SECURITY PROFESSIONAL

ASIS INTERNATIONAL® Singapore Chapter



Content Page

Chapter Chairperson's Note 2

Past Events:
World X 4
Women in Security Gathering 6
CPP Review Course 7
Webinar by Kamlesh 8
Q2 Networking Dinner 9

Member Spotlight: 10
Saravanan Sammugam

Membership Matters: 13
We're Glad You're Here

Contributed Articles:
A Proposal for Professionalising Private Security in Singapore 14
Defeating the Fenceline: The UAS Threat to Civilian Critical Infrastructure 18

Calendar of Events 23

Members' Update 24

Editorial Team 28

Management Committee 2025 - 2026 29

Chairperson's Note

Dear Members,

Channel News Asia[1] reported that the recent Shangri-La Dialogue reflects a world becoming more contested and uncertain. Countries are placing renewed focus on hard power such as defence capability, deterrence, and readiness. At the same time, cooperation is not going away. It is simply changing shape. Instead of large institutions, we are seeing smaller and more practical groupings coming together to tackle specific issues like maritime security and subsea infrastructure.

When we step back, the direction is clear. Competition between nations is increasing, but cooperation remains necessary. The US is asking partners to step up while China is engaging more selectively. Countries in our region are taking on a bigger role. Security today is also broader than before. It is no longer about physical security but now includes technology, supply chains, and critical infrastructure. From AI to undersea cables, the landscape is becoming more complex. For us, it is a simple reminder to stay ready, keep learning and stay connected.

Closer to home, I would like to congratulate Sujoy on his election to the ASIS International APAC Board. Thank you for your service as our Secretary and Assistant Treasurer. I am confident you will continue to contribute strongly to your new role.

We had previously invited members to step forward to fill the vacancy. After careful deliberation, the MC has co-opted Mitesh as our newest MC member while Ing Kerne will take on the role of Assistant Treasurer. Congratulations to Sujoy, Mitesh and Ing Kerne on their new appointments.

It has been a busy quarter for the Chapter. Our members took part in the WorldX ITE event, guiding students on their career paths. We also launched our third mentorship programme, our biggest so far, with 21 mentor-mentee pairs. Our Professional Development team ran an online seminar on the implications of AI, and WIS continued to bring members together through its regular gatherings. We also completed another successful CPP Review Course. To round things off, we had our Q2 networking session, with thanks to Corning International for their support.



As we step into second half of 2026, we have more planned. We will continue with our certification courses, talks, and quarterly networking events. We are also working on our Uniform to Civilian resource suite to support SAF and Home Team professionals transitioning into private security.

Our Malaysian Chapter has shared details of their KL conference in August (tentatively 27 August 2026.) We are exploring organising a delegation to travel up and learn from them. In addition, the ASIS International APAC Conference will be held in Singapore on 15 and 16 October, so do block your calendars.

As we cross the mid-point of 2026, let us keep learning, keep connecting and keep doing our part as security professionals.

With warm thoughts and gratitude,



Jeffrey Lam
Chairperson
ASIS International (Singapore Chapter)

Reference

1. https://www.channelnewsasia.com/commentary/shangri-la-dialogue-sld-hegseth-defence-subsea-cable

When Worlds Collide

ASIS Singapore Chapter (Nextgen) & The Astronauts Collective

World X @ ITE College West (26 Feb 2026) & ITE College Central (April 2026)

There's something quietly extraordinary about watching a room full of young people light up — not because of a flashy presentation or a slick sales pitch, but because a real person sat down with them and said: "Let me tell you what I actually do."

That's exactly what happened at World X @ ITE College West on 26 February 2026, and again at ITE College Central in April 2026, when members of the ASIS Singapore Chapter's Nextgen community showed up — in force — to be exactly that: real people with real stories.

A Career Carnival Like No Other
World X, organised by The Astronauts Collective (TAC), is a career carnival unlike anything a typical school talk can offer. Over 100 industry professionals descend on an ITE campus, set up stations, and spend the day in genuine conversation with hundreds of Nitec and Higher Nitec students. No lecturing, no PowerPoints — just honest, human conversations about careers, journeys, and the messy, exciting reality of working life.

The students roam freely, approach whoever catches their eye, and walk away with something more valuable than a brochure: a genuine connection. For many, it was the first time they had sat across from someone working in the security and risk industry and asked: "How do I get there?"

20+ Volunteers, Hundreds of Conversations
Across both editions, more than 20 ASIS Singapore Chapter members volunteered their time. They came from all corners of the profession — cybersecurity specialists, risk consultants, operations managers, site security evaluators — each with a unique story to tell.

They didn't just answer questions. They engaged, they laughed, they shared the detours and unexpected turns that brought them to where they are today. And you could feel it — the shift in the room as curiosity turned into inspiration. Watching a student lean in, eyes wide, asking "how do I get there?" — that's the moment that makes it all worth it.



Hundreds of ITE students networking with industry professionals across the event floor



A volunteer walks a student through education and career pathways in the security industry



The ASIS Singapore Chapter (Nextgen) team at World X @ ITE College West, 26 February 2026

Beyond the Carnival: The Jumpstart Mentorship Programme
But the connection doesn't stop when the carnival ends. Through TAC's mentorship programme Jumpstart, ASIS members have committed to something deeper: a six-month structured mentorship pairing each volunteer as a dedicated mentor to an ITE student.

One mentor, one mentee, six months of guidance, encouragement, and real-world perspective. It's a partnership that extends well beyond a single day of inspiration — it's about walking alongside these young people as they take their first steps into the working world.

The impact of both initiatives together is hard to overstate. Career discovery is one thing. Sustained mentorship is another. Together, they give students not just a glimpse of what's possible, but a hand to hold as they reach for it.

Thank You

To every ASIS member who gave up their weekday to show up, share their story, and invest in the next generation — thank you. Your time is not a small thing. To those who have signed up as Jumpstart mentors, you are doing something that truly matters. And to our partners at The Astronauts Collective, thank you for building a platform that makes this kind of work possible.

We'll be back.

Until next time,

Matt
ASIS Singapore Chapter — Nextgen

Women in Security

WIS Gathering

“In April and May this year, two Women in Security networking events brought energy and connection to our community. We thank Convergint for graciously hosting our April gathering at Que Pasa, and Microsoft for welcoming us at their office premises in May. Both evenings were well attended, buzzing with conversation, new names, and shared purpose. We swapped insights, sharpened our social skills, and traded practical tips on building meaningful networks. In an open, casual exchange, we tackled challenges together and learned from one another, leaving each event inspired, better connected, and ready to strengthen collaboration across the security landscape future.”

1.The new campaign aims to inspire Singaporeans to stay vigilant, and to be prepared by acquiring the necessary skills and knowledge to respond effectively to terror threats. They would like to share the various resources for the new campaign for further sharing within Dell and ASIS communities. Please see table below for the relevant resources.

