

News & Update

- Knowledge Series
- CAAP
- SVRP
- AiSP Cyber Wellness
- Ladies in Cyber
- Special Interest Groups
- CREST Singapore
- The Cybersecurity Awards
- IOT Innovation Day
- Upcoming Events

Contributed Contents

- Success in the Cloud:
Three Common sense
Principles Data
- IBM
- How To Defend Against
Hackers: Three Cyber
Intelligence Viewpoints
- The Cybersecurity Awards
2021 Winner – Ms
Shamane Tan

Professional Development

Membership

NEWS & UPDATE

New Partners

AiSP would like to welcome Beyond Trust, Blackpanda, and Singtel as our new Corporate Partner. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem.



Continued Collaboration

AiSP would like to thank Acronis and Netwitness (an RSA Business) for their continued support in developing the cybersecurity landscape:



14th Annual General Meeting

AiSP held its 14th Annual General Meeting on 30 March at Lifelong Learning Institute. Mr Johnny Kho AiSP President reported on the following to AiSP members who attended the meeting

AiSP held its 14th Annual General Meeting on 30 March at Lifelong Learning Institute. Mr Johnny Kho AiSP President reported on the following key highlights to AiSP members who attended the meeting

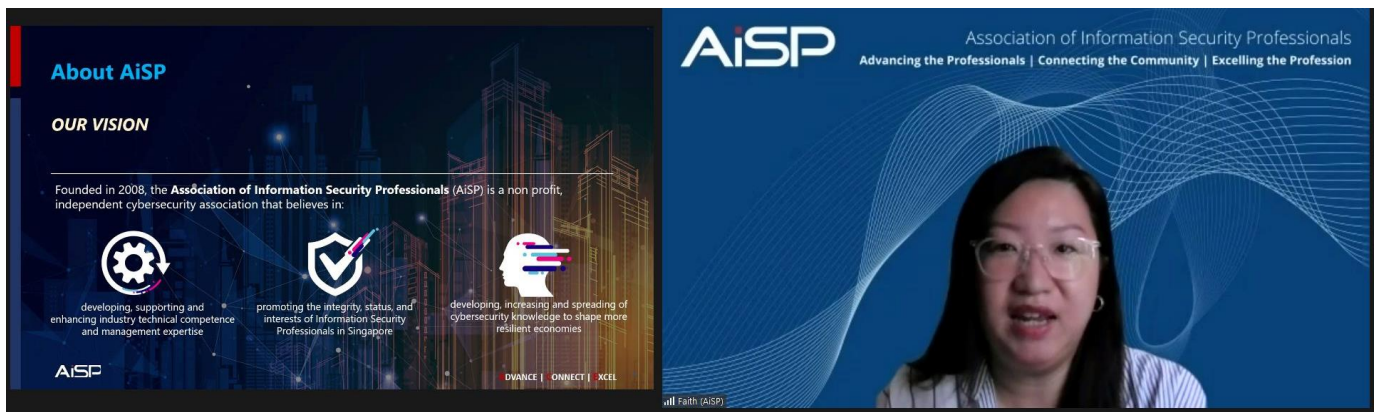
- 1) Growth in Membership and Partnership through Secretariat outreach
 - a. There are 11 APP, 43 CPP and 1724 members to date.
- 2) Inaugural fellowship in recognition of our long-time contributing volunteers
 - a. AiSP has launched its AiSP Fellowship with Mr Alex Lim, Mr Cecil Su and Mr Freddy Tan as first batch of fellows conferred during the meeting.
- 3) Achieving the next milestone in Regionalization
 - a. Forming of the Southeast Asia Cybersecurity Consortium (SEACC) is in progress and AiSP has been actively reaching out to the ASEAN countries and AiSP will be working closely with our ASEAN partners to actualize this initiative.
- 4) Keeping the momentum with new Committee Members
 - a. Welcoming Tony Low and Andrew Ong to the Elected Executive Committee 2022




