SECURITY PROFESSIONAL

ASIS INTERNATIONAL® Singapore Chapter

Contents Page

Chairperson's Message

Dear Members,

I am honoured to address you as the newly appointed chairperson of our esteemed organisation. It is with great enthusiasm and a strong sense of responsibility that I assume this role, and I look forward to working with each and every one of you.

As we all know, security is a critical aspect of modern life, and the challenges we face are constantly evolving. ASIS International exists to promote best practices, foster innovation, and support the professional development of our members. Together, we can make a positive impact on the safety and security of our communities and businesses.

Over the years, our organisation has achieved significant milestones. However, we cannot rest on our laurels, and we must continue to evolve and adapt to stay ahead of emerging threats and trends. As Chairperson, I am committed to fostering collaborations, and continuous improvement within our association.

In the coming year, we have several exciting initiatives planned, including overseas visits for members, collaboration with institutions to enrol new security professionals, and a series of networking events to foster connections and knowledge-sharing among members. We will also be working closely with industry partners and government agencies to support the security profession.

I believe that the success of our association depends on the active participation and engagement of each member. I encourage you to get involved, share your expertise and ideas, and take advantage of the resources and opportunities available to you through our organisation. Together, we can achieve great things and make a positive impact on the world.

Thank you for your support, and I look forward to working with you in the year ahead.

YONG Hwee Fong, APP
Honorary Chairperson

Past Event: Hotel Security Round Table

Article Contributed by:
Ian Milne, CPP, PSP

Convention & Event Mgmt (CEMS) held their annual Safety & Security Asia Exhibition at Marina Bay Sands (MBS) from 16 to 18 November 2022. There were numerous security related events planned to run concurrently with the exhibition.

A conference was planed for the morning of Friday, 18 Nov 2022. However, the event was cancelled with less than two weeks before the exhibition. CEMS reached out to ASIS Singapore Chapter for assistance.

CEMS and ASIS Singapore had been working closely together in preparation of the ASIS & ISRM Conference (17 Nov 2022). Ian Milne CPP, PSP, agreed to represent the chapter and be the event emcee and panel discussion moderator. Ian's day job is in hospitality security, he holds the position of Senior Manager, Safety & Security Design APAC, at Marriott International.

The program would start with a keynote speech from Adrian Picar, President, Accommodation Establishments Security & Safety Coordinating Council inc. Adrian is based in the Philippines and is also the regional safety & security lead for Shangri-La Hotels. After the speech a round table discussion was planned. The panel consisted of Adrian Picar; Micky Khoo, Director, Safety & Risk Mgmt, Raffles Hotel; and Edwin Pinto, Director of Security Shangri-La Hotels & Resorts Singapore.

However, due to the short notice, the event attendance was low. But this gave an excellent opportunity to make the event much more interactive. The speakers, moderators and attendees moved from the large conference hall to a more comfortable setting in the exhibition VIP lounge. Using a projector screen the group received an almost personal presentation from the keynote speech from Adrian Picar.

The presentation was interspersed with collaborative questions and answers, open sharing by all present, motivated by the various interesting topics which included learning points of how the security hospitality industry in Philippines managed COVID, typhoons, kidnapping, armed security, and many more.

Once the presentation had finished the group seamlessly moved into conversations covering issues close to their hearts, from global, regional and national perspectives. This informal format allowed us all to engage at ease with our hotel security peers.

Overall, when it was time to finish up, all who attended agreed that despite the short notice and low turnout we had all gained from the experience and looked forward to a similar event in the future.

Hotel Security Roundtable Event attendees; safety, security and risk professionals from Raffles Hotel, Crown Plaza Changi Airport, ParkRoyal Collection, W Hotel Sentosa, Shangri-La Singapore and Philippines, Marriott international.

Past Event: Q1 Networking Dinner 2023

Article Contributed by:
Collin Goh

The Chinese New Year "Lo Hei" Networking Dinner was co-hosted on 3 February 2023 at Hub@Alexandra Techno Park - Roof Terrace by the APSA Singapore Chapter and ASIS International (Singapore Chapter). We would like to express our gratitude to Hikvision for sponsoring the event. Sharing Hikvision's Non-CCTV portfolio, members gained valuable insights into Hikvision's diverse range and capabilities in the AIoT market.

