness of key actors within Cyprus, identifying key shortcomings as well as strengths in their approach to the crisis. The presentation also reviewed the key triggers that were missed by many across the globe, and to what extent key principles and standards have helped manage the situation so far.
Protecting the Public and COVID-19 – A View From The Regulator

Ian Todd, Chief Executive of the SIA provided an update on the regulator’s response to the COVID-19 emergency. As the country enters into an extended period of lockdown he shared his observations on how the industry has risen to the challenges in these unprecedented times. The current COVID-19 pandemic has presented new and unexpected challenges on the private security industry. Private security professionals and the industry at large have worked to ensure critical services remain open for business, supporting their customers and continuing to operate as a business during this crisis.

Fever Screening – Does it Have a Role to Play?

In collaboration with industry leaders in security services, G4S, this informative CPD seminar explored fever screening in more detail. Our panel of experts discussed how to implement a screening process, key considerations as well as the limitations through lively debate. Taking the necessary preventative measures to maintain staff wellbeing has never been more important. Fever screening has quickly emerged as one possible aid to the efforts in identifying individuals suffering from elevated temperature – one possible virus symptom. What is it? How does it work? How could it be deployed? What are the limitations? These are just some of the common questions. We offered some guidance in this webinar. It’s important to issue clarity in this area.

How Will Global Crisis Change the Way Security Services Are Delivered

Hosted by Rick Mounfield CSyP FSyl and TrackTik Vice President for the Security Industry - Mark Folmer FSyl, this webinar discussed how in the face of COVID-19, there has been a sudden shift in the demand for security services—to the point where security personnel are now, most likely, the first person you interact with when you go to grocery stores, pharmacies or hospitals. The webinar included a panel of challenging debate, made up of Philip Ingram MBE, Darren Carter, Marc Bannister and Rick Mounfield.
Membership Matters Advisory Group (MMAG): How you can get Involved

John Sephton MSyI, MMAG Chairman and Syl Director

As a bonus, participation in the group does carry a continuous professional development (CPD) score of one point per hour which you can use on your Security Institute CPD submission, helping you get to 36.

The MMAG is open to new members and in all honesty, I would recommend joining the group and having a voice into the Institute and hear the latest updates from Headquarters and what is going on within your Institute.

How does the Membership Matters Advisory Group function?

The MMAG meets via conference call approximately every six weeks and these meetings are minuted and points discussed. The call has participation from members of the head office and members who are currently MMAG members. To monitor progress we use an excel spreadsheet to track ideas and thoughts with an owner to each point so we know who needs to provide an update. During the meetings, the other chairs of the appropriate departments will give an update to where the progress is or was not achievable and to provide feedback to the call. Completed items will then be moved to the completion area and new ideas or thoughts added to the sheet.

The MMAG is an ongoing process, ideally with a rotation of participants on each call, delivering a wider range of outlook to their experience of membership. Saying this, we do have some regulars who join the call every time and I appreciate the contributions from everybody who does find time to attend these calls.
What has come out of the Membership Matters Advisory Group?

Like Magistrates Court where all legal cases start before being forwarded on to Crown Court for serious offences, all ideas generally start at this group before being progressed on to wider consultation within the Security Institute and finally Board consideration through to implementation. There have been a couple of areas which have started as an idea at the MMAG and progressed into their own areas of participation. Some of these areas are the Special Interest Groups (SIGs), Mentoring Platform and the Professional Development Platform which all now form part of the membership benefits.

Briefly just to touch on the SIGs, this started as an idea within the MMAG and have now become a home for lots of dedicated professionals discussing their areas of expertise. However, the groups are open to all who have an interest in the area or considering a shift in careers. If you wish to participate in the various SIGs then contact Becky from the SyI HQ, but there will be a revamp on the portal soon with the SIGs having their own dedicated area which you can apply to join.

Just to round off, the Security Institute is a professional membership organisation which takes pride in not only acknowledging and creating standards for the industry but also the time it devotes to listening to the membership. Like everything in life, you only get what you put in, but contributing to the various groups makes your membership even more worthwhile. I became a member of the MMAG and the Validation Board before I ran for the Main Board, so you can get as much as you put in and joining the MMAG is a great way to have your thoughts heard. Contributing to the MMAG will mean you are more informed of the ideas that are currently being generated within the Security Institute and what is in the pipeline.

I would like you to consider if you would like to join the Membership Matters Advisory Group and I really hope to hear your thoughts and contributions either via email or on a conference call. If you are interested in participating in the MMAG please don’t hesitate to get in touch and when invited to the calls have a think beforehand if there is anything you wish to discuss.

On a final note, thank you for reading this and to join the group email either myself john@security-institute.org or Becky O’Dell becky@security-institute.org to express your interest in the group and participation in the next conference call, it is open to all membership levels and we hope to hear from you soon.
I hope this article finds you in good health. A general greeting message which in today’s circumstances has never had a more profound meaning. I genuinely hope this short update from a few of our Special Interest Groups (SIGs) finds everybody in good health, especially during these unprecedented and challenging times.

I find myself writing this article in a completely different location in the country to where I expected to be living and working in April having moved home (280 miles), changed jobs and adapted to completely new ways of working (virtually and remotely), all accomplished during a global pandemic with only two face-to-face meetings (adhering to social distancing of course). I still can’t believe it when I think about it!

I achieved these significant changes during this extraordinary period of time because of the ingenuity, dedication, resilience and tenacity shown by many people from across a multitude of business functional areas, including those from our very own community – the security professionals. It makes me extremely proud when I reflect (from my own personal experience over the last 4 months) - irrespective of the organisation we work for/with or the sector or industry we work in - on the contribution the whole security community has made when tackling the challenge to adapt — quicker than they ever imagined - to new and agile ways of working, at pace, and with a flexible and scalable mindset.

I have learnt a great deal about myself over this relatively short period too and have been immensely impressed with my colleagues across our profession, with the ‘can do’ attitude and innovative approach over the last few months in designing, developing, deploying and managing the effective and efficient integration of protective security measures through tactical, operational and strategic collaboration across all three security dimensions (physical, personnel and people and cyber security) to meet the ever-changing and complex operating environment we find ourselves immersed in at present.

I hope we don’t forget the fantastic achievements we have made in such a short space of time so far in 2020, and we continue to work together to share our knowledge and experiences to ensure ‘security’ continues to be seen as a key enabler to meet our everyday political, economic, social, technological, legal and environmental needs.
Special Interest Group Overview

Live and in operation:

<table>
<thead>
<tr>
<th>Special Interest Group (SIG)</th>
<th>Chair</th>
<th>Co-Chair</th>
<th>Co-Chair</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security, Education, Accreditation, Training &amp; Standards (SEATS)</td>
<td>Rob Kennedy CSyP FSyl</td>
<td>Bev Griffiths</td>
<td>Tracey Lilly MSyl</td>
</tr>
<tr>
<td>Business Continuity, Emergency Planning, Crisis Management &amp; Resilience (BECRes)</td>
<td>Rod Stobie MSyl</td>
<td>Alan Cain FSyl</td>
<td></td>
</tr>
<tr>
<td>Built Environment Security (BESSIG)</td>
<td>Mark Tucknutt MSyl</td>
<td>Gareth Hulmes MSyl</td>
<td></td>
</tr>
<tr>
<td>Heritage &amp; Faith</td>
<td>Stephen Meek MSyl</td>
<td>Jonathan Brady</td>
<td></td>
</tr>
<tr>
<td>Cyber &amp; Convergence (CCSIG)</td>
<td>Kevin Duffey</td>
<td>Post Available</td>
<td></td>
</tr>
<tr>
<td>Nuclear &amp; Radiological Security (NRSSIG)</td>
<td>John Gribbin MSyI</td>
<td>Scott Anderson MSyI</td>
<td></td>
</tr>
<tr>
<td>Insider Risk</td>
<td>David BaMaung CSyP FSyI</td>
<td>Ian Crossley MSyI</td>
<td></td>
</tr>
<tr>
<td>Counter Terrorism (CTSIG)</td>
<td>Chris Stevens CSyP MSyI</td>
<td>Post Available</td>
<td></td>
</tr>
</tbody>
</table>

Planned to go live in the next 3 months:

<table>
<thead>
<tr>
<th>Special Interest Group (SIG)</th>
<th>Chair</th>
<th>Co-Chair</th>
<th>Co-Chair</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inclusive Security (ISSIG)</td>
<td>Anna-Liisa Tampuu ASyI</td>
<td>Lisa Reilly</td>
<td></td>
</tr>
<tr>
<td>Drones, Counter Drones and Protection</td>
<td>Phillip Wood CSyP FSyI</td>
<td>Geoff Moore MSyI</td>
<td></td>
</tr>
<tr>
<td>Dealing with Protest, Activism and Demonstration</td>
<td>Ray Fellows CSyP MSyI</td>
<td>Kenny McCleod</td>
<td></td>
</tr>
<tr>
<td>Travel and People Risk (TPRSIG)</td>
<td>Simon Jamieson</td>
<td>Post Available</td>
<td></td>
</tr>
</tbody>
</table>

Ideas for new groups in the future:

<table>
<thead>
<tr>
<th>Special Interest Group (SIG)</th>
<th>Chair</th>
<th>Co-Chair</th>
<th>Co-Chair</th>
</tr>
</thead>
<tbody>
<tr>
<td>Healthcare Security</td>
<td>Martin Nicholas MSyI</td>
<td>Jayne King FSyI</td>
<td></td>
</tr>
<tr>
<td>Chief Security Officer (CSOSIG)</td>
<td>Post Available</td>
<td>Post Available</td>
<td></td>
</tr>
<tr>
<td>Fraud</td>
<td>Alan Day FSyI</td>
<td>Tony Maher MSyI</td>
<td></td>
</tr>
<tr>
<td>Technical Security Officer (TSOSIG)</td>
<td>Post Available</td>
<td>Post Available</td>
<td></td>
</tr>
<tr>
<td>Historic Houses</td>
<td>Mike McBride FSyI</td>
<td>Post Available</td>
<td></td>
</tr>
</tbody>
</table>
Know your Institute

Special Interest Group Spotlight

As our Chairman Professor Alison Wakefield PhD CSyP FSyl alluded to in the February edition of The Institute Quarterly “... it is a very exciting time for the Institute and its members. It is increasingly being recognised that the three dimensions of security are interdependent and rely upon one another if we are all to achieve successful security outcomes. The Security Institute is in an excellent position to address these opportunities and support government and industry in converging all aspects of security, through our close partnerships and growing influence.” A proclamation which certainly resonates with me and my personal experiences during these last few months.

Our Special Interest Groups (SIGs) are at the core of our Institute and play a fundamental role in the contributions the Security Institute makes across government and wider industry as well as providing plenty of shared learning opportunities for personal and professional development. Our SIGs are there for the benefit of all our members, so please get involved.

For further information about our any of the SIGs highlighted in this article or if you are interested in creating a new group, please get in touch with: Becky (Becky@security-institute.org) or myself (Alex@security-institute.org). We look forward to hearing from you.

SEATS SIG

The further professionalism of the security sector is, of course, a prime objective of the Security Institute. The Institute is growing year on year as more individuals not only see the benefit of joining for themselves but also view the Institute as a vehicle for change. It is a fair assumption that the Institute has within its membership individuals with an altruistic mindset that seek to enhance the professionalism and profile of the business of security. New members that share the Institute’s values and culture will of course only invigorate the advance towards achieving this strategic objective. The SEATS SIG therefore has a vital role to enhance the knowledge skills and behaviours across all sectors from the ground up to raise competence levels and enhance professionalism.

The role of the SEATS SIG is unique. The reasoning behind this is that we anticipate this SIG will become the conduit for all other SIGs to advance. There is some fantastic progress being made by the various SIGs within the Institute, most likely this good work will need to be communicated at some point in the form of educational training, this is where the SEATS SIG will assist. We are here to help! The SEATS SIG will also push the broader agenda to raise the standard of security at all levels across all sectors whilst also rise to any challenges that the Institute is asked to overcome.

Initially, we encourage the various SIGs within the Institute to engage with us as at an early stage to assist their progress with educational issues. In the near future, there will also be a survey shared across the industry to gain an insight into what the industry requires. This will ultimately shape the strategic objectives of the SEATS SIG as we move forward.
The CTSIG remains in its infancy in comparison with other more established groups. That said, the inaugural meeting in December 2019 identified that the subject has many potential subgroups all of which will require a degree of ownership to develop.