Knowledge Series Events

Cryptography on 31 Mar 22

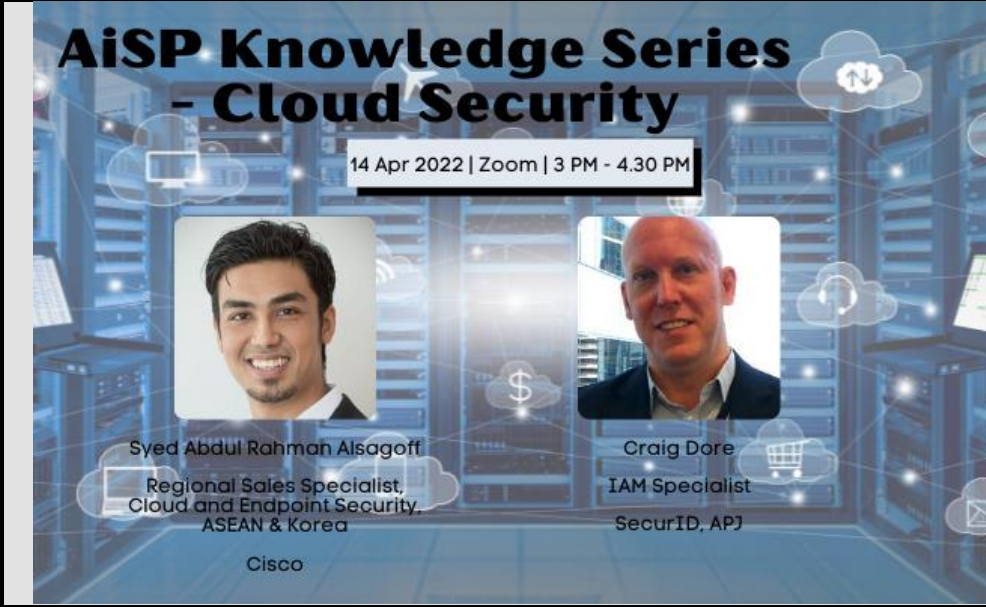
As part of Digital for Life movement, we hope to help Singaporeans of all ages and walks of life to embrace digital learning as a lifelong pursuit. Today, we had our knowledge series focusing on Cryptography. We would like to thank our Corporate Partners, Mastercard and Responsible Cyber Pte. Ltd for sharing insights on Cryptography.




Cloud Security on 14 April




AiSP Knowledge Series – Cloud Security









ORGANISED BY:



SUPPORTED BY:

IN SUPPORT OF:



[back to top](#)

In this Knowledge Series, we are excited to have Cisco and SecurID, an RSA Business to share with us insights on Cloud Security. Based off Information Security Body of Knowledge (BOK) 2.0 content topics, AiSP has been organising a series of knowledge-sharing & networking events to enable our members with a better understanding of how IS-BOK can be implemented at workplaces.

Evolving Security Strategy for a New World

By: Syed Abdul Rahman Alsagoff, Regional Sales Specialist, Cloud and Endpoint Security, ASEAN & Korea, Cisco

Just as how the pandemic has forever changed the way we work and conduct business, the methods and thinking of how we protect our digital assets need to evolve and change as well. Now more than ever, enterprises need to protect their workforce with security that is scalable and effective but yet simple and adaptive enough to manage. Key concepts like Zero Trust Network Access, SASE, Cloud and As A Service were developed by the industry as an attempt to achieve just that. But where and how do you really start?

In this session, we will look back into the threats that were most prevalent in 2021 and look forward into what Enterprises are investing in a drive to real outcomes organisations need as they accelerate digital transformation in a post-Covid era.

Top Myths About Zero Trust

By: Craig Dore, IAM Specialist for SecurID, APJ

Join the session with our IAM Specialist in APJ on his views around the Top Myths on Zero Trust. Many global security leaders have and are still looking to adopt a Zero Trust model to help reduce cyber breaches in their organisations. For this to be implemented effectively, we need to discuss the misconceptions of Zero Trust.