Asia Pacific Security Association (APSA), the leading association for security professionals, has chapters in 14 different nations, including Thailand, India, the Philippines, Singapore, Malaysia, South Korea, China, Hong Kong, Indonesia, Vietnam, Japan, Macau, Nepal, and Sri Lanka.

Hikvision was founded in 2001 and has its headquarters in Hangzhou. It has 66 subsidiaries and branch offices throughout the world, making it able to ensure quick responses to the needs of customers, users, and partners with its products. Hikvision is currently the world's leading manufacturer of artificial intelligence (AI) technologies and the internet of things (IoT) infrastructure in the AIoT space, with revenue expected to reach $10.1B in FY 2022. Its products are used by a wide range of industries. In order to more efficiently provide localised service support to its partners and clients, HIKVision established a local R&D team and RMA centre in Singapore in 2011.

The evening concluded with presentation of 20 lucky draw prizes and adjournment to Hikvision's Experience Centre for networking late into the evening.

Past Event: Field Visit to Axis Communications

Article Contributed By:
Sujoy Dutta, CPP

ASIS Singapore Chapter organised its first Field Visit of the year to Axis Experience Centre on 28th February 2023. Axis is a network technology company and industry leader. It offers solutions in video surveillance, access control, intercom, and audio system. Their experience centre showcases the latest state of art technology in network video, access control and audio solution. The event was attended by international and local ASIS members.

The event kick started with introduction of Axis and its product range from Roger Khoo, National Sales Manager of Axis. Jeffrey Lam, Senior Manager from Axis talked about the recent technology trends that are affecting the security industry. He mentioned how the use of AI and machine learning can help to derive actionable insight which will increase the security and operational efficiency. Jeffrey also talked about the importance of cybersecurity compliance, as the industry moves to hybrid architecture of on-premises and cloud architecture. Marie-Helene Mansard, Director of Business Development from Axis shared the use of 5G technology and how it would act as a key business enabler. Attendees got a chance to get the touch and feel on the latest cameras and other sensors in the experience centre, while Roger and his team explained the behind the scenes technology of these solutions. The use of technology has become pervasive in the security industry.

Boudewijn Pesch, Vice President of APAC Axis, shared how his team is working in helping to make technology a business enabler for the security industry looking beyond security. Sujoy Dutta, Secretary of ASIS Singapore Chapter, thanked members for joining the event and presented Axis Communication with a plaque as a token of appreciation for hosting the event.

The field visit ended with light refreshment and networking drinks at Axis Communication cafeteria.

State of Affairs, a Personal View

Article Contributed by:
Danny Chan

COVID-19 is arguably one of the most impactful events in modern history. But it is not the pandemic itself that scientists have been warning us about for years, but rather the reactions by governments. Ask yourself, when was the last time when so many of us are forced by our governments to stay at home? But with the worst of COVID-19 behind us, I feel that we have more headwind than we have a tailwind.

In the wake of the global dislocations caused by the pandemic, the Eastern European conflict, the rising cost of living, and the intensification of the contest between great powers, we are in the midst of a polycrisis. The term appeared to have first been used in the late 1990s by the French social scientists Edgar Morin and Anne Brigitte Kern, who employed it to describe the “interwoven and overlapping crises” facing humanity.

But with every crisis or polycrisis, lies an opportunity. Some say that successful people are simply more focused and committed, but that alone is not enough. The “Parable of Oranges” by Randall L. Ridd provides insights into this. The most important difference had to do with real intent rather than just going through the motions. When someone is motivated by money, position, and prestige versus someone who is driven by an intense desire to get the job done well. On the simplest task, they pursued excellence. They were serving versus self-serving and positive outcomes followed. Intent is critical to what we do as a society can see why we do what we do and judge us by it.

Physical Security in the New Normal

Article Contributed By:
Keith It

Welcome back! Following the COVID-19 pandemic, employees are beginning to return to offices. As organisations worldwide try to find their footing in the new norm, exploring between working remotely and in-office, the trend of returning is nonetheless afoot. Physical security measures and practices during pre-COVID times will have to gear up and perhaps, make some pivotal shifts, now that workplaces are buzzing once again.

This article will explore three factors that physical security professionals would want to consider as part of their planning considerations in light of the new working norm.

