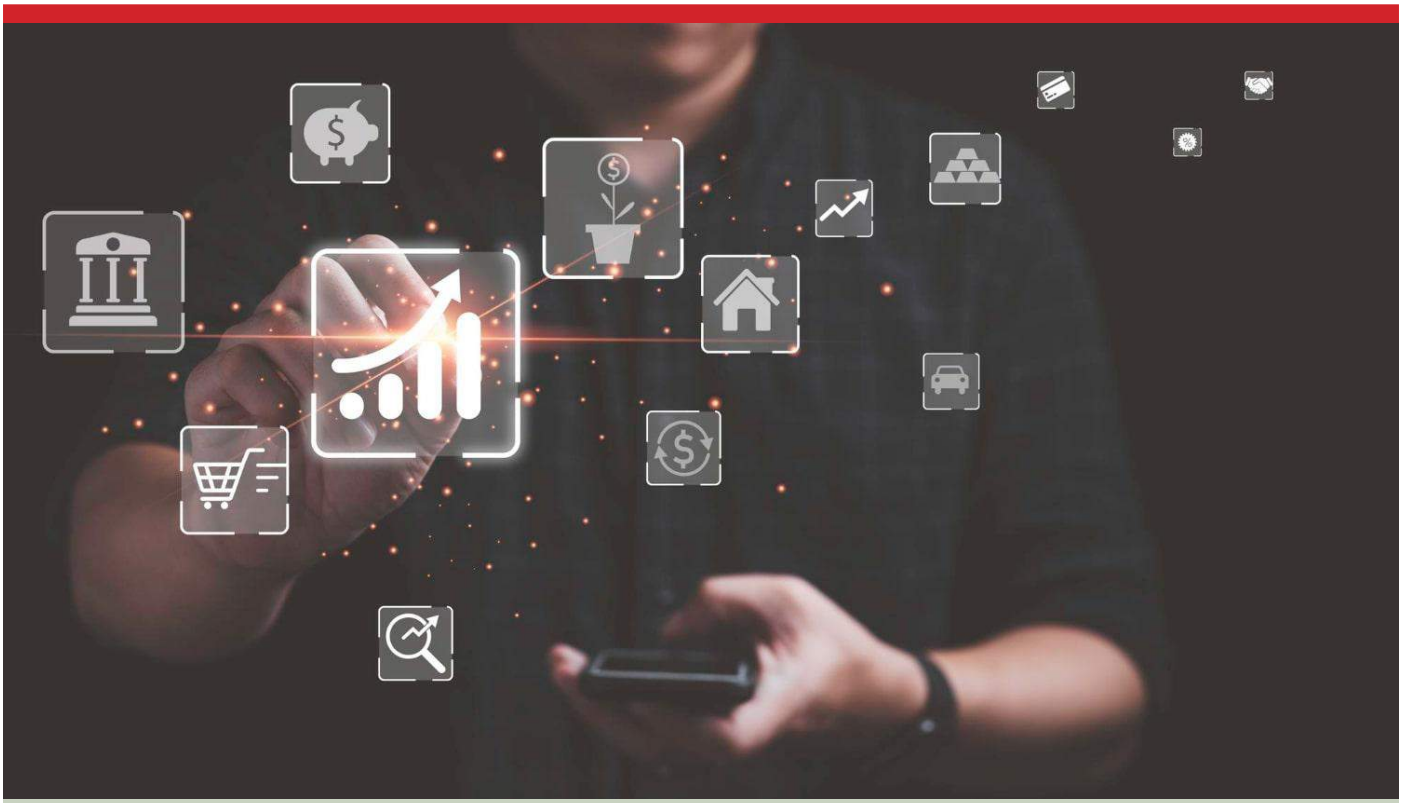
OCTOBER 2024 | Q3 Issue

SECURITY PROFESSIONAL

ASIS INTERNATIONAL® Singapore Chapter



Contents Page

Chairperson's Note

Dear Members,

With the year drawing to a close, I'm excited to share some updates that will shape the months ahead for our community.

We are thrilled to announce that the ASIS International Asia Pacific Conference will take place in Singapore from the 4th to 5th of November, bringing together industry leaders and experts to explore key trends, share innovations, and foster collaboration across the region. This is a fantastic opportunity for networking and learning, and we hope to see many of you there.

As we prepare for this major event, we are looking for passionate individuals who are eager to take on leadership roles, particularly someone to oversee ground operations for the conference. This is a chance to make a lasting impact while building valuable experience.

In addition to the conference, we are approaching the end of our current management committee's term. I encourage any members interested in shaping the future of our Singapore Chapter to step forward and join the next term's management committee.