Examples of potential subgroups are:
- Threat, Vulnerability, Risk, Assessment experience;
- Crowded Places;
- Asset Protection; including in design and by identifying best practice;
- Potential impact of Martyn’s Law on venues in Manchester initially and potentially across the country – what qualifications required for those carrying out assessment?, who would carry responsibility for recommendations being delivered or ignored?

Threat Vulnerability and Risk Assessment’s (TVRA’s) are the basis upon which the security world develops security requirements and recommendations to mitigate actual, and lower the residual, risk. As well as seeking the experience or qualifications expected of a professional individual to provide security advice there is also the desire to expand the knowledge of the wider Security Institute membership of this important skill set.

‘Crowded Places’ is a stream of work for which NaCTSO, a police organisation, has led on for several years the emphasis is one of advice. Although the advisory documents produced have provided useful guidance, there is seen a need for employed security professionals to provide site-specific recommendations with justifications, while holding Professional Liability is an expectation of clients.

The group is keen to pursue the following aspects: Case Studies of Crowded Places; Responsibility and Interested parties in securing; Sharing Information between professionals; Feedback i.e. what works and maybe what to avoid; Appreciation of the costs involved and need to support recommendations.

There is a wealth of knowledge and experience in the subject of Asset Protection across the Security Institute membership from which others could benefit. The sharing would seek to impart the design requirements and identify best practice delivered on projects which have been completed.

Martyn’s Law is to be linked to the issue of licence premises requiring them to have carried out CT risk assessment. The CTSIG identified a number of pertinent questions surrounding the qualifications required to complete this work and also the level of responsibility/liability passed to those that did so as areas of concern.

Staff and personnel performing security tasks at licensed premises and Crowded Places are vital to the safety of users and the immediate response to an incident. They also accomplish an essential role in deterrence and intelligence for any reconnaissance measures. Awareness and response training are a critical requirement for all persons engaged in these roles and having a method of delivery which is easily delivered and understood in a minimum period of time, but also adequate for the individual to appreciate the value of their role is required in an industry which often relies on staff where the turnover is rapid.

The CTSIG has the potential to be one of the largest in the Institute due to the subject matter and breadth of spokes leading from the central hub. It will require the involvement of members to ensure that it can deliver the initial elements identified which it is anticipated will occur once the current COVID-19 lockdown is over and normality returns.
Setting up the Inclusive Security SIG (ISSIG) is an important step to mark the work ahead for the Institute to explore how inclusion in security can lead to innovation in our broader field of security, and how we can bring about change together. Diversity and inclusion are not only one of the key vehicles for innovation, but they also bring a competitive advantage. Diversity of knowledge and experience fosters diversity of ideas, creates a variety of perspectives and leads to the growth of the talent pool. Lack of diversity in an organisation, or in a sector more broadly, can limit innovation and adaptation to the evolving marketplace.

This has relevance to security in numerous ways, from better engagement with clients and employees at the front line to increased boardroom innovation and to enhanced processes. It also encourages organisations to ‘think outside the box’ and bring about positive disruption. If the security risks of employees are to be effectively managed when they travel or work from home, it is essential that security practices are inclusive not divisive. To better achieve the understanding required to create inclusive security practices, security professionals need to reflect the diversity of those we serve.

For a sector that is often judged according to its poorest practices, and seen as under-regulated and under-professionalised, addressing diversity and inclusion can help us to, as a sector, tackle image problems and be taken more seriously by stakeholders that are further along the diversity and inclusion journey, including both clients and those we want to attract to the sector.

The ISSIG aims to explore and understand how engagement with all groups of society will pave the way to innovation and how inclusivity can lead to enhanced practices in the broader field of security. The group will foster a variety of perspectives, for increased productivity, creativity and diversity of the talent pool.

- Diversity: refers to the make-up of the workforce and highlights efforts to ensure that staff from a variety of backgrounds and with a variety of personal characteristics are employed across all levels of the organisation.

- Inclusion: ensuring that all groups (including minority groups) have equal positions and voices to those of their fellow colleagues within the organisation.

Thus, this SIG aims to change the face of the field of security and risk management by fostering more opportunities for all groups of society to access and thrive within the industry.
The aim of the NRSSIG is to foster innovation and share good practice on improving security outcomes in the nuclear/radiological environment and raise professional standards. The current membership brings together security professionals, regulators, owners, operators, designers and end users of nuclear and radiological materials and facilities. A key objective is to build a shared understanding amongst all stakeholders of security challenges in the nuclear/radiological environment. This, in turn, fosters collaboration and coordination with stakeholders in sharing a wide range of security risk management techniques that can inform delivery appropriate, proportionate and cost-effective security strategies. All business is conducted within a forum using only publicly available information.

The group meets on a quarterly basis on a rolling programme where each meeting is hosted by a member. This provides an added dimension where members gain an insight to the diverse business areas within its membership.

The BESSIG brings together security professionals and built environment stakeholders with the aim of improving security outcomes in the built environment, raising professional standards and in doing so, creating new opportunities for security professionals through greater market demand for secure buildings, infrastructure and public spaces.

The BESSIG has a vital role to play in providing commercial and educational benefits to its members. In particular, the BESSIG seeks to:

- Increase collaboration and co-ordination amongst security suppliers (supply chain), regulators and end users;
- Build a shared awareness and understanding amongst all stakeholders of the latest and future security challenges that we can best address by working together;
- Promote the benefits of security risk management in delivering appropriate, proportionate and cost-effective security solutions;
- Identify, communicate and promote the adoption of best practice in the procurement of built environment security;
- Encourage and reward innovation that leads to advances in built environment security performance, offers additional benefits for stakeholders and society at large;
- Collaborate, for mutual benefit, with other SIGs of the Security Institute;
- Highlight the benefits of professional membership and the use of services offered by registered security professionals.
**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>6 February (London)</td>
<td>CSyP Application Workshop</td>
<td>Attend SyI and CPD Partner events</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>20 February (London)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 March (London)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19 March (London)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 April (Webinar)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7 May (Webinar)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21 May (Webinar)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>31 Mar</td>
<td>SyI Validation Board Meeting</td>
<td>Committee work on a voluntary basis (per hour)</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>1 April</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>28 April</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29 April</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19 May</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20 May</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18 February</td>
<td>Members Lunch</td>
<td>Attend SyI and CPD Partner events (Whole event)</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>26 March</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7 April</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24 April</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15 May</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22 May</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2nd April</td>
<td>SyI Morning Feature Webinars:</td>
<td>Attend SyI and CPD Partner events (Whole event)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>23rd April</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>28 April</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29th April</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7th May</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14th May</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20th May</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27th May</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20th May</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27th May</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2nd April</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23rd April</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>28 April</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29th April</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7th May</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14th May</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20th May</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27th May</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14th May</td>
<td>Nineteen Events Webinar Series:</td>
<td>Attending Institute and CPD Partner organisational events (per hour)</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>14th May</td>
<td>'Post lockdown impact on the way we securely access commercial &amp; residential premises' webinar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14th May</td>
<td>'COVID-19 – An Outbreak of Learning' webinar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14th May</td>
<td>'The current Coronavirus crisis &amp; how we can prepare for ‘Post Traumatic Growth’ webinar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14th May</td>
<td>'Securing organisations and the supply chain during the pandemic’ webinar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>31 March</td>
<td>CSARN webinar series:</td>
<td>Attending Institute and CPD Partner organisational events (per hour)</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>23 April</td>
<td>'Pandemics without borders - protecting our people' webinar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21 May</td>
<td>'COVID-19 / Critical discussions for the new normal' webinar</td>
<td></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></td>
<td>2</td>
</tr>
<tr>
<td>Various Dates</td>
<td>SASIG Webinar series</td>
<td>Attending Institute and CPD Partner organisational events (per hour)</td>
<td></td>
<td>2</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.
Connect your team with G6PTT. Radio without boundaries.

G6 Push to Talk brings you the best from the communications world; the power of network radio using 3G, 4G, LTE & WiFi to give unparalleled global coverage.

This system is the result of our successful collaboration with TASSTA; leading edge design and engineering for a changing world. Adaptable, scalable and flexible to fit any operational environment.

The functionality of two-way radio but with no coverage restrictions, and with advanced features that will transform the way you operate.

Get in touch to see what we can do for you.

Communication connects everything that we do. G6 Global exists to create the best communications system for your operational needs.

www.g6-global.com  +44 (0)1454 610050
Roy Cooper, an Associate member of the Security Institute, won the UK OSPA’s Lifetime Achievement award in late February.

Roy has been actively working in the security industry for nearly 50 years. Starting as an apprentice back in 1972. Throughout his career he undertook various appointments working for a number of system installers. Roy went on to develop and manage Professional Security Magazine, which is now one of the most widely distributed and respected publications in the industry.

In 2012 he co-founded the Women in Security Awards – providing an opportunity to raise the profile, awareness and significant achievements of leading women in what is widely known as a male dominated industry.

In 2013, he introduced SecurityTwenty, a regional roadshow which has become one of the most successful in the UK. Each roadshow has a charity dinner which raises money for local security related charities, typically raising around £20K per year.

It is in recognition of his unbridled passion, professionalism, enthusiasm and significant contribution over the past two decades in reporting and addressing key issues, voices and news on all aspects of the security industry.
The richness of the security industry never fails to stimulate me, several weeks ago two things happened out of the blue: I was contacted by the CMI and interviewed for a forthcoming blog and article around COVID-19 and how major organisations and my HNW clients are managing the current pandemic, and a children’s charity contacted me and asked for some free crisis management advice as they had reached out to another consultant who had demanded a huge fee for crisis management advice.

As, a former Police Officer, I jumped at the opportunity to assist a charity, particularly a children’s charity as I spent many years in child protection whilst in the Serious and Organised Crime Directorate of the Metropolitan Police Service (MPS).

I must state for the record, these are my thoughts, gained over thirty years conducting strategic and major investigations, in command leadership positions, in several crisis management roles and in particular from the Avian Flu Pandemic in 2005-8 (H5N1), in which I was the operational lead for my Command.

In July 2008, the UK Parliamentary Committee for pandemics were predicting that up to 75,000 British People will die in the ‘inevitable’ flu pandemic that could kill as many as 50 million people worldwide. Furthermore the Committee warned, that surveillance of emerging disease threats around the world needs to be overhauled to provide early warning of potential pandemics.

Additionally, if we look back further to 2002, to the SARS pandemic, we can clearly see that an unfavourable range of economical, social and political effects were experienced by many nation states, their citizens and global organisations.

My research indicated that at the time of the 2002 and 2008 pandemics, the effects were negligible and mainly temporary, if noted at all by most of the general population however, the impact to the wider global economy, financial markets and organisations has changed significantly since 2008, as the world has become a more complex, interdependent, fragile and many commentators suggest, more susceptible to global disruptions such as pandemics.

For much of the past twenty years, the West has relied on countries in the Far East (mainly China) to produce, manufacture and supply a large proportion of our cheaper consumables (wearables) and everyday technology however, as time has moved on, we now see that the Far East is becoming a major producer of key components for multiple sectors including our automotive, technology (5G), clothing, food and more recently the emerging health market.
The emergence of the COVID-19 pandemic has shone a bright light on the above dependencies and has left many of corporate clients realising that their main suppliers and many of their third party supply lines are in serious threat as key components, if not their entire product lines emanate from China or other Far East locations. I am spending a large part of my time advising around third party supply lines resilience and managing investigations and audits into failures to provide correct reassurance.

We are seeing stocks running low across the ‘visible’ market place but what many of us are not witnessing are the hidden shortages that many of my clients are experiencing, recently I heard a senior consultant friend of mine say “remember we cannot sell a car that is 99% complete”. He went on to explain that many of the critical components (engine management systems) in a modern car come from the Far East and are in short supply at this time.

It is worth stating for completeness that many of the initial countries that experienced the first infections are claiming to have the disease under control and that we in the UK and Europe are someway behind however, my experience in dealing with several real world crises is that we are still very much in the thick of it and the wider social and economical consequences are still to be felt by all of us as the true consequences will be all-encompassing and protracted.

I predict that the very fabric of many of our society and business sectors will change dramatically, and that many of the small, medium and large companies will fail to manage this latest crisis and their internal crisis management systems will not be sufficiently robust enough to manage the current situation and therefore will not recover from the sustained period of uncertainty that will follow.

So what can we do to overcome this uncertainty? I am reminded of the saying “the best time to plant a tree is 25 years ago, the second best time is today”, I am spending most of my time at the moment working with several global clients managing the day-to-day activities of their Crisis Management Teams (CMT’s) looking at what can be achieved in the current situation to best manage this ‘uncertainty’.