Campaign Film – Closer Than You Think
Play Your Role Microsite *www.sgsecure.gov.sg/play-your-role*

2.SGSecure produced a new animation video to educate the community on the various roles an SGSecure Responder can play to keep Singapore safe from terrorism. More importantly, it seeks to address concerns or misconceptions such as one’s reservation to report a loved one suspected of radicalisation, and the level of commitment required to be an SGSecure Responder. The video is uploaded on MHA’s YouTube channel, our SGSecure website and social media accounts : SGSecure Responders’ Network Motion-Graphic Animation Video.





Certified Protection Professional (CPP) Review Course

Held from 27 to 30 April 2026





The course attracted seven participants, including a security professional from Australia who travelled to Singapore specifically to attend the programme, demonstrating the strong reputation of the Chapter's professional development offerings.

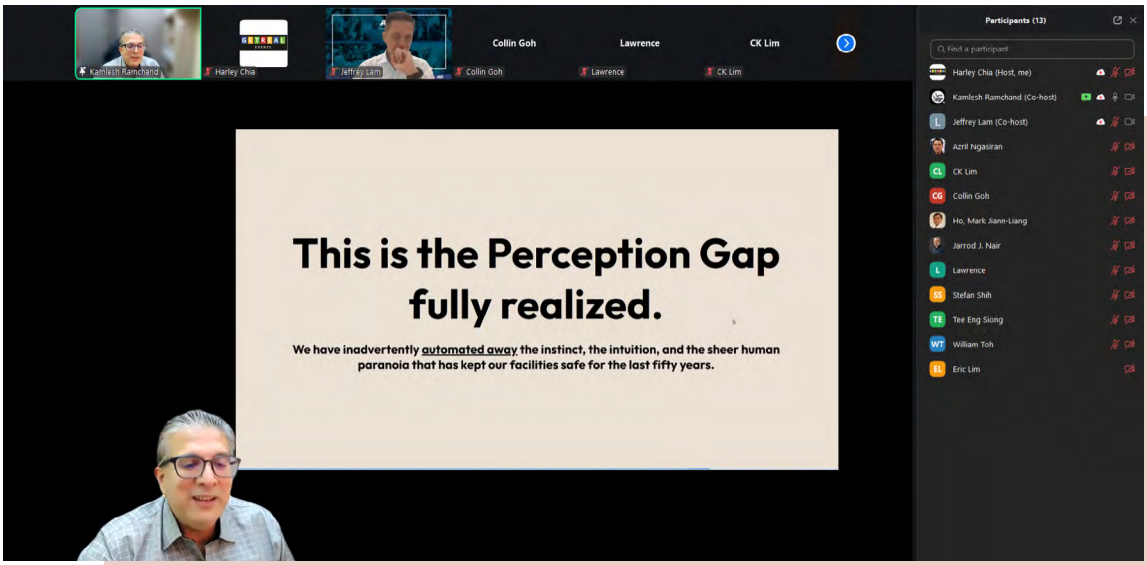
The review course was facilitated by experienced ASIS Singapore Chapter members and CPP-certified security practitioners: Dex Yuan, Jarrod Nair, Lim Choon Kwang, and Melvin Pang. Participants benefited from their extensive industry knowledge, practical insights, and guidance in preparing for the CPP certification examination.

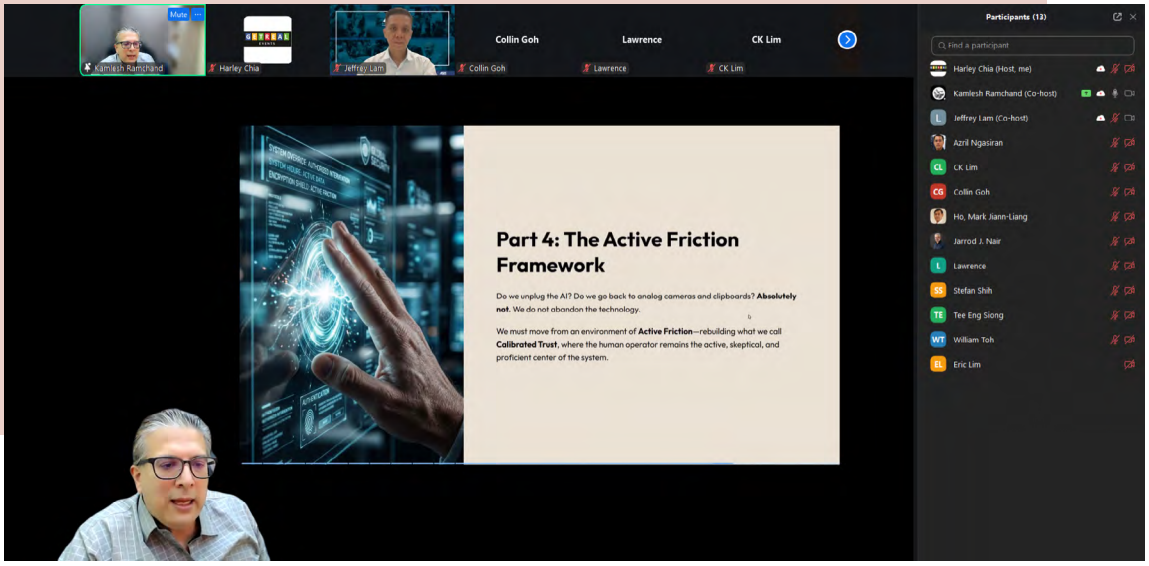
The Chapter would like to thank the trainers and participants for contributing to the success of the programme.

Looking ahead, ASIS International (Singapore Chapter) will continue to support professional development within the security industry through its upcoming Professional Security Professional (PSP) Review Course from 3–5 August 2026, followed by another CPP Review Course from 24–27 August 2026.

Webinar on

Security Gaps in an AI Age.





On 22 April 2026, ASIS Singapore Chapter hosted a webinar on Security Gaps in an AI Age. Our esteemed speaker Mr Kamlesh spoke on the potential pitfalls of over reliance on AI tools in security operations.

It was an engaging presentation and conversation for our members and external guests.

Q2 Networking Dinner

Strengthens Industry Connections

ASIS International (Singapore Chapter) successfully hosted its Q2 Networking Dinner 2026 on Thursday, 25 June 2026, at La Table d'Emma, Mercure ICON Singapore Hotel. The evening brought together 68 security professionals, providing members with an excellent opportunity to reconnect, exchange ideas, and strengthen professional relationships within Singapore's security community.

The event was made possible with the valued support of Corning International Singapore, our event collaborator and partial sponsor for the evening. As part of the programme, Corning delivered an insightful presentation on its latest low-loss fibre optic technology, highlighting how innovations in fibre infrastructure can support the increasing demand for high-performance, secure, and reliable connectivity. Members gained valuable insights into emerging technologies and their practical applications across the security and critical infrastructure sectors.