SAVE THE DATE!

4th & 5th November 2024

ASIS Asia Pacific Conference 2024

Your involvement is key to our ongoing success. I also invite you to contribute to our newsletter. Whether sharing a case study, an industry insight, or personal experiences, your voice can inspire and inform our entire community. Together, we can create content that reflects the wealth of knowledge within our network.

As we move forward together, I wish you all good health and continued success. Let's work collectively to ensure that the coming months are not only productive but truly memorable.

Wishing you good health,
YONG Hwee Fong, APP
Chairperson 2023-2024

Past Event:

Professional Development PSP Review Course

From 14 to 16 August 2024, the first PSP Review Course of the year took place at The Bencoolen, running from 9am to 5pm daily. We had six dedicated participants: four from the private sector and two from the Ministry of Defence. We extend our best wishes to all as they prepare for their upcoming PSP exams, confident that their hard work and commitment will lead to success.

Past Event:

Women-in-Security Top Women in Security ASEAN Region 2024

On 12 September 2024, 25 participants gathered at Axis Communications office @ Suntec for the Top Women in Security ASEAN Region Awards. Now in its fifth year, the awards honoured 30 finalists from eight ASEAN nations, representing sectors such as banking, financial services, critical infrastructure, law enforcement, defence, consumer goods, and managed services.

The event aims to recognize women who have made significant contributions to advancing the security industry within the ASEAN region. It was supported by key security organisations, including regional chapters of ASIS International, ISACA, OWASP, AiSP, and professional women in security groups from Singapore, Malaysia, Indonesia, the Philippines, and Thailand.

This event underscores the vital role women play in shaping the future of security across Southeast Asia.

Past Event:

NextGen Student Member Visit at Daimler Trucks

On 23 September 2024, Daimler Trucks hosted a special reception for 10 student members of ASIS International (Singapore Chapter) at their office located at 1 Gateway. The visit provided students with valuable insights into the security industry, allowing them to explore potential career pathways and sign up for student internship programs.

This event aimed to strengthen the connection between academic institutions and the security industry, helping students apply their theoretical knowledge in real-world settings. By fostering industry engagement, Daimler Trucks and ASIS International hope to inspire the next generation of security professionals and bridge the gap between education and the evolving demands of the security sector.

Demystifying Cybersecurity: Security Operations in Simple English

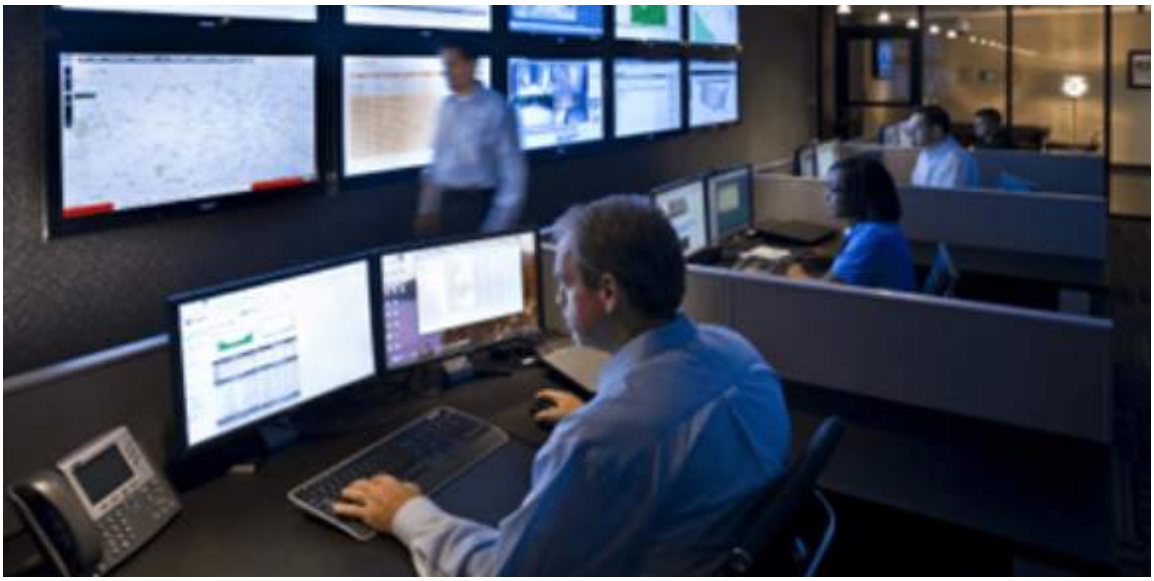
Contributed by:
By Daniel Chan, APP

Introduction
If you have been following my series on CISSP domains, thank you for staying tuned! We have navigated through the complexities of Security and Risk Management, Asset Security, Security Architecture and Engineering, and Communication and Network Security. Now, it is time to dive into the seventh domain: Security Operations. Rest assured, I will break it down in terms that would make it easy for a layperson with no CISSP knowledge to understand.