After I had assisted the charity in question, I was asked by a second and then a third to also assist them and due to other commitments, I reached out to colleagues in the Security Institute, the Security Commonwealth, TINYg and the ASC and was inundated with offers of assistance from the UK and Cyprus.

I have now passed several of these kind offers of assistance on to the charities and I think we have now shown that working with charities on a pro bono basis is good for the soul and the industry. I would like to personally thank all the people that offered their help, they know who they are.

The advice I provide is often complex, bespoke to the client and differs for each of the sectors. However, there are general points that can be passed across all sectors and companies, I have decided to share some of these points as I believe in a time of crisis, the worse thing we (consultants) can do is to close down discussion, withdraw advice and to not share lessons learned from other similar events or incidents.
My top ten tips for my clients are as follows: I give these in the hope that they may assist companies of any size to weather this storm and to remember, “Do not decide on a permanent solution to a temporary problem”.

Most Crisis Management Plans (of which I have constructed and reviewed many) tend to be somewhat linear based methodologies designed to cope (survive) a number of simplistic or commonplace incidents or events such as IT failures, cyber enabled crimes, kidnaps, environmental systems failures (HVAC) etc, but experience shows us that such approaches are not suitable for a crisis management incident of this nature (COVID-19) as previous/current approaches tend to be limited and are based on previous knowledge and outcomes.

I am witnessing some companies struggling to cope with out-dated and cumbersome business continuity plans that are onerous, difficult to implement and inflexible to say the least. Hopefully the following Top Ten Tips will assist with the Crisis Management Meetings that are currently being held:

1. In respect of your Business Continuity and Crisis Management Plans, having a flexible, agile and focused approach is vital. Every Company, no matter what size should develop their plans and capabilities to deal with the COVID-19 issue, understanding it will hugely impact their working practices, procedures and will increase disruption across their companies for many months if not years.
2. If organisations do not have the right skills within their Crisis Management Team (CMT), Business Continuity Team (BCT) or Recovery Team (RT), seek the services of a qualified and experienced advisor as soon as possible (remember the Tree analogy).
3. Ensure that the CMT or BCT is meeting on a regular basis to start to ‘make sense’ of Covid-19 issues and how they will impact your specific Company/sector.
4. It is vital that you commence ‘surveillance’ monitoring (sense-checking) of every aspect of your organisation (HR, Talent Management, IT, Comms, 3rd Party Suppliers, Supply Chains, Stakeholders, Sponsors, Transport, etc).
5. Understand / assess what vulnerabilities you have and how to address them effectively i.e. risk reduction strategies, your response capability, what contingencies you already have in place and is your recovery strategy still valid, useable and realistic?
6. Now is the time to strengthen / check your decision making abilities, if you are not sure obtain external verification / advice from a trusted source.
7. Check any previous ‘lessons learned’ within your organisation or from your immediate network, similar organisations and companies (SARS 2002 / H5N1 2008).
8. Hold weekly / daily CMT Meetings to manage and co-ordinate your current and longer terms responses and resources. Create a meaningful agenda and remain focused on achieving all the stated aims/points. Be mindful of current updates from the Government, Medical sources, Industry bodies etc.
9. If you do not have a dedicated Pandemic Plan, or your previous BC Plan is limited, develop one as soon as practicable. Ensuring it is flexible, agile, capable and responsive.
10. It is critical to have a strategic approach to everything you do, use a mnemonic such as ‘SMEACS’ when planning and responding to this latest crisis.

• Situation
• Mission
• Execution
• Administration
• Control
• Safety

Lastly, it is important to remember that there is no single right answer and that each company requires a bespoke solution to their specific issues. If any person wants to know more around any of the above please contact me further and I will provide additional information, advice and assistance. Good luck.
Human intelligence - HUMINT- has been with us from the start. Spies, according to Colonel John Hughes-Wilson, are the heart of intelligence and have been from time immemorial. Human intelligence - spies and spying - represents the oldest form of intelligence and the most numerous. From Sumerians to tomorrow's headlines, from all-out war to stealing commercial secrets, there will always be spies. Spying is all about trust and betrayal, hope and fear, love and hatred. Spying to collect information on “the other” is eternal, and it has always been centred on people and personalities. Families spy, businesses spy, nations spy. Human intelligence is a vast field; it is much more than just spies born from the fantasies of Fleming.

For a start, there are many forms of HUMINT, from debriefing defectors and refugees to interrogating prisoners of war, and from running agents behind enemy lines to exquisitely thoughtful, polite, diplomatic exchanges at cocktail parties. As its name implies, HUMINT means dealing with the most treacherous and unreliable source of information of all: human beings. In the urban warfare setting, you cannot get away from the human. The collection of information is only one facet of human intelligence. The information deduced from the intelligence collected is essential, as it is responsible not only for formulating policy but also for altering and developing operational capacities in the field. Human intelligence information often proves crucial for locating and neutralising adversaries and for allowing quick action and reaction in the attainment of national security goals.

Spies are often dynamic, curious, funny, intuitive and insightful young people. They appear to be modest and, impersonal in appearance so that they can infiltrate the operating environment. They must be “brilliant in their ways but discreet in their presence”. Technology in the intelligence sector has reached levels of excellence, even though it is unwise to attribute excessive trust in it. It is not possible to consider it a panacea. Indeed today, the human factor is indispensable for identifying and contrasting new forms of hybrid and insidious threats. Fundamental to the agent is knowing how to master both verbal and para-verbal communication techniques. The searching for information by the agent is composed of three phases: a) the search for the source, b) the recruitment, c) the management or “manipulation”.

The tools that can be used to approach and recruit the source could be the classic but dangerous money, or the religious or political ideal, but also a deep feeling of revenge against something or someone who could induce the source to collaborate. Most reasons that frequently can induce a person to collaborate can be summarized in the acronym MICE - money - ideology - coercion - egotism. Some intelligence services can make use of more invasive “recruiting” techniques, such as sexual blackmail, the so-called “honey trap”. Once the source has been identified, and the attachment tool has been established, we move on to recruitment. This first step is very delicate and risky since the agent could blow his or her cover, even before approaching the source. The “enticement” should be carried out with caution and possibly by an agent other than the one who will subsequently manage the cause. The agent could resort to some techniques derived from neuroscience to persuade the target to provide as much interesting “news” as he has in his possession. To obtain this result, it is essential to establish an empathic bond between the source and the agent; it is possible to start a relationship of superiority/subjection between the two figures so that the source can diligently and confidently carry out the indications suggested to him.
The Agent’s training

The training sessions are very important to the agent who will assume the necessary techniques to acquire a security role and control. The spy’s training also involves the use of NLP techniques (Neuro-Linguistic Programming) to optimise the relationship between source/agent. NLP helps the agent to operate naturally by building an empathic connection with the target, based on the mirroring technique. This action represents the starting point for empathically “tuning in” to the same frequency as the interlocutor. Once the relationship is established, the source will be unconsciously predisposed to respond positively to the agent’s stimuli and requests. At that point, it is necessary to avoid conflicting approaches that can lead to differences of opinion otherwise a breakdown will be inevitable. Classroom exercises are fundamental to training where the would-be spies, divided into small groups, practice role-playing where they are being continuously monitored by a supervisor, who will make the necessary corrections and suggestions in real-time, encouraging and providing feedback to trainees. The new operating schemes are assimilated thanks to continuous repetition of practice in the field, which can be divided into four recursive phases: understanding, training, tutoring and learning. The duration of the process is a few months even if the agent can try his hand immediately, experimenting with what is learned in the classroom in the field.

Paradoxically, HUMINT can, therefore, be used to aid the efficient execution of the mission and make the targets reachable, reducing messy and chaotic operations.

In this particular historical moment today, we need more and better intelligence the threat has changed skin, becoming increasingly “invisible to the eye”. The threat is made up of individuals hiding behind a device or making themselves anonymous and not identifiable.

At the same time, they are always potentially ready to intervene at any time and at the first signal, sacrificing their lives for their cause.

Technology has become essential to combat and avoid global threat. Nevertheless, we still need human beings who cannot be separated from the use of TECHINT. In the new evolutionary approach in the intelligence field, human intelligence, must be used and integrated with all the other information specialities such as OSINT, SIGINT, MASINT, and TECHINT. We have to remind ourselves, that it is not the machine that attacks or neutralises the opponent, but the man behind it. Human-machine interaction is indispensable to interpreting the information and behaviour of the opponent, indeed, he needs to use technology as a tool, and at the same time, he must use his knowledge of the pertinent culture. Napoleon said: “there are but two powers in the world, the sword and the mind. In the long run, the sword is always beaten by the mind”. For this reason, despite extensive technological development, HUMINT remains the critical factor in identifying and predicting the real purpose of the opponent, despite hiding behind sophisticated weapons and technical devices in an increasingly low-intensity war.
I joined the Police in 1989 and eventually moved on to managing serious and fatal road traffic collisions and the subsequent trauma associated with these types of incidents. I realised that the medical training we had was extremely limiting when managing these casualties, and these experiences changed my career.

In 1996 I applied to become an Authorised Firearms Officer (AFO). I passed the rigorous selection following extensive testing and scrutiny as is expected. I held many positions, honing many skills and competencies, including National Firearms Instructor, National Tactical Firearms advisor, Rifle (Sniper) S.P.E.A.R. PDR Lvl 2 Coach, Weapons control and restraint (TCMS) and advanced medical skills. I took on the medical training known as ‘D13 Casualty Care for Police Officers’ which is governed, certified and endorsed by The Royal College of Surgeons of Edinburgh and the Faculty of Pre-Hospital Care (Thurgood Hall et al). This forms part of the National Police Firearms Training Curriculum or NPFTC.

I spent 19 years developing this area holding the lead portfolio for two police forces and steering this area of business for the region. I liaised at Chief Officer level with other agencies to introduce new and innovative skills including analgesia for casualties (one of only 5 forces nationally to administer such treatments). I became an Advanced Provider of the Faculty of Pre-Hospital Care RCSEd having passed several medical courses. I had the privilege to be invited to the UK Special Forces Patrol Medics re-accreditation course at Hereford and successfully completed this, along with numerous other courses including FPOSi, PHTC, CeeR, MIRA, FREC 3, FREC 4 Cadaver IO training, Penthrox. This experience allowed me to forge some great training opportunities and friendships with so many other professionals.

I continued to develop my firearms teams, maintain my operational competencies and still enjoy representing the Faculty of Pre-Hospital Care assessing and teaching courses. I received numerous attestations and commendations during my career, and I continue to this day to maintain my qualifications.

I retired in January 2019 after 30 years and felt quite lost after having been in an Institution for 30 years, and then I met Rick Mounfield CSyP FSyl of The Security Institute and he got me thinking!

When I started working in the Police in 1989 the thought of suicide body born improvised explosive devices or marauding terrorist attacks killing, stabbing and driving cars at innocent members of the public was unheard of in the UK. Planning tactics to interdict and prevent such events is now the norm. Twenty-five credible threats have been foiled by the security services in the past 3 years. New innovative systems have been developed such as Citizen Aid (Thurgood et al), where I act as an Ambassador. The onset of Martyn's Law (named after a Manchester bombing casualty) is now supported by the UK government Security minister Brandon Lewis..."The prime minister, Home Secretary and I are all 100% behind Figen and are working to improve security measures at public venues and spaces”. This is being made into legislation.”
Matt Maer, director of security at Canary Wharf Group, said: “This legislation has the potential to make a significant impact on public security, improving the situation for people as they go about their daily lives” (Alistair Bunkall Sky Security correspondent 24/2/20)

Which led me to questioning how effective is the medical interventions and training on the market today?

The D13 training programme (Thurgood Hall et al) forms 24 hours of contextualised scenario-based learning. There are two elements to this package. D13.1 Standard and D13.2 Enhanced roles. It covers the trauma fields to the highest standards and teaches the medic to operate in suboptimal conditions with real capability and intent with minimal kit. It simplifies what is a complex process into simple and effective lifesaving interventions. It covers such areas as catastrophic haemorrhage control, airway management interventions with adjuncts and concurrent oxygen therapy. Added to this, a thorough systematic primary survey that is advanced in approach and lifesaving in conclusion. Following the breathing assessments allied to use of innovative chest seals and advanced splinting techniques the trained medic will assist in stabilising the casualty within the first 10 minutes often referred to as the “Platinum 10 minutes”. After the Platinum period, the casualty can be managed within the Golden hour for definitive care.

