

SECURITY PROFESSIONAL



Singapore
Chapter



Contents Page

Chairperson's Note	2	Past Event	13
		New Members' Tea Party	
Contributed Article	3	Past Event	14
Advances in Mass Personnel Screening		Q2 Networking Dinner	
Contributed Article	6	Past Event	16
Demystifying Cybersecurity: Security Architecture and Engineering in Simple English		Women-In-Security Get Together	
Contributed Article	9	Past Event	17
Security Intelligence for Business Resilience		PSP Review Course	
Contributed Article	11	NextGen Committee	18
Sustainable Security Practices: Protecting our organisation and the Environment		Update from NextGen Committee	
		Upcoming Events	19
		Members Update	20 - 23

Chairperson's Note

Dear Members and Colleagues,

Greetings from the Singapore Chapter!

As we embark on another exciting year in our association's journey, I wanted to take a moment to highlight the importance of embracing the next generation and fostering their interest in the security profession. The future of our industry lies in the hands of those who are passionate about protecting people, organisations, and critical assets. By inspiring and guiding the younger generation, we can ensure a robust and sustainable future for the security profession.

To this end, I encourage all our members to actively engage with educational opportunities offered by the Chapter, serve as mentors to aspiring professionals, and create opportunities for them to gain hands-on experience. Let us share our knowledge, insights, and experiences, nurturing the talents that will shape the security landscape of tomorrow.

One of the ways we can make a significant impact is through collaboration with other ASIS Chapters in Asia. By co-organizing conferences and events, we can combine our strengths, knowledge, and resources to elevate the standard of excellence across the region. Let us work together to foster stronger ties, share best practices, and create a supportive network that spans beyond borders.

I would also like to emphasise the invaluable role that our sponsors play in our endeavours. Their support enables us to deliver high-quality events, training programs, and networking

sessions. Through collaboration with our sponsors, we can leverage their expertise, resources, and innovation to create exceptional experiences for our members. Let us continue to foster these partnerships, ensuring that our events and initiatives remain at the forefront of the industry.

Lastly, I want to extend my deepest gratitude to all our dedicated volunteers who tirelessly contribute their time and efforts to create value for our members. Each one of you plays a vital role in the success of our association. I encourage more members to consider volunteering in their own unique ways, whether it be through organising events, mentoring others, or contributing to our publications. Your involvement will not only enrich your professional journey but also enhance the overall experience for all our members.

Together, we can create an inclusive and vibrant community where ideas flourish, connections are made, and excellence is celebrated. Let us continue to build a strong foundation for the future, inspiring the next generation, collaborating with our peers, engaging our sponsors, and volunteering in meaningful ways.

Thank you for your unwavering support, and I look forward to the exciting opportunities that lie ahead.

Wishing all good health,

YONG Hwee Fong, APP
Honorary Chairperson

Advances in Mass Personnel Screening

Article Contributed by:

Richard Stuart, APAC Manager, Xtract One Technologies Inc

Is the Walk-through Metal Detector Obsolete for Security?

For years, walkthrough metal detectors (WTMD) have been the go-to solution for patron security screening in public spaces. However, with recent advances in sensor and processing technology, these devices are becoming increasingly outdated and can even be considered obsolete technology.

Challenges of legacy Walk Through Metal Detectors

- Processing time is slow due to the need to divest all personal items and yet there are still high nuisance alarm rates which guards need to resolve.
- As a result of having slow processing time, more WTMD are required for a given throughput – usually measured in people per hour (ppl/hr). Therefore the costs of operating a fleet of WTMDs is high: large numbers of systems, numerous guards, and of course a significant amount of space is required. And in many locations x-ray scanners are also used thereby further increasing operating costs.
- There is a high level of close contact between visitors as they wait in the queue, and between visitors and guards at the WTMD itself. Many patrons find this invasion of personal space offensive. Further, close human proximity makes it easier for infections to be transmitted.
- Organisers of any event that needs to screen large numbers of patrons in a short time, such as at sports events, know that there will be long queues and mounting frustrations for patrons and guards alike.

- Many systems are susceptible to environmental interference, for example wind can move the WTMD towers, and create further nuisance alerts.



Queues are a threat

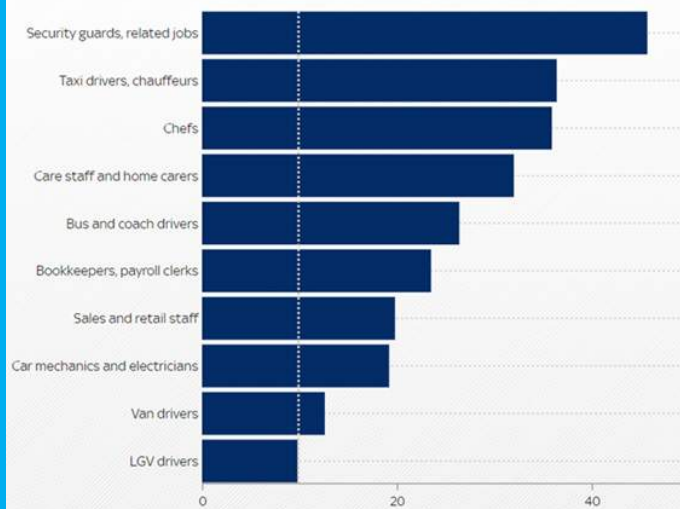
The queues are themselves a security threat – a bad actor does not need to pass through security – they can simply carry out their act in the queue.