COVID-19 has upended the traditional office model. Hybrid working means that workspaces may be redesigned while flexible working schedules may translate into different capacities in a premise during different days and times.

Physical security professionals will want to review whether the prevailing security measures implemented pre-COVID are still sufficient or robust enough to continue safeguarding people, premise, property in view of these shifting changes to employee movement in and out of the working environment.

Following the above shift in working trend brings us to the importance of conducting security outreach programmes to employees. Outreach programmes are useful as messages that reinforce spotting and reporting suspicious behaviours, preventing security threats, among others, help the employees stay attuned to prevailing security risks. **Outreach programmes can take the form of email, signage and town hall / all hands meetings, among others.**

With the new working norm, face to face training sessions or online awareness or a combination of both are avenues that security professionals can adopt to inculcate the identification and prevention of security risks.

If anything, COVID-19 has taught us that the best of plans can go awry. Regardless, contingency or emergency planning remains relevant and important. A contingency or emergency preparedness plan can help to mitigate risks and provide initial response to an emergency or crisis situation.

The contents of these plans need to be reviewed to adapt to the shifts to the operational environment, changes to the working patterns unique to the organisation, etc.; with exercises – taking into consideration the organisation's new working arrangements – to validate the revised plans.

These factors are by no means exhaustive. However, it is hoped that they help to set the course for physical security professionals to take cognisance of as they enter into the new working norm.

Industrial Internet-of-Things (IoT) Cybersecurity: The Why and The How

Article Contributed By:
Daniel Chan, APP

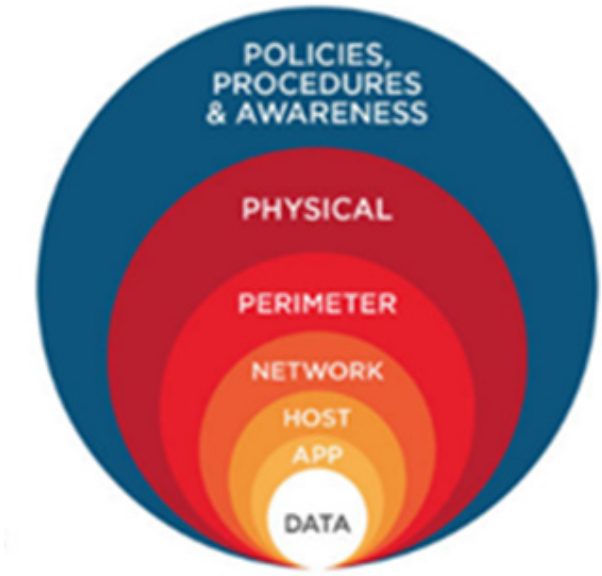
Industrial IoT (IIoT) cybersecurity is becoming increasingly important as more devices and equipment are connected to the internet. With this increased connectivity comes the risk of cyber-attacks such as data exfiltration or sabotage. This can result in significant financial losses, operational disruptions, safety hazards, and reputational damage. As security practitioners, it is important to understand what IoT security is, its importance, recommended frameworks and strategies, and suitable protective measures such as encryption standards.

What is IoT security and why is it important?

IoT security refers to the measures taken to secure internet-connected devices and systems from cyber-attacks. IIoT devices can include a wide range of equipment, including sensors, machines, and other infrastructure, all of which are connected to the internet. The importance of IIoT security lies in the fact that these devices can be vulnerable to attack due to their connectivity, making them susceptible to hacking, malware, and other types of cyber-attacks.

In an industrial setting, a cyber-attack can have severe consequences, including production or operational disruptions, equipment damage, and even harm to human life. This is why it is critical for companies to invest in IoT security strategies and measures to protect their assets and employees.

Strategies & Frameworks to Consider for IoT Security



Defence-in Depth. Like physical security, the "defence in depth" approach is very much applicable to IoT security. This approach involves layering multiple security measures to create a more comprehensive defence system. For example, a typical IoT security framework may include measures such as:

- Access control: Ensuring that only authorised personnel can access the devices and systems.
- Data encryption: Encrypting data to protect it from unauthorised access.
- Intrusion detection: Detecting and responding to suspicious activity on the network.
- Device management: Monitoring and managing devices to ensure they are running securely.

Risk Assessment. Conducting a risk assessment is vital to identifying the potential threats and vulnerabilities that could affect the IIoT systems. This assessment should include an inventory of all devices, software, and communication channels that are part of the system.

