SEPTEMBER 2023 | Q3 Issue

SECURITY PROFESSIONAL

ASIS INTERNATIONAL® Singapore Chapter

Contents Page

Chairperson's Note

Dear Members and Colleagues,

Embrace the Future of Security Together
I trust this message finds you well and in good spirits. Thank you for your unwavering belief in the value our Chapter has delivered thus far. Together, we've achieved remarkable milestones, and our journey continues to be defined by the collective dedication to excellence.

1. **Celebrating Our Success:** It's important to take a moment to reflect on our accomplishments. Our chapter has grown stronger year by year because of your active participation, insights, and contributions. And it is through each and everyone of you that is making us who we are today.

2. **Expanding Horizons:** In the ever-evolving landscape of security, it's crucial that we remain hungry for knowledge and curious about what other professions can offer. Let's not limit ourselves to the boundaries of our discipline. Let's explore synergies with other fields, learn from diverse perspectives, and challenge ourselves to think outside the box.

3. **Site Visits and Networking:** Knowledge gained outside the confines of textbooks and classrooms is often the most valuable. I encourage each of you to attend as many site visits and networking sessions as possible. These experiences not only broaden our understanding but also allow us to build meaningful relationships with fellow professionals.

4. **Giving Back:** Our strength as an association lies in our collective willingness to give back. I call upon each member to consider volunteering their expertise in our committees:

- Professional Development Committee: Share your insights and help us shape the future of our profession.
- Social and Event Committee: Contribute your creativity to make our gatherings memorable.
- Next Generation Committee: Mentor and guide the emerging talent in our field.
- Women in Security Committee: Promote diversity and inclusion in our industry.

Your involvement in these committees is an investment in the future of security. It's a way to ensure that our knowledge and expertise is passed on to the next generation and that we continue to evolve as an association.

As we embark on this journey together, remember that the future of security is dynamic, and we must adapt to thrive. Let us be the leaders who not only safeguard our organisations but also shape the security landscape of tomorrow.

With your faith in the association, our dedication and your passion in this profession, I am excited to see what we can achieve together as we embrace the future of security.

Wishing you good health,

YONG Hwee Fong, APP
Honorary Chairperson

Demystifying Cybersecurity: Communication and Network Security in Simple English

Article Contributed by:
By Daniel Chan, APP

In my previous article submission on “Demystifying Cybersecurity: Security Architecture and Engineering in Simple English”, we likened the intricate domain of Security Architecture and Engineering to the comforting and familiar structure of a house. As we continue our journey, let us delve into the bustling world of Communication and Network Security, the fourth domain of the CISSP. Picture a vast, intricate highway system, with data packets as vehicles, and you’ll grasp the essence of this domain.

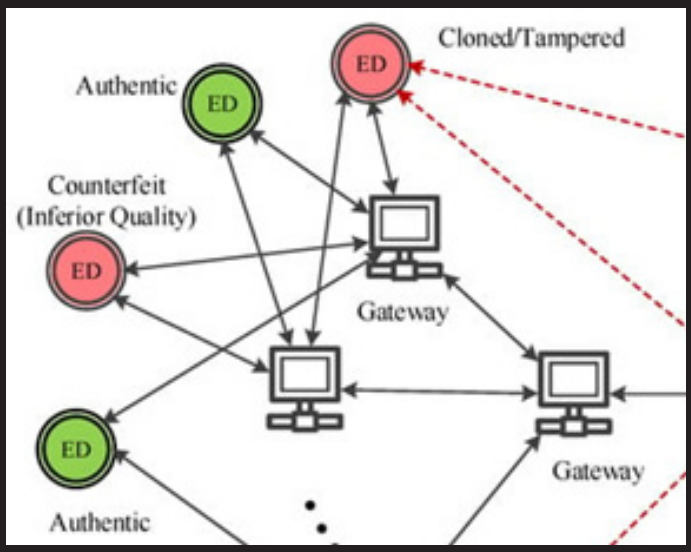
Understanding the Highway of Data: Communication and Network Security

When you think of a highway, you picture cars zooming past, each with a destination in mind. Similarly, in the digital realm, data packets travel across networks, moving from one device to another. Each vehicle, whether it is a compact car or a massive truck, represents a packet of data. Just as highways need traffic rules, signs, and barriers for safe transit, digital data requires specific protocols and structures to ensure it reaches its destination smoothly and securely.