And queues and the close contact between guards and visitors have become of greater concern during the pandemic. These concerns are real – in the early stages of the pandemic, figures from the UK show that security guards had the highest death rate of any occupation.

Male COVID-19 death rate

Selected occupations

Figures per 100,000 population. Dotted line marks the average (9.9 per 100,000)



SOURCE: ONS • Figures for England and Wales residents aged 20 to 64 years. Deaths involving COVID-19 registered up to 20 April.

As venues reopened after the lockdowns, many organisations realised that continuing to use WTMD technology has become unacceptable.

Security is complicated

There are many conflicting drivers within a security process – these are driven by the different objectives of the various stakeholders.

- Security

There is a need to prevent threats, especially mass casualty threats entering the venue.

- Marketing/ Customer Experience

There is a desire to allow patrons to enter the venue as quickly as possible. Visitor experience is important. Many venues recognise that revenue is lost while people are standing in a queue and reduced if they have a stressful security experience.

- Operations

There is a need to contain costs, recruit staff and yet maintain flexibility for different types of events.

A change in the requirements of any one factor impacts many other facets:



Balancing all these areas of the business is extremely difficult. Fortunately there are new technologies that provide venues with the ability to better address the conflicting aims.



New Generation Weapon Detection Systems – making a better first impression

Businesses and organisations, that deal in large numbers of visitors, are turning to AI-powered weapons detection technology and that utilise advanced sensor technology. These new technologies coupled with superior processing power, deliver a more comprehensive, accurate, and cost-effective security solution.

By embracing these new technologies, companies can enhance their overall security operations, provide a safer environment for employees and customers, reduce throughput time, reduce or eliminate queues, and free up more space at the venue entrance.

These new generation systems focus on detecting weapons (guns, knives etc) and allow visitors to walk through without the need to divest personal items such as phones, keys and other metallic items.

As there is no need to stop and divest, throughput is increased and queues are quickly dispersed.

There are also significant economic benefits – although old technology WTMD are cheap, their slow throughput requires multiple systems and many guards – and the guards are costly. For example, Moody Center (a 15,000 seat arena in Austin, Texas, USA) required 42 walk through metal detectors and 84 guards. These were replaced with 9 new generation weapons detection systems which require only 27 guards. At a recent Harry Styles concert, over 10,000 visitors were screened in less than 25 minutes. The return on investment is measured in months for such venues.

With the faster throughput and lower nuisance alarm rates, guards are better able to focus on detecting threats.

Many venues benefit from the latest technology. The advent of new, high throughput weapons detection technology, that differentiates between threat objects and benign objects,

reduces queues and uses less space is improving the user experience and security process for a diverse range facilities:

Stadiums: the challenge for stadiums is how to get huge numbers of people in and out safely, and for the crowd to be feeling safe, and not frustrated from queues. Many stadiums have already been the first adopters of such technology.

Theme Parks: travelling with the family can be a challenge on most occasions, but having impatient kids waiting at the door and being delayed by the security checks, is surely one of the most stressful experiences that parents have to endure. Utilising high throughput weapons detection technology is proven to be a significant stress reliever – and gives the family more time in the park.

Performing Arts Centres, Museums and Art Galleries: such venues find that old style security checkpoints is completely at odds with the welcoming, peaceful environment expected by patrons.

Factories and Warehouses: with thousands of employees entering and leaving each day, the challenge for premises management is to make the staff feel trusted, while able to detect the occasional disgruntled employee, who wants to “throw a spanner in the works” – or worse.

Places of Worship: worshippers want to feel safe when they enter such premises. But sadly, as we know all too well, the bad actor likes to take advantage of the assembled congregation.

Education Facilities: students, and their parents want to feel safe while they study. Peak hours put a heavy strain on the security team, and legacy equipment just cannot cope.

As advancements in security continue, the future of security screening is looking bright, with innovative solutions promising more efficient and effective screening processes.



Demystifying Cybersecurity:

Security Architecture and Engineering in Simple English

Article Contributed by:
Daniel Chan, APP

In today's world, where digital interactions and transactions are commonplace, understanding cybersecurity has become as essential as understanding basic life skills. One of the vital components of this field is Security Architecture and Engineering. Even though it may sound technical and intimidating, this jargon can be translated into simple, everyday language. For those who are already familiar with the Certified Information Systems Security Professional (CISSP) certification, this concept is a crucial one in the field of cybersecurity, which is the **third** domain out of the **eight** in the CISSP. This sharing will be the first of a series of articles that seeks to demystify the eight domains of the CISSP.