The Heart of Security Operations
Think of Security Operations as the beating heart of your organization's security efforts. Just as your physical security team monitors CCTV feeds and patrols the premises, cybersecurity operations keep a vigilant eye on the digital landscape. It is like having a team of digital security guards, constantly on the lookout for any suspicious activity.

Investigations: Digital Detective Work
Remember those crime scene investigation shows? Security operations involve a fair bit of digital detective work. When an incident occurs, whether it is a potential data breach or a suspicious login attempt, security professionals spring into action. They collect digital evidence, analyze log files, and piece together the puzzle of what happened.

Imagine you are investigating a break-in at a physical facility. You would check for forced entry, review security camera footage, and dust for fingerprints. In the digital world, we're looking at things like unusual network traffic patterns, examining system logs, and tracking digital footprints left by potential intruders.



Incident Response: The Cyber Fire Brigade

Just as every building needs a fire response plan, every organization needs an incident response plan for cyber emergencies. When a security incident occurs, it's not the time for improvisation. A well-prepared incident response team is like a well-drilled fire brigade – they know exactly what to do when the alarm bells ring.

The incident response process typically involves:

1. Preparation: Having tools, procedures, and trained personnel ready.
2. Identification: Detecting and confirming that an incident has occurred.
3. Containment: Limiting the damage, like putting out a fire before it spreads.
4. Eradication: Removing the threat, akin to clearing a building of hazardous materials.
5. Recovery: Restoring systems to normal operation.
6. Lessons Learned: Reviewing the incident to improve future responses.

Disaster Recovery and Business Continuity: Weathering the Digital Storm

Remember the last time a power outage hit your neighbourhood? Those who had flashlights and backup generators were probably feeling pretty smug. In the digital world, disaster recovery and business continuity planning serve the same purpose – ensuring that when things go wrong, you are not left fumbling in the dark.

Disaster recovery focuses on restoring IT systems after a major disruption, while business continuity ensures that critical business functions can continue during and after a disaster. It's like having a Plan B, C, and D for your digital operations.

Logging and Monitoring: The All-Seeing Eye

In the physical security world, you might have security guards keeping watch and logging any unusual events. In cybersecurity, logging and monitoring serve a similar purpose. Systems constantly generate logs – records of activities and events. Security professionals monitor these logs, looking for any signs of trouble.

It is a bit like having a super-powered security camera that not only records everything but also alerts you to potential issues. "Hey, boss! That server just tried to contact a known malicious IP address. Might want to check that out!"

Change Management: Controlled Evolution

Change is inevitable, but in the world of security operations, uncontrolled change is a recipe for disaster. Change management ensures that modifications to systems are implemented in a controlled, documented manner. It's like renovating a high-security facility – you don't just let contractors wander in and start knocking down walls. Every change is planned, approved, and carefully executed.

Asset Management: Know What You're Protecting

You cannot protect what you do not know you have. Asset management in security operations involves maintaining an inventory of all IT assets – hardware, software, data, and even human resources. It is like having a detailed map of your kingdom, knowing every nook and cranny that needs defending.

Patch Management: Fixing the Cracks
Software vulnerabilities are like cracks in your fortress walls – they need to be patched up before attackers can exploit them. Patch management involves identifying, acquiring, testing, and installing updates to systems. It is a never-ending task, much like maintaining a large physical structure. You would not ignore a crack in a dam, would you?

How Security Operations Relate to Other Domains
Security Operations does not exist in isolation. It is intimately connected with the other CISSP domains we have explored:

- It implements the policies and procedures defined in Security and Risk Management (Domain 1).
- It protects and manages the assets identified in Asset Security (Domain 2).
- It operates within the framework established by Security Architecture and Engineering (Domain 3).
- It monitors and defends the networks outlined in Communication and Network Security (Domain 4).
- It enforces the access controls defined in Identity and Access Management (Domain It assesses and tests the security measures discussed in Security Assessment and Testing (Domain 6).