There are other courses out there such as the FREC (First Response Emergency Care) pathway. This takes 5 days and details emergency aspects but is broadly medicine based.

So which course is more suitable for the medic to deliver simple, robust, lifesaving interventions contextualised in situations like Westminster Bridge/ Borough Market or 7/7? Is there a strong and robust Clinical Governance (CG) to clinically govern the taught medical interventions and support the medic/security officer? How able and capable is the CG to withstand any civil litigation? Do security companies have such governance or even Advanced/Specialist medics? How would a company refute or mitigate any lawsuits and thus avoid reputational damage?

Members of staff and/or members of the public do some extraordinarily abnormal things in the deadliest of situations……. Why? Who taught them to do that? Who told them not too? All the instincts of survival come to the fore, yet some people still go above and beyond the norm to help and give first aid to the injured.

How do the risk assessments conducted by a security company direct what type of medical training it should have for its staff? What does the Strategic Threat and Risk Assessment or STRA state about the security company’s position? How effective will the medics be under these conditions? Does the medical training reflect what the Security Officer is likely to face?

The Faculty of Pre-Hospital Care supports the National College of Policing in the D13 training programme. Therefore, it enjoys statistical data extrapolated from several sources. We see numerous incidents where specialist Firearms Officers dealt with a large range of medical emergencies (Medical training Police officers Specialist
Our Membership

role: a retrospective review Mssrs Hartley Howells Thurgood 2010-
15).

This data was secured through prudent incident recording. This
deﬁned more speciﬁc patient demographics and ultimately helped
develop a more robust clinical governance to manage the scrutiny
of independent investigations. Such data enhances the training
programme as well!

“Some extremely challenging incidents were dealt with and
examples of excellent care predominate. In particular three terror
incidents and multiple casualty calls were attended; exceptional
eXamples of triage and decision making, with prompt effective care
in high pressure environments, were illustrated” ( FPHC Feb 2019 )

Effective recording of medical incidents, cogent risk assessments
and appropriate Clinical Governance that reﬂect the incidents
or potential incidents that staff will be facing is critical to looking
for the right medical course. If the incidents are more medicine
based than trauma then there are plenty of courses available. If
the incidents are more trauma based, then the D13 curriculum
is relevant. But how do you know? Managing the expectations of
the organization where stewarding, badged under SIA, has come
to the fore now. There is more of a “push” for Corporate social
responsibility. How does the medical training programme assist in
mitigating reputational damage? A tiered medical response to such
traumatic events is extremely effective which the Police service and
general public has clearly beneﬁted from.

I have administered medical interventions in hostile suboptimal
conditions for over two decades. Many times, there was no
immediate medical support or where the medical support was
not allowed to operate. And it felt like a lifetime passed you by!
Where medical support cannot respond or cannot reach you,
often referred to as the therapeutic vacuum, it teaches you to
recognise time critical injuries quickly and secure the casualty within
the “platinum” 10 minutes. And then make simple but effective
lifesaving decisions. The D13 training programme is contextualised
with the medical skills that are ‘scenario speciﬁc’ and ‘attack speciﬁc’
underpinned and trained with experience. It has been tried and
tested in the ﬁeld and withstood the considerable scrutiny of civil,
coroners and criminal courts alike. It is both lawfully, tactically and
medically sound.

Whether you’re a chef in a kitchen, FAW medic, SIA Steward or
Internationally renowned company the D13 Medical training
curriculum can deliver great beneﬁts and develop organisations and
staff accordingly. Whether there be a marauding terrorist attack,
serious assault, roadside collision or serious injuries that effect our
family and friends.

For instance, following the aftermath of a marauding terrorist attack
Hemant Oberoi, the Head Chef at The Taj Hotel Mumbai, spoke on
his lifesaving efforts in the midst of the terror attack:

“What else can you do. We had to protect our guests. I stayed and it
was the right thing to do. It wasn’t a question of bravery...”

The D13 programme provides an extremely effective and
professional response to medical trauma emergencies. And once
trained, the Security Officer will be more capable, more potent
and more credible. And this training is supported, endorsed
and certiﬁcated by the very eminent Faculty of Pre-Hospital Care,
The Royal College of Surgeons of Edinburgh. Supported by a
professional medical institute.

Thank you to The Security Institute for asking me to pen this article.
Thank you, Andy / John, for mapping my career and for saving and
protecting people.

I’d like to ﬁnish with the quote and dedication given by Mr Andrew
Thurgood who developed the D13 curriculum as below...

All police officers dedicated to deploying these skills and knowledge
in extraordinarily challenging circumstances ( Thurgood et al )
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 Syl membership and wider network
- Inclusion in the Corporate Partner Showcase on the Syl 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

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.

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.
Earlier this year former Labour Member of Parliament and Security Institute Vice President, the Rt Hon Bruce George FSyI died after a long illness. Bruce made a significant and lifelong contribution to the private security industry, as well as many other areas, although the focus here will be upon the former. The longevity and commitment of him to the private security industry is now very clear, but when as a parliamentarian he introduced his first private member's bill to regulate the private security industry in 1977, which followed several other MPs and Lords, he was described by one leading industry commentator (Peter Heims) as, ‘the latest flash in the pan’.

Bruce was to introduce his private member’s bill to regulate private security another four times in 1988, 1990, 1992 and 1994. And unlike some other parliamentarians who tried, he had no financial interests to declare with the industry, other than his own pure curiosity. His pressure in the 1970s was to lead to the Labour Government publishing a Green Paper on regulation, which any progress towards, was subsequently smothered for a decade, by the election of a deregulating government in 1979.

It was the early 1990s which was to produce Bruce’s finest hour in the battle for regulation. Using his membership of the House of Commons Defence Committee he was able to secure an enquiry into the physical security of MoD facilities, which exposed poor standards in the security industry. He organised a conference at the House of Commons on private security regulation, in which the then Shadow Home Secretary, a certain Tony Blair spoke, in which he supported regulation. Behind the scenes he was pushing him and his deputy Alun Michael for regulation.

Then the Home Affairs Committee decided to conduct an enquiry into regulation, a committee we must remember with a Conservative majority at this time, not inclined to regulation. Bruce did much to convince them to advocate his model of regulation. Indeed when giving evidence himself and pressed by the Chairman, Sir Ivan Lawrence, that Bruce’s preference for a Gaming Board style would be better replaced by Ofwat, Ofgas type of regulator, Bruce’s very quick and witty reply - and typical of his ability to win arguments by humour - was: ‘To that suggestion, my reply would certainly contain the word off!’ The committee was to go on and endorse his views with a report recommending a model of regulation close to his own. With the election of the Labour government in 1997 it was only a matter of time, with Bruce continuing to lobby behind the scenes. A White Paper was followed by the 2001 Private Security Industry Act and then the formation of the Security Industry Authority. They were not perfect and Bruce was always demanding more, but they owe a great deal to his work.

It would be wrong to assume Bruce was only interested in regulation too, he was fascinated by all aspects of private security. He built one of the largest collection of books and papers I have seen on the subject. He was always reading about it and keen to attend events and conferences to learn more. He was also a prolific writer on the subject. I was lucky enough to work with him on a book and many articles, but he wrote many more and has written some of the most interesting and important accounts of the history of private security. For these reasons he was made a Visiting Professor at my university in Portsmouth and he would regularly come and give lectures to students, both before and after retiring as an MP. His interest was genuine and sincere and was not driven by cheap partisan opportunism or money. It was no surprise to me that when he retired he continued to research and participate in the industry. His recognition by many in the sector was genuine and he certainly proved he was no ‘flash in the pan’ when it came to private security. I doubt the private security industry will ever have such an interested and critical friend in parliament again.

The Security Institute Directors, Staff and Membership send our deepest sympathy to Bruce’s Family and Friends.
Announcements

Petri Hitches

Obituary by Rick Mounfield CSyP FSyI

Petri Hitches, an Affiliate member of the Institute, sadly passed away in May. A well respected and admired member of the International Security Industry who leaves behind a wife (Yoko) and a daughter (Nina), of whom he was immensely proud as she’d recently graduated and started her career.

Petri has worked within the Security industry for over twenty years, working in Japan, France, Poland and the UK, introducing new products, developing markets and keeping in contact with all those he met along the way, with a little text, a quick phone call or a sneaky coffee.

He was in the final stages of completing a corporate partnership with the Security Institute for Spotter RF, a US based C-UAS company.

In the short time he was involved with the Institute, he made a big impact. The Security Institute Directors, Staff and Membership send our deepest sympathy to Yoko and Nina.

Keep Us Updated

To help us ensure you gain the most of your Institute membership and to stay informed of any changes within the Institute, please ensure that your account information is accurate and up-to-date.

If there are any changes that we need to know about, whether it be a change in name, occupation, address or contact details - please let us know by changing your details under ‘Settings’ in the Members Area of our website.
The Security Institute is proud to have received the Bronze Award from the Defence Employer Recognition Scheme (ERS).

The ERS recognises commitment and support from UK employers for defence personnel. This award reflects the Institute’s position as an armed forces-friendly organisation, open to employing reservists, armed forces veterans (including the wounded, injured and sick), cadet instructors and military spouses/partners. It also aligns our values with those outlined in the Armed Forces Covenant. We are proud to support Defence personnel and encourage other employers within the security industry and beyond to do the same.

The Institute will now work towards earning a Silver Award from ERS. If you or your company are interested in the Defence Employer Recognition Scheme (ERS) then please visit: https://www.gov.uk/government/publications/defence-employer-recognition-scheme/defence-employer-recognition-scheme#about-the-scheme
World Earth Day: How the Security Institute is prioritising Environmental Issues

This last quarter, on April 22nd we joined the rest of the world to help celebrate Earth Day. Earth Day is an annual event that helps spotlight environmental issues and demonstrates support for environmental protection. 2020 marked the 50th anniversary of the first Earth Day.

At the Security Institute, we recognise the importance of environmental protection and are working towards operating as a carbon-neutral organisation. We are supporting the organisation OffsetEarth, invest in projects that remove more greenhouse gasses than your own carbon footprint puts in.

We have been supporting OffsetEarth and their work for over 5 months now, and in that time this has directly helped plant 545 Trees. This has contributed to several global environmental initiatives including but not limited to landfill gas extraction and forest management and protection in the Amazon Rainforest.

In total, this has offset over 29 tonnes of CO2 emissions. This is equal to 72,371 miles driven or approximately 22 long haul flights. According to scientific research, this will have saved approximately 88 square metres of sea ice.

We are proud to be supporting the work of Offset Earth, if you’d like to track our impact please visit: https://offset.earth/thesecurityinstitute
Introducing the Security Education Accreditation Training & Standards (SEATS) Special Interest Group

The further professionalism of the security sector is of course a prime objective of the Security Institute. The Institute is growing year on year as more individuals not only see the benefit of joining for themselves, but also view the Institute as a vehicle for change. It is a fair assumption that the Institute has within its members the individuals with an altruistic mindset that seek to enhance the professionalism and profile of the business of security. New members that share the Institute’s values and culture will of course only invigorate the advance towards achieving this strategic objective. The role of the SEATS SIG therefore has a vital role to enhance the knowledge skills and behaviours across all sectors from the ground up to raise competence levels and enhance professionalism.

The role of the SEATS SIG is unique. The reasoning behind this is that we anticipate this SIG will become the conduit for all other SIGs to advance. There is some fantastic progress being made by the various SIGs within the institute, most likely this good work will need to be communicated at some point in the form of educational training, this is where the SEATS SIG will assist, we are here to help! The SIG will also push the broader agenda to raise the standard of security at all levels across all sectors whilst also rise to any challenges that the institute is asked to overcome.

Initially we encourage the various SIGs within the institute to engage with us as at an early stage to assist their progress with educational issues. In the near future there will also be a survey shared across the industry to gain an insight into what the industry requires. This will ultimately shape the strategic objectives of the SEATS SIG as we move forward.