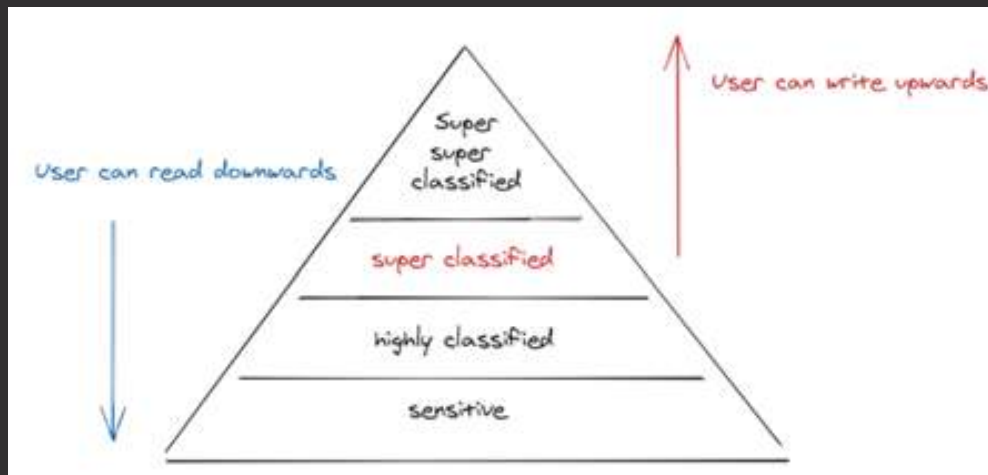
Decoding Security Architecture and Engineering

To start, let us visualise the following analogy. Picture your own house. It is a thoughtfully designed structure with various safety measures. Walls, doors, and locks form physical barriers against intruders. Smoke detectors and fire extinguishers are in place to manage fire risks, while a security alarm provides another layer of safety.

The principle of Security Architecture and Engineering in cybersecurity mirrors this. Just as you would construct a house with meticulous planning, cybersecurity also involves installing or utilising security software with a strategic blueprint. As such, the onus is on security practitioners to design and implement security measures in an orderly, structured way, akin to how an architect designs a house.

Elements of Security Architecture and Engineering

Security Models (The Blueprint). Think of these as the blueprint for a building. Security models provide the fundamental structure of how security is implemented within a digital environment. They provide the theoretical basis that outlines how security policies will be enforced. For instance, a model might define that only an individual with the correct authorisation (akin to having the right key) can access specific data (equivalent to entering a room). For instance, the Bell-LaPadula model focuses on maintaining the confidentiality of information. It stipulates a 'no read up, no write down' policy, similar to a rule that only an individual with the right key can access a specific room.



System Security Architecture. This is all about creating a comprehensive outline of the security infrastructure. It maps out how different components will interact and cooperate to maintain the system's security. We typically use walls, doors, windows, and alarm systems in a house together to ensure the safety of its occupants, the different elements or aspects of a cybersecurity system need to be used together as well. These could include a variety of cybersecurity layers such as firewalls, antivirus software, intrusion detection systems, etc. All these play unique roles but they all work towards the same goal of security. In the digital world, this could involve different elements such as firewalls blocking unauthorized access, intrusion detection systems alerting on suspicious activities, and secure network architectures like Demilitarised Zones (DMZs)

segregating sensitive parts of the system.

Cryptographic Systems (Locks). Imagine the most sophisticated lock on a door, but for digital information. Cryptography involves the process of scrambling data in such a way that only those with the correct 'key' can decipher and understand it. This field is vast and includes various methods like symmetric and asymmetric encryption, each with its own strengths and use cases. This can be likened to having different types of sophisticated locks for different doors, each chosen based on the level of security needed. Real-world examples include SSL/TLS protocols which are commonly used to ensure secure communications on the internet, or symmetric encryption algorithms like AES that secure your data at rest.

Physical Security Considerations. While we often think of cybersecurity in the digital realm, the physical security of computer systems is equally important. This could involve shielding servers from physical damage like fires or floods or restricting unauthorised access to the hardware. It also includes things like ensuring the safe disposal of old hardware so that no sensitive data can be retrieved from it. For example, datacentres often employ biometric access controls and CCTV surveillance systems to ensure only authorised personnel can access the servers.

The Significance of Security Architecture and Engineering

Without a thoughtfully designed security architecture, an organization's cybersecurity measures can become disjointed and less effective, similar to having a house with robust doors but weak windows. Therefore, a sound security architecture ensures that every part of the system functions harmoniously to provide the most robust protection possible.