The Essence of Network Security

The Digital Highway Blueprint. Architects design highways with various factors in mind: traffic volume, terrain, safety, and more. Similarly, network architects design our digital highways. They ensure that data, from a simple email to a high-definition movie, can travel smoothly and securely. For instance, streaming platforms like Netflix rely on robust network architectures to ensure that movies and shows play without buffering or interruptions.

Traffic Rules for Data. Roads have traffic signals, speed limits, and lane markings. Similarly, in the digital realm, we have protocols. These are sets of rules ensuring data doesn’t crash into other data. For example, the Transmission Control Protocol (TCP) ensures that data packets reach their destination in the correct order, much like ensuring cars on a highway maintain their lanes and follow traffic signals.



Security Checkpoints. Firewalls act as the toll booths on our digital highway. They inspect data and ensure only the authorised packets can pass through. For instance, when you access your online banking, firewalls ensure that only you can see your account details, blocking any malicious attempts to access your information.

Guarding Against Digital Highway Robbers
Every highway has its challenges, from carjackers to unexpected roadblocks. Our digital highways are no different:

Watching for Suspicious Activity. Intrusion Detection Systems (IDS) are akin to highway patrol cars. They monitor the flow of data, ready to raise an alarm if they spot something unusual. For instance, if someone tries to

access a company's confidential files without permission, the IDS flags this activity, much like a patrol car chasing an errant vehicle.

Secure Tunnels. VPNs (Virtual Private Networks) are like secure, underground tunnels on our digital highway. If you have used a VPN to access work files from home, you have travelled through this secure tunnel, shielded from the prying eyes of hackers, much like a VIP car convoy ensures privacy and security for its passengers.

Ensuring End-to-End Safety
Just as it is not enough to have a safe highway, but the entire journey from start to end (including smaller roads, alleys, and driveways) must be secure, in the digital world, we need end-to-end communication security. This ensures that data remains safe, not just on the main network but even when it moves to smaller, interconnected networks.

Safe Journeys. Just as delivery trucks have seals to ensure packages are not tampered with, encrypted data ensures that information remains confidential from its starting point to its destination. When you send a message on apps like WhatsApp, end-to-end encryption ensures that only the recipient can read it, keeping eavesdroppers at bay.

Challenges on the Digital Highway
As our digital world expands, with more devices connecting and more data flowing, the challenges increase:

Diverse Destinations. Our digital highway sees a variety of 'destinations', from smartphones to smart fridges. Each device presents unique security challenges. For instance, securing a corporate server is different from securing a smart thermostat, yet both are crucial in today's interconnected world.

Rapidly Changing Landscape. New technologies, like 5G or cloud computing, constantly reshape our digital highways. These advancements, while beneficial, also introduce new security considerations. For instance, as more companies adopt cloud storage, ensuring the security of data stored off-site becomes paramount.

Conclusion
As our journey through the vast landscape of cybersecurity continues, understanding the principles of Communication and Network Security becomes even more crucial. It is about more than just smooth data flow; it is about ensuring every piece of information, every 'vehicle' on our digital highway, reaches its destination safely. By grasping these principles, we are all better equipped to navigate the digital age securely.

As we progress in this series, we will delve deeper into the remaining domains, using familiar analogies to make the complex world of cybersecurity accessible to all. Stay tuned!