Security Policy & Education. It is also key to develop a security policy that outlines the security controls and measures that will be implemented to protect IIoT systems. This policy should be based on the results of the risk assessment and should be regularly updated to reflect changes in the threat landscape. Furthermore, education to raise awareness of such security policies are also crucial in helping to cultivate good IIoT cybersecurity hygiene.

Access Control. Implementing strong access control mechanisms to restrict access to the IIoT system is recommended. This can include using strong passwords, multi-factor authentication, and role-based access control.

Secure Communication. Using secure communication protocols to protect the confidentiality, integrity, and authenticity of data transmitted between devices in the IIoT system is also a fundamental feature. This can include using encryption and digital signatures to protect the data in transit.

Device Security. It is important to ensure that all devices in the IIoT system are securely configured and maintained. This includes disabling unused services and ports, keeping devices up to date with security patches and updates, and using trusted firmware and software.

Monitoring and Logging. IIoT business users should also consider implementing monitoring and logging mechanisms to detect and respond to security incidents. This can include using intrusion detection systems, monitoring logs for unusual activity, and setting up alerts for security events – e.g. Security Information & Event Management (SIEM) tools.

Incident Response. One can consider developing an incident response plan that outlines the steps to be taken in the event of a security incident. This plan should include procedures for isolating affected devices, collecting evidence, and communicating with stakeholders.

Encryption is an important part of IoT security, as it helps to protect data as it is transmitted over the network. Some of the commonly used encryption standards for IoT devices include:

Transport Layer Security (TLS). This is a protocol used to encrypt data transmitted over the internet. TLS is widely used in web browsing and other applications.

Advanced Encryption Standard (AES). This is a symmetric-key encryption standard used to protect data at rest. AES is widely used in IoT devices with higher processing power and capabilities due to its high level of security.

Elliptic Curve Cryptography (ECC). This is a public-key encryption standard used in endpoint IoT sensors or devices with limited processing power. ECC is more efficient than other encryption standards and is therefore well-suited for IoT devices.

ASCON. This is a lightweight authenticated encryption algorithm, and it is one of the cryptographic primitives that is being considered for use in IoT devices as it is well-suited for use in IoT devices that have limited processing power and memory. It provides both confidentiality and integrity for the data that it encrypts. Additionally, ASCON is designed to be resistant to various types of attacks, including side-channel attacks that attempt to extract the encryption key by analysing the physical properties of the device.

When selecting an encryption standard for an industrial IoT system, it's important to consider factors such as the level of security required, the processing power of the devices, and the potential impact on performance.

Conclusion

In conclusion, industrial IoT security is crucial to protect devices and systems from cyber-attacks that can cause significant financial and reputational damage, operational disruptions, as well as safety hazards. The implementation of a comprehensive IoT security framework should include the defence-in-depth approach, risk assessment, security policy and education, access control, secure communication, device security, monitoring and logging, and incident response. It is also important to consider the appropriate encryption standards, depending on the level of security required and the processing power of the devices. By prioritising IoT security, companies can effectively mitigate the risks of cyber-attacks and ensure the safety of their employees, assets, and operations.

Sources:

1. https://ascon.iaik.tugraz.at/specification.html

2. https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines

3. "Lightweight Authenticated Encryption for the Internet of Things: A Comparative Analysis" by Bilal Javed et al. and "Security and Privacy in the Internet of Things: Current Status and Future Directions" by Li Da Xu et al.

Contributed Article

The Future of Scamming

Article Contributed By:
Eddie Koh, CPP, PSP

Scammers have always been a part of the global economy, but the rise of technology and the internet has led to an explosion in the number and variety of scams. The most recent trend in scamming is the use of social media and online platforms to target individuals and businesses.

One popular scam is the "phishing" scam, in which scammers send emails or messages that appear to be from a legitimate source (such as a bank or government agency) in order to trick people into giving away personal information or money.