I know some of you who are physical security experts would be asking me: What about drawing in the analogy of dead bolts for the doors, motion detectors, fire extinguishers, etc.? What about the security operations cycle? All of these will be covered in future articles as part of this series. For example:

- The dead bolt can be seen as a firewall (Domain 4: Network Security). This can be seen as the first line of defence that prevents unauthorized access.
- Motion detectors can be seen as part of intrusion detection systems (again, Domain 4), which monitor and alert on suspicious activity.
- The fire extinguisher can be seen as antivirus software (Domain 7: Security Operations), which mitigates damage once a threat (i.e., a fire or virus) is detected.

Conclusion

As we navigate the increasingly digital landscape of our lives, understanding the basic principles of cybersecurity becomes essential. Security Architecture and Engineering highlights the importance of strategic planning and structured implementation in securing our digital world. It is a reminder that a well-structured cybersecurity system, grounded in these principles, is our best defence against the myriad of cyber threats. By understanding these principles, we all can safeguard our valuable data from various cyber threats. As we grow more aware of these principles, we all can play our part in building a safer, more secure digital world.

Sources:

1. *CISSP For Dummies, 6th Edition* by Lawrence C. Miller and Peter H. Gregory.

Security Intelligence for Business Resilience

Article Contributed by:

Anthony Lee, CPP, PSP, CBCP

Introduction

Security intelligence is a key component of business resilience, as it provides organisations with the necessary information to help them identify and mitigate potential risks and threats. Security intelligence can be obtained from a range of sources, including external security intelligence providers, internal security monitoring systems, and public sources such as news reports and official government sources. With this information, organisations can create comprehensive risk assessments and develop strategies to protect their data, systems, and operations. Additionally, security intelligence can provide organisations with the tools they need to respond quickly to potential threats and minimize the impact of any security incidents.

Referring to Disaster Recovery Institute (DRI) International's 8th annual predictions report, the ten predictions by DRI International for year 2023 includes the following major business disruptions with adverse impact:

- A major IT service provider will be hacked, disrupting financial markets, utility companies etc.
- A major city in the developed world will experience unprecedented flooding from a storm-related event.
- The drive to find alternate energy supplies will intensify, while power cuts hit many developed countries.
- Global security concerns will multiply, thus changing government positions and future commercial investment.

Therefore, it is important to businesses to plan for, and mitigate the risks associated with the following consequences from major business disruptions:

- Facility denial - no access to facility e.g. major fire of premises, severe building damage from earthquake or typhoon.
- Staff denial - staff is unable work e.g. pandemic case in hospital or under quarantine
- IT/Infrastructure Denial – outage of IT services or main power supply.
- Supply Chain Denial e.g. disruption in supply of goods affecting inbound and/or outbound deliveries.

Business Resilience

Business resilience can be defined as *“the adaptive capacity of an organisation in a complex and changing environment.”* What makes an organisation resilient? Below are some of the main traits of a resilient company or organisation.

- Adaptive, flexible, and responsive
- Distributed command structure
- Decision-making capability at various levels
- Emphasis on both internal and external preparation
- Intelligent use of data

Security intelligence involves monitoring internal and external sources of information to identify potential threats and vulnerabilities, as well as developing strategies to respond to them. Security intelligence also involves leveraging data to gain insights into the tactics and techniques used by attackers, so that organisations can better protect themselves.

Additionally, security intelligence can also be used to help organisations analyse the effectiveness of their security measures and make improvements where necessary.

Security Intelligence

The definition of intelligence by the United Nations is: *"Intelligence is accurate, processed information, delivered in sufficient time to enable decision-makers to take the necessary action."*

The main objectives of Security Intelligence are to:

- Assess, prepare for and mitigate threats before they become a problem.
- Take a proactive approach to risk management based on concise recommendations and actionable assessments.
- Remain aware of strategic and tactical developments and their implications.
- Protect your bottom line by proactively protecting your assets and operation.

The importance of accurate intelligence cannot be over-emphasized in order to win the hearts and minds of business leaders and staff from a corporate security angle. Owing to heaps of misinformation and disinformation presented by a plethora of social media in the modern technology era driven by the global internet and 5G data connectivity, social media intelligence (SOCINT) and open-source intelligence may sometimes be unreliable or not very good. Therefore, it is vital that every piece of open-source intelligence be corroborated with other reliable sources to ensure veracity and relevance. By so doing, a good security intelligence program will facilitate the information flow to staff characterised as follows:

- Stay informed, be proactive
- Actionable intelligence. What good is information if you can't act on it?
- Timely, accurate and relevant

In general, the types of security intelligence can be categorised as:

- **Strategic threat intelligence** is intended for policymakers both in businesses and government agencies
- **Operational threat intelligence** feeds for business / organisation operations and security management
- **Tactical threat intelligence** is the most rapidly updated

The above types of intelligence can be presented in various form of security and/or geo-political risk reports, such as:

- International geopolitical Intelligence –

global or regional reports with strategic risk analysis.

- Country reports – operational and summary reports with risk rating.
- Tactical Intelligence Reports – real-time information on local security issues
- Pre-travel custom intelligence – travel security brief and tactical monitoring.