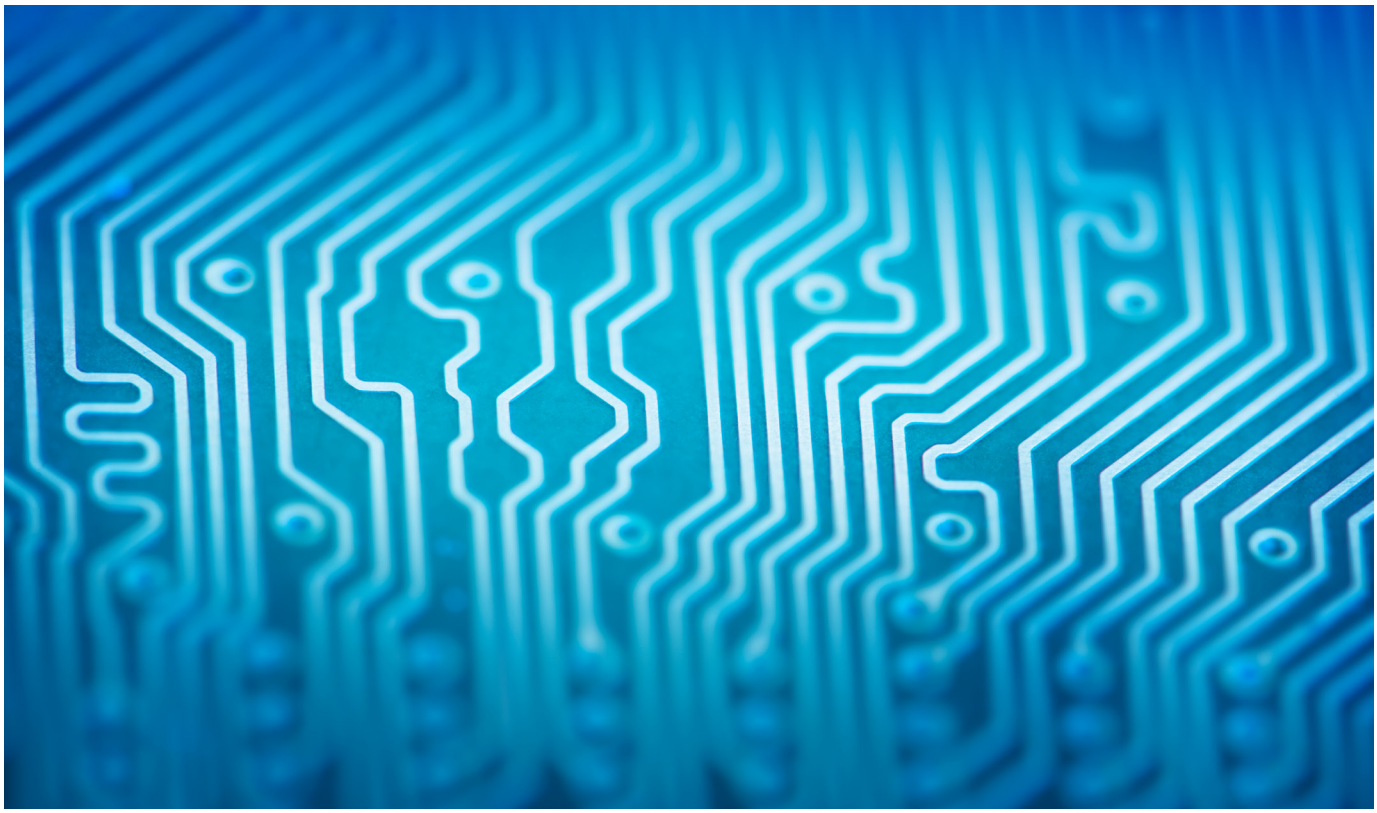
Sources:
1. Harris, Shon. CISSP All-in-One Exam Guide, 8th Edition. McGraw-Hill Education, 2018.

2. Chapple, Mike & Seidl, David. CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide, 8th Edition. Sybex, 2018.

Contributed Article

A Simple Introduction to Quantum Computing

Article Contributed by:
Yeh Ing Kerne, CPP



As a lay person, we have probably only seen the term “quantum” being used in superhero movies and sci-fi stories. It conjures up ideas of extremely complex science or immense power. We ask ourselves if quantum is a real thing or simply a fancy word to spice up a story.

And then we start reading about quantum computing in the news. It makes us wonder if someone in the marketing department had just stuck a fancy sounding word in-front of a boring sounding one, in order to help sell more computers. But quantum computing is a reality and probably will become mainstream in a decade or less.

What is quantum computing? Why is it different from the computers of today (or what is being termed as classical computers)? And why should a security practitioner even care about it? Ok, lets try to answer these 3 questions in a simple way.

The quantum in quantum computers
The quantum in our topic of discussion refers to quantum mechanics, a rather esoteric field within physics that basically deals with physics at the atomic and subatomic level.

Suffice to say that quantum computers leverage quantum mechanics in a computing device to perform computations. Quantum bits, or qubits for short, are the basic building blocks of a quantum computer. This segues to our next question: why are quantum computers different from classical computers?

The differences with classical computers

As mentioned earlier, quantum computers use qubits as their device to represent and manipulate information or data. In classical computers (i.e. the computers we are using today), bits in a binary state ("0" or "1", "on" or "off") perform the same function. It is the grouping of these bits into larger sets (bit, nibble, byte, kilobyte, so on and so forth) that enables the capabilities and outputs that our beloved devices of today produce for our work and enjoyment.