SEATS SIG Champions

Chair: Rob Kennedy CSyP FSyl, Education Training Sustainability Champion

Rob is a motivated and determined security risk management professional who is passionate about raising the levels of professionalism within the industry and the recognition that security is a science in its own right. Currently, Rob is the Training & Development Manager & Security Advisor for SecuriGroup based in Colchester with specific interest in training, consultancy, and academic development in a plethora of security related topics including but not limited to: Criminology, Counter Terrorism, Security Risk Management, Enterprise Risk Management, Business Continuity, and Crowd Management. More recently, Rob had the honour of assisting Glasgow Caledonian University as an associate lecturer to deliver their Integrated Security Operations programme. Rob has also achieved numerous qualifications including a Foundation, a BA (Hons) and Masters, in Security & Risk Management from the University of Leicester during his time in the security sector and understands the need for sustainable training and education.
Co-Chair: Bev Griffiths,
Educational Resilience Champion

Bev is the Capability Lead at the Emergency Planning College and has a wealth of experience in Health, Local Authority, Government, Training, Consultancy, Resilience, Health and Safety, Crowded Places, Event Management. Bev’s academic background enables her to work with key partnerships in the UK and Internationally and provide extraordinary support to private and public organisations in the management and development of Crowd and Public Safety, Security and Safety, City Resilience, Business Continuity, Communications and Media. A well-regarded speaker and chair and a member of many professional groups, Bev takes an active interest in improving the profession and assisting in the education and development of learners in the field. Bev also advises on National Occupational Standards & Qualifications; Risk, Cyber Resilience, Crisis Management and Incident Management, from policy to operations and is experienced in blended learning, e-learning, consultancy, auditing, and training.

Co-Chair: Tracey Lilly MSyI,
SIA Licensing Champion

Tracey is the Senior Manager for Quality and Standards with the Security Industry Authority and brings with her a wealth of experience of working in government administration. She is also skilled in risk management, coaching, academic publishing, compliance, team building, quality assurance and an area some dread; public speaking. Tracey is a qualified teacher with PGCE and MA in Education, she is also ISO 9001:2015 qualified.

Andrew Turner MSyI,
Transition Champion

Andrew is a Security Consultant based in the south of England near Southampton following a police career spanning 27 years. Eighteen of these were as a Search Advisor and Coordinator specialising in security and Counter Terrorism (CT) operations. This role provided the opportunity to develop an extensive knowledge of defensive and offensive CT search operations, major crime scenes and victim recoveries. He gained his experience at numerous high-profile incidents and large-scale events such as Royal Ascot, The Americas Cup, Royal and Diplomatic events and operations on behalf of HM government. Andrew was also responsible for implementing policies and procedures to ensure the safety and professionalism of both staff and organisation. He implemented measures necessitating that staff and management received focused and relevant training to ensure a consistent ‘blue ribbon’ service delivery whilst maintaining high levels of security confidence and efficient work practises. Such experience has been valuable since finishing his Police career and transiting into the new challenge of the private security sector. Andrew’s sole trader knowledge in security as a whole and in particular his specialist knowledge around the use of explosive search detection dogs and working in confined spaces has been of enormous benefit to the security of numerous private events. He also continues to consult on security requirements for spontaneous or high-profile international media platforms such as NATO or Royal events in London. Whilst Andrew has extensive experience and multiple professional, vocational and bespoke qualifications he found formal security focused qualifications to be necessity, and recently completed a Level 5 Security Consultancy programme and is currently working toward attaining his Level 7 Advanced Diploma in Security and Management.
Perin Bhatt ASyI,  
Security Officer Champion

Perin, has been involved with the security industry since 2001 as a front-line officer and supervisor. Perin is also an advocate of education and training which has proved advantageous for his own development and acknowledges he enjoyed his training and educational experience with PerpetuityArc but continues to ‘learn’, developing interests in Counterterrorism, Security Surveys and Security Risk Assessment. Perin has also been awarded ‘Employee of the Month’ several times by his employer for his dedication and professional approach in the workplace. Perin is currently an Associate member of The Security Institute.

Richard Benyon MSyI,  
Security Technical Champion

Richard has been involved in the electronic security industry for over 35 years. During this period Richard has worked as an installation/commissioning engineer, he has also worked in technical sales for manufactures of security products and run and owned two successful security installation companies working on many “blue chip” projects, and several government projects. Over the last 35 years, Richard has witnessed a decline in standards and technical knowledge and is, therefore, keen to raise the profile of the electronic security industry and recognised the lack of training and suitable qualifications for this area to raise standards and have qualified and licenced security technicians similar to colleagues working in one of the SIA licencing areas.

Gavin Butler,  
Cyber Champion

Gavin has a first degree in criminology from the University of Westminster (PCL) and a Masters in Security Management and Information Technology from the University of Leicester. Gavin has industrial experience as an independent security consultant, advising mainly on museum security and retail security. Since 1994 he has also been lecturing extensively in Information Technology Security. He was a leading academic on the Masters of Science in IT Security at the University of Westminster and later led the development of cyber security programmes at Bucks New University, helping to develop the careers of a number of influential individuals within the IT security industry over the last 20 years+. Gavin is a qualified lecturer as a Fellow of the Higher Education Academy (HEA). Gavin has also tutored at Bramshill Police National Training Faculty. Gavin is currently an External Tutor for Portsmouth University working with Professor Mark Button in the Institute of Criminal Justice Studies. Gavin is also an External Assessor for Leicester University and an External Examiner for the University of Chester.
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.

ACCREDITED SECURITY MANAGEMENT QUALIFICATIONS

**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 /
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 our members are up to date with the latest employment trends, and are the best equipped to achieve their career aspirations.

We are aware that due to the on-going COVID-19 pandemic that many companies are implementing new work from home policies, where possible. Working from home can be a difficult transition for many, and it presents a range of new challenges for professionals to overcome.

To support our members during this prolonged period of lockdown, we were proud to launch our ‘COVID-19 Remote Working Pack’ at the of March. The collection of online resources available on our Professional Development Platform, which members can access from the Members’ Area of our website and through our mobile app, provides a range of support that helps professionals best prepare for success during these challenging and unprecedented times.

The Pack offers guidance designed to help you effectively work from home. It includes advice for how to maintain a high-level of output, and remain productive during these difficult times. There are video resources that directly address how you can avoid procrastination, whilst working in an environment often filled with distractions. Furthermore, it gives helpful advice for how best to adapt communication within teams, as well as how you can successfully manage employees remotely.

Topics such as well-being, resilience and mindset are also addressed with resources in the Pack, all intended to help you cope with the unpredictable changes that we are all currently facing.

It is also important to note that using the platform is great way to acquire valuable free CPD Points.
New: ‘Making the Most of Retirement’ Online Programme

At the end of March, we ran our first ever Security Institute webinar. We wanted to run an online session that highlighted the range of resources available to all members of the Security Institute through our Professional Development Platform, the webinar called ‘Making the Most of the Professional Development Platform’ gave a great overview of the broad variety of tools that you can access on the platform and a recorded version is still available to watch in the Members’ Area of our website.

A few of the attendees from this session questioned why there wasn’t a programme that collated all the resources available that address the transition from professional life to retirement. We recognised the demand for such a programme that offers tips for a smooth transition into retirement and outlines the several different avenues that can be explored to remain professionally involved whilst not working.

Less than two weeks later the ‘Making the Most of Retirement’ was launched. Whether your retirement is approaching fast or you’re years away from this significant milestone, it’s never too early to start preparing. Learn about the factors to consider and the many options available to you once you reach retirement age, ensuring that you can remain professionally fulfilled and make the most of your retirement.

The programme also offers advice for passing on your expertise during retirement. Becoming a mentor and assisting active professionals with their careers and development, is a great way to remain professionally active during retirement and allows others to benefit from your years of experience and in-depth knowledge. Members of the Security Institute can engage in a mentoring relationship through our online Mentoring Platform available here: https://securityinstitute.onpld.com/

Utilising the Professional Development Platform and participating in a mentoring relationship, either as a mentor or mentee, are two fantastic ways to earn CPD points remotely.
The Security Institute promote and encourage continued professional development through education. In collaboration with our education partner, PerpetuityARC Training, we offer award-winning accredited qualifications, a BTEC Level 3, a BTEC Level 5, and an iQi Level 7 for those wishing to enhance their professional security management skills.

All learners can currently enjoy a 25% discount until the end of June, on the three Security Institute courses using code: PerpARC25 - this cannot be used in conjunction with any other discount. Terms and conditions apply.

When considering undertaking a qualification there are many questions that prospective learners ask, this article will answer some of these frequently asked questions about the Security Institute’s qualifications.

General Questions

When can I start the courses?
All three of our qualifications have continual intakes – as soon as you book and pay (in full), you will be registered on the Online Learning Platform and details on how to access and start your course will be emailed to you.

Do learners receive feedback?
Learners receive in-depth feedback with points for future improvement. Feedback is supplied by experienced academics in the field.

What guidance and support is available?
Each learner also has access to our in-house tutorial service - if you are struggling in anyway, you can contact the PerpetuityARC Team where a dedicated tutor will be assigned to you. Tutorials are arranged to suit you in terms of time, date and method (Skype, FaceTime, Whatsapp, Zoom, Conference Call or Email.

How are the courses delivered?
All courses materials are delivered via the Online Learning Platform and for the Level 5 and Level 7 courses, where independent research is required, access to the PerpetuityARC eLibrary is also provided. Completed assignments are uploaded to this platform and on the platform, you can find useful documents pertaining to: how to write an essay, how to reference in Harvard Style, how to avoid plagiarism and how to dedicate time to study in the “Student Resources” section.

How do I sign up?
Learners can head over to the PerpetuityARC webpage dedicated to The Security Institute’s suite of training courses: https://www.perpetuityarc.com/syi/. By selecting the course they wish to enrol on, a “book now” tab will become available and learners will be automatically taken to the online booking form.
FAQs about the BTEC Level 3

Are there any eligibility criteria?
There are no pre-requisites.

What is the course duration?
The course is designed to take 6 months, but extensions can be granted for those struggling to meet deadlines. Deadline extensions must be requested.

What are the modules?
This course is made up of 9 modules. Each student MUST complete 6 to pass. There are three mandatory modules that students must complete:
• Introduction to Security Management
• Security Department Management
• Information Security Management
Students then have to pick 3 modules from the following:
• Health & Safety in Security Management
• Securing Retail Organisations
• Principles of Counter Terrorism
• Managing Organisational Risk, Crisis and Disaster
• Preparing for Strategic Security
• Securing Corporate Assets (Physical Security Management)

Students cannot do more than 6 modules but have access to all study material for each module.

Should an employer want to put a cohort onto the course, the employer can pre-select what modules (from the electives) they wish their workforce to study and a report of the cohort’s work can be sent to the employer.

How is the course assessed?
Learners have to submit 1 assignment per module. These assignments are comprised of short-written answers (generally 9 questions per module) and each question comes with a recommended word count.

What is the background of the typical learner?
Learners embarking on this course typically are new to security or are looking to work towards supervisory roles. Learners often have some experience in the field but would like to validate this with a recognised qualification. Quite commonly, learners embarking on this course have been out of academia (school, college, other training courses requiring written submissions) for some time. It is a great introduction to writing and security management theory.

Who is the awarding body?
Pearson is one of the UK’s leading accreditation and qualification bodies. They facilitate and regulate UK GCSE’s and A-Level exams/marking standards and are globally recognised across an array of industries.

How much does the course cost?
Excluding VAT: £999 pp
Including VAT: £1198.80 pp
FAQs about the BTEC Level 5

Are there any eligibility criteria?
The course is open to all who operate within the private and public security sectors, and have:

- a minimum of 3 years security management experience
- or 3 years in the armed forces in a supervisory role,
- or have successfully completed the Security Institute’s BTEC Level 3 Certificate in Security Management

Candidates will be updated on their enrolment throughout the application process and the Training Team is on hand to assist with any application queries.

What is the course duration?
The course is designed to take 12 months, but extensions can be granted for those struggling to meet deadlines. Deadline extensions must be requested. Students can complete the Dip in fewer than 12 months, if they so wish.

What are the modules?
This course is made up of 5 modules. Each student MUST complete all 5 to pass. Module titles are:

- Understanding Security
- Threats to Security
- Risk Management
- The Legal System
- Management

How is the course assessed?
Learners have to complete 2 essays per module (approximately 1,500 words each). Learners will have to draw on their own experiences as well as a range of texts beyond the supplied reading materials.

Within each module, learners will have a theoretical type question (example: what is meant by the phrase “security management must be commensurate with risk?”) and a more practical question (example: design a workplace poster to deter employee theft from taking place).

What is the background of the typical learner?
Learners embarking on this course typically have worked in security for some time, but perhaps have no formal qualifications to validate their experience. This course provides those who wish to make a move into Supervisory / Management roles with the necessary skills to apply theory to best practice within in the workplace, whilst also enabling the learner to develop their soft skills (writing and research abilities).