Security Intelligence and Crisis Management

A disaster can strike any organisation, large or small. organisations spend years building their brands but a single event could wipe out this investment. As part of crisis management methodology, security intelligence is useful to inform the risk management process in order to reduce the probable causes of major business disruptions as far as practicable, and mitigate the likelihood of security threats. However, black swans e.g. terrorist attack, ransomware attack, pandemic and other crises such as natural disasters may still occur. Therefore, any resilient business will have in place a business continuity program to establish a strategic and tactical capability to prepare for, and mitigate the risks of any major business disruption to a level acceptable to its company management. Naturally, as part of security risk management, emergency response plans are vital for first-line business operations to deal quickly and effectively with any crisis. As the saying goes, "A Crisis is not a Disaster. Failure to Plan for a Crisis is a Disaster."

Conclusion

Business resilience is the ability of an organisation to quickly adapt to disruptions while maintaining continuous business operations and safeguarding the organisation's resources and assets. It involves the implementation of strategies, technologies, and processes including security intelligence to protect the organisation from potential threats, while also enabling the organisation to quickly respond to and recover from these threats. Business resilience involves the organisation having a comprehensive understanding of its external environment and the potential threats that exist, as well as the resources and capabilities necessary to mitigate and manage these threats. Additionally, business resilience also involves the organisation having the capability to detect and respond to potential threats via actionable intelligence, as well as the capacity to quickly recover from them.

Sustainable Security Practices: Protecting our organisation and the Environment

Article Contributed by:

Jeffrey Lam, PSP

Sustainability is an increasingly important concept that encompasses environmental, social, and economic dimensions. It spans various aspects, from social justice and intergenerational equity to energy efficiency. Rather than being a passing fad; it is a critical concept that affects both the long-term viability of our organisations and our environment. Both the public and private sectors have recognised its significance and have initiated initiatives to foster a sustainable business environment.

In Singapore, the government implemented a Carbon tax in 2020, and companies listed on SGX with a capitalization of more than S\$2 billion are now required to provide annual sustainability reports. In the private sector, companies are demanding third-party certifications such as ISO 14000 and EcoVadis from their vendors to demonstrate their commitment to sustainability.

From a security operations standpoint, there are several ways we can support this sustainability initiative. 3 key areas in reducing our impact to the environment is discussed below:

Waste and Pollution Reduction:

Transportation is a significant contributor to pollution (not to mention business costs considering the prices of current CoE). Drones and robots can help reduce the need for security personnel to travel to sites. Using centralised management platforms and remote access technologies, one can also efficiently manage security operations across geographically dispersed sites.

Another aspect to address is the use of toxic chemicals. While PVC is commonly used in

cables and hardware housing, it contains hazardous additives and releases harmful substances during manufacturing. Utilising Low Smoke Zero Halogen (LSOH) cables and PVC-free plastics reduces toxicity and minimises the environmental impact. Additionally, transitioning to digital documentation and workflows for paperless operations reduces the consumption, printing, and waste generation.

Finally, evaluating if new equipment uses recycled materials and minimises excessive packaging also contributes to waste reduction.

Energy Efficiency:

While access control and video surveillance systems may appear to consume low energy, ancillary services and IT equipment supporting them contribute to overall energy consumption. Evaluating the lighting requirements for cameras and employing energy-efficient lighting solutions can significantly reduce energy usage. Optimising data compression also enhances energy efficiency in IT equipment, such as servers and switches.

Integrating access control systems with building automation systems can also improve energy efficiency. The building automation system can estimate occupancy levels based on data from the access control system and adjust lighting and air-conditioning accordingly. Power-over-Ethernet (PoE) is recognised as a more energy-efficient option to powering low voltage devices. Considering its implementation over traditional power supplies in security systems can yield significant energy savings.

Hardware Reduction:

Crime Prevention Through Environmental Design (CPTED) encourages the use of architectural features that serve aesthetic purposes while clearly defining boundaries. Decorative fencing, bike racks, and sign boards can double as physical barriers. This helps to establish territory and demarcate boundaries. Heavy-duty planter boxes can also serve as crash bollards, combining functionality with security.

Technological advancements can also help reduce reliance on security hardware. Modern access control systems that utilise NFC or Bluetooth technology enable the use of mobile phones as access credentials. This also simplifies the card management processes saving valuable manpower time for security operation professionals.

Cameras are typically installed to aid security operations. However, by embedding video analytics into the camera, we can expand its use to enforce safety policies. Examples include monitoring employees' use of Personal Protective Equipment (PPE) and identifying obstructions to fire exits. ([see article in the 2022Q4 newsletter](#)).

Conclusion

Implementing sustainable physical security practices requires additional planning and effort, but it is a crucial and strategic choice. It's a common misconception that promoting sustainability would incur additional costs. However, by improving energy efficiency, reducing transport and reducing hardware, there are opportunities for total costs to be equal or even lowered. By integrating these practices into our security operations, we not only reduce environmental impact but also ensure regulatory compliance and support overall business goals. Most importantly, by embracing sustainability in security operations, we actively contribute to building a greener and more resilient future.