However, the qubit has one up on the bit: the qubit can exist in multiple states simultaneously as compared to the strictly binary state of a bit. In other words, the qubit can represent both binary states at once (basically being "0" and "1" at the same time). This phenomena is called superposition, and enables quantum computers to perform certain computations in parallel, potentially leading to faster calculations when compared to classical computers.

Another trick up the qubit's sleeve is entanglement. Entanglement is when two or more qubits become linked in such a way that the state of one qubit is inherently connected to the state of another, regardless of the physical distance between them. This enables quantum computers to perform complex calculations by manipulating multiple qubits simultaneously.

These properties enable quantum computers to perform computations that would be extremely challenging for classical computers. An example would be factoring large numbers into primes, which quantum computers could potentially solve more efficiently than classical computers. Factoring is a bedrock used in some of today's data encryption technologies.

Why should security practitioners care?

While not yet deployed into the mainstream, experts foresee that quantum computing will disrupt security both in the cyber and real worlds.

Quantum computing could in theory solve in an extremely short time the ciphers used in encryption that protects electronic communications and data.

Current technology would take an inordinate amount of time to accomplish developing cryptographic and encryption methods that are safe from attacks utilising quantum computing.

There are fears that quantum computing could be used in hyper-personalised manipulation campaigns or accelerate the development of extremely realistic deepfakes. Disinformation could also be optimised and propagated using quantum algorithms to maximise its impact and escape countermeasures.

On the flip side, quantum computing could usher in an era of extremely secure communications and encryption based on the theories such as Quantum Key Distribution.

Artificial Intelligence is now a key feature of technologies in the physical security sphere. Quantum computing could advance AI by processing vast amounts of data at never seen before speeds, enabling faster and more accurate pattern recognition which can boost anomaly or threat detection at a vast scale.

In conclusion

Quantum computing's potential to revolutionise computing is undeniable. The breakthroughs in so many industries and sciences seem to be finally attainable. However, the same transformative power also brings about significant risks, challenging existing security methods and even society at large. It probably would not be wrong to describe it as walking a tightrope, as we try to balance the advantages against the possible threats presented by quantum computing. But instead of fearing all new technologies, we perhaps should first seek to understand it and how it could be leveraged in our profession of security.

From Panic to Preparedness: How Emergency Communication Systems Ensure Safety and Security in Physical Environments

Article Contributed by:
Rajesh Parsad, CPP, PSP, PCI

Introduction

In today's world, safety and security in physical environments have become paramount concerns. Whether it is in educational institutions, corporate workplaces, public transportation systems, or healthcare facilities, ensuring the well-being of individuals is of utmost importance. Emergency communication systems play a crucial role in achieving preparedness and response capabilities during crisis situations.

Understanding Emergency Communication Systems

Emergency communication systems are tools designed to facilitate effective communication during emergencies. They serve as a vital link between those in need of assistance and the first responders who can address the situation. Over time, these systems have evolved to adapt to the changing landscape of emergencies and advancements in technology. With modern emergency communication systems, organisations can leverage various components and features to ensure timely and accurate dissemination of critical information.

The Need for Preparation

Emergencies can strike at any moment, often with little or no warning. It is essential for organisations to be proactive in their planning and preparedness efforts. This includes establishing and regularly updating emergency response protocols, conducting comprehensive training and drills for personnel, and creating well-defined emergency action plans. By taking these measures, organisations can minimise the impact of emergencies and enhance the effectiveness of their emergency communication systems.

Ensuring Effective Communication

One of the biggest challenges during emergencies is maintaining effective communication amidst chaos and uncertainty. Noise, confusion, and information overload can impede the transmission of important messages. Emergency communication systems provide a solution to overcome these challenges by offering wide area coverage and the ability to disseminate messages to individuals across various locations. Additionally, these systems prioritise messages and allocate communication channels to ensure that critical information reaches the intended recipients promptly.

Components of Effective Emergency Communication Systems

To achieve optimal results, emergency communication systems incorporate several key components. Alerting mechanisms, such as visual and audible alerts, are essential in capturing the attention of individuals in high-stress situations. Clear instructions and concise messages are crucial for ensuring that recipients understand what actions to take. Furthermore, multi-channel delivery options allow for flexibility in reaching individuals through different communication channels. Integration with other safety systems, such as fire detection and alarm systems, and access control systems, enhances the overall effectiveness of emergency communication systems.