Who is the awarding body?
Pearson is one of the UK’s leading accreditation and qualification bodies. They facilitate and regulate UK GCSE’s and A-Level exams/marking standards and are globally recognised across an array of industries. The BTEC Level 5 sits on the framework of qualifications in and around the same level as a foundation degree.

How much does the course cost?
Excluding VAT: £1630 pp
Including VAT: £1956 pp
FAQs about the IQ Level 7

Are there any eligibility criteria?
The course is open to all those who operate within the private and public security sectors and typically meet one of the following criteria: completion of the Security Institute Diploma, and five years’ experience working in security management or a related management field, or a security-related degree and seven years’ experience of working within the security sector, or a non-security related degree plus ten years’ experience working in security management or a related field. Or have completed the Security Institute BTEC L5 Diploma in Security Management.

What is the course duration?
The course is designed to take 9 months but extensions can be granted for those struggling to meet deadlines. Deadline extensions must be requested.

What are the modules?
This course is made up of 3 modules. Each student MUST complete all 3 to pass. Module titles are:
• Critical Thinking
• Conduction Research
• Written Projects – The Dissertation

How is the course assessed?
Learners have to complete 1 assignment per each module:
• Module 1 – 2,000 words (+/-10%)
• Module 2 – 2,000 words (+/-10%)
• Module 3 – 7,000 words (+/-10%)
Learners will have to draw on their own experiences as well as a range of texts beyond the supplied reading materials.

What is the background of the typical learner?
Learners embarking on this course will typically be working at a managerial or higher level and have worked within the Security Sector for a number of years working in or towards senior management, and will have already studied up to degree level. A Level 7 in academic terms is the same level as a Masters, and therefore learners will be researching and writing at this level.

Who is the awarding body?
Industry Qualifications (IQ) are a leading UK awarding body specialising in accrediting courses in the security sector and beyond. Working with various overseas partners, IQ are evolving as an internationally recognised accreditation agency providing qualifications across a range of levels. The IQ Level 7 sits on the framework of qualifications in and around the same level as a Master's Degree.

How much does the course cost?
Excluding VAT: £1860 pp
Including VAT: £2232 pp
Perin Bhatt ASyI has worked in the security industry since 2001, beginning his career at one of the largest private security service company in the UK. After 5 years in the industry, which encompassed various roles and responsibilities, Perin took the decision to take a career break. He used this time to further develop his skills and knowledge in security as he had come to the conclusion that the security industry was going to be career of choice.

Before he went on my career break he did some research and made contacts with several companies and organisations that provided security training/education courses. Whilst looking around he stumbled on the Security Institute’s range of qualifications, ran by our education partner PerpetuityArc, which specifically catered to his needs as a professional aspiring to attain a security management position.

The breadth of security covered in the modules was a particular draw for the course, which provided the in-depth knowledge that he had been wanting from a qualification.

Speaking on the qualification, Perin stated:
‘The courses that the Security Institute provide are essential for attaining career progression, and are an essential boost if you are aspiring for a security manager or director role. Undertaking this course has directly helped me improve my security skills, reducing the threats and risks for clients’.

Perin also spoke highly of the level of support that he received from the Perpetuity Arc team whilst studying with us, describing it as ‘excellent’. We ensure that all students receive the level of support they need to succeed, and gain the most out of the course. Since 2006, Perin has achieved more qualifications and certifications, continuing his professional development. He has managed to achieve a number of proud achievements within the workplace as well, earning employee of the month not only for his direct employer but also for client organisations. Using the skills and knowledge he as acquired, Perin hopes to continue making recommendations and implementing policies that made significant contribution in the areas of security, evacuation and health & safety.
ABOUT US

Turret Training’s Faculty shares a fervent passion to deliver excellent medical training and specialist advanced critical trauma care to individuals, company’s at corporate level, law enforcement and military units. Coupled with a shared experience of over 79 years of operational work in non permissive environs, the team bring a unique, personable and dedicated approach to the delivery of this training. The structure of the team affords a flexible approach of training delivery ranging from First Aid at Work (FAW) to Citizens Aid to Critical Incident Management courses that will meet the needs of the client. This bespoke specialist level of training is supported by a number of specialist advisors and eminent boards of certification.

SERVICES

We provide Clinical Governance (CG) and are supported through our Advisory Board from current members of The Royal College of Surgeons of Edinburgh Pre Hospital Emergency Medicine (PHEM). Such programmes are mapped across from current training curriculums and are updated and reviewed on a monthly basis from the above Faculty members including current UK Emergency services and UK Armed Forces. Further specialist courses can be provided upon request.

First Aid at Work course
Emergency First Aid at Work course
Penthrox Analgesia course
Critical Trauma Care course
Citizens Aid course

Critical Incident Management
Refresher Emergency First Aid at Work course
Refresher First Aid at Work course
Refresher Critical Trauma Care course

turretmedtraining@gmail.com 07976 904534 www.turretmedtraining.com
The current pandemic means more people are now working remotely and adapting business to the virtual environment. This is throwing up all manner of new challenges that we need to work through and doing this with a mentor can now be invaluable. In a time of crisis mentoring just requires a little bit more creativity and adaptation.

In ordinary circumstances, many mentors focus on the career development side of mentoring. Although this remains important, other functions such as demonstrating emotional and social support are especially valuable in these uncertain times. This may involve a mentor listening to understand mentee’s struggles and concerns, acknowledging and validating the challenges they are facing and the distress they are feeling.

As a role model a mentor can share their own experiences during the shutdown of normal work, discussing how the break in physical routines, the restricted access to others, and the bombardment of information can feel overwhelming and isolating. Simply giving mentees permission to take a break from the news and their work routines to engage in self-care can be very beneficial. A bit of humour can also help to break the tension.

The career development functions of mentoring can still continue regardless of social distancing. Mentors can still create a safe space for career conversations. Mentees may be worried that they’ll be laid off, that their work will no longer be noticed by their managers, or that progress toward advancement and promotion will be derailed.

Facing an uncertain future, mentees are more likely to use their connection with a mentor to lower anxiety and to work with the mentor to develop a vision of how they can not only weather the storm but continue to thrive in their careers.

Online meetings may be a new alternative in which to model and teach new skills and behaviours — and the learning may flow in both directions. Mentors might discover that their mentees have much to teach them about virtual work and new technologies.

Whether you typically meet in-person on a regular basis or haven’t spoken in a while, now is a good time to reach out to your mentor/mentee. There is good evidence that mentoring via video conferencing yields the equivalent outcomes to in-person mentoring. Alternatively, methods such as email, chats, and text messaging allow flexibility in keeping the lines of communication open but are more limited and can be prone to misunderstandings.
How to continue and deepen a mentoring relationship in a time of social distancing:

1. Communicate with each other, find time for a phone call or a video meeting, even if it is only for a few minutes. Everyone is experiencing plenty of uncertainty and new demands. Let your mentoring relationship be something you can depend on.

2. Make adjustments to your normal mentoring routines. Work out the best medium for meeting in the online environment. You might need to work around childcare, or other commitments that are now part of this new working environment.

3. Keep it real. If you have children at home because schools are closed, or if you are having to work in a room with other members of your family, don't hide those personal challenges. Use them to develop a friendly connection, sharing your situation makes it more comfortable for your mentor/mentee to share theirs.

4. Show care and compassion. Test your listening skills and focus on your mentee’s concerns. Financial, health, job, and family matters are all likely to be pressing issues. Demonstrate that you hear and understand.

5. Offer support that will enable mentees to overcome challenges on their own. Mentors aren’t there to be a rescuer or fix everything for mentees. Instead, they provide strategies, skills, and resources that mentees can use to learn and to grow so that they can address their challenges themselves.

Although social distancing is necessary during the pandemic, it doesn’t mean you can’t maintain a mentoring relationship. Use this time to explore new ways of staying connected, show that you care, validate feelings of distress, develop talent, and challenge yourself to get out of your mentoring comfort zone.
If there’s one thing certain during this period of uncertainty created by the on-going COVID-19 crisis, it’s that every time there’s a major news story or world event, hackers jump at the chance to take advantage to launch attacks against unsuspecting victims, and unfortunately the COVID-19 pandemic is no different.

Between January and March, more than 4,000 coronavirus-themed web domains have popped up. It is suggested that around 5 per cent of these are suspicious and 3 per cent malicious (March 2020). The websites would likely be used as part of email campaigns to lure victims to click on dangerous links.

Cybersecurity firms are reporting a notable increase in attacks against a range of targets, all using the ongoing COVID-19 pandemic as a hook to trick their victims into running malware.

Cybercriminals are using the coronavirus to spread several different types of malware. Some of these campaigns imitate “trusted” organisations like the World Health Organization to infect their victims. Researchers say that attackers aren’t just using the coronavirus as a cover for spreading malware. There is evidence of what appears to be the first case of a coronavirus-themed business email compromise attack, designed to trick businesses into turning over money. There has also been an increase in targeted attacks against executives in conjunction with this pandemic.

Another big vulnerability is hackers accessing sensitive data through Wi-Fi networks. Individuals are typically using their home networks for their work to further isolate data or accessing public Wi-Fi.

Individuals have also been targeted by Coronavirus-themed phishing emails with infected attachments containing fictitious ‘safety measures’, such attacks have recently become more targeted, with greater numbers focusing on specific sectors like shipping, transport or retail to increase the likelihood of success.

One way to fight back against these attacks is by ensuring the employees are aware of the threats they are facing and educating the workforce.
Quickly train employees to work from home safely and securely
In response to the coronavirus pandemic, many organisations are implementing work-from-home policies. Yet for many businesses, managing an entirely remote workforce is completely new, which means they may lack the processes, policies and technologies that enable employees to work from home safely and securely. In addition, many employees may be unfamiliar or uncomfortable with the idea of working from home.

How We Are Helping
COVID-19 has resulted in an unprecedented demand for Cyber Security training, to help our members better adjust to the current situation and ensure that they are best prepared for success we have partnered with Amica Interactive, an industry leader in cyber, governance, risk and compliance training.

We can offer Amica’s Cyber Security for Home Users free to all grades of Security Institute members, you can sign-up to receive your login information here: https://event.bookitbee.com/27379/cyber-security-for-home-users-online-course

The course provides easy-to-understand advice and tips to help individuals better understand Cyber Security in the Home and On-The-Move. The content is designed to familiarise individuals with the risks they face and will make them a little more “tech-savvy” and most importantly improve their security awareness.

The course covers such topics such as, the Importance of Cyber Security, Phishing, Ransomware, Virtual Private Networks (VPNs), Multi-Factor Authentication (MFA), Protecting Your Wireless Router, Staying Safe On Social Media, Securing Your Mobile Phone (both iPhone and Android), Smart TVs, The Internet of Things (IoT) etc.

In response to the current circumstances, Amica Interactive have also taken the decision to make their Cyber Security for Home Users course available to all at the discount price of £9.99, non-members can access the course here: https://www.amicainteractive.co.uk/
It’s counter terrorism – but not as we’ve known it

Detective Chief Inspector Steve McGrath
Head of Information, Capability and Business Engagement, NaCTSO

Detective Chief Inspector Steve McGrath from National Counter Terrorism Security Office (NaCTSO) tells us how we can all make a significant contribution to national security, wherever we find ourselves, both now and in the post COVID world.

Can you help keep the UK safe from terrorism sat at your kitchen table?

Well, yes – everyone can.

Recent events have forced all of us to rethink the way we do business, and Counter Terrorism Policing is no exception. The ‘lockdown’ response to the coronavirus pandemic has focussed the minds of leaders in the public and private sector on how their organisations could adapt to staff working from home. This applies to us at the NaCTSO too.

As we look ahead to a return to normality – whatever that might be in the post COVID-19 world – some will no doubt choose to maintain a degree of agile working.

Even before the dreadful events that forced huge numbers of us to set up a home office, there was a trend towards a more flexible approach to working.

Be it work/life balance, better mobile tech, the high cost of commercial premises or just the dread of commuting – more employers and employees have opted for more choice to work from wherever suits them and the business best.

To this extent, I’d like to think that CT Policing was ahead of the game when it comes to partnership working with commercial organisations. Our strategy has moved – not entirely but significantly – to digital self-service, where we are less dependent on being in the same place at the same time to deliver a great service to you.

We are still here for those who need the site visit and the face-to-face contact, but much of what we offer is now available and easy to access, anywhere and at any time. It’s an approach that is proving popular.