Real-World Example: The SolarWinds Incident
To illustrate the importance of robust security operations, let us consider the SolarWinds incident of 2020. Attackers managed to insert malicious code into SolarWinds' Orion software, which was then distributed to thousands of organizations through routine updates. This breach highlighted the critical need for:

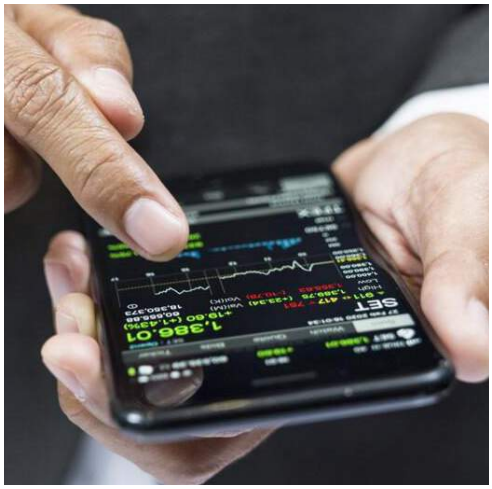
- Rigorous change management and software development security practices
- Comprehensive logging and monitoring to detect unusual activities
- Effective incident response procedures to contain and mitigate the breach
- Strong asset management to identify affected systems
- Thorough patch management to apply fixes once available

Conclusion: The Never-Ending Vigilance
Security Operations is where the rubber meets the road in cybersecurity. It is a domain that requires constant vigilance, adaptability, and a proactive mindset. Just as a physical security team never rests, always watching for potential threats, cybersecurity operations professionals are the unsung heroes working tirelessly behind the scenes to keep our digital world safe. Remember, in the ever-evolving landscape of cybersecurity, standing still is moving backwards. Therefore it is important to keep learning, stay alert, and may your logs always be clean and your patches up to date!

(Source: Cybersecurity and Infrastructure Security Agency, "Alert (AA20-352A) Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations," December 17, 2020)

How to Stay Ahead of The Digital Asset Threat Landscape

Contributed by:
Jag Foo, CPP, PSP, PCI



A Long History of Hacks in Digital Assets
The digital asset space has always been a major target for malicious actors. From the early days of cryptocurrency to the rapidly evolving world of Web3, billions of dollars have been lost to hacking exploits.

As the industry continues to grow, so does the attack surface and sophistication of attacks. High-profile incidents involving significant financial losses continue to serve as a stark reminder of the dangers in the blockchain arena. We've witnessed how even established platforms can be compromised, particularly with major centralized crypto exchanges in the last few months.

Recent Hacks: WazirX, DMM Bitcoin, and Indodax

DMM Bitcoin Hack (May 2024 - $305M Lost):
Ranked among the largest crypto heists in history, this attack likely stemmed from a private key compromise. Speculation points to social engineering or malware as the methods used to gain access. This incident revealed the potential exposure even highly secure platforms face when confronted with sophisticated phishing or impersonation techniques.

WazirX Hack (July 2024 - $235M Lost):
This attack on one of India's largest exchanges highlighted the risks tied to social engineering. Hackers exploited vulnerabilities in the multisig wallet system through phishing and address tampering. The attackers tampered with the whitelisted addresses, tricking signatories into approving fraudulent transactions that they believed to be legitimate. The loss of $235 million has left a significant mark, reminding us of how human error and system deficiency can be exploited by highly skilled attackers.

Indodax Hack (September 2024 - $22M Lost):
Just recently, Indodax, one of Indonesia's leading crypto exchanges, suffered a breach that resulted in the theft of $22 million worth of assets. This included Ethereum (ETH), Bitcoin (BTC), Tron (TRX), and Polygon (MATIC) tokens. The hack has raised serious concerns about the platform's hot wallet security.

The Growing Threat of State-Sponsored Actors (APT)
Among the most dangerous adversaries in the crypto world are **Advanced Persistent Threats (APT)**, especially those sponsored by nation-states like North Korea. Lazarus Group, a notorious North Korean hacker entity, known for targeting major financial institutions and crypto platforms, is suspected to be involved in all 3 incidents.

These groups have vast resources and employ highly skilled teams to orchestrate long-term attacks. Their methods include cyber espionage, malware deployment, and social engineering, which makes them a persistent and complex threat to the digital asset ecosystem.

Social Engineering: A Persistent and Growing Threat
Social engineering remains one of the most effective methods attackers use to compromise systems. By targeting the weakest link—the human element—hackers can bypass even the most secure systems. Phishing emails, impersonation tactics, and fake job offers are just a few tactics attackers use to deceive employees and individuals into granting access to critical information or approving malicious transactions. The WazirX and DMM Bitcoin hacks serve as clear examples of how systems and assets can be compromised through targeted social engineering campaigns.

For Users and Employees:

- **Education and Training:**
  Regularly educate employees and users about phishing, social engineering, and cybersecurity best practices. Awareness is the first line of defence. Adopt the mindset of "Don't Trust, Always Verify" when interacting with unsolicited messages or requests.