The Role of Technology

With the rapid advancement of digital technology, emergency communication systems have embraced various advancements in their functionalities. Integration with mobile devices enables individuals to receive alerts and updates in real-time, regardless of their location. Real-time monitoring and reporting capabilities provide first responders with valuable insights into the situation, allowing for prompt decision-making and response coordination. While technology presents opportunities for enhancing emergency communication systems, organisations must also remain cognizant of potential limitations and ensure proper safeguards are in place.

Emergency Communication Systems in Specific Environments

Different physical environments require tailored approaches to emergency communication systems. In educational institutions, these systems play a vital role in safeguarding students, faculty, and staff. Corporate workplaces benefit from the ability to disseminate critical information to employees across large office complexes. Public transportation systems rely on emergency communication systems to alert passengers of any disruptions or potentially hazardous situations. Healthcare facilities prioritise the seamless communication between medical staff and patients, ensuring swift response during emergencies. Similarly, entertainment venues utilise these systems to manage crowds and address any emergencies that may arise.

Legal and Regulatory Requirements

Implementing emergency communication systems entails adhering to local codes and regulations. Each jurisdiction may have specific requirements that organisations must meet in terms of system capabilities, effective communication range, and redundancy. Compliance with these guidelines is essential to ensure that emergency communication systems fulfil their intended purpose and meet the necessary safety standards established by regulatory bodies.

Case Studies: Successful Implementations

Real-world examples of successful emergency communication system implementations can shed light on their efficacy. One such case study involves a school district that implemented an emergency communication system to enhance safety measures and communication protocols. By integrating the system with their existing safety infrastructure, the district achieved a streamlined response during critical situations. Another example showcases how a business complex utilised an emergency communication system to coordinate disaster response efforts among tenants and personnel, resulting in enhanced preparedness and overall security.

Evaluation and Testing

To maintain the reliability and effectiveness of emergency communication systems, regular evaluations and maintenance are necessary. Periodic testing allows organisations to identify any vulnerabilities or malfunctions in the system and ensure that updates are implemented promptly. By adhering to a robust evaluation and testing schedule, organisations can instil confidence in the functionality and reliability of their emergency communication systems.

Addressing Potential Challenges and Concerns

Implementing emergency communication systems comes with its set of challenges and concerns, including cost considerations and budget planning. Organisations need to allocate sufficient resources to procure and maintain these systems while ensuring scalability and adaptability to their specific environment. Additionally, accessibility and inclusivity must be considered to guarantee that individuals with disabilities can effectively receive and interpret emergency messages. Cybersecurity measures are also of utmost importance to safeguard sensitive information and protect the system against potential threats and breaches.

Training and Education for Effective Emergency Communication

A comprehensive training program for system operators and end-users is critical to effectively utilise emergency communication systems. System operators should receive thorough training on system functionalities, troubleshooting, and emergency response protocols. End-users must be educated on emergency response procedures, including how to interpret and respond to messages delivered through the system. By investing in training and education, organisations can maximise the potential of their emergency communication systems and ensure optimal response during emergencies.

Public Perception and Trust in Emergency Communication Systems

Building public trust in emergency communication systems is essential to ensure their effectiveness. Transparency and reliability play significant roles in developing trust among individuals who rely on these systems in times of crisis. Lessons learned from previous emergencies and the successful utilisation of emergency communication systems are crucial in shaping public perception and establishing trust in their capabilities.

Collaboration and Partnerships

Synergy between emergency communication system providers and end-users is crucial for success. Collaboration with first responders and emergency services can enhance communication and coordination efforts during emergencies. By fostering strong partnerships, organisations can leverage the expertise and experience of these stakeholders to optimise their emergency communication systems and ensure a thorough and effective response.

Future Trends and Innovations

As technology continues to advance, emergency communication systems are likely to be influenced by emerging trends and innovations. Artificial intelligence (AI) and predictive analytics have the potential to enhance the capabilities of these systems, enabling more accurate and timely predictions about potential emergencies. Furthermore, advancements in the integration of the Internet of Things (IoT) can result in accelerated response times and more efficient communication during crises.

Summary

In summary, emergency communication systems are powerful tools that provide a crucial link between individuals in need and the help they require during emergencies. By understanding the purpose, components, and capabilities of these systems, organisations can ensure safety and security in physical environments. With proper planning, training, and implementation, emergency communication systems can significantly enhance preparedness, response capabilities, and, ultimately, save lives.