The pandemic and its terrible toll aside, this year is set to be a positive one for those of us in policing tasked with leading the nation’s protective security effort. So far in 2020 we have marked the second anniversary of our Action Counters Terrorism, ACT Awareness e-Learning tool with the launch of
Version 2. This 45 minute, interactive package is a basic introduction to counter terrorism, including guidance on the simple steps to take to mitigate the threat, how to spot suspicious activity, what to do if you have concerns and how to react in the event of an incident. Version 2, with updates to keep abreast of the threat, is now live.

ACT Awareness e-Learning was developed in collaboration with Highfield eLearning, and business resilience experts at retail giant Marks and Spencer. It is free for anyone to use, and can be done on a laptop or tablet. The course can be completed in short bursts or all at once. Feedback from a survey of 20,000 users gave the course a 96% ‘would recommend’ rating. In total over 400,000 individuals have taken part since the initial launch in April 2018.

Also, in March and shortly before COVID-19 came to dominate our lives, we launched the ACT App, giving businesses quick access to a library of sector-specific products to help them keep their staff, customers and estates safe. We now have over 1,600 company subscribers, representing over 4000 individuals, who receive live-time updates from us about key developments and incidents relating to CT. Subscription is free but at present, unlike e-Learning which is available to the public, is restricted to company registrations only.

Feedback from users has been overwhelmingly positive and many asked if we could expand our remit temporarily to share more general business-related coronavirus messages from policing, government agencies and industry bodies.

In the future, we will be launching an Information Sharing Platform that will enable a better two-way flow of information between CT Policing and our partners in business. Again this will operate 24/7, so that we will always be available to respond to your needs, whether on site, on the move or at your kitchen table.

Please take time to learn more about what we can do to help you play an important part in keeping everyone safe. Please encourage your staff – whatever their role – to take the e-Learning course, and for those whose responsibilities include security and resilience, download our app.

More information about ACT Awareness e-Learning and the ACT App, including how to sign up, is available at the NaCTSO website.
The Security Benevolent Fund (SBF) was founded in 2006 by Myself Past Masters John Purnell of the Worshipful Company of Security Professionals (WCoSP). We identified the need to create a safety net for the most vulnerable people working in and retired from the security profession. As we know, many people working on the front line are at the lower end of pay scales, some on zero hour contracts and often when illness or injury strikes they need help, guidance and support to get back to work or to return to normal life. Financial hardship following injury at work, but only qualifying for Statutory Sick Pay, is unfair and causes great strain in an already stressful situation.

The SBF can be the glue to help families in times of stress or bereavement. Many of the applications are from those who have worked in the manned guarding or door supervisor sectors, although we are here for the wider security profession. In general, these are the sectors that offer little in the way of benefits. For example, no payment when you cannot work after being assaulted doing your job; receiving SSP when unable to work, and having to rely on state benefits for a permanent or semi-permanent disability. Low or no death in service life insurance because companies have reduced margins on contracts, and employee benefits are discarded. Becoming terminally ill when you are the sole worker in the household or the main carer for your elderly parents; or homeless after a family break down without access to counselling. On the run from an abusive partner, trying to protect your daughter whilst working as a security officer and sofa surfing. Life can be a real challenge.

The SBF is different, working to influence employers by highlighting anonymously the social issues of their present and past employees. The goal is that in the near future, Gold Standard companies will include insurance to look after employees if they are injured in the line of duty, with death in service cover to help with funeral expenses, as well as protecting their workers and family’s future. We are seeing more and more applicants with mental health problems, a disproportionate number that lack self-confidence, and take a job where they can ‘hide away’. Some are subjected to bullying and harassment at work but consider they are lucky to have a job. Whilst this is not always true, it is something that we hear often from the people that come to the SBF for help.

We are hearing from an increasing number of people expressing disturbing symptoms of depression and emotional instability. PTSD is an anxiety disorder caused by very stressful, frightening or distressing events. This is not just affecting veterans, our Trust has donated money to the charities Combat Stress and PTSD Resolution, but also to the security officer that witnessed a workplace suicide and was the first responder. The manned guarding sector is improved and we have seen robust structure in some companies that support to the worker, the team and the wider family. We can offer a helpful link to those that want to do more.
Who do we seek to help?
SBF is the only charity dedicated to working with this sector, a profession that has great importance to the UK economy, integral to counter terrorism operations and public safety. Our interventions to date have produced a long list of successes, including:
Charles died of a heart attack getting ready to commence his shift, leaving 4 young children. Earning £9.00 per hour without any insurances, we learned that Charles’s widow was going to borrow money from a payday lender to bury him. We supported her along with family and friends. “This financial support really assisted me and my family at this very difficult time. We are all so thankful to the financial support received and cannot thank the SBF enough”

An urgent application for assistance was received from a charity for the homeless on behalf of Simon who at the time was sleeping rough. He had worked as a security officer and had various short-term security jobs (he had an SIA Licence) as he moved around the country. Simon had been a victim of abuse as a child, suffered from mental health issues as a result, which made it difficult for him to hold down a job, so he had often travelled from place to place, sleeping rough and trying to find work where he could. Whilst sleeping rough, he was the victim of a random attack which left him with life changing injuries meaning he could no longer work and was reliant on benefits. Our intervention helped him into permanent safe accommodation, no longer in danger of attack in what can be a ruthless world. “This is just one case of many. The fact that the SBF listened and reached out to support, means more people like Simon can be helped in the future. Our thanks go out to everyone involved”

Matt had worked as a security guard for a variety of companies over many years. He was signed off work with mental health issues but hoped to be able to return to work in due course. He had recently split up with his long-term partner and, as a result found himself homeless – his partner being the sole tenancy holder. He was sleeping on the sofa at his family’s house but could not stay there. Our intervention helped him get accommodation, he now sees his young son and Matt is working and studying to be a security supervisor. “The SBF helped me to get back to some form of normality, giving me the opportunity to once again see my Son. I cannot thank the SBF enough for their generosity and actually caring enough to get involved and support me”

Nancy was a sofa surfer with a 6 year-old daughter. She was not looking for money, but support. Who could she turn to, to get out of this hell? One of our Trustees knew who could support her, it was important that she kept her job and income. Two years later she has a new life, she works in security but now is a supervisor – Nancy and her daughter are doing well.

“It is the kind, caring nature of the people within the SBF that helped turn my life around”

The immediate future
At first glance we may look back on relative social and economic success that most of us have enjoyed in recent years. Yet, there has always been that underlying social need, some of which would seem to have manifested itself in the last 6 months during which we have received an increase in applications of some 25-30%. Now that the dreaded Coronavirus has struck we can only expect the needs of those associated with the security sector will be sustained, if not further increased.

We have been able to support many of those applications: those who have fallen victim to exceptional circumstances, almost always beyond their control, frequently as a result of serious physical illness and increasingly, mental ill-health.

To quote the Michael Barley, Master WCoSP “ Kindness, compassion and humanity are needed now more than ever. We like to think this is personified in what the SBF has done and continues to do to support those in our profession less fortunate. We can only anticipate this will be needed even more in the current, almost unprecedented circumstances of Covid-19. Now is the time to make a difference “.

The SBF website gives guidance of how to apply for a grant from the fund: www.securitybenevolentfund.org.uk
The SBF urgently needs additional funds to assist the ever-increasing numbers seeking support. We would be enormously grateful for any donations to the fund. Please send donations to: https://www.gofundme.com/the-securitybenevolent-fund or by post to: The Security Benevolent Fund, Clerk to the Worshipful Company of Security Professionals, 4 Holmere Farm Cottages, Goose Green, Thetford, IP25 7AS. Contact: clerk@wcosp.org
In June 2017, eight members of the public were killed and 48 people were injured after a van was driven into pedestrians on London Bridge. Three attackers then exited the vehicle and stabbed people in nearby pubs. After the atrocity, the Metropolitan Police requested the urgent installation of Hostile Vehicle Mitigation (HVM) systems on the eight London Thames bridges with immediate effect. Hardstaff Barriers delivered the requested barriers the very same evening.

Over the following week, Hardstaff completed the installation of HVM products on Westminster Bridge, Vauxhall Bridge, Lambeth Bridge, Waterloo Bridge, Blackfriars Bridge, Southwark Bridge, Tower Bridge and London Bridge to protect and keep people safe. The rapid delivery of these key installations across London astonished many stakeholders and exceeded expectations.

Over the following months, Hardstaff worked closely with the police, councils and bridge owners to amend the deployments, allowing access to bridge chambers and helping to minimise carriageway, footway and cycleway obstructions.

Hardstaff is a Corporate Partner of the Security Institute and holds a number of important accreditations for the supply, installation, repair, maintenance and removal of HVM products, including ISO 9001:2015, ISO 14001:2015 and ISO 45001.

As the trusted contractor for the UK Government's National Barrier Asset (NBA) framework, security and safety are at the heart of Hardstaff Barriers' work. While undertaking this important role, the company has provided HVM barriers for a variety of high-profile events - from the State Opening of Parliament to visits from the President of the United States.
The NBA is a government framework for surface-mounted HVM products, such as high-security gates, pedestrian portals and barriers, which are designed to prevent vehicle attacks on key structures or crowded spaces. The NBA is available to all public and private sector organisations.

The NBA has been deployed at other important events including conferences for the Labour and Conservative parties, UEFA Champions League Final, Commonwealth Heads of Government Meeting, Notting Hill Carnival, Edinburgh Fringe Festival, MTV Music Awards at Wembley, Trafalgar Square U2 music event and Hyde Park Winter Wonderland.

Hardstaff’s clients include police forces, National Counter Terrorism Police, security services, major event providers, airport operators, construction firms, highway maintenance providers and a nuclear power station. The company’s UK expertise has been recognised by securing similar frameworks in Europe, supplying barrier systems to the Dutch Police and Government as part of a joint venture.

In recent years, Hardstaff Barriers has provided safety barriers at numerous prestigious events including Wimbledon, London Marathon, Lords Cricket Ground and Trooping the Colour.

Hardstaff Barrier’s range of HVM products provide protection against vehicle as a weapon attacks, which have been a factor in many terrorist incidents. As a result, HVM measures have significantly increased across London and the rest of the UK over recent years.

Hardstaff has been granted Fit For Nuclear (F4N) status by the Advanced Manufacturing Research Centre (AMRC) after demonstrating its commitment to working in the nuclear industry. The company also holds a Fleet Operator Recognition Scheme (FORS) Gold standard, which is only awarded to exceptional fleet operators.

Niall Griffin, Hardstaff Secure General Manager, said: “Hardstaff Barriers has been involved in the deployment of surface-mounted HVM since its inception.

“Our operatives’ experience, coupled with my own knowledge from time served as a Counter Terrorism Security Co-ordinator, make our team as strong as the protection we can provide.”
With lockdown measures slowly being lifted, we are all looking for positive measures we can put in place to take control. Helping to provide certainty will bring optimism to individuals, groups, and companies alike. To deliver this, you need to look at what your technology systems can do for you right now. You, your investors, your customers, and your staff want to know when your site will be open and working again. Now is the time to start planning. Your security system should be at the heart of your strategy. Used correctly, it can help you emerge from lockdown safely, efficiently, and as quickly as possible, whilst ensuring you can continue to operate.

Security is more than access control
Site managers, health and safety executives, directors, and security professionals need to start looking at their security systems in a new way. Gently shifting your view from one that sees access control as just a security system, to one that facilitates the control of people movement will greatly increase the safety of your site at multiple levels.

Social distancing advice will still be in place as we continue to come out of lockdown. My own personal experience of this has been amazing, with most people I see (while out walking the dog) keeping well over two metres apart. Despite this, it’s obvious that putting new occupation limits in areas or zones within your building will help this behaviour to continue. Look at how your access system could keep track of zonal people counts to actively allow or deny access as the building is used. At the point of access denial, it should also be possible to alert the individual as to why it’s happened, ensuring a feeling of safety within the building.

Reduce contact points
Your staff are most likely using plastic cards to gain access to your building. Issuing new ones is a high contact activity. New cards will be required for all new employees and these often get shared, lost, or forgotten every week. Switching to secure access using mobile phone technology will make huge differences with regards to cost reductions and a contact-free environment. Deployment of the new credential is achieved easily and securely via email with second-factor authentication, removing the need to visit a security office or reception on arrival at the site.
Biometric solutions will also be under scrutiny as many require fingerprint contact, but with the emergence of facial recognition technology, contactless versions are now available and still very much worth considering. Access solutions that support mobile technology will also enable the biometrics built into the phone to authenticate the access decision.