- **Red Team Exercises:**
  Simulating real-world attack scenarios, known as Red Teaming, can help identify potential vulnerabilities within your organisation. This keeps staff alert and sharp in recognizing and responding to threats.

- **Eliminate Single Points of Failure:**
  Using **Multi-Party Computation (MPC)**, which distributes signing authority and key shards across multiple geographically dispersed locations and systems, ensures that no single compromised key shards or entity can result in asset theft.

- **Data Encryption:**
  Using cryptographic and encryption technology such as **Trusted Execution Environment (TEE)** can help assure the privacy and integrity of sensitive data such as private key shards, API keys and security policies, preventing tamper from 3rd parties or within.

- **Zero-Trust Architecture:**
  Implement a **Zero-Trust Security Model** by incorporating **Multi-Factor Authentication (MFA)**, multi-party approvals, and robust role-based access controls to limit exposure and reduce the likelihood of unauthorised access.

- **What You See Is What You Sign (WYSIWYS):**
  Ensuring that the transaction details displayed to signatories match the actual underlying data is critical. This prevents attackers from manipulating transactions between the user interface and the back end.

- **Regular Penetration Testing & Bug Bounty Programs:**
  Partner with multiple cybersecurity vendors to perform regular penetration testing. **Bug bounty programs** can incentivize ethical white-hat hackers to identify vulnerabilities before malicious actors do.

For Processes:

- **Segregation of Duties:**
  Divide responsibilities to minimise risks. For example, splitting transaction approval among different roles ensures that no single person has unilateral control over critical processes. Roles and permissions should always be set in accordance with the principle of least privilege.

- **Strong Password and Anti-Virus Management:**
  Use password managers, enforce strong password policies, and require MFA for access to critical systems. Having a strong anti-virus system helps detect and stop any possible virus and malware threats early before it can compromise any critical assets or data

- **Asset Segregation:**
  Maintain a strict separation between hot wallets (used for daily operations) and cold wallets (used for long-term storage). Cold wallets should never be exposed to the internet, reducing the risk of compromise.

Conclusion: Why Continued Vigilance and Proactive Defense Matter
The recent high-profile hacks of WazirX, DMM Bitcoin, and Indodax serve as stark reminders that no platform, no matter how secure, is immune to sophisticated attacks. The growing threat of Advanced Persistent Threats like the Lazarus Group means the industry must remain ever-vigilant. Social engineering and phishing attacks that lead to compromise private keys will continue to be a leading attack vector, making user education and rigorous security protocols absolutely vital.

By embracing a zero-trust architecture, leveraging cryptographic technologies like MPC and TEE, and continuously improving security awareness, the digital asset industry can stay ahead of the threat landscape. Vigilance, robust defence mechanisms, and ongoing education are the keys to securing the future of digital assets.

About the author:
Jag is a Partner at Safeheron, a digital asset security technology service company

Transforming Physical Security: The Impact of AI and Digital Innovation

Contributed by:
Jeffrey Lam, PSP & Peter Tan, CPP, PSP, PCI

The physical security landscape is undergoing a profound transformation, driven by advancements in technology and automation. In Singapore, the Ministry of Home Affairs (MHA) has spearheaded several digital transformation initiatives to enhance security operations, improve efficiency, and reduce manpower dependence. These include the Industry Transformation Map (ITM) as well as the Outcome-Based Contracts (OBC). This article delves into technologies such as IoT, AI, 5G, robotics, and cloud platforms, which reshape physical security by offering 'real-time response and predictive threat management.

IoT Sensors and Continuous Monitoring

IoT devices, including smart cameras, motion sensors, and environmental sensors, provide continuous, real-time monitoring of our environment. These devices collect vast amounts of data on movement, sound, temperature, and more. Using embedding smart chips, they can filter out false positives and adapt to environmental changes. By transmitting only processed data or metadata instead of raw footage, these sensors streamline operations, providing security teams with focused, actionable insights. This technology reduces response times and enhances overall security, preventing incidents before they escalate into breaches.

AI and Predictive Analytics: Anticipating Threats Before They Occur

AI and data analytics are at the core of modern physical security, transforming raw sensor data into actionable intelligence. While video analytics has been with us for a decade, newer AI-driven systems can identify patterns, detect anomalies, and predict potential security breaches based on historical data. For example, AI can distinguish between regular foot traffic and suspicious loitering, immediately alerting security personnel to potential threats. The predictive capabilities of AI allow security teams not just to react but to anticipate incidents, shifting from a reactive to a proactive security model.