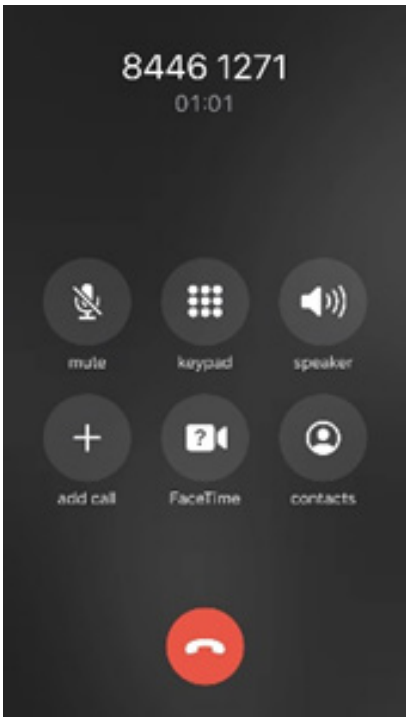
Believe it or not, the few paragraphs above are AI generated. Tools such as ChatGPT allow a user to conduct natural language conversations with software, and the software to respond in a way that on many occasions, pass off as a real human.

Consider 4 years ago, Google highlighted new technology for a digital assistant to make a phone call to a restaurant to make reservations, or to a hairdresser to make an appointment.

Click this link to see it on YouTube

In the same year 2018 - comedian Jordan Peele produced a deepfake video of President Obama saying things he wouldn't say. Watch it here.

Consider that most scamming and phishing attempts currently received on email or text are poorly formatted, or have spelling mistakes, or bad grammar. In Singapore, the IMDA has gone on a campaign over the past few years educating the public on how callers with a +65 prefix are possibly scam calls. This may cause people to instinctively trust what appear to be legitimate local numbers. Well, the scammers have found a way to call from a non +65 number.



Caption: This is a call the author received on 22 Dec 2022

How else can scammers up their game? What if they automated the process using natural language tools and deep-faked voices (or more scarily, deep-faked video)? What if you received an urgent video call from your boss asking you to buy some gift cards? Or from a frantic child saying they have been kidnapped and that her captors are demanding a ransom?

No matter how technology evolves to counter scammers and phishers, the bad actors will always come up with something more sophisticated. Scammers rely on impulsive actions to get what they want. It is up to the individual to be the final line in the defense of their personal information and money.

Some of us are fortunate enough to have corporate training on good cybersecurity hygiene, but continual personal training and practice in critical thinking is the key to keeping safe. Always think of the veracity of the message before you respond.

Editor's note: As the team is working on this edition of the newsletter, a similar article was published in the Straits Times. We are linking to it here if you'd like further reading.

Calendar of Events

Q2 Networking Dinner

Q2 Networking Dinner is scheduled for May 2023.

More details will be released in our website soon.

CPP Review Course

The upcoming CPP review course will be held in September 2023.

Interested please contact us at Education@asis-singapore.org.sg

PSP Review Course

The upcoming CPP review course will be held in June 2023.

Interested please contact us at Education@asis-singapore.org.sg

Members' Update

Warm Greetings to the following new ASIS International Members!

Mr	Arthur Chew Boon Kwang		Mr	Koh Beng Hong	
Mr	Ashish Kumar Jaiswal		Mr	Koh Jian Hao	APP
Ms	Ashwini Ramoo		Mr	Mohamed Zayed Bin Shariffudin	
Ms	Aw Hwee Lee		Mr	Mohammad Sulaiman	
Mr	Bosco Thomas		Mr	Mohd Izarudin Amanudin	
Mr	Edmund Wong		Ms	Monica Tomar	
Mrs	Eunice Hong		Mr	Muhammad Zahed Zulkeplee	
Mr	Frankie Man		Mr	Munisamy Ramakrishnan	
Mr	Glenn Koh	CPP	Mr	Renaldo Tan Wee Hong	
Mr	Goh Kwan Way Marc	APP	Mr	Richard Stuart	
Mr	Hanis Roslee		Mr	Shashank Mesvani	
Mr	Jack Phua Kok Hua		Mr	Sjorn Lim Ming Yu	
Mr	James Koh		Mr	Toh Keng Wi	
Mr	Jason Siow	APP	Mr	Tommi Lee	
Mr	Jitendra Kumar		Mr	Vikneshwaran Ganesan	
Ms	Karen Wong	CPP	Mr	Vincent Gok	

Congratulation to Newly Certified Members!