New Members' Tea Party

Article Contributed by:
Sujoy Dutta, CPP

ASIS Singapore Chapter ushered its new local chapter members through a Welcome Tea Party. The event was held at the Mastercard office on 4th May 2023.

The event was graced by Danny Chan, Global Board of Directors ASIS International and Choon Kwang Lim, CPP, PSP, ARVP ASIS International Region 13B. Danny Chan shared the global perspective of ASIS with the new members and how the association is committed to the professional development of its members in the region. Danny encouraged new members to be more active in the local chapter and take the opportunity to gain experience and network with each other.

Choon Kwang, shared about the key initiatives of the region and the journey of the Singapore local chapter and its growth.

Sujoy Dutta, Secretary ASIS Singapore chapter, welcomed all the new members in the group and shared about the different initiatives the local chapter is taking and explained how the members can take the most benefit out of it. Sujoy also shared about the membership experience and encouraged new members to connect more with the industry professionals.

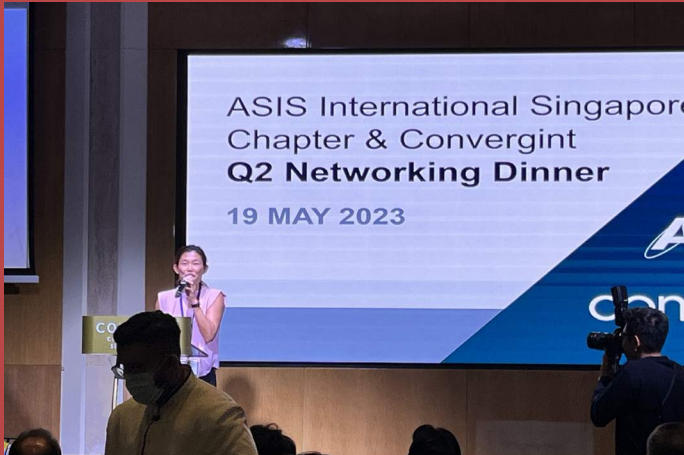
Singapore Chapter management committee members, Matt Lee, Simon Tan, and Jeffrey Lam also attended the event.

Keng Fong Chow and Julie Noh, the new members, mentioned that it was a fantastic opportunity to meet with the management committee, other new members and learn from each other.

The event ended with networking over tea and snacks.

Q2 Networking Dinner 2023

Article Contributed by:
Collin Goh



We have arrived in the second quarter of 2023. The Conrad Centennial Singapore was the venue of the second quarter's ASIS International (Singapore Chapter) networking event. We'd like to sincerely thank Convergent for being the event's lead sponsor.

They have specialised knowledge in a number of different industries, which allows them to fully comprehend their clients' unique business and service requirements. Convergent was developed with the express goal of providing scalable global service, with local leaders granted the authority to make decisions close to the client.



Convergent is an international systems integrator that provides a wide range of services and solutions including security, fire alarm, life safety, audio/visual, and building automation in collaboration with a global network of technology partners and manufacturers.












Convergint is a global systems integrator focused on delivering results for our customers through unparalleled service

Why partner with Convergint?

- ✓ **Culture of service**
Values and Beliefs drive our culture of service
- ✓ **Commitment to excellence**
Vertical expertise that understands specific business and service needs
- ✓ **Innovation**
Services and solutions designed to deliver measurable business results
- ✓ **Certified colleagues**
Our greatest strength is our people, we invest over \$20 million per year on training and certifications
- ✓ **Global platform**
Integrated, consistent delivery by our own certified colleagues
- ✓ **Partnerships**
Strategic alignment with the world's leading technology partners

In **Asia Pacific**, Convergint draws on over 20 years of experience, with a team of over 1000 professionals in more than 50 locations

Our services & solutions

-  Security systems
-  Audio-visual systems
-  PA systems
-  Advanced solutions
-  Managed services
-  Design & consulting services
-  Project implementation services
-  System maintenance services
-  Embedded services

Women-In-Security Get Together

Article Contributed by:

Jennifer Lim

It was truly a great experience. It provided a remarkable platform for women to connect, an opportunity to network and share knowledge and be inspired by incredible role models. Seeing successful women professionals sharing their experiences, challenges, and accomplishments served as an inspiration for aspiring women interested in the field. By showcasing diverse role models, the event conveyed the message that women can thrive and excel in security-related roles.



It was good to see all of us engaging in conversations, exchanging ideas, and learning from the experiences of others fostering a sense of team spirit and support.

Attending the ASIS Women in Security event was an empowering and eye-opening experience that highlighted the significance of diversity and the need for more women in the security field industry and create a supportive space for women professionals. I strongly encourage more women to join the security industry.