Take some simple measures and look at ways you can remove contact points around your building. Your security system will be full of contact points, most notably the push to exit button. Look at replacing these with contactless IR buttons or an access reader instead. Replacing the opening mechanism on your door to a motorised one will make a big difference.

Explore the tools in your access control system
COVID-safe and immunity passports are phrases we are now hearing on a regular basis. How our post-COVID world will look is currently unclear but businesses will need simple ways to use these to influence an access decision. You may want to consider creating a portal where your staff can register themselves as ‘at risk’ or showing symptoms (I know the excellent company I work for has already implemented this). COVID-19 test results or requested staff data can be used to enforce how and when people gain access to your building. Access control systems have the capability to import this data or link to the databases you hold to facilitate this in an automated way.

Even with the implementation of these measures, incidents can and will occur. Managing your response to those is essential for keeping disruption to a minimum and ensuring staff safety. Having the ability to send messages or evacuation alarms to individuals or groups of people in certain areas is vital. Explore the communication, alarm, and evacuation tools within your access control system and look at ways communication can be achieved via emails, texts, and mobile phone push notifications. Ensuring people receive information quickly and with clear instructions will make a huge difference.

We are, of course, still unclear about when our country, our cities, and our buildings will be fully functional again but this doesn’t mean it’s too soon to start planning. The measures you put in place now will mitigate risk in the future.

Get yourselves ready, put your strategy in place, and be one of the first to get back on your feet and keep your business open. For more information visit: https://security.gallagher.com/COVID-19
On March 9th, Accenture hosted our Cyber-Convergence Special Interest Group (CCSIG) for our ‘Women in Cyber’ event in celebration of International Women’s Day.

The event is focused on celebrating diversity and inclusion in the security profession and in particular the Cyber pillar. The speakers explored various topics and projects on Cyber that will enhance the industry from a diversity perspective.

Our CCSIG Chair and Security Institute Director, Mahbubal Islam CSyP FSyl, led the day’s proceedings and helped handpick the lineup of expert speakers. Our Chairman Professor Alison Wakefield PhD CSyP FSyl was the first speaker of the day, outlining the need for greater diversity within the security industry and the ways in which the Security Institute is helping support efforts that champion diversity.

This was followed by Dr Victoria Baines, who gave a rousing talk exploring her perspective on women in the Cyber Security sector. She started her talk with real-life examples of explanations she had heard from business leaders for their lack of diversity within the sector, getting the entire audience involved with the discussion.

A speaker from the Senior National Cyber Security Centre (NCSC) then took the stage, and highlighted the measures that had been taken within the civil service to create a more inclusive work environment.

Paul Barnard CSyP MSyl, the Security Institute’s Director responsible for our Next Generation in Security Initiative, rounded off the first part of morning’s proceedings chairing a panel discussion on ‘Developing Inclusive Cyber Workforce’. Panellists included: James Gosnold: Independent Security Consultant and CISO at Cyber Trooper, Rekha Babber: Managing Director at Templar Cyber Academy and Astana Davar: Security Consultant. The panel created a lively discussion amongst attendees, debating changes that can be made by recruiters and offering advice for those wanting to enter the sector.
After a short networking break, the line-up continued with Jill Trebilcock, the Deputy Chair of the Cyber Security Alliance. Jill outlined the purpose and objectives of the Cyber Security Alliance and discussed the parts being planned by various organisations including the Security Institute under the leadership of Mahbubul Islam. Jill stressed that all working within the sector are encouraged to contribute to the work of the on-going Alliance, and that there are various routes through which cyber security professionals can get involved.

This was followed by another panel discussion that covered the issues surrounding facial recognition and security surveillance, creating some insightful debate on the morality of these new technologies and if or how they should be implemented by security professionals in both the private and public sector.

Our Chief Executive Rick Mounfield CSyP FSyI then closed the day’s proceedings, summarising the important takeaways from the talks of the day and expressed how much insight he had personally gained from attending.

The event had a great turnout and received fantastic feedback from attendees, there was a buzz during all networking breaks with attendees discussing their work and making new connections with others in the industry.

If you would like to get involved with the CCSIG or any of our other Special Interest Groups please email becky@security-institute.org.

Disclaimer: This event took place before any government restrictions on public gatherings, and all attendees were sent instructions to follow the current government guidelines via email in the lead up to the event. Both the Security Institute and Accenture provided all attendees with anti-bacterial hand wash and other sanitary products through-out the event.
The Register of Chartered Security Professionals was very fortunate to be able to hold its Annual Celebratory Dinner for Chartered Security Professionals on 12th March, just a few days before the lockdown started.

Held at the magnificent Stationers Hall in the City of London, attendees were able to celebrate another successful year for the Register and witness certificate presentations to fourteen new Chartered Security Professionals.

Guests in attendance included the Master of the Worshipful Company of Security Professionals Mike Barley, After-Dinner Speaker Commissioner Ian Dyson QPM of the City of London Police, compere Bob Martin JP CSyP FSyI, CSyPs and guests, and members of the Register management Board. Two key supporting organisations (SIA and CPNI) were also represented, alongside leading universities which provide academic qualifications in security. Unable to attend in person was Lord Alex Carlile, who accepted a position as Patron of the Register of Chartered Security Professionals during 2019.

In welcoming guests, host Baroness Henig of Lancaster CBE DL, Chairman of the Registration Authority, made reference to the rising levels of interest in the Register, as seen by the number of attendees at the CSyP Application Workshops. These continue to be held online for potential applicants with free sessions held weekly in order to meet demand for participants across the globe. Recruitment success in 2019 could also be measured in the additional number of volunteers trained who are now participating in assessing applicants.

It was an extra special evening for those Chartered Security Professionals receiving certificates from Baroness Henig, whilst David Gill CSyP FSyI read citations which demonstrated their diversity, impressive backgrounds and achievements.
New Chartered Security Professionals included:
• Simon Harris MSyI (Sony Picture Entertainment)
• Richard Spence MSyI (FCO)
• Adam Reed MSyI (Sky)
• Amanda Seevaratam (DE & S Abbeywood)
• Paul Barnard MSyI (Ward Security)
• Spencer Bowdler MSyI (Strategic Security Consultant)
• Matthew Hatchard MSyI (Scutum)
• Pete Jones MSyI (Third Millenium)
• Rob Kennedy FSyI (Securigroup)
• Professor Alison Wakefield PhD FSyI (University of West London).

The Register would like to thank the generosity of its sponsors Dallmeier electronic UK, The Security Event, Wagestream and Bidvest Noonan, all of whom were represented.

Plans for 2020 will focus on delivery of the agreed Business Plan which was developed and published in 2019, and all CSyPs will have the opportunity to contribute to this. The 2021 Annual Celebratory Dinner will be held on 11th March 2021, and it is intended to return to Stationers’ Hall.

You can view the full collection of professional photographs taken throughout the evening here: https://www.flickr.com/photos/syinstitute/albums/72157713606188776

Disclaimer: This event took place before any government restrictions on public gatherings, and all attendees were sent instructions to follow the current government guidelines via email in the lead up to the event. All attendees were provided with anti-bacterial hand wash and other sanitary products through-out the event.
Nick Elton CSyP MSyI
Chief Inspector

Nick started his policing career in Cleveland Police in 1994, steadily making his way through the ranks and also serving in Surrey and Wiltshire Police. In 2013, he commenced a four-year secondment with Office for Security and Counter Terrorism where he worked on the Communications Capabilities Development programme. It was during this secondment that he realised the value that membership of professional bodies and associations can bring to one’s career. Not only through the resources available on member websites but also through networking opportunities and contacts. He was made a Chartered Fellow of the Chartered Management Institute in 2013 and a Fellow of the Institute of Directors in 2016. Upon completing the secondment in 2017 he transferred to Hampshire Constabulary and was promoted to Chief Inspector. Working on a similar development program in force he recognised the value that becoming a Chartered Security Professional would entail. Not only contributing to his current role but how the mandatory CPD associated with such an accreditation would stand him well not only professionally but also in a personal context. He joined the Security Institute in early 2019 and started to work towards becoming a Chartered Security Professional. “I found the process very challenging not only in completing the application form and evidencing the required competencies, but also the interview and presentation at the end of the process”, Nick commented. “I was very fortunate to have a former senior police officer on the interview panel and the other panel member was a cyber security expert working for the government, which is my area of expertise. Both interviewers were able to draw out the best of my evidence that I had to present, they clearly understood and had researched my application as the follow-up questions were very bespoke to my area of expertise and clearly both members of the interview team were very knowledgeable on the competencies that I had given on my application form”.

Since becoming a Chartered Security Professional Nick said “Membership of certain bodies and accreditations don’t always go far with employees particularly in the public sector, however, I have found that since qualifying as a Chartered Security Professional it has enhanced my policing career. I have found that it is recognised by stakeholders and law enforcement partners alike as well as academic institutions. My own force has recognised the value of becoming a Chartered Security Professional and the efforts that were required to achieve it and asked me to sit on the Force Security Board and design and deliver an internal cyber exercise. I have also benefited from making many new contacts on LinkedIn since being able to use the CSyP post-nominals. Furthermore, I have found recognition of the Chartered Security Professional accreditation within academia, in the summer 2018 Honours awards I was appointed Visiting Professor to the Faculty of Faculty of Computing, Engineering and the Built Environment at Birmingham City University, since becoming a Chartered Security Professional I have been invited to sit on numerous boards including the Industrial Advisory Board.”

“I have long aspired to have my experience, knowledge, practice skills, leadership and professional commitment to CPD externally audited and validated; the Chartered Security Professional accreditation has achieved all of this. In a dynamic climate CPD is essential if you are to not become static, the Chartered Security Professional accreditation actively encourages me to keep abreast in an ever-changing world”.
At the end of March we started 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 are running weekly CSyP Workshop Webinars through all of May, June and July.

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.
Upcoming Events

Members Lunch
Tuesday 11th August 2020
Time: Doors open at 12pm
Venue: Doggett’s Coat & Badge, 1 Blackfriars Bridge, London, SE1 9UD

Come and find out what’s available in your Institute and how to access it, and let’s get to know each other. This event will be hosted by the membership engagement team, and diaries permitting you will be able to meet some of the elected Board and existing members, as well as other new members.

Book here: https://event.bookitbee.com/27577/110820-members-lunch

Gala Awards Dinner
Tuesday 8th December 2020
Time: TBC
Venue: SEA Life London, Riverside Building, Westminster Bridge Rd, Lambeth, London SE1 7PB

The Institute encourages and recognises excellence, it has developed an annual Awards Ceremony. Recognising individuals and companies for going the extra mile.

Always aiming to deliver a unique and memorable experience, this year’s ceremony will take place at Sea Life London. Guests will be treated to a 3-course dinner with fantastic views of the marine tanks.

Book here: https://event.bookitbee.com/25071/300620-gala-awards-dinner

Syl Annual Conference
Thursday 22nd October 2020
Time (provisional): 9am - 8pm. Registration opens 8.30am
Venue: 1 Wimpole St, Marylebone, London W1G 0AE

We are back again for our premier CPD event on the 22nd October 2020. Following on from our very successful Annual Conference 2019: People-Centred Security. Tickets are now available to join us again, where we will be at a new and exciting conference venue. Come and join us! Guest speakers will provide valuable insight into the latest security knowledge, as well as an update from the Security Institute.

More details will be released soon.

### 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>1st - 3rd September</td>
<td>INTERSEC Saudi Arabia</td>
<td>Saudi Arabia</td>
</tr>
<tr>
<td>8th – 10th September</td>
<td>Counter Terror Expo</td>
<td>London</td>
</tr>
<tr>
<td>8th – 10th September</td>
<td>IFSEC</td>
<td>London</td>
</tr>
<tr>
<td>22nd – 23rd September</td>
<td>The Security Event</td>
<td>Birmingham</td>
</tr>
<tr>
<td>29th September</td>
<td>ST20</td>
<td>Belfast</td>
</tr>
<tr>
<td>1st October</td>
<td>ST20</td>
<td>Dublin</td>
</tr>
<tr>
<td>6th -7th October</td>
<td>Behavioural Analysis</td>
<td>London</td>
</tr>
<tr>
<td>9th - 10th November</td>
<td>Global MSC</td>
<td>Bristol</td>
</tr>
<tr>
<td>24th November</td>
<td>ST20</td>
<td>Glasgow</td>
</tr>
<tr>
<td>2nd - 3rd December</td>
<td>ISE</td>
<td>London</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.

security-institute.org