SECURITY PROFESSIONAL

ASIS INTERNATIONAL® Singapore Chapter



Content Page

Chapter Chairperson's Note 2

Past Events:
Seminar: Securing Digital Assets 4
Women in Security:Showing Up, Connecting & Growing 5
Bringing the CPP Review Course to NUS 6
Recruitment Trends & Observations in the Security Industry: A Southeast Perspective 7
Q3 Networking Dinner 8
Connecting, Learning and Celebrating

Member Spotlight: 9
Lim Chye Heng, CPP

Contributed Articles: 12
When Sustainability Meets the Threat Surface

Calendar of Events 15

Members' Update 16

Editorial Team 20

Management Committee 2025 - 2026 21

Chairperson's Note

Dear Members,

A few years ago, learning something new meant spending hours reading articles, attending courses, and talking to experts. Today, AI can explain, analyse and summarise a topic in minutes. That got me thinking. If everyone has access to information, perhaps what sets us apart is no longer just what we know, but what we can do with that knowledge.

As security professionals, that often means helping others understand risk and act on it. Identifying a vulnerability or assessing a risk is usually the easy part. Getting stakeholders to commit and employees to change behaviours can be a slow and sometimes uncertain process. This requires communication, credibility, relationships, influence, and sometimes a fair bit of persistence.

Recently, the Singapore Police warned of a scam involving AI-generated deepfakes and the impersonation of senior government officials during a fake Zoom meeting. The lesson is simple. Communicating how technology may be misused matters but helping people recognise the threat and respond correctly is even more important.

With this in mind, we have deliberately focused our recent networking talks on developing soft skills.

During our Q2 networking dinner, we explored personal branding. The speaker discussed how we can build credibility through the way we present ourselves, communicate with others and develop professional relationships. When people trust us, they are more likely to listen to our recommendations and support our solutions.

At our Q3 networking dinner, we looked at influencing behavioural change. Creating policies and processes is often the easy part. The real challenge is getting people to adopt the right behaviours and develop a security-focused mindset.



We hope these sessions provided you with practical ideas to become more effective security professionals.

Of course, we have not forgotten about technical development.

On 15-16 October, the ASIS International APAC Conference will be held in Singapore. Paid-up members are entitled to a S$100 discount off the standard registration fee. This will be followed by the ASIS international Special Dialogue on 10 November. This half day session will be held in conjunction with the Safety & Security Show. Both events offer excellent opportunities to learn about emerging trends, hear from industry experts and connect with fellow professionals.

As technology continues to evolve, technical expertise remains important. But in a world where information is increasingly available to everyone, our ability to communicate, influence and build trust are equally important.

Let's keep learning, keep connecting, and keep sharing with one another.

With warm thoughts and gratitude,



Jeffrey Lam
Chairman 2025-26
ASIS International Singapore Chapter

Seminar:

Securing Digital Assets

On 22 July 2026, the ASIS International (Singapore Chapter) held a seminar on digital asset security at the Mastercard office hosted by Sara (Saravanan Sammugam). An intimate group of ten attended the one-hour session. The speaker was Jag Foo, CFtP, CPP, PSP, PCI, Chief Security and Policy Officer at Safeheron, an institutional custody infrastructure provider. He began with the idea that everything else rests on. In traditional finance, a bank can reverse a transfer and a password can be reset. With digital assets, a confirmed transfer is final. There is no chargeback, no reset and no helpdesk. The private key is not a password; it is the asset. Whoever holds it controls the funds.

Jag then set out the threat landscape. He cited about US$3.4 billion stolen in crypto hacks during 2025, including the US$1.5 billion Bybit breach, and roughly US$17 billion lost to scams and fraud. He grouped institutional losses into five routes: private-key compromise, social engineering, supply-chain attacks, abuse of approvals, and insider misuse.



The most striking part of the session covered the new face of social engineering. Attackers no longer depend on misspelt domains. They now work through infrastructure people already trust. Jag's examples included a phishing email that led to a genuine GitHub authorisation page, fake AI-tool download pages served through sponsored search results and hosted on Squarespace and Google Sites, and a "screenshot" attached to a support ticket that was in fact a trojan. He also covered the Arup case, where a finance employee on a video call with deepfaked executives authorised US$25.6 million in transfers. His conclusion was that the old advice to "spot the fake" no longer works. The process itself has to be the control.