FAQ

What is the difference between emergency communication systems and traditional communication methods during emergencies?

Emergency communication systems offer broader coverage, priority messaging, and integration with other safety systems, ensuring efficient and accurate dissemination of critical information during emergencies.

How can emergency communication systems be integrated with existing safety systems?

Emergency communication systems can be integrated with fire detection and alarm systems, access control systems, and other safety systems to enhance overall security and response capabilities.

What are the legal requirements for implementing emergency communication systems?

Organisations must comply with local codes and regulations that specify the necessary capabilities, effective communication range, and redundancy requirements for emergency communication systems.

How can organisations ensure the confidentiality and security of emergency communication systems?

Organisations can implement robust cybersecurity measures and protocols to protect sensitive information and protect the system against potential breaches or threats.

Are emergency communication systems able to withstand power outages?

Some emergency communication systems are equipped with backup power options such as battery backups or generators, ensuring continued functionality even during power outages.

Conclusion

Recognizing the significance of safety and security, organisations must invest in robust emergency communication systems. These systems serve as lifelines during emergencies, enabling timely and effective communication that can save lives. By embracing the latest technologies, adhering to legal requirements, and collaborating with stakeholders, organisations can ensure the safety and security of individuals in physical environments, mitigating panic and confusion while supporting efficient response efforts.

Networking Event at ParkRoyal @ Kitchener

Article Contributed by:
Collin Goh

The Singapore Chapter had the pleasure of hosting a networking event at ParkRoyal @ Kitchener. The event was a great success, providing our members with valuable opportunities to connect, share experiences, and foster professional relationships. We truly appreciate all those who attended and contributed to making it a memorable event.

During the event, the Chapter announced some exciting upcoming activities that we believe will greatly benefit our members:

1. Special Interest Group for Intel and Security Ops: This is a special interest group dedicated to Intel and Security Operations. This initiative aims to create a platform where members can gather and exchange relevant experience and expertise. By coming together, we can enhance our knowledge and perspectives, ultimately improving our effectiveness in our respective fields.

2. 2023 ASX ASIS - Outstanding Security Performance Award (OSPA): This prestigious event focusing on "Fostering Regional Partnerships - A Security Perspective" will be held in Bangkok on 9th November 2023. We strongly encourage our members to attend. It's a unique opportunity to engage in insightful exchange with security professionals from across the Asia-Pacific region. Such interactions can broaden our horizons and provide valuable insights into the ever-evolving security landscape.

A Special Thanks to Genetec
We would like to extend our sincere gratitude to Genetec for being the lead sponsor for our Q3 networking event. Genetec, with more than 25 years of experience, started as a modest group of engineers. Their journey began with creating a groundbreaking IP-based video surveillance system called Omnicast.

Omnicast revolutionised the industry by offering scalability, flexibility, and ease of use unmatched by any other system on the market. Genetec's ability to creatively explore various technologies to solve new problems has been a hallmark of its success.

Over the past five years, Genetec's video and access control products have gained recognition as leading solutions in the industry. What sets Genetec apart is their commitment to working closely with their clients. This collaboration has enabled them to develop industry-specific solutions that provide enhanced protection, deeper insights, and optimised operational performance for their clients.

As we progress through the third quarter of 2023, we're excited about the opportunities and initiatives ahead. We look forward to your active participation in our special interest group and your presence at the 2023 ASX ASIS OSPA event in Bangkok.

Once again, our heartfelt thanks to Genetec for their support, and we're eager to see where the rest of the year takes us in our pursuit of excellence in the security industry.

TSX Penang 2023 and Overseas Field Visit

Article Contributed by:
Marie Helene Mansard

I joined ASIS during COVID and Technology Security Conference (TSX) Penang in August 2023 was my first time attending a TSX gathering in real life. In addition to having the opportunity to talk to peers from ASIS Singapore Chapter and ASIS Malaysia Chapter, I have learnt about trends that are and will continue to impact the security domain for the following years.

Craig Foster, from Grab was explaining convergence between Integrated Facilities Management (IFM) and Security. He was helping us to consider security not as a cost to the business but as a business value to the organisation activity. I was interested by their technology and data driven approach, in order to improve the workplace experience services for employees and workplace effectiveness.

Craig was sharing tips about what to take into consideration in IFM outsourcing contracts such as operational excellence, risk mitigation, efficiency and cost control. IFM needs nowadays to be fully integrated with Smart Building and Security.