Newly Attained CPP

Mr	Azril Ngasiran	CPP	Mr	Rick Wong Soon Wah	CPP
Mr	Clement Chan	CPP	Mr	Shaymentyran Shaem	CPP
Mr	Glenn Koh	CPP	Mr	Sheo Boon Chew Winson	CPP
Mr	James Hammond	CPP	Mr	Sia Wang Ting	CPP
Mr	James Wong Li Ren	CPP	Mr	Thirukumaran Sankaran	CPP
Mr	Lawrence Tan Jun-Ming	CPP	Mr	Vincent Soh Chee Yong	CPP
Mr	Lye Kah Meng Joseph	CPP			

Newly Attained PSP

Mr	Abdul Razak Daseran	CPP, PSP	Mr	Shamus Yeo See Yew	PCI, PSP
Ms	Kee Ling Min	PSP			

Members' Update

Congratulation to Newly Certified Members!

Newly Attained PCI

Mr	Adrian Wong Voon-Ming	CPP, PCI, PSP

Newly Attained APP

Mr	Eugene Chua	APP	Mr	Francis Zhang	APP

Certified ASIS International Members

Certified CPP, PSP, PCI members

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

Certified CPP, PSP members

Mr	Abdul Razak Daseran	CPP, PSP	Mr	Lee Choon-Wai Anthony	CPP, PSP
Mr	Chua Boon-Hwee	CPP, PSP	Mr	Melvin Cheng Tze-Hui	CPP, PSP
Mr	Eddie Koh	CPP, PSP	Mr	Tan Wee Hock	CPP, PSP
Mr	Ian D Milne	CPP, PSP	Mr	Willie Heng Chin-Siong	CPP, PSP
Mr	Kagan Gan	CPP, PSP	Mr	Xiao Gaoping	CPP, PSP
Mr	Kenneth Lau Yip Choy	CPP, PSP			

Certified PSP, PCI member

Mr	Shamus Yeo See Yew	PCI, PSP

Certified CPP members

Mr	Abdul Redha Bin Abdullah	CPP	Mr	Azharie B Mohamed Mudakir	CPP
Mr	Alfian Idris	CPP	Mr	Azril Ngasiran	CPP
Mr	Andrew Fan Tuck-Chee	CPP	Mr	Balasubramaniam Selvam	CPP
Mr	Ang Boon Kiat, Peter	CPP	Ms	Beverly F Roach	CPP
Mr	Anton Chan	CPP	Ms	Cheng Yen Hwa	CPP

Members' Update

Certified ASIS International Members

Certified CPP members

Mr	Chia Wai Mun	CPP
Mr	CHIU CHING CHIU	CPP
Mr	Clement Chan	CPP
Mr	Daniel Ng	CPP
Mr	Desmond Ho Kok Tong	CPP
Mr	Dicky Fadly Zaini	CPP
Mr	Edmund Lam	CPP
Mr	Edwin Goh	CPP
Mr	Fabrice Marty	CPP
Mr	Firman Latib	CPP
Mr	Glenn Koh	CPP
Mr	Hartmut Kraft	CPP
Mr	Ho Jiann Liang	CPP
Mr	Ho Kai-Quan Den	CPP
Mr	Isaach Choong	CPP
Mr	James Hammond	CPP
Mr	James Wong Li Ren	CPP
Mr	Jarrod James Nair	CPP
Mr	Jeffrey Yeo	CPP
Mr	JK Wong	CPP
Mr	Jonathan Yap	CPP
Mr	Julian Tan	CPP
Mr	Justin Chen Jianan	CPP
Mr	Kan Young Loong	CPP
Ms	Karen Wong	CPP
Mr	Kelvin Koh	CPP
Mr	Ken Ang	CPP
Mr	Ken Tong	CPP
Mr	Koh Kwang Wee	CPP
Mr	Krishnamoorthy Arunasalam	CPP
Mr	Lai Zihui	CPP
Mr	Law Chee Keong	CPP
Mr	Lawrence Tan Jun-Ming	CPP
Mr	Leonard Ong	CPP
Mr	Leong Hoe Meng	CPP
Mr	Leong Keng Weng	CPP
Mr	Lim Choon Kwang	CPP
Mr	Lim Chye Heng	CPP
Mr	Lim Teong Lye	CPP
Mr	Lim Thian Beng	CPP
Mr	Look Kang Yong	CPP
Mr	Lye Kah Meng Joseph	CPP
Mr	Magalingam Veeman	CPP
Mr	Marcus Tan Chong Lay	CPP
Mr	Mark Chow	CPP
Mr	Mark Nuttall	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	Ong Kim Poh	CPP
Mr	Paul Rachmadi	CPP
Mr	Perry Peter Yeo	CPP
Mr	Ramani Matthew Sachi	CPP
Mr	Ren Huajun	CPP
Mr	Richard Goh	CPP
Mr	Rick Wong Soon Wah	CPP
Mr	Sachin Kumar Sharma	CPP
Mr	Sam Wai Peng	CPP
Mr	Shaymentyran Shaem	CPP
Mr	Sheo Boon Chew Winson	CPP
Mr	Sia Wang Ting	CPP
Mr	Simon Tan Eng-hu	CPP
Mr	Soon Koh Wei	CPP
Mr	Stanley Aloysius	CPP
Mr	Sujoy Dutta	CPP
Mr	Surendran Chandra Segaran	CPP
Mr	Taaouicha Mujahid	CPP
Ms	Tam Yuen Yee Jeannie	CPP
Mr	Tan Gwee Khiang	CPP
Mr	Tan Hock Seng	CPP
Mr	Tan Kok Soon	CPP
Mr	Tay Choon Teck	CPP
Mr	Teo Kee Kiat	CPP
Mr	Thirukumaran Sankaran	CPP
Mr	Tony Er	CPP
Mr	Vincent Soh Chee Yong	CPP
Mr	Wayne G Edmonds	CPP
Mr	William Toh	CPP
Mr	Wilson Loh	CPP
Mr	Yeh Ing Kerne	CPP
Mr	Yuen Kin Wai (Dex)	CPP