Date: 13th April 2022 (Wed)

Time: 3PM – 4.30PM

Venue: Zoom

Registration:

https://zoom.us/webinar/register/3216450910823/WN_JpANjQrMTAqIsl3V70astQ

IS Governance on 28 April



AiSP Knowledge Series – IS Governance

AiSP Knowledge Series - IS Governance

28 Apr | MS Teams | 3PM - 4.30PM

Suresh Menon
Sr. Technical Specialist
Cloud-Security & Compliance
Microsoft Singapore



Organised by



Supported by



In support of



In this Knowledge Series, we are excited to have Microsoft to share with us insights on IS Governance. Based off Information Security Body of Knowledge (BOK) 2.0 content topics, AiSP has been organising a series of knowledge-sharing & networking events to enable our members with a better understanding of how IS-BOK can be implemented at workplaces.

Fasttrack your Compliance Journey

Speaker: Suresh Menon, Sr. Technical Specialist Cloud-Security & Compliance, Microsoft Singapore

Data breaches are becoming more common than ever before. Yet, nearly 51% of organizations are still unprepared to deal with a data breach.¹ And as your data continues to grow exponentially, so will your risk of breaches and compliance violations.

Afterall, today's employees are often using multiple devices, apps and locations to store and access business-sensitive data. What's more, it can be challenging to keep up with regulatory demands when you're faced with an average of 220 daily updates from global regulatory agencies. The good news is, staying compliant and secure is simpler with the right technologies.

In this webinar, learn how you can reduce risk without compromising productivity by using:

- Machine learning and automation to reduce manual data management tasks
- Microsoft Information Protection to safeguard sensitive data across clouds, apps and endpoints
- Microsoft 365 Compliance to keep up with everchanging privacy regulations, data growth and insider risks

The key to building a more secure and profitable business begins with the way you manage your data. Register now to get started.

Date: 28th April 2022 (Thu)
Time: 3PM – 4.30PM
Venue: MS Teams
Registration: <https://forms.office.com/r/EtSn0UFibu>

About our Knowledge Series

As part of knowledge sharing, AiSP is organising regular knowledge series webinars based on its **[Information Security Body of Knowledge 2.0](#)** topics. Our scheduled topics for webinars in 2022 are as follows (*may be subjected to changes*),

1. Cloud Security, 13 Apr 22
2. IS Governance, 28 Apr 22
3. Identity & Access Management, 18 May 22

Please let us know if your organisation is keen to be our sponsoring speakers in 2022!

AiSP members who registered for the event, can playback the recorded event via their member profile in Glue Up. If you did not sign up for the event, please email secretariat@aisp.sg for assistance. Please refer to our scheduled 2022 webinars in our [event calendar](#).

Cybersecurity Awareness & Advisory Programme (CAAP)

CISCO & SCCC I CAAP Event on 10 March

Thank you for joining us on 10 March for the AiSP x SCCC I event. We hoped you have gained a lot of insights from the sharing by Ms Wendy Ng, AiSP EXCO member. Thank you CISCO for supporting the event too.

Strategic Thrusts, that anchor our vision

Upcoming CAAP Event

AiSP hope to elevate Cyber Security Awareness as integral part of SME Business Owner Fundamentals and Establish a Self-Sustainable Support Ecosystem programme with active participation from Agencies, Business Associations, Security Communities and Vendors.

Anti-Ransomware Day 2022

On this Anti-Ransomware Day, it is a timely reminder for organisations to review their existing cybersecurity architecture to mitigate against modern day threat attacks. As an advocate partner with Cyber Security Agency of Singapore (CSA) SG Cybersafe Partnership Programme, Fortinet together with our industry partners will share more about the ransomware attack trends and the importance of practicing good cyber hygiene to strengthen your cybersecurity posture.




Supported by:

Ransomware Protection, everywhere you need it.

Protect the possibilities with Fortinet Security Fabric.

Click [here](#) to register.