When outsourcing this, we can get the security operations team focusing more on safe travels and business resilience and other security topics. One approach for Security contracting could be the outcome based model for security services, integrating technology and manpower: IT, data, FM, guarding, cybersecurity, sensors, etc.

Graham Ong-Webb from STE shared about the increasing complexity in Security 3.0 when it comes to detecting, responding and countering threats. Challenges consist of dense population centers, intricate urban architecture and complex infrastructure (physical and digital). Graham was highlighting that criminals WILL breach security lines therefore our role is also

to manage insecurity. He was considering the cost of criminal activity on the global economy, sharing about governments' investments in security and military: 75% of spending is used to counter violence. He explained the concept of Industry 4.0 that will help to digitalise value chains, products and services offering, business models and customer access. He mentioned that Malaysia already started this journey by putting industry forward. He presented how technology can help with the multidimensional approach of Security 4.0 such as Artificial Intelligence (AI) and big data, IOT and sensors, advanced robotics, and of course cybersecurity.

Anthony Lee, CPP, PSP then introduced a maturity model for sustainable security with 4 levels to manage risks better and be more strategic. He took several examples from the transportation industry.

Effie Chen, from BluOcean Security brought us through the major trends she can identify for safety and security domain:

- Cloud and hybrid cloud adoption.
- Integration and conversion when transforming existing systems: data migration, system integration and compliance are growing concerns.
- Mobile access and mobile credentials are increasingly used together with Bluetooth, NFC, biometrics, passwords, and face recognition, from smartphones.
- This goes with growing privacy and transparency concerns, especially when it comes to customers or employees information.
- Cybersecurity has to be carefully managed as hacking options are accessible to people without any cyber background. Security teams could be a target because hacking them will give access to the company's assets.
- Increasing use of AI in video analytics. This includes device analytics on the edge of cameras

Lastly, Jason Teo from Infineon shared about manufacturing facilities going through transformation for more decarbonisation and digitalisation. When facing hybrid threats, an Integrated Security Operations Centre, taking care of both physical and IT security, could be a solution. We ended with recommendations from the panel of speakers to security professionals about staying agile, relevant to the business, dynamic instead of static, embracing new technologies, continuous learning and being proactive.

I also had the opportunity to participate in site visits to the Dell factory and the Boston Scientific factory in Penang. During these visits, I have seen this quote from William Pollard on the wall: "Learning and innovation go hand in hand. The arrogance of success is to think that what you did yesterday will be sufficient for tomorrow".

Seems to me a perfect conclusion for the event!

Field Visit to AETOS 5G Integrated Command Centre

Article Contributed by:
Edison Koh, CPP, PSP, PCI

As part of its commitment to foster continuous growth and innovation, ASIS International (Singapore Chapter) held its second field visit of the year at the AETOS 5G Integrated Command Centre (ICC) on 20 September 2023. The visit was attended by both international and local ASIS members, providing them with the opportunity to glean valuable insights into the ICC's unified capabilities.

Implementing Singapore's largest 3D digital twin, the ICC visualises unified operations island-wide and beyond borders onto a single agnostic platform – Aquila-X. Using an AI alert and response model, the ICC delivers enhanced outcomes in security, safety, facilities management, and sustainability tracking.

The field visit commenced with an introduction of AETOS and its comprehensive range of services presented by Amanda Tan, External Communications Lead of Strategic Communication and Marketing. The attendees then went through a detailed tour and presentation of the ICC, guided by other representatives of AETOS, including Alex Lum, Assistant Vice President of Trust and Safety, Lek Shao Hua, Assistant Vice President of Operations, and Tong Tien Onn, Assistant Manager of Integrated Command Centre.

Calendar of Events

Field Visit to SMRT Depot

The chapter will be organising a field visit to SMRT Depot on 19 October 2023.

Registration is closed.

Q4 Networking Dinner and AGM

Please see the update from the our ASIS Website.

Calendar of Events

Women-in-Security Fireside Chat

Moderator

Ms Marie-Helene Mansard

Women-in-Security
ASIS International
(Singapore Chapter)

Panelists

Dr Jolene Jerard

Executive Director

Centinel

Mr Sumit Ray

Vice President

Dell Technologies

Dr Magda Chelly

Managing Director | CISO

Responsible Cyber Pte. Ltd.