Members' Update

Certified ASIS International Members

Certified PSP members

Mr	Jeffrey Lam Boonkee	PSP	Mr	Mayank Sinha	PSP
Mr	Kamlesh Gope Ramchand	PSP	Mr	Soh Wei Jye	PSP
Ms	Kee Ling Min	PSP	Mr	Stanley, Tse Chi-Fung	PSP
Mr	Kevin Loh	PSP	Mr	Wee Ting-Jin	PSP
Mr	Lee Huan Chiang	PSP			

Certified APP members

Mr	Daniel Chan	APP	Mr	Goh Kwan Way Marc	APP
Mr	Eugene Chua	APP	Mr	Jason Siow	APP
Mr	Faizul Salamon	APP	Mr	Koh Jian Hao	APP
Ms	Foong Yi Ling	APP	Mr	Ong Poh Tiong	APP
Mr	Francis Zhang	APP	Mr	Soo Wei Lun	APP
Mr	Gan Da	APP	Ms	Yong Hwee-Fong	APP

Editorial Team

Eddie Koh, CPP, PSP
Editor

Monica Tomer
Editor

Yong Hwee Fong, APP
Contributor

Ian Milne, CPP, PSP
Contributor

Collin Goh
Contributor

Sujoy Dutta, CPP
Contributor

Danny Chan
Contributor

Keith It
Contributor

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.

This will be a valuable platform to share your knowledge with fellow Chapter members. CPP/PSP/PCI/APP board-certifi ed members will also be pleased to note that published articles may earn up to 9 CPE credits in recertification.

Interested please email us at memberservices@asis-singapore.org.sg
Submission close on 15 May 2023

Management Committee 2023-2024

Honorary Chairperson
Ms. Yong Hwee Fong, APP

Honorary Vice-Chairperson
Mr. Jeffrey Lam, PSP

Honorary Secretary
Mr. Sujoy Dutta, CPP

Honorary Asst. Secretary
Mr. Collin Goh

Honorary Treasurer
Mr. Edison Koh, CPP, PSP, PCI

Honorary Asst. Treasurer
Mr. Lim Chye Heng, CPP

Honorary MC Members
Mr. Anthony Lee, CPP, PSP
Ms. Marie-Helene Mansard
Mr. Simon Tan
Mr. Hartmut Kraft, CPP
Mr. Matthew Lee

Registered Mailling Address:
ASIS International (Singapore Chapter)
5 Temasek Boulevard, Suntec Office Tower 5, #17-01, Singapore 038985

Website: www.asis-singapore.org.sg

Email: memberservices@asis-singapore.org.sg