Beyond the technical sharing, the networking dinner provided a relaxed and engaging environment for members to build new connections, share industry experiences, and discuss the evolving challenges and opportunities facing the security profession. The lively discussions throughout the evening reflected the Chapter's ongoing commitment to fostering collaboration, professional learning, and knowledge exchange among security practitioners.

ASIS International (Singapore Chapter) extends its sincere appreciation to Corning International Singapore for its generous support and informative presentation, as well as to all members and guests whose participation contributed to another successful networking event. We look forward to welcoming members to our upcoming programmes as we continue to connect, educate, and inspire the security community.









Member Spotlight: Saravanan Sammugam

Regional Security Manager, AP – Mastercard



Q **How did you get into a security management career?**

A From Airbase Operations to Corporate Security. I began my career in the Republic of Singapore Air Force (RSAF), where I spent 21 years in roles that demanded precision, discipline, and operational leadership. As a trained Explosive Ordnance Disposal (EOD) engineer and later the Operations Warrant for the Sembawang Airbase Platform Operability Cell, I was responsible for managing base security, emergency preparedness, infrastructure operability, and crisis coordination. Through these experiences, I developed a strong portfolio of transferable skills — **risk management, operational leadership, crisis response, security governance, stakeholder engagement, and the ability to manage high pressure environments with clarity and discipline** — skills that form the backbone of modern security management.

After two decades in uniform, I sought new challenges and began planning my transition into the private sector. My operational background and security-related experience positioned me well for corporate security roles, and I was eventually offered a position as a Security Operations Centre (SOC) Manager for an international bank. Stepping into the corporate world allowed me to apply my militaryhoned skills in a new environment, adapt to emerging technologies, and continue growing as a security professional. This journey from airbase operations to corporate security has shaped my approach to leadership, resilience, and safeguarding organisations in an increasingly complex threat landscape.

Q **What do you like about security management?**

A What I enjoy most about security management is the purpose behind the work — the responsibility of protecting people, assets, and operations so that organisations can function with confidence. Security management is not just about responding to threats; it is about anticipating risks, building resilience, and creating an environment where others can focus on their mission knowing they are safe. The blend of strategy, technology, and human factors keeps the work dynamic and meaningful.

I also appreciate the leadership aspect of the profession. Security management requires clear communication, sound judgement under pressure, and the ability to bring diverse stakeholders together during critical moments. Every day presents a new challenge, and each challenge is an opportunity to improve processes, strengthen teams, and enhance organisational readiness. It is a field where experience, adaptability, and continuous learning truly make a difference — and that is what keeps me passionate about the work.

Q **How long have you been at your current position? How many people report to you/To whom do you report?**

A I currently serve as the Regional Security Manager for Mastercard, overseeing security operations across Southeast Asia and Japan. I have been in this role for the past four years, and in total, I bring over 11 years of experience in the security industry.

Q **What is a typical day like for you?**

A A typical day begins with reviewing and prioritising emails, followed by scanning regional and global news to identify any developments that may impact our operations across Southeast Asia and Japan. Some days pass quietly, but many involve navigating complex challenges — from geopolitical tensions and natural disasters to security incidents and cyber threats affecting our people and business continuity. My role spans a wide spectrum: delivering security awareness training, advising country managers and key stakeholders, reviewing policies and standards, conducting risk assessments, security project management and liaising closely with legal partners and government agencies.

Alongside my professional responsibilities, I am also pursuing part-time studies. I am a strong believer in continuous learning, guided by a principle I embraced during my time in the SAF: learn, unlearn, and relearn. This mindset keeps me adaptable, grounded, and committed to staying ahead in an everevolving security landscape.

Q **What was an especially memorable moment for you on the job?**

A One of the defining moments of my career came during a severe typhoon in Manila that triggered widespread flooding across the city. As roads became impassable and communities were cut off, many of our employees and their family members found themselves stranded in increasingly difficult and uncertain conditions.

In response, we activated an emergency evacuation plan with our security partners. I led the operation, coordinating the movement of affected staff, assessing evolving risks and working closely with multiple stakeholders to ensure that every individual was accounted for and brought to safety. It was a complex and high-pressure situation, with conditions changing by the hour and difficult decisions needing to be made quickly.

What stayed with me was not the operation itself, but the relief on the faces of our colleagues and their loved ones when they finally reached safe ground. Moments like these underscore the true purpose of security leadership. Beyond managing risks and responding to crises, our responsibility is ultimately about protecting people, providing reassurance in times of uncertainty, and ensuring that no one is left behind when they need help the most.

While I have been fortunate to experience many meaningful moments throughout my career, this remains one of the most memorable. It reinforced my belief that the measure of effective security is not simply preventing incidents, but making a tangible difference in people's lives when it matters most.

Q **Do you recommend a career in security to others?**

A I always encourage others to consider a career in security, but I also believe it is a profession that must be embraced with genuine commitment. Security is not just a job — it requires a sense of responsibility, integrity, and the mindset of an ambassador for the organisation and its people. We are entrusted with safeguarding staff, assets, and operations, and that responsibility cannot be taken lightly.

To thrive in this field, you need passion, critical thinking, and the ability to remain calm when situations become challenging. Security professionals often operate in highpressure environments, and the work demands both resilience and purpose. For those who are driven by service, problemsolving, and protecting others, it is an incredibly meaningful and rewarding career.

Q **How were you introduced to ASIS? Why did you decide to become involved?**

A Danny Chan, whom I report to, also serves as Chair of the ASIS Asia Pacific Board and sits on the Global Board of Directors. He was the person who first encouraged me to join ASIS, a decision that would go on to shape my professional journey in meaningful ways.

Within the security community, Danny is widely respected not only for his expertise and leadership, but also for his commitment to developing others. Many practitioners seek his counsel, mentorship and perspective, and he generously invests his personal time in guiding and nurturing the next generation of security professionals.

What has impressed me most is that his influence extends well beyond the workplace. His dedication to service, continuous learning and giving back to the profession inspired me to become actively involved in ASIS and eventually take on the role of Professional Development Lead for the ASIS Singapore Chapter.

Danny's example has shown me that true leadership is not measured by title or position, but by the number of people whose lives and careers are positively shaped by your actions.

Q **Please give an example of how your ASIS membership has helped your career.**

A My ASIS membership has been invaluable to my career. It has allowed me to connect with a wide network of security professionals, creating meaningful relationships within the community and giving me the opportunity to learn from others' real world experiences. These shared lessons are truly invaluable, especially in a field where practical insights often matter more than theory.

Beyond networking, ASIS has provided a platform for collaboration. When incidents or emerging threats arise, we can discuss common challenges, share best practices, and align our approaches to safeguard our operations and staff. This sense of community and collective learning has significantly strengthened my professional growth and broadened my perspective as a security leader.

Membership Matters: We're Glad You're Here

The Singapore chapter is a small, active community of security professionals who show up, share what they know, and look out for one another. If you are a member, you are part of that -- and we would like to keep it that way.