Geo-Location Technologies and Real-Time Resource Allocation

Geo-location technologies enable precise tracking of security personnel, vehicles, and even drones, enhancing the speed and efficiency of incident response. Integrated with AI, these systems can dynamically allocate resources, automatically dispatching the nearest security officer or drone to an incident site. This approach not only reduces response times but also ensures that human resources are deployed in a way that ensure overall security effectiveness.

Automated and Adaptive Incident Response
Automated incident response systems integrate AI, IoT, and robotics to manage security events with minimal human intervention. Upon detecting a breach, such systems can autonomously initiate lockdown procedures, sound alarms, and notify security teams. Advanced robotics can engage directly with intruders, issuing audio warnings or deploying non-lethal deterrents. This blend of automated and human-driven responses creates a layered, adaptable security strategy that improves incident outcomes and minimizes risks.

Cloud Computing & 5G and Remote Management
The combination of cloud computing and 5G connectivity revolutionizes remote management in security operations. Cloud platforms offer scalable storage solutions and centralized access to data, eliminating the need for costly on-site equipment. High-speed 5G networks enable real-time video streaming and data transmission, allowing security teams to manage operations from anywhere in the world. The seamless integration of remote and on-site security operations provides a unified, coordinated response, enhancing the overall resilience of security systems.

Integrated Systems and Coordinated Responses
The digital transformation of physical security involves the integration of previously siloed systems—such as video surveillance, access control, and intrusion detection—into a cohesive, unified platform. These integrated systems cross-reference data across multiple sources, enhancing situational awareness and enabling quicker, more coordinated responses to incidents. For instance, when the system detects an access breach, linked cameras can immediately focus on the entry point while security personnel are dispatched, creating a synchronized, multi-layered defence.

Cybersecurity
With the increasing reliance on digital technologies, cybersecurity becomes a critical component of physical security. Security systems are vulnerable to cyberattacks, including attempts to disable cameras, manipulate sensors, or access sensitive data. Strong cybersecurity measures—such as end-to-end encryption, multi-factor authentication, and continuous monitoring—are essential to protect against these threats. Regular updates, patches, and robust network security protocols ensure that security technologies remain resilient against evolving cyber risks.

The Future Role of Drones and Robotics in Security
Drones and robotics offer capabilities that extend beyond traditional surveillance methods. Drones provide aerial surveillance, monitor large areas quickly, and can detect anomalies like heat signatures, even in low-visibility conditions. Robotics can perform repetitive or dangerous tasks, such as patrolling perimeters or inspecting hazardous environments. This reduces human fatigue as well as exposure to high-risk situations. As AI and robotics evolve, drones and robots will take on more complex roles, from autonomous patrolling to direct engagement with threats.

Ethical Considerations and Future Implications
While technological advancements significantly enhance security, they also raise ethical questions regarding privacy, data security, and the potential for misuse. Balancing the need for security with individual rights is a growing challenge and requires clear policies and robust governance. Future innovations should focus on ethical AI and transparency. This would maintain public trust while harnessing the full potential of these technologies.

Towards a Smarter, More Resilient Future
Digital transformation is fundamentally reshaping the physical security landscape, enabling smarter, faster, and more coordinated responses to threats. The integration of IoT, AI, robotics, and cloud computing offers unprecedented situational awareness and operational efficiency. However, as physical and cybersecurity converge, a comprehensive approach is crucial to guard against evolving risks. This includes addressing ethical and cybersecurity challenges associated with these systems. By balancing these innovations with these considerations, we can build a resilient, adaptive security infrastructure that makes a smarter, safer world.

Member Spotlight

Simon Tan, CPP

Each quarter, we'll chat with a remarkable member of our community to learn about their experiences and what inspires them.
This month, we feature Simon Tan, Regional Security Manager, Asia Pacific for Shell.

Q **How did you get into a security management career? What do you like about security management?**

A I have always wanted to join a uniform organisation like the Army, Navy or the Police since young. During my National Service, I was drafted into the SAF Commando Formation. The training was tough but interesting. To be qualified as a Commando we must go through various courses such as Airborne course, fast roping training, explosive training and many more. Eventually, I decided to sign-on as a Commando Officer and served as a professional soldier for 23 years. At that time, we must retire at the age of 45 as a combat officer. Hence, I started to reach out to my network outside of the SAF and start researching what the career options are for someone like me. In the end, I decided to go into something that is related to security or crisis management. In 2011, I retired early from the armed forces and joined an international risks consulting firm as a Security and Crisis Consultant. The nature of security consulting is that I was exposed to various industries and businesses which gave me a chance to understand security issues and concerns of each of the different industries. After 4 years, I was given the opportunity to join Shell as the Southeast Asia Security Manager managing security risks for a cluster of 6 countries.