AiSP Cybersecurity Awareness E-Learning

	
<h3>AiSP Cybersecurity Awareness E-Learning</h3>	
<p>On 7 January 2022, the Association of Information Security Professionals (AiSP) launched the Cybersecurity Awareness E-Learning. It was launched by Ms Gwenda Fong, Assistant Chief Executive (Policy & Corporate Development) of Cyber Security Agency of Singapore.</p> <p>In this E-Learning, we will bring you through a set of materials that will prepare your Business and your employees to embark on an exciting journey in digital transformation and start your Business to be more secure.</p> <p>We will be covering:</p> <ol style="list-style-type: none"> 1. Providing businesses with an understanding of the current digital business landscape 2. Deep dive into understanding the Digital better Transformation Journey 3. Risk and threats for the Business to understand some of the most crucial aspects and assessments. 4. How you can start to explore and secure your Business by handling data securely and setting up your initial cybersecurity framework 5. Providing an understanding of your Business Obligations and the various regulations that will impact your process and impact the Business. Sharing of different policies and guidelines such as PDPA, Cybersecurity Act, Computer Misuse Act 6. Your responsibility to ensure in the event of an incident, how the enterprise should handle 	 <p style="text-align: center;">AiSP Cybersecurity Awareness E-Learning</p> 
<p>Why Should You Take This E-Learning & How Will It Help You?</p> <p>Through this E-learning, we prepare your business and your employees to kickstart your journey in digital transformation and be more cyber safe. With the various contents provided in the E-Learning</p>	

which will be update consistently, you have be able to have a better understanding on the digital business landscape and how to set up your initial cybersecurity framework.

An e-certificate will be given once you have completed the core modules for the e-learning and passed the quiz.

Why Is this E-Learning Special?

AiSP works very closely with our partners to produce contents that are up to date and relevant from you and your business. The content will be updated consistently to ensure our subscribers have at least **1 new** content updated in the platform.

Subscription Plan

Individual	Bundle (Min. 5 pax) [#]
\$7.90/month (Before GST)	\$6.00/pax/month (Before GST) [*]

^{*}Minimum 1 year subscription

[#]Please submit subscribers' Name, Organisation & Designation, Contact Email and Contact Number separately in Excel format.

Please contact AiSP Secretariat at secretariat@aisp.sg to sign up for the E-Learning or if you have any queries.

Payment Details

Bank	:	DBS Bank 12 Marina Boulevard DBS Asia Central @ Marina Bay Financial Centre Tower 3 Singapore 018982
Bank Code	:	7171
Branch Code	:	012
Account Name	:	AISP (GLOBAL) PTE LTD
Account No	:	072-033821-9

SME Cybersafe provides



Enhanced Security
Awareness & Training



Cohesive Security
Knowledge Resources




Security Solutions &
Services Support


Click [here](#) to find out more about the E-Learning.

Student Volunteer Recognition Programme (SVRP)

SVRP Nomination has officially concluded, and results have been released on our website [here](#). Our student volunteer drive is ongoing till Dec 2022 for those who are interested to volunteer but not sure where to start. Please click [here](#) to apply today. Nomination period is from 1 Aug 2021 to 31 Jul 2022.




Nomination Period:
1 Aug 2021 to 31 Jul 2022



Nomination Period:
1 Aug 2021 to 31 Jul 2022

CALL FOR NOMINATION! STUDENT VOLUNTEER RECOGNITION PROGRAMME


Tier	Requirements
Bronze	Completion of one of three pillars or complete three of three pillars with minimum 50% attained hrs. + Skills: 30 Hours or more + Events: 60 Hours or more + Leadership: 30 Hours or more
Silver	Completion of two of three pillars + Skills: 30 Hours or more + Events: 60 Hours or more + Leadership: 30 Hours or more
Gold	Completion of all three pillars + Skills: 45 Hours or more + Events: 60 Hours or more + Leadership: 45 Hours or more



Scan the QR Code for the Nomination Form

The SVRP for the secondary school and pre-university students is on merit basis and evaluation would be slightly different as cyber security is not offered as a subject nor co-curricular activities (CCA) in most schools in Singapore at the moment. The students would be given Certificate of Merit when they achieved the following (see A, B, C or D):

<p>Example A</p> + Leadership: 10 Hours + Skill: 10 Hours + Outreach: 10 Hours	<p>Example C</p> + Leadership: 0 Hour + Skill: 50 Hours + Outreach: 0 Hour
<p>Example B</p> + Leadership: 0 Hour + Skill: 20 Hours + Outreach: 20 Hours	<p>Example D</p> + Leadership: 