Here is a quick reminder of what your membership includes.

ASIS International

- **Annual fee** - USD 250 (new members: plus a one-time USD 20 application fee)
- **Multi-year option** - 3-year membership at approximately 10% discount (USD 675 vs USD 750)
- **Membership cycle** - Anniversary-based, not calendar year
- Access to global standards, best practices, and guidance
- Member pricing for GSX and other flagship events
- Discounts on certifications, webinars, and e-learning
- Access to ASIS Connects, the global professional community platform

ASIS Singapore Chapter

- Chapter membership runs at SGD 100 per calendar year, separate from your international dues.
- Priority access and discounted rates for local events: seminars, certification prep, site visits
- Four sponsored networking dinners per year -- which alone exceed the chapter fee in tangible value
- Complimentary networking sessions with industry peers
- Study groups, special interest discussions, and the chapter library

Your Renewal, Your Community

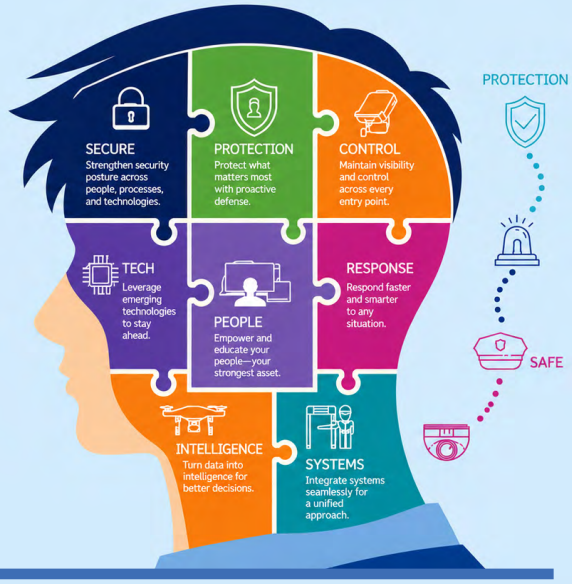
Every member who renews helps keep this community going. The dinners, the events, the familiar faces you catch up with after a few months apart -- these exist because people like you choose to stay involved.

Renewals are triggered by email, so the simplest thing you can do right now is log in to the ASIS International website and make sure your contact details are current. It takes two minutes and ensures your renewal notice reaches you when it should.

For questions or assistance with membership, contact the Singapore Chapter membership team at MemberServices@asis-singapore.org.sg.

A Proposal for Professionalising Private Security in Singapore

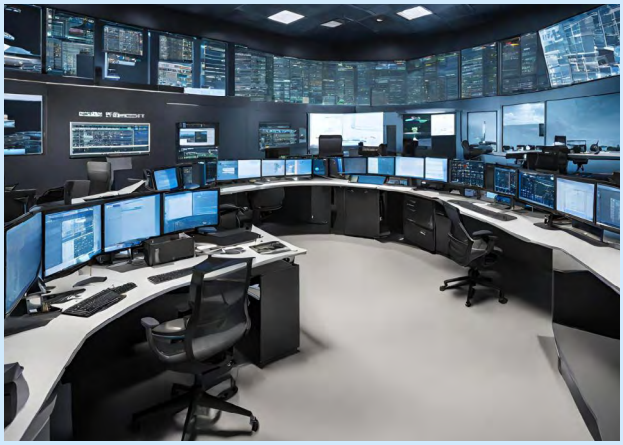
Contributed by:
Muhammad Hafiz Bin Rohani, CPP



The private security industry in Singapore saw significant improvements in recent years, where initiatives such as the Progressive Wage Model (PWM) introduced in 2016 have improved wages, skills development, and career pathway for security professionals. Furthermore, the Security Industry Transformation Map (ITM) inducted in 2018 seeks to transform the traditionally manpower reliant industry to one that utilises technology in mitigating threats, to counter increasing demands for security services and manpower cost due to the shrinking supply of SOs in the market. The private security industry in Singapore is poised to transform itself into an efficient, smart, and digitalised workforce competent in security technologies to augment and enhance security operations in a volatile global threat environment.

Despite these initiatives, the industry still faces key challenges. There is a mismatch between the skillsets of security officers and the technological demands of modern security systems. While digitalisation is increasing, many workers lack the technical expertise needed to effectively use these tools. Furthermore, the industry struggles to attract professionals in managerial, technical, and risk management roles. Another major gap is the absence of a strong, localised body of knowledge and academic pathways in security studies within Singapore, limiting the development of expertise and research in the field.







To counter these foreseen challenges, a three-step approach based on Button and George (2006) concept of 'width and depth' in private security regulation, and Simonsen (1996) foundational steps towards professionalisation could arguably overcome these gaps in knowledge and practice to expand career pathways, develop new and existing security body of knowledge contextualised to Singapore's and the region's threats and challenges, and ultimately professionalise Singapore's security practitioners. With technological solutions and established security and risk management principles, the industry could aspire to engender a professional and well-trained security workforce capable of delivering effective security outcomes, protecting lives, property and information critical to organisations with reduced reliance on manpower.

1. Expanding and Deepening Regulation

The concept of "width" and "depth" in regulation as promulgated by Button and George (2006) could be adopted in our governance of private security in Singapore:

- **Width** refers to the range of roles covered by regulation. The author argues that Singapore's current regulatory regime is too narrow, focusing mainly on security officers, agencies, and certain technical roles.

- **Depth** refers to the competency levels of professionals within the industry.

The private security sector encompasses multiple specialisations, including operational, technical, managerial, consultancy, and investigative roles. However, managerial and consultancy roles are not fully regulated, despite their significant responsibilities, such as planning security operations and handling sensitive information.

To address this gap, it is recommended to extend licensing requirements to include security managers, administrators, and consultants. This would enhance accountability, improve professional credibility, and align Singapore with broader international practices. Regulation could also be integrated with existing frameworks like the PWM to standardise career progression.

Expanding regulation would also broaden career opportunities and change the perception of the industry. By recognising diverse specialisations, it could attract professionals from technical and engineering backgrounds and allow existing workers to transition into new roles, thereby strengthening overall competencies.





2. Enhancing Skills Development and Career Pathways

There is a critical necessity to diversify and deepen skills within the workforce. Currently, career pathways are limited, with insufficient development in technical and managerial tracks.

To support the industry's transformation, it is suggested to move towards:

- Expanding career pathways to include technical and managerial specialisations
  Introducing more targeted training programmes and qualifications
- Encouraging cross-disciplinary learning (e.g., combining operational, technical, and managerial skills)

Vocational and academic institutions can play a role by offering relevant courses, such as security system integration and security engineering programmes. Similarly, tertiary education providers could include business, finance, and management modules to strengthen leadership capabilities among security professionals.

This approach would create a more versatile workforce capable of integrating technology with operational security needs, in line with the goals of the Security ITM.

3. Building a Localised Body of Knowledge

A key argument is that true professionalisation of the security profession requires a robust academic foundation. Established professions such as law and medicine derive their status from well-developed bodies of knowledge and formal education systems (Simonsen, 1996).

In Singapore, however, security education remains underdeveloped. While there are skill-based certifications and diploma programmes, there are limited degree and postgraduate opportunities. Currently, only one undergraduate programme in security studies exists, and postgraduate options are lacking.

In order to counter these deficiencies, expanding academic offerings to include graduate and postgraduate programmes in security management and related disciplines could be a viable solution. These programmes should integrate areas such as:

- Risk management
- Criminology
- Cybersecurity
- Law and regulations
- Crisis and business continuity management
- Behavioural sciences

By strengthening academic research and scholarship, Singapore can develop a localised body of knowledge tailored to its unique security challenges. This would enable practitioners to apply theoretical insights to real-world problems and contribute to innovation in the industry.

Over time, this knowledge ecosystem could produce thought leaders, improve training quality, and attract younger talent to the profession.

Conclusion

In conclusion, the future of Singapore's private security industry depends on building a highly skilled and adaptable workforce capable of meeting evolving demands. As the industry shifts toward technology-driven and outcome-based operations, improving the quality—not just the quantity—of security professionals is essential.
Professionalisation can be achieved through:

- Expanding regulatory frameworks to include all relevant roles
- Diversifying career pathways and enhancing training
- Developing a strong academic foundation and body of knowledge

By implementing these strategies, the industry can transform into a respected profession with clear career progression, improved capabilities, and greater attractiveness to new talent. Ultimately, this will strengthen the effectiveness of security operations and contribute to the safety and resilience of organisations and society as a whole.

References
1. Button, M. and George, B. (2006). Regulation of security: New models for analysis, in M. Gill (ed.) Handbook of Security. London: Palgrave Macmillan, pp. 583-585.
2. Simonsen, C. (1996) 'The Case for: Security Management Is a Profession', in International Journal of Risk, Security and Crime Prevention, 1(3), pp. 229 232



Defeating the Fenceline:

The UAS Threat to Civilian Critical Infrastructure

Contributed by: James Wong CPP, PSP

The Dual-Use Reality of Drone Technology

Unmanned Aerial Systems (UAS) have become a ubiquitous presence in our airspace. We see them heavily deployed across military operations, public safety, and commercial logistics. However, like any mature technology, drones possess a dual-use reality. The same platforms utilized for site surveys and emergency response are increasingly being leveraged for malicious intent.





Adversarial Threats to Civilian Sites

The adversarial use of drones against civilian infrastructure is no longer a theoretical risk. Threat actors are actively using UAS across several distinct attack vectors:

- Corporate Espionage: Drones allow adversaries to bypass traditional physical perimeters and access areas previously considered secure by their elevation. For example, UAS equipped with Wi-Fi penetration tools can hover near building exteriors to intercept network traffic. Furthermore, they can capture high-resolution imagery of sensitive boardrooms or research laboratories located several stories above ground, effortlessly defeating ground-level privacy measures.

- Aiding Physical Intrusions: During a physical breach, UAS platforms provide a significant tactical advantage. A drone offering aerial overwatch can track the movement of uniformed security patrols in real-time. This allows intruders to navigate blind spots and perfectly time their entry or exit to avoid detection.

- Destruction of Operational Technology (OT): Drones pose a direct kinetic threat to critical infrastructure components that are traditionally out of reach from ground-level intruders. Rooftop HVAC systems, cooling towers, and exposed power routing are highly vulnerable. A hostile drone carrying an explosive payload—or simply functioning as a kamikaze device crashing directly into the equipment—can severely damage OT, resulting in immediate and costly facility downtime.

The Challenge of Untraceable Platforms

While commercial drones are typically manufactured with serial numbers and require registration with local authorities—measures intended to aid in regulation, deter misuse, and facilitate post-incident investigations—threat actors actively circumvent these controls. There is a growing proliferation of "ghost drones," which are custom-assembled by users from disparate parts. Because they are built from the ground up, they completely bypass serial number and registration requirements, making post-incident attribution incredibly difficult.

Furthermore, the theft of legitimate, high-capacity commercial platforms is an emerging problem. Recently, there have been reports of large agricultural drones—heavy-lift systems designed for spraying pesticides across farmland—being stolen[1]. When hijacked, these powerful platforms provide adversaries with capable tools that can easily be repurposed to drop substantial payloads or execute kinetic attacks, all while remaining detached from the identity of the malicious operator. The severity of the UAS threat is so pronounced that even China—the country that manufactures the world's most popular DJI drones—has banned the sale and importation of drones into Beijing over profound security fears[2].

The Aerial Vulnerability Gap and Flight Realities

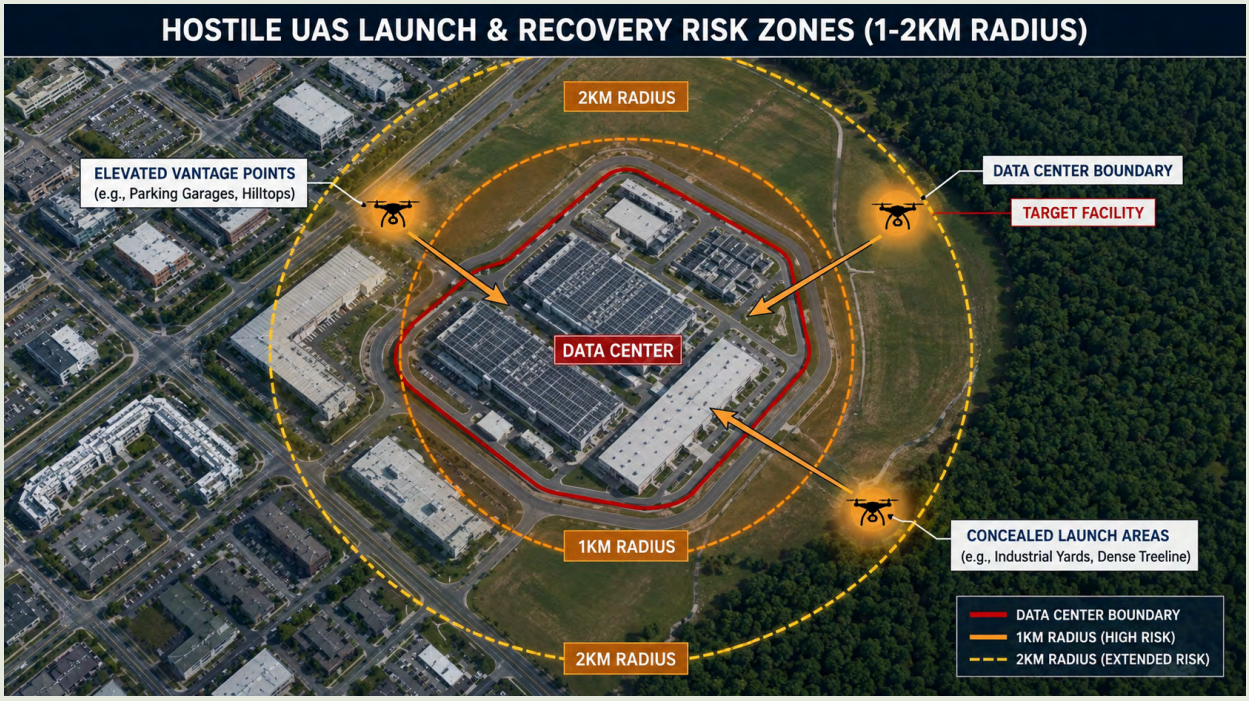
This proliferation of untraceable, high-capacity platforms exposes a severe vulnerability gap in civilian infrastructure. Most sites are designed with robust, multi-layered defenses against ground-level intrusion—fences, bollards, and biometric access controls—but are rarely architected to defend against a three-dimensional threat.



While military and law enforcement agencies have access to advanced Counter-UAS (C-UAS) technologies, the private sector remains heavily restricted from deploying active countermeasures like jamming or kinetic interception due to strict regulatory frameworks.

To understand how to defend against this, we must first understand the operational limitations of the platform itself. A drone's flight time and battery life are drastically reduced when carrying heavy payloads, such as explosives or heavy surveillance equipment. This physical reality dictates that a hostile pilot must establish a launch and recovery site relatively close to the target. Consequently, security assessments must expand beyond the immediate fenceline to identify elevated vantage points and concealed areas within a 1-to-2-kilometer radius that could serve as hostile launch zones.

1. 15 STOLEN AGRICULTURAL DRONES RECOVERED AT NJ WAREHOUSE https://abc7ny.com/amp/post/stolen-agricultural-drones-recovered-nj-warehouse/18979538/
2. China to ban drone sales in Beijing over security fears https://www.straitstimes.com/asia/east-asia/china-to-ban-drone-sales-in-beijing-over-security-fears



Operational Resilience: Architecting for Survival

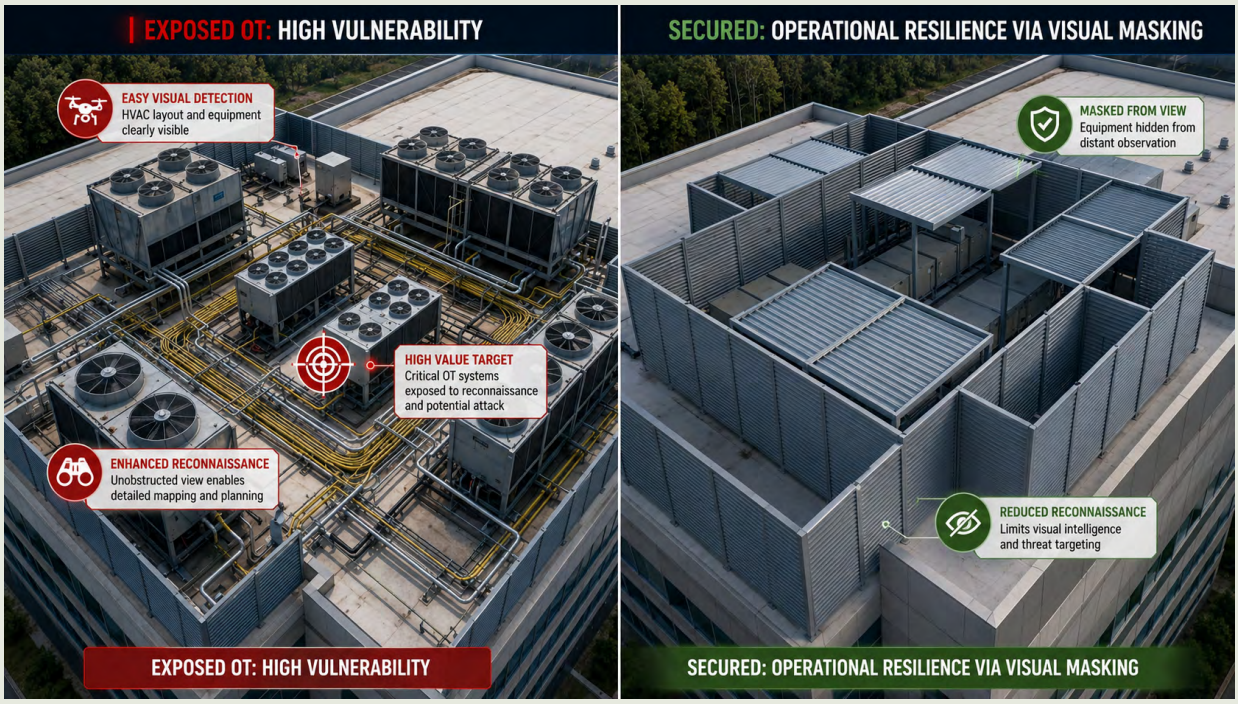
So, how do corporate security teams adapt when active C-UAS defense is restricted?

Some low-tech solutions have emerged from modern conflict zones. In Ukraine and Russia, troops have strung extensive nets across supply chain routes in hopes of tangling hostile drones. While creative, applying this to a civilian critical infrastructure setting introduces immediate complications, including architectural hurdles, maintenance burdens, and legal challenges like the unintended trapping of local wildlife.

The hard reality is that facility security must pivot heavily toward operational resilience. When you cannot legally shoot a drone down, your site must be engineered to survive the impact and maintain Business Continuity Management (BCM). This requires practical, immediate shifts in how we protect our sites:

- Visual Masking and Deception: A drone pilot cannot attack what they cannot see. Implementing physical canopies, louvered screens, or false roofs over critical rooftop OT prevents adversaries from identifying target vulnerabilities during hostile reconnaissance.

Architectural aluminum louvered screens — mounted on a steel subframe at a 45-degree blade angle — block direct overhead sightlines while maintaining necessary airflow. While a hostile pilot may identify the screen at close range, doing so requires flying within detection distance, effectively forcing a tradeoff: the closer the drone gets to confirm its target, the greater the risk of being spotted by security personnel or onsite detection systems — and the higher the chance of a premature collision with the structure itself.



- Redundancy of Critical Systems: Single points of failure exposed on rooftops or exterior yards must be eliminated. Backup generators, secondary cooling loops, and decentralized power routing ensure that if a kinetic strike disables one node, the facility does not suffer a catastrophic outage.

A rooftop cooling tower serving a single chiller plant is a textbook aerial target. Distributing cooling capacity across two physically separated units — connected via a cross-linked piping manifold — means that if one node is disabled, the surviving unit automatically ramps to full load. This N+1 architecture already underpins Uptime Institute's Tier III and IV standards; the UAS threat simply adds a compelling new argument for enforcing it.

- Tailored Emergency Response: BCM plans must account for the unique aftermath of a drone strike. This includes training response teams on how to handle the hazardous, intensely hot fires caused by ruptured lithium-polymer (LiPo) drone batteries, which behave very differently than standard facility fires.

LiPo batteries sustain combustion through an internal chemical reaction requiring no external oxygen — making standard CO_2 and dry chemical suppression ineffective. Response SOPs should default to high-volume water immersion for any drone strike debris, and metal containment bins should be pre-positioned near rooftop access points. Critically, coordinate with your local fire Authority Having Jurisdiction (AHJ) before an incident, not during one.

Tabletop exercises should incorporate a drone strike scenario at least annually. A well-structured exercise should stress-test three decision points: initial detection and confirmation of a hostile UAS, containment of the strike aftermath including LiPo fire response, and activation of BCM protocols to maintain or restore operations. The goal is not just familiarizing responders with the LiPo hazard — it is ensuring that the transition from security incident to emergency response to business continuity happens without hesitation. Gaps identified in exercises are far cheaper to resolve than gaps discovered during an actual event.

The recent targeted drone strikes on AWS data centers in the UAE[3] serve as a stark reminder of this necessity. The threat is no longer over the horizon; it is already in our airspace. We must engineer our critical infrastructure not just to deter the threat, but to absorb the blow, isolate the damage, and maintain continuous operations.

3. Amazon says drones damaged three facilities in UAE and Bahrain https://www.bbc.com/news/articles/cgk28nj0lrjo



About the Author
James Wong, CPP, PSP, *is a security risk assurance specialist focusing on operational resilience and physical security assessments for critical infrastructure. Combining a background in elite law enforcement and corporate security with his experience as a certified Unmanned Aircraft Pilot, his "adversarial" mindset helps organizations prepare for worst-case scenarios. He was recently awarded the 2025 OSPA for South East Asia Outstanding Security Consultant.*

Calendar of Events

ASIS International (Singapore Chapter) Calendar of Events

While the MC will do our best to make these events happen, unforeseen circumstances may sometimes prevent us from doing so.

Month	Date	Activities	Venue
Jun	3	ASIS MC Meeting	VITA and Zoom
	18	AWS	TBC
	25	Q2 Networking Dinner	La Table d'Emma
Jul	8	ASIS MC Meeting	VITA and Zoom
Aug	3-5	PSP Review Course	TBC
	24-27	CPP Review Course	TBC
	12	ASIS MC Meeting	VITA and Zoom
Sep	9	ASIS MC Meeting	VITA and Zoom
	TBC	Q3 Networking Dinner	TBC
	8-9	APP Review Course	
Oct	14	ASIS MC Meeting	Zoom
	11	ASIS MC Meeting	VITA and Zoom
Nov	TBC	Q4 Networking Dinner + AGM	VITA and Zoom



50% Membership Fee Promotion

Join the ASIS Singapore Chapter and enjoy 50% off membership fees for new sign-ups from **1 July to 30 September**.

Don't miss this limited-time opportunity to connect with a global network of security professionals.

Members' Update



Warm Greetings to the following new ASIS International Singapore Chapter Members!

Ms	Blair Ferguson		Mr	Marc Klintfalt	
Mr	Bryan Ang	CPP	Mr	Mervyn Asher	
Mr	Chao Zhen Wang		Mr	Migom Doley	
Mr	Choon Wee, Jackie Ong		Mr	Muhammad Shahrul Bin Isnin	
Mr	Fabian Lim		Mr	Neil Tang	
Mr	Fan Sheng Chen		Mr	Pan Lin	
Mr	Fauzi Rudy		Mr	Qinyong Lai	
Mr	Hao Jun Chan		Mr	Rene Shepherson	
Mr	Harikaran Pillai		Mr	Renfu Marcus Seng	
Mr	Hong Liang Chua		Mr	Samuel Zhang Junyang	
Ms	Hui Jie Zhang		Ms	Sandra Ang	
Ms	Ismail Umar Sumaiya Begam		Mr	Shaun Goh	CPP
Mr	Kah Ong Keon Lim		Mr	Sirong Lee	
Mr	Keith Ng		Mr	Stanley Chi-Fung Tse	PSP
Mr	Kim Meng Ow		Mr	Wong Teng Chao	
Mr	Li Hang Cheng				

Congratulation to Newly Certified Members!

Newly Attained CPP

Mr	Bryan Ang	CPP	Ms	Michelle Ang Shan Yun	CPP
Mr	Hock Chye Seah	CPP	Mr	Shaun Goh	CPP
Mr	John Yim	CPP	Mr	Wei Lun Soo	CPP

Newly Attained PSP

Ms	Abigail Wong	PSP	Mr	James Wong Li Ren	PSP

Newly Attained APP

Ms	Yi Yan Lee	APP

Members' Update



Certified ASIS International Members

Certified CPP, PSP, PCI members

Mr	Adrian Voon-Ming Wong	CPP, PCI, PSP
Mr	Chua Boon-Hwee	CPP, PCI, PSP
Mr	Colin J Spring	CPP, PCI, PSP
Mr	Galvin Lee	CPP, PCI, PSP
Mr	Jag Foo	CPP, PCI, PSP
Mr	Melvin Pang-Boon-Choon	CPP, PCI, PSP
Mr	Pandian Govindan	CPP, PCI, PSP
Mr	Peter Tan	CPP, PCI, PSP
Mr	Quek Wei Chew	CPP, PCI, PSP
Mr	Rajesh	CPP, PCI, PSP
Mr	Shamus See Yew Yeo	CPP, PCI, PSP
Mr	Shi Sheng Koh	CPP, PCI, PSP
Mr	Stefan Shih	CPP, PCI, PSP

Certified CPP, PSP members

Mr	Abdul Razak Daseran	CPP, PSP
Mr	Boon Kiat, Peter Ang	CPP, PSP
Mr	Choon Kwang Lim	CPP, PSP
Mr	Eddie Koh	CPP, PSP
Mr	Gaoping Xiao	CPP, PSP
Mr	Ian D Milne	CPP, PSP
Mr	Jon Sheng Johnson Teo	CPP, PSP
Mr	Kenneth Lau Yip Choy	CPP, PSP
Mr	Kin Wai (Dex) Yuen	CPP, PSP
Mr	Lawrence Yong Qi Tan	CPP, PSP
Mr	Lee Choon-Wai Anthony	CPP, PSP
Mr	Melvin Tze-Hui Cheng	CPP, PSP
Mr	P Vikneswaran	CPP, PSP
Mr	Willie Chin-Sion Heng	CPP, PSP