What do I like about security management? In security management, it is never the same routine every day. Today I may be conducting a Security Risks Assessment on an Oil Rig, the next day I may be handling a security incident. I also get to meet different internal stakeholders and network with many external industry partners. The job challenges me to be creative and think out of the box to help businesses navigate an increasingly volatile security threat landscape.

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

A I have been in my current role for almost 3 years, and I have a small team of 13 people reporting to me. My Line Manager is the Global Chief Security Officer of the company.

Q

What is a typical day like for you?

A

I am an early person and I usually wake early to workout. After this, I will go to the office or to one of the sites for meetings. My work requires me to meet with a lot of business and country leaders hence most of my days are lined up with meetings. Like all Singaporeans, lunch time is important to me as that allows me some down time and catch up with my Singapore based colleagues. After work, I will go home to be with my family and play with my dog. Sometimes, I will attend networking events or courses after work. Shell puts a lot of emphasis on staff development, so all staff are expected to set aside time for training and courses. Hence, some portions of my time are used to attend courses or training each year. To me learning is extremely important for my job so as to arm myself to respond to a rapidly changing and volatile world.

Q

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

A

During my time as a security consultant, I was tasked to provide executive protection for a government linked company leadership team travelling to Türkiye. During the trip, there were protests against the local government's plan to build a commercial building over an iconic park in the capital. The protest location was just down the street from the delegate's hotel, and it could potentially impact the delegate if the situation deteriorates. As the hotel was built along a river, part of the plan is to evacuate the delegates using watercrafts. On the last day of the trip, we received news that the soccer fans were joining the protest and immediately the executive protection team knew riots would break out that afternoon. I then instructed the executive protection team to evacuate the delegate via the standby boats to get across the river and go to the airport. The team executed the evacuation as per rehearsal and plan. The delegates safely arrived at the airport without any incident.

I still remember the delegates thanking each Executive Protection Officer for keeping them safe. That's one of the most memorable moments in my security career.

Q

Do you recommend a career in security to others?

A

Yes, I would recommend a career in security to others. There is so much to learn in this field, and it is gaining more attention by the business leaders especially in today's poly-crisis landscape.

Q

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

A

I came across ASIS when I was researching on the internet for industry recognized security certification. I joined ASIS because I wanted to take the CPP exam and get my hands on the high-quality security related materials on their website. After I joined the Singapore Chapter, I also realised that my network has also grown by attending the various organised activities.

Q

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

A

ASIS has helped me in my successful career shift from the military to private sector. The membership helps me meet great friends and mentors who are readily lend a helping or share their experience with me. Through ASIS, I expanded access to a network of professionals, valuable resources, and career development opportunities that significantly boosted my career progression.

Calendar of Events

ASIS International (Singapore Chapter) APAC Security Conference 2024

ASIS International (Singapore Chapter) will be organising APAC Security Conference 2024 on 4 - 5 November in Singapore at Tang Marriott Hotel Orchard, Level 3 Grand Ballroom.

AGM and Q4 Networking Dinner

The chapter will be having Annual General Meeting 2024, election and Q4 Networking Dinner on 6 December 2024.

**Details will be released soon.*

Members' Update

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

Mr	Chia Sze Chuan
Mr	Deng Jing Ming Jason
Mr	Donny Kurtiyono
Mr	Douglas I Hornell-Scott
Mr	Foo Siang Siang Rendall
Mr	Gabriel Heng Aik Fine, CPP
Mr	Julius Cesar Parras
Mr	Lim Aik Boon
Mrs	Lynn Huang
Mr	Manas Nag
Mr	Muhammad Muzaffar Bin Mohamed Ali
Mr	Nyeo Chew Kian
Mr	Ramani Murugiah
Mr	Shawn Pereira
Mr	Then Yik Nian

Members' Update

Certified ASIS International Members

Certified CPP, PSP, PCI members

Mr	Adrian Wong Voon-Ming	CPP, PCI, PSP	Mr	Peter Tan	CPP, PCI, PSP
Mr	Colin J Spring	CPP, PCI, PSP	Mr	Quek Wei Chew	CPP, PCI, PSP
Mr	Jag Foo	CPP, PCI, PSP	Mr	Rajesh	CPP, PCI, PSP
Mr	Koh Shi Sheng	CPP, PCI, PSP	Mr	Shamus Yeo See Yew	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	Lee Choon-Wai Anthony	CPP, PSP
Mr	Charles Fabian Khoo	CPP, PSP	Mr	Melvin Cheng Tze-Hui	CPP, PSP
Mr	Chua Boon-Hwee	CPP, PSP	Mr	Peter Ang Boon Kiat	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	Mr	Yuen Kin Wai (Dex)	CPP, PSP