PSP Review Course

The Singapore Chapter organised its first run of the PSP review program for 2023 at the Parkroyal on Kitchener Hotel from 19 to 21 June. Attended by 7 participants comprising security practitioners and system integrators from both the public and private sectors in Singapore.





Update from Next-Gen Committee

Article Contributed by:

Matt Lee, NextGen Committee Lead

I would imagine we have quite a bit of these pictures taken at the dinner.

Once again, my heartfelt appreciation for the unwavering support and participation by the Management Committee, Singapore Chapter and importantly our students from SUSS who have embraced this opportunity. Let us continue to work together towards our shared goal of shaping a brighter future in Security!

Please contact Sujoy Dutta or myself to find out more information on our NextGen activities for 2023 and how you can volunteer in this space.

Feedback from Collin and Leon Chew

“ Dear Matt and Sujoy,

I hope this email finds you well! I am writing to share with you some feedback from my peers.

Zoom sharing session

Regarding the sharing session, they found it to be very useful and informative in explaining more about the ASIS membership. The most useful thing for them was learning about the mentorship programme and the importance of networking and learning skills relevant to you. They felt that ASIS would be useful in their careers and would like to see more industry related talks and events in future.

Networking Dinner

Collin: Thank you Matthew, Sujoy and Hwee Fong for the invitation! Really had a blast at the ASIS Q2 dinner. Feedback wise I definitely think it is a useful opportunity to network with industry leaders and gain more exposure to the different realms and roles of the security industry. Great to see familiar faces that we know through

our dad as well. Food was amazing too hahaha

Leon: I think the networking dinner was a great opportunity to start expanding my network of security professionals. As a student, strong connections with industry partners can open up many opportunities such as internships and attachments, which can help me apply the theoretical knowledge and put them into practice while learning more about the demands of a career in this industry. I loved the exposure and meeting new people and I'm looking forward to more events!

Additionally, I am very happy to share that some of my friends are interested in joining the student membership and they would also like to help build up the student programme as well! As mentioned, we're looking to do so after January next year once we've stepped down from the committee.

Looking forward to working together and have a great week ahead!

Calendar of Events



Q3 Networking Dinner

Q3 Networking Dinner is scheduled for 25 August 2023.



Technology Security Exchange (TSX) 2023 – Penang

Registration is now open for Technology Security Exchange (TSX) 2023. Join us at Penang on 17 August 2023 to talk about future strategies & technologies that leads to a sustainable security program.

Registration can be made by the link [here](#)



CPP Review Course

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

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



Overseas Field Visit – Penang

Riding on the inaugural Technology Security Exchange (TSX) Conference on 17 August 2023 which is co-organized by ASIS International Singapore Chapter and Electronic Security Committee amongst others, the ASIS Singapore Chapter is organizing a Field Visit to Dell and Boston Scientific in Penang on 18 August 2023.

Members' Update



Warm Greetings to the following new ASIS International Members!

Ms Aw Hwee Lee
Ms Julie Noh
Mr Koh Yi Xuan
Mr Linus Lim

Mr Saravanan Sammugam
Mr Selva Kumaran
Ms Shirlene Ang
Mr Teo Thiam Chye

Congratulation to Newly Certified Members!

Newly Attained CPP and PSP

Mr Teo Jon Sheng Johnson CPP, PSP

Newly Attained CPP

Ms Foong Yi Ling CPP
Mr Gan Da CPP
Mr Glen Martin Balde Arquiza CPP
Ms Kee Ling Min CPP, PSP
Mr Muhammad Zahed Zulkeplee CPP
Mr Zhou Qinhui CPP

Newly Attained PSP

Mr Dion Yeo Lai Ye PSP

Members' Update



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	Teo Jon Sheng Johnson	CPP, PSP
Mr	Kagan Gan	CPP, PSP	Mr	Willie Heng Chin-Siong	CPP, PSP
Ms	Kee Ling Min	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	Damien Lim	CPP
Mr	Alfian Idris	CPP	Mr	Daniel Ng	CPP
Mr	Andrew Fan Tuck-Chee	CPP	Mr	Den Ho Kai-Quan	CPP
Mr	Anton Chan	CPP	Mr	Desmond Ho Kok Tong	CPP
Mr	Azharie B Mohamed Mudakir	CPP	Mr	Dicky Fadly Zaini	CPP
Mr	Azril Ngasiran	CPP	Mr	Edmund Lam	CPP
Mr	Balasubramaniam Selvam	CPP	Mr	Edwin Goh	CPP
Ms	Beverly F Roach	CPP	Mr	Fabrice Marty	CPP
Ms	Cheng Yen Hwa	CPP	Mr	Firman Latib	CPP
Mr	Chia Wai Mun	CPP	Ms	Foong Yi Ling	CPP
Mr	Ching Chiu Chiu	CPP	Mr	Gan Da	CPP
Mr	Clement Chan	CPP	Mr	Glen Martin Balde Arquiza	CPP