Emcee

Ms Chow Keng Fong

Regional Resiliency Lead

Dell Technologies

Fireside Chat Topic

1. *Overcoming challenges and stereotypes in a male-dominated profession.*
2. *Strategies for nurturing women talent and promoting growth within this profession.*
3. *Insights on navigating career progression in this profession, while maintaining personal well-being.*
4. *The role of women in driving technological advancements and digital transformation through this profession.*
5. *Leveraging networking opportunities and collaborative partnerships to enhance professional growth.*
6. *Promoting diversity and encouraging young women to pursue security professional as a career*

4th October 2023
Wednesday

Time
2:00pm - 5:00pm

Venue
Dell Technologies
Changi Business Park Central 1

Ladies only Event

REGISTER NOW

Scan QR Code
For Registration

Registration Closes on 25 Sep

Organised By:

ASIS INTERNATIONAL® Singapore Chapter

Supporting Organizations

DELL Technologies

Members' Update

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

Ms	Abigail Wong		Mr	Moritz Metzger	
Ms	Ava Gui		Mr	Ong Chia Choong	
Mr	Benjamin Low		Mr	Ong Chin Kai	
Mr	Cheng Chee Siong		Mr	Pang Jing Chyi	CPP
Mr	Darrill Chan		Mr	Sansurash Krishnan Samy	
Ms	Gawon Kim		Mr	Scott R Haylock	
Ms	Ho Ying Ting		Mr	Senthilkumar Deveyan	
Mr	Joshua Jordan		Ms	Serene Gay	
Mr	Kenneth Ong		Mr	Tan Chin Chye	
Mr	Louis Lyu		Ms	Trisha Natanael	
Mr	Low Aik How		Mr	Zulkifli Rahmat	
Mr	Michael Pazarcevic				

Congratulation to Newly Certified Members!

Newly Attained CPP

Mr	Shamus Yeo See Yew	CPP, PSP, PCI

Newly Attained PSP

Mr	Ang Boon Kiat, Peter	CPP, PSP	Mr	Dex Yuen Kin Wai	CPP, PSP

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	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
Mr	Lee Choon-Wai Anthony	CPP, PSP			

Certified CPP members

Mr	Abdul Redha Bin Abdullah	CPP	Mr	Den Ho Kai-Quan	CPP
Mr	Alfian Idris	CPP	Mr	Desmond Ho Kok Tong	CPP
Mr	Andrew Fan Tuck-Chee	CPP	Mr	Dicky Fadly Zaini	CPP
Mr	Anton Chan	CPP	Mr	Edmund Lam	CPP
Mr	Azharie B Mohamed Mudakir	CPP	Mr	Edwin Goh	CPP
Mr	Azril Ngasiran	CPP	Mr	Fabrice Marty	CPP
Mr	Balasubramaniam Selvam	CPP	Mr	Firman Latib	CPP
Ms	Beverly F Roach	CPP	Ms	Foong Yi Ling	CPP
Ms	Cheng Yen Hwa	CPP	Mr	Gan Da	CPP
Mr	Chia Wai Mun	CPP	Mr	Glen Martin Balde Arquiza	CPP
Mr	Ching Chiu Chiu	CPP	Mr	Glenn Koh	CPP
Mr	Clement Chan	CPP	Mr	Hartmut Kraft	CPP
Mr	Damien Lim	CPP	Mr	Ho Jiann Liang	CPP
Mr	Daniel Ng	CPP	Mr	Isaach Choong	CPP

Members' Update

Certified ASIS International Members

Certified CPP members

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

Members' Update

Certified ASIS International Members

Certified PSP members

Mr	Dion Yeo Lai Ye	PSP	Mr	Low Kay Boon	PSP
Mr	Jeffrey Lam Boon Kee	PSP	Mr	Mayank Sinha	PSP
Mr	Kamlesh Gope Ramchand	PSP	Mr	Soh Wei Jye	PSP
Mr	Kevin Loh	PSP	Mr	Stanley, Tse Chi-Fung	PSP
Mr	Lee Huan Chiang	PSP	Mr	Wee Ting-Jin	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

Collin Goh
Contributor

Edison Koh, CPP, PSP, PCI
Contributor

Marie Helene Mansard
Contributor

Daniel Chan, APP
Contributor

Rajesh Parsad, CPP, PSP, PCI
Contributor

Yeh Ing Kerne, 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
Submission close on 1 Dec 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 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