Certified CPP members

Mr	Abdul Redha Bin Abdullah	CPP	Mr	Dicky Fadly Zaini	CPP
Mr	Alfian Idris	CPP	Mr	Edwin Goh	CPP
Mr	Andrew Fan Tuck-Chee	CPP	Mr	Firman Latib	CPP
Mr	Anton Chan	CPP	Ms	Foong Yi Ling	CPP
Mr	Azharie B Mohamed Mudakir	CPP	Mr	Gan Da	CPP
Mr	Azril Ngasiran	CPP	Mr	Goh Jun Xian	CPP
Mr	Balasubramaniam Selvam	CPP	Mr	Hartmut Kraft	CPP
Ms	Beverly F Roach	CPP	Mr	Ho Jiann Liang	CPP
Ms	Cheng Yen Hwa	CPP	Mr	Isaach Choong	CPP
Mr	Chia Wai Mun	CPP	Mr	James Hammond	CPP
Mr	Clement Chan	CPP	Mr	James Wong Li Ren	CPP
Mr	Damien Lim	CPP	Mr	Jarrod James Nair	CPP
Mr	Daniel Ng	CPP	Mr	Jeffrey Yeo	CPP
Mr	Den Ho Kai-Quan	CPP	Mr	Jonathan Yap	CPP

Members' Update

Certified ASIS International Members

Certified CPP members

Mr	Joseph F. Jasunas	CPP
Mr	Julian Tan	CPP
Mr	Justin Chen Jianan	CPP
Ms	Karen Wong	CPP
Mr	Kelvin Koh	CPP
Mr	Ken Ang Guorong	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 Thian Beng	CPP
Mr	Lim Yeong Sing	CPP
Mr	Look Kang Yong	CPP
Mr	Lye Kah Meng Joseph	CPP
Mr	Magalingam Veeman	CPP
Mr	Marcus Tan ChongLay	CPP
Mr	Mark Chow	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	Patrick Tse	CPP
Mr	Perry Peter Yeo	CPP
Mr	Ren Huajun	CPP
Mr	Rick Wong Soon Wah	CPP
Ms	Rohaiza Ahmad Asi	CPP
Mr	Sachin Kumar Sharma	CPP
Mr	Sam Wai Peng	CPP
Mr	Sanjay Sharma	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
Ms	Tam Yuen Yee Jeannie	CPP
Mr	Tan Boon Hoe	CPP
Mr	Tan Gwee Khiang	CPP
Mr	Tan Hock Seng	CPP
Mr	Tan Yean Sang	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	Zhou Qinhui	CPP

Members' Update

Certified ASIS International Members

Certified PSP members

Mr	Chan Jianhui	PSP	Mr	Kevin Loh	PSP
Mr	Dion Yeo Lai Ye	PSP	Mr	Mayank Sinha	PSP
Mr	Jeffrey Lam Boon Kee	PSP	Mr	Soh Wei Jye	PSP

Certified APP members

Mr	Daniel Chan	APP	Ms	Lim Yan Ling	APP
Mr	Eugene Chua	APP	Mr	Mohammed Nuh	APP
Mr	Faizul Salamon	APP	Mr	Ong Poh Tiong	APP
Mr	Francis Zhang	APP	Mr	Ow Weng Hong	APP
Mr	Jason Siow	APP	Mr	Soo Wei Lun	APP
Mr	Koh Jian Hao	APP	Ms	Yong Hwee-Fong	APP

Editorial Team

Eddie Koh, CPP, PSP
Editor

Perry Yeo, CPP
Editor

Yong Hwee Fong, APP
Contributor

Sujoy Dutta, CPP
Contributor

Chow Keng Fong
Contributor

Daniel Chan, APP
Contributor

Jag Foo, CPP, PSP, PCI
Contributor

Jeffrey Lam, PSP
Contributor

Matthew Lee
Contributor

Peter Tan, CPP, PSP, PCI
Contributor

Simon Tan, CPP
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
Submissions close on 15 Nov 2024

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. Lim Chye Heng, CPP

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

Honorary MC Members
Mr. Anthony Lee, CPP, PSP
Ms. Chow Keng Fong
Mr. Mitesh Shah
Mr. Jarrod James Nair, CPP
Mr. Matthew Lee
Mr. Simon Tan, CPP

Registered Mailling Address:
ASIS International (Singapore Chapter)
1, Coleman Street, B1-32 The Adelphi, Singapore 179803
Website: www.asis-singapore.org.sg

Email: memberservices@asis-singapore.org.sg