Members' Update

Certified ASIS International Members

Certified CPP members

Mr	Glenn Koh	CPP	Mr	Noriman Salim	CPP
Mr	Hartmut Kraft	CPP	Mr	Ong Kim Poh	CPP
Mr	Ho Jiann Liang	CPP	Mr	Paul Rachmadi	CPP
Mr	Isaach Choong	CPP	Mr	Perry Peter Yeo	CPP
Mr	James Hammond	CPP	Mr	Peter Ang Boon Kiat	CPP
Mr	James Wong Li Ren	CPP	Mr	Ramani Matthew Sachi	CPP
Mr	Jarrood James Nair	CPP	Mr	Ren Huajun	CPP
Mr	Jeffrey Yeo	CPP	Mr	Richard Goh	CPP
Mr	JK Wong	CPP	Mr	Rick Wong Soon Wah	CPP
Mr	Jonathan Yap	CPP	Mr	Sachin Kumar Sharma	CPP
Mr	Joseph F. Jasunas	CPP	Mr	Sam Wai Peng	CPP
Mr	Julian Tan	CPP	Mr	Sanjay Sharma	CPP
Mr	Justin Chen Jianan	CPP	Mr	Shaymentyran Shaem	CPP
Mr	Kan Young Loong	CPP	Mr	Sheo Boon Chew Winson	CPP
Ms	Karen Wong	CPP	Mr	Sia Wang Ting	CPP
Mr	Kelvin Koh	CPP	Mr	Simon Tan Eng-hu	CPP
Mr	Ken Ang	CPP	Mr	Soon Koh Wei	CPP
Mr	Ken Tong	CPP	Mr	Stanley Aloysius	CPP
Mr	Koh Kwang Wee	CPP	Mr	Sujoy Dutta	CPP
Mr	Krishnamoorthy Arunasalam	CPP	Mr	Surendran Chandra Segaran	CPP
Mr	Lai Zihui	CPP	Mr	Taaouicha Mujahid	CPP
Mr	Law Chee Keong	CPP	Ms	Tam Yuen Yee Jeannie	CPP
Mr	Lawrence Tan Jun-Ming	CPP	Mr	Tan Gwee Khiang	CPP
Mr	Leonard Ong	CPP	Mr	Tan Hock Seng	CPP
Mr	Leong Hoe Meng	CPP	Mr	Tan Kok Soon	CPP
Mr	Leong Keng Weng	CPP	Mr	Tay Choon Teck	CPP
Mr	Lim Choon Kwang	CPP	Mr	Teo Kee Kiat	CPP
Mr	Lim Chye Heng	CPP	Mr	Teo Khai Ming	CPP
Mr	Lim Teong Lye	CPP	Mr	Thirukumaran Sankaran	CPP
Mr	Lim Thian Beng	CPP	Mr	Tony Er	CPP
Mr	Look Kang Yong	CPP	Mr	Vincent Soh Chee Yong	CPP
Mr	Lye Kah Meng Joseph	CPP	Mr	Wayne G Edmonds	CPP
Mr	Magalingam Veeman	CPP	Mr	William Toh	CPP
Mr	Marcus Tan ChongLay	CPP	Mr	Wilson Loh	CPP
Mr	Mark Chow	CPP	Mr	Yeh Ing Kerne	CPP
Mr	Mark Nuttall	CPP	Mr	Yuen Kin Wai (Dex)	CPP
Mr	Mitran Balakrishnan	CPP	Mr	Zhou Qinhui	CPP
Mr	Muhammad Hafiz Bin Rohani	CPP			
Mr	Muhammad Iskandar Bin Idris	CPP			
Mr	Muhammad Zahed Zulkeplee	CPP			
Mr	Muhsin Ben Moasi	CPP			
Mr	Nilo S Pomaloy	CPP			

Members' Update

Certified ASIS International Members

Certified PSP members

Mr	Dion Yeo Lai Ye	PSP	Mr	Low Kay Boon	PSP
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	Jason Siow	APP
Mr	Eugene Chua	APP	Mr	Koh Jian Hao	APP
Mr	Faizul Salamon	APP	Mr	Ong Poh Tiong	APP
Mr	Francis Zhang	APP	Mr	Soo Wei Lun	APP
Mr	Goh Kwan Way Marc	APP	Ms	Yong Hwee-Fong	APP

Editorial Team



Eddie Koh, CPP, PSP
Editor



Monica Tomer
Editor



Yong Hwee Fong, APP
Contributor



Jeffrey Lam, PSP
Contributor



Collin Goh
Contributor



Sujoy Dutta, CPP
Contributor



Anthony Lee, CPP, PSP
Contributor



Daniel Chan, APP
Contributor



Jennifer Lim
Contributor



Richard Stuart
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-certified 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 Sep 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. Mitesh Shah

Mr. Jarrod James Nair

Mr. Matthew Lee

Mr. Simon Tan

Registered Mailing 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