Certified CPP, PCI members

Mr	Manik Dhir	CPP, PCI

Members' Update

Certified ASIS International Members

Certified CPP members

Mr	Abdul Redha Redha Bin Abdullah	CPP
Mr	Alfian Idris	CPP
Mr	Andrew Tuck-Chee Fan	CPP
Mr	Anton Chan	CPP
Mr	Ayden Elijah Koh	CPP
Mr	Azharie B Mohamed Mudakir	CPP
Mr	Balasubramaniam Selvam	CPP
Ms	Bao Yi Ow	CPP
Mr	Benjamin R Simar	CPP
Mr	Boon Hoe Tan	CPP
Mr	Boon Chew Winson Sheo	CPP
Mr	Boon Teck Kho	CPP
Mr	Choon Loong Loke	CPP
Mr	Choon Teck Tay	CPP
Mr	Chye Heng Lim	CPP
Mr	Clement Chan	CPP
Mr	Damien Lim	CPP
Mr	Daniel Ng	CPP
Mr	David Kaye	CPP
Mr	Edwin Goh	CPP
Mr	Eugene Chua	CPP
Mr	Firman Latib	CPP
Mr	Francis Zhang	CPP
Mr	Goh Jun Xian	CPP
Mr	Gwee Khiang Tan	CPP
Mr	Hartmut Kraft	CPP
Mr	Huajun Ren	CPP
Mr	Ing Kerne Yeh	CPP
Mr	Isaach Choong	CPP
Mr	James Wong Li Ren	CPP
Mr	Jarrod James Nair	CPP
Mr	Jeffrey Yeo	CPP
Mr	Jianhao Lee	CPP
Mr	Jiann Liang Ho	CPP
Mr	Jing Chyi Pang	CPP
Mr	Joseph F. Jasunas	CPP
Mr	Justin Jianan Chen	CPP
Mr	Kah Meng Joseph Lye	CPP
Mr	Kai-Quan Den Ho	CPP
Mr	Kang Yong Look	CPP
Ms	Karen Wong	CPP
Mr	Kee Kiat Teo	CPP
Mr	Kelvin Koh	CPP
Mr	Ken Guorong Ang	CPP
Mr	Kim Poh Ong	CPP
Mr	Koh Wei Soon	CPP
Mr	Krishnamoorthy Arunasalam	CPP
Mr	Kwang Wee Koh	CPP
Mr	Lawrence Jun-Ming Tan	CPP
Mr	Leonard Ong	CPP
Mr	Marcus ChongLay Tan	CPP
Mr	Mark Chow	CPP
Mr	Max Hirsch	CPP
Mr	Mitran Balakrishnan	CPP
Mr	Muhammad Hafiz Bin Rohani	CPP
Mr	Muhammad Iskandar Bin Idris	CPP
Mr	Muhsin Ben Moasi	CPP
Mr	Nilo S Pomaloy	CPP
Mr	Noriman Salim	CPP
Mr	Patrick Tse	CPP
Mr	Paul Rachmadi	CPP
Mr	Perry Peter Yeo	CPP
Mr	Qinhui Zhou	CPP
Mr	Sanjay Sharma	CPP
Mr	Sekar Sivalingam	CPP
Mr	Shaymentyran Shaem	CPP
Mr	Siang Siang Rendall Foo	CPP
Mr	Simon Eng-hu Tan	CPP
Mr	Sujoy Dutta	CPP
Mr	Surendran Chandra Segaran	CPP
Mr	Thian Beng Lim	CPP
Mr	Thirukumaran Sankaran	CPP
Mr	Vikneshwaran Ganesan	CPP
Mr	Wai Mun Mun Chia	CPP
Mr	Wai Peng Sam	CPP
Mr	Wayne G Edmonds	CPP
Mr	William Toh	CPP
Mr	Wilson Loh	CPP
Ms	Xin MincThung	CPP
Ms	Yen Hwa Cheng	CPP
Mr	Yeong Sing Lim	CPP
Ms	Yuen Yee Jeannie Tam	CPP
Mr	Zihui Lai	CPP

Members' Update

Certified ASIS International Members

Certified PSP members

Mr	Abdul Khandar Bin Abd Aziz	PSP	Mr	Kay Boon Low	PSP
Mr	Bryan Tang	PSP	Mr	Kevin Loh	PSP
Mr	Dion Yeo Lai Ye	PSP	Mr	Kim Heng Tan	PSP
Mr	Isaac Yip	PSP	Mr	Mayank Sinha	PSP
Mr	Jeffrey Boonkee Lam	PSP	Mr	Wei Jye Soh	PSP
Mr	Jianhui Chan	PSP			

Certified PCI members

Mr	Hemant Kumar Haridas	PCI
Mr	Karanbir Singh Sandhu	PCI
Mr	Rupesh H K	PCI

Certified APP members

Ms	Abigail Wong	APP	Mr	Kok Kheam Tay	APP
Mr	Chin Chye Raymond Teo	APP	Mr	Ngan Leng Tan	APP
Ms	Ching Peng Chin	APP	Mr	Poh Tiong Ong	APP
Mr	Daniel Chan	APP	Mr	Swee Chye Loh	APP
Mr	Edzel See	APP	Mr	Teo Thiam Chye	APP
Mr	Faizul Salamon	APP	Mr	Wei Lun Soo	APP
Mr	Jason Siow	APP	Mr	Weng Hong Ow	APP
Mr	Jeremiah Ong Wei Yi	APP	Ms	Yan Ling Lim	APP
Ms	Jia Hui Tay	APP	Mr	Zi Han Quak	APP

Editorial Team



Perry Yeo, CPP
Editor



Muhammad Hafiz Bin Rohani, CPP
Contributor



James Wong, CPP, PSP
Contributor

Calling for Articles

Share your experience and knowledge now and earn up to 9 CPE points.

Article should not contain more than 1,000 words in words document with illustrations, diagrams,and/or photos.

We are seeking articles of interest from all members, which may relate to terrorism, physical security, executive protection, investigations, product counterfeiting, supply chain security, crisis management or business continuity management. Articles may relate to current or emerging issues, best practices or challenges faced by security professionals responsible for the protection of people, property, and information in their organisations.

Members with CPP/PSP/PCI/APP will pleased to note that published articles may earn up to 9 CPE credits through the CPE self-reporting page during recertification.

Please email the articles to memberservices@asis-singapore.org.sg
Submissions close on 1 December 2025

Management Committee 2025-2026

Honorary Chairperson

Mr. Jeffrey Lam, PSP

Honorary Vice-Chairperson

Mr. Eddie Koh, CPP, PSP

Honorary Secretary

Mr. Ian D Milne, CPP, PSP

Honorary Asst. Secretary

Mr. Azril Ngasiran, CPP

Honorary Treasurer

Mr. Collin Goh

Honorary Asst. Treasurer

Mr. Yeh Ing Kerne, CPP

Honorary MC Members

Ms. Ava Gui

Ms. Chow Keng Fong

Mr. Saravanan Sammugam

Mr. Lim Chye Heng, CPP

Mr. Matthew Lee

Registered Mailling Address:
ASIS International (Singapore Chapter)
1 Coleman Street, The Adelphi, B1-32, Singapore 179803

Website: www.asis-singapore.org.sg

Email: memberservices@asis-singapore.org.sg