He closed with practical defences. The first is a simple habit he calls the "3 Firsts": don't click first, don't sign first, verify first. On the technical side, institutions can remove the single point of failure through multi-party computation, where the complete key never exists in any one place, supported by hardware enclaves, hardware security modules and a policy engine that enforces approvals before any signature is possible.

A lively Q&A session followed the talk. Participants pressed Jag on points from across the presentation, and the discussion continued after the formal programme ended.

The Chapter thanks Jag Foo for sharing his expertise, and Mastercard for hosting the event.

Stay connected. Stay secure. See you at the next one!

Women in Security:

Showing Up, Connecting & Growing

Our Women in Security networking journey continued with two wonderful gatherings in July and August. In July, we stepped away from our usual setting to visit The Albatross Exhibition, where the experience sparked conversations, curiosity and plenty of laughter. In August, we came together once again to reconnect, network and broaden our knowledge through an insightful sharing on Intellectual Property by Christabel Koh. Both gatherings reminded us that learning does not always have to take place in a formal setting. Sometimes, the best learning happens through conversations, shared experiences and the connections we make along the way.

What makes these meet-ups especially meaningful are the ladies who consistently show up. Every gathering is an opportunity to strengthen relationships, exchange perspectives and learn something new. By making the time to participate, engage and contribute, each woman is also quietly building her own personal brand, confidence, charisma and knowledge. It is wonderful to see familiar faces returning, new friendships developing, and women supporting women as we grow both personally and professionally.

Most importantly, this community becomes stronger with every woman who chooses to be part of it. So, to all the ladies in Security, come join us at our next gathering! Bring your experiences, your curiosity and your unique voice. You never know who you might inspire, or who might inspire you. Let's keep showing up for ourselves, for one another and for the women who will follow in our footsteps.



Bringing the CPP Review Course to NUS

From 8 to 11 September, ASIS Singapore Chapter conducted a private four-day Certified Protection Professional (CPP) Review Course at the National University of Singapore (NUS) campus, designed specifically for the university's security team. Nine NUS staff members took part in the intensive programme.

The course was led by two experienced practitioners, Dex Yuan, CPP, and Melvin Pang, CPP, PSP, PCI, who guided participants through the CPP body of knowledge across the four days. Sessions covered key domains including Physical Security, where participants examined how to test security measures by prioritising site-specific threats, identifying worst-case scenarios and determining where an adversary must be detected, and Crisis Management, which explored how organisations prepare for, respond to and recover from major incidents.

Holding the course on-site allowed the trainers to connect the material directly to the participants' own working environment. The interactive format encouraged lively discussion, with participants sharing real-world experiences from managing security on a large, busy campus.

The programme was a great success, and we thank NUS for hosting and for its commitment to developing its security professionals. We also extend our appreciation to Dex and Melvin for generously sharing their time and expertise.

Interested in a private course for your organisation? ASIS Singapore Chapter offers private CPP and PSP review courses for corporate teams, tailored to your organisation's needs and conducted at your own office. Contact us to find out more.



Melvin Pang leading the Crisis Management session



Nine NUS security staff took part in the four-day course



Covering Physical Security: testing security measures



Melvin Pang, CPP, PSP, PCI

Recruitment Trends & Observations in the Security Industry: A Southeast Asia Perspective

On 21 September 2026, ASIS Singapore Chapter hosted an exclusive chapter webinar on the talent landscape shaping security leadership in the region. Held on Zoom from 5:00pm to 6:00pm (SGT), the session drew 24 attendees from among our members and the wider security community.

Our speaker was Chris Meager, Managing Partner of Enteles Search, who brought nearly three decades of experience in the security profession, including 27 years focused on corporate security recruitment. Chris has placed security professionals in more than 60 countries and works with organisations worldwide on CSO and senior security appointments.

Chris shared his observations on the hiring trends currently reshaping the security function, the skills and competencies employers are now seeking, and the talent attraction and retention challenges specific to South East Asia. He also offered his outlook for security leadership roles, giving attendees practical insight into how they can position themselves for the next step in their careers. The session closed with a lively Q&A, as participants raised questions on career progression and building high-performing security teams.



Event poster: Recruitment Trends & Observations in the Security Industry

Chris is a member of ASIS International, The Security Institute and AIRIP, sits on the Advisory Board of the Association of Corporate Investigators, and was named a Top 30 Global Security Influencer in 2024 and UK Security Influencer in 2026.

We thank Chris for his time and insights, and all attendees for joining us.

Q3 Networking Dinner

Connecting, Learning and Celebrating

On 23 September 2026, ASIS Singapore Chapter welcomed 89 members and guests to our Q3 Networking Dinner at Pan Pacific Singapore. The evening brought together security professionals from across industries for an evening of good food, meaningful conversation and professional learning.

The highlight of the evening was a sharing session by our invited speaker, Kenneth Kwan, Founder and Global Change Leadership Speaker at Deep Impact Pte Ltd, titled “Human-Centred Change: Small Steps That Create Big Changes”. Kenneth spoke about how security leaders can guide their teams and organisations through change, from building buy-in and communicating clearly to sustaining new ways of working. His practical insights resonated strongly with attendees, many of whom are navigating transformation within their own security functions.

As the dinner included this professional sharing, attendees are eligible to claim 1 CPE point towards maintaining their ASIS certifications, one more reason to join us at our quarterly dinners.



Kenneth Kwan on human-centred change



89 members and guests joined us



Lucky draw winner with BluOcean Security

The food was excellent, and the evening was made even more exciting with our lucky draw, where five fortunate attendees walked away with electronic prizes.

Special thanks to our sponsor, BluOcean Security, whose generous support made the evening possible. We are grateful for their continued commitment to the security community in Singapore.

Thank you to Kenneth for his insightful sharing, and to everyone who joined us. We look forward to seeing you at our Q4 Networking Dinner!



Another happy lucky draw winner



Lucky draw prize presentation



Five electronic prizes were given away

Member Spotlight: Lim Chye Heng CPP

Multi-Cluster Security Manager at Amazon Web Services (AWS)



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

A I started my career with the Police Force, which gave me a good foundation in security operations, discipline and risk management.

I later moved into private security, where I had the opportunity to see security from a different perspective and understand how it supports business operations, people and organisational resilience.

Over the years, my role gradually expanded from day to day security operations into managing teams, regional programmes and broader security responsibilities across multiple locations.

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

A What I enjoy most is the variety of the work. Security management is not only about systems, procedures or responding to incidents. A big part of it is working with people, understanding the business and making decisions based on the risks we see.

In my current role, I also enjoy the opportunity to work with teams across different countries. Every location has its own challenges, so there is always something to learn.

I also get a lot of satisfaction from developing people and seeing team members grow. For me, a good security team is one that can make sound decisions and operate confidently, even when the manager is not there.

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

A I have been in my current regional security role since 2023, with responsibility for data centre security operations across several locations in ASEAN.

I currently have about 30 reports and also work closely with a wider group of security professionals, service providers and stakeholders across the region.
I report to Regional Security Manager within the APJC security organisation.

One thing I have learned in a regional role is that leadership is not only about the people who report directly to you. A large part of the job is working across teams and influencing people where there may not be a direct reporting relationship.

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

A There is probably no such thing as a typical day, which is part of what makes the role interesting. A normal day could include reviewing security operations across different locations, discussing project requirements for new sites, looking at security risks, working through compliance issues or meeting with service providers.

I also spend quite a bit of time working with managers and team members, as well as colleagues from other functions and regions.

As my role has become more regional, I try to look beyond the immediate issue. Instead of only asking how we solve a problem today, I also look at whether there is something we can improve in our process so the same issue can be prevented or managed better in future.

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

A One memorable experience was supporting our operations during a period of civil unrest.

We had done quite a bit of preparation beforehand, including setting up our command structure, information channels and response processes. When the situation developed, the team was able to respond calmly, keep track of what was happening and make decisions as conditions changed.

Most importantly, our people remained safe and our operations were not disrupted.

What stood out for me was seeing the team work together under pressure. It was a good reminder that crisis management is not something you start when an incident happens. The preparation, relationships and exercises that take place beforehand are just as important.

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

A Yes, definitely.

Security today is much broader than many people realise. There are opportunities in physical security, investigations, intelligence, risk management, technology, crisis management, business continuity and many other areas.

It can be a very rewarding career for someone who enjoys solving problems, working with people and dealing with situations where the answer is not always straightforward.

Technology will continue to change the way we work, but I believe judgement, communication and the ability to understand risk will always be important skills in this profession.

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

A I joined ASIS in 2018 because I wanted to broaden my exposure beyond my own organisation and learn from other security professionals.

What I found useful was the opportunity to meet people from different industries and hear how they deal with similar security challenges. Sometimes we become very familiar with the way our own organisation does things, so it is helpful to hear different views and approaches. Over the years, ASIS has given me a good platform to continue learning, exchange ideas and stay connected with the wider security community.

I also believe that professional associations are most useful when members are willing to contribute, share their experiences and support others in the profession.

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

A One of the main benefits for me has been the exposure to security professionals from different industries.

Most of my current work is focused on data centre security and regional operations, so it is useful to hear how people in other sectors approach areas such as risk management, technology, crisis response and leadership.

It helps me look at issues from a different perspective instead of only through the lens of my own organisation.

The networking and sharing within ASIS have also given me ideas that I can bring back to my work. More importantly, it reminds me that security is always evolving and that we need to keep learning, regardless of how much experience we have.

When Sustainability Meets the Threat Surface

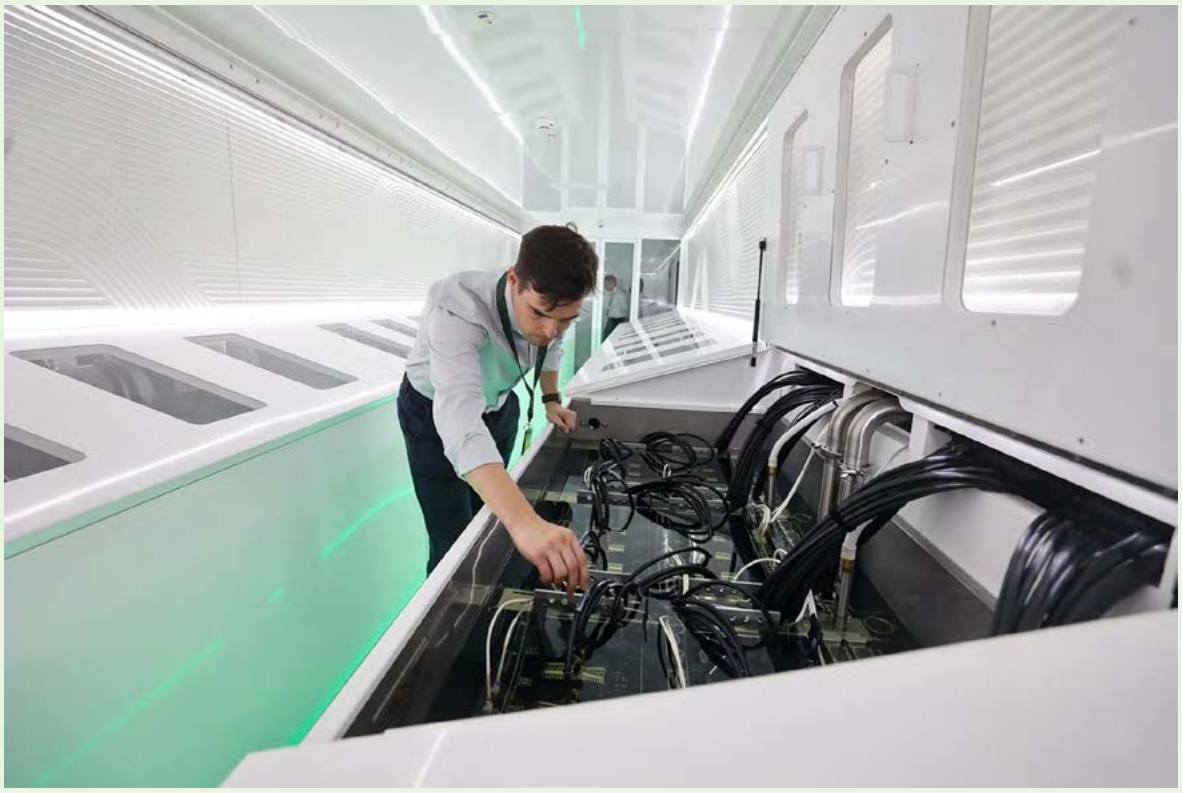
Security risk in Singapore's green data centre push

Contributed by: Daniel Chan, APP



Singapore's data centres consumed about 7 per cent of the country's electricity in 2020, roughly 3.40 terawatt-hours, up from 5.3 per cent the year before.[1] That figure is the reason the Government has spent the past two years rewriting how these facilities are built and run. The Green Data Centre Roadmap, launched in May 2024, set a target Power Usage Effectiveness of 1.3 or lower at full IT load within ten years, and offered at least 300 megawatts of new capacity to operators who can deliver it.[2]

Most of the commentary has treated this as an energy story. I want to make the case that it is also a security story. The measures that make a data centre greener change what security professionals have to defend, and in three specific ways they make our job harder rather than easier. For ASIS members in Singapore, this is worth understanding now, while the standards are still being written.



1. Efficiency removes the thermal buffer that used to absorb failure

The single largest efficiency gain available to a tropical data centre is to stop over-cooling it, and Singapore is pursuing that gain deliberately.

In August 2025, IMDA launched SS 715:2025, the Singapore IT Energy Efficiency Standard for Data Centres. It requires IT equipment to operate safely at temperatures of up to 35 degrees Celsius and targets at least 30 per cent savings in IT equipment energy use.[3] Running warmer saves a great deal of power. It also means there is less headroom before hardware is at risk when cooling fails. The operational technology security firm Dragos notes that server room temperatures can become unacceptably hot within about five minutes once backup cooling is absent.[4]

We have already seen what that looks like here. On 14 October 2023, a chilled water system fault at an Equinix facility in Singapore raised temperatures in the data hall and took DBS and Citibank services offline for more than twelve hours. Speaking in Parliament on 6 November 2023, Minister of State Alvin Tan reported that approximately 2.5 million ATM and payment transactions could not be completed and 810,000 attempts to access the two banks' digital platforms failed.[5] No attacker was involved. A cooling plant simply stopped working. The lesson for our profession is that the facility layer now sits on the critical path for national services, and the efficiency agenda is steadily shortening the time we have to respond when that layer fails.

2. Sustainability cannot be proven without instrumentation, and instrumentation is attack surface



Reporting on power and water usage effectiveness requires dense, continuous measurement across power, cooling and IT load. Every one of those measurement points is a networked device.

The platforms that collect this data, broadly known as Data Centre Infrastructure Management (DCIM) systems, were designed for engineering visibility rather than adversarial conditions. They commonly speak building automation protocols with weak authentication, and they are often commissioned by facilities teams working outside the security function's line of sight.

Researchers at Cyble found more than 20,000 DCIM instances reachable from the public internet, including thermal and cooling dashboards, humidity controllers, uninterruptible power supply controllers, rack monitors and transfer switches. Many used default passwords or were badly out of date. An intruder holding that access could raise temperature thresholds, disable cooling, alter voltage settings or switch off backup procedures.[6] Dragos has separately documented that the PIPEDREAM malware framework, which it attributes to the group it tracks as CHERNOVITE, contains a module capable of manipulating the kind of OPC-UA server nodes found in data centre plant.[4] Put plainly, the same instrumentation that proves a facility is green is the instrumentation that can be turned against it.

3. Singapore is about to regulate sustainability and resilience in a single instrument

The two agendas are being merged in law. That means security leaders can no longer treat sustainability as someone else's portfolio.

When a single license conditions the right to operate on both energy performance and incident reporting, the security function and the sustainability function answer to the same regulator on the same piece of paper.

MDDI and IMDA released the draft Digital Infrastructure Bill on 1 July 2026, with public consultation closing on 22 July 2026. It creates a data centre license for facilities with a critical load of 3 megawatts or more, under which IMDA assesses energy efficiency, water efficiency and renewable energy characteristics. A separate Major Foundational Digital Infrastructure licence applies at 10 megawatts and above, or to cloud providers earning S$100 million or more from users in Singapore, and requires security measures, business continuity plans and reporting of both cybersecurity incidents and service disruptions to IMDA.[7] The intent was signalled early. When the Government first announced the legislation in March 2024, it named non-cyber risks explicitly, including fires, water leaks and cooling system failures.[8] In the same month the Bill went out for consultation, CSA updated its Code of Practice for critical information infrastructure, requiring boards to maintain a documented cyber resilience framework reviewed annually.[9]

Conclusion

None of this is an argument against greener data centres. Singapore has little choice, and the roadmap is sound engineering policy. The point is narrower. Efficiency measures shrink the margin for error in the physical plant. Sustainability reporting adds thousands of networked sensors to facilities that were never designed as hardened environments. And Singapore law is about to hold operators accountable for both at the same time.

For ASIS members, the practical consequence is that the boundary between facilities engineering and security is disappearing. Cooling systems, UPS controllers and environmental sensors belong in the risk register alongside access control and CCTV. Business continuity exercises should rehearse a plant failure, not only a breach. And when a data centre operator is asked how green it is, the security function should be in the room, because the answer now describes part of the attack surface.

References

1. Ministry of Communications and Information, written parliamentary reply on data centre electricity consumption and carbon emissions, 27 July 2021. https://www.mddi.gov.sg/newsroom/mci-response-pq-data-carbon-emissions-data-centres-sg/

2. Infocomm Media Development Authority, Green Data Centre Roadmap, launched 30 May 2024, as reported by Data Center Dynamics. https://www.datacenterdynamics.com/en/news/singapore-to-unlock-300mw-of-data-center-capacity-through-industry-energy-efficiency-initiatives/

3. Infocomm Media Development Authority, "Singapore IT Energy Efficiency Standard for Data Centres Launched" (SS 715:2025), 13 August 2025. https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2025/sg-it-energy-efficiency-standard-for-data-centres-launched

4. Dragos, "Data Centre Operations: Cooling Systems Are Possible Targets for Operational Disruption", 8 May 2024. https://www.dragos.com/blog/data-centre-operations-cooling-systems-are-possible-targets-for-operational-disruption

5. Minister of State Alvin Tan, statement in Parliament on the 14 October 2023 DBS and Citibank outage, 6 November 2023, as reported by Mothership. https://mothership.sg/2023/11/impact-oct-14-dbs-citibank-outage/

6. Cyble research on exposed Data Centre Infrastructure Management systems, January 2022, as reported by BleepingComputer. https://www.bleepingcomputer.com/news/security/over-20-000-data-center-management-systems-exposed-to-hackers/

7. Ministry of Digital Development and Information, Public Consultation on the Digital Infrastructure Bill, 1 July 2026. https://www.mddi.gov.sg/newsroom/public-consultation-on-digital-infrastructure-bill/

8. Ministry of Digital Development and Information (then the Ministry of Communications and Information), "New Digital Infrastructure Act to enhance resilience and security of digital infrastructure and services", 1 March 2024. https://www.mddi.gov.sg/newsroom/new-digital-infrastructure-act/

9. Cyber Security Agency of Singapore, updated Code of Practice for critical information infrastructure, July 2026, as reported by Computer Weekly. https://www.computerweekly.com/news/366646154/Singapore-to-hold-CII-boards-accountable-as-AI-reshapes-OT-threat-landscape

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
Sep	30	NextGen Graduation (Dell)	Dell Office
Nov	4	MINDEF Event (MINDEF)	TBC
	TBC	ASIS AGM & Q4 Networking Dinner	TBC



Membership Promotion



Renew now to receive your **renewal gift** at the 2027 Q1 Networking Dinner.



New international or new local membership: **$100 for 15 months** (October 2026 to end of 2027).

Members' Update



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

Mr	Chee-Chong Chng		Mr	Rajagopalachariyar Narayanasamy
Mr	Edmund Tan		Mr	Shawn Leo
Mr	Guo Wei Frederick Thung		Mr	Simon Lau
Mr	Hsiao Min Ong		Mr	Sun Huai Ee
Mr	Nallaperuma Arachchilage Kanchana Dhananjaya Bandara		Ms	Vanessa Low
			Mr	Zhao Xiong Lim

Congratulation to Newly Certified Members!

Newly Attained CPP

Mr	Julius Cesar Parras	CPP	Mr	Mark Sun	CPP
Mr	Kelvin Lee	CPP	Mr	Teo Thiam Chye	CPP

Newly Attained PSP

Mr	Shaun Goh	PSP	Mr	Swee Chye Loh	PSP

Newly Attained APP

Mr	Chin Chye Raymond Teo	APP	Mr	Fan Sheng Chen	APP

Members' Update



Certified ASIS International Members

Certified CPP, PSP, PCI members

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

Certified CPP, PSP members

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

Certified CPP, PCI members

Mr	Manik Dhir	CPP, PCI

Members' Update

Certified ASIS International Members

Certified CPP members

Mr	Abdul 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	Azril Ngasiran	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	Bryan Ang	CPP
Mr	Choon Loong Loke	CPP
Mr	Choon Teck Tay	CPP
Mr	Chye Heng Lim	CPP
Mr	Clement Chan	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	Hock Chye Seah	CPP
Mr	Huajun Ren	CPP
Mr	Ing Kerne Yeh	CPP
Mr	Isaach Choong	CPP
Mr	Jarrod James Nair	CPP
Mr	Jeffrey Yeo	CPP
Mr	Jiann Liang Ho	CPP
Mr	Jing Chyi Pang	CPP
Mr	John Yim	CPP
Mr	Joseph F. Jasunas	CPP
Mr	Julian Tan	CPP
Mr	Julius Cesar Parras	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	Kayden Kho	CPP
Mr	Kee Kiat Teo	CPP
Mr	Kelvin Koh	CPP
Mr	Kelvin Lee	CPP
Mr	Ken Guorong Ang	CPP
Mr	Khai Ming Teo	CPP
Mr	Kim Poh Ong	CPP
Mr	Kin Chong Chan	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	Mark Sun	CPP
Mr	Max Hirsch	CPP
Ms	Michelle Ang Shan Yun	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	Ryan Chan	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	Teo Thiam Chye	CPP
Mr	Thian Beng Lim	CPP
Mr	Thirukumaran Sankaran	CPP
Mr	Wai Mun Chia	CPP
Mr	Wai Peng Sam	CPP

Members' Update

Certified ASIS International Members

Certified CPP members

Mr	Wayne G Edmonds	CPP	Ms	Yen Hwa Cheng	CPP
Mr	Wei Lun Soo	CPP	Mr	Yeong Sing Lim	CPP
Mr	William Toh	CPP	Ms	Yuen Yee Jeannie Tam	CPP
Mr	Wilson Loh	CPP	Mr	Zihui Lai	CPP
Mr	Yean Sang Tan	CPP			

Certified PSP members

Mr	Abdul Khandar Bin Abd Aziz	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	Stanley Chi-Fung Tse	PSP
Mr	Jianhui Chan	PSP	Mr	Teck Loon Teh	PSP
Mr	Kay Boon Low	PSP	Mr	Wei Jye Soh	PSP

Certified PCI members

Mr	Karanbir Singh Sandhu	PCI
Mr	Rupesh H K	PCI

Certified APP members

Ms	Abigail Wong	APP	Mr	Kok Cheam 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	Ms	Rachel Tan Yu Yan	APP
Mr	Edzel See	APP	Mr	Swee Chye Loh	APP
Mr	Faizul Salamon	APP	Mr	Weng Hong Ow	APP
Mr	Fan Sheng Chen	APP	Ms	Yan Ling Lim	APP
Mr	Jason Siow	APP	Mr	Yi Yan Lee	APP
Mr	Jeremiah Ong Wei Yi	APP			

Editorial Team



Perry Yeo, CPP
Editor



Daniel Chan, APP
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 be 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 2026

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

Mr. Mitesh Shah

Registered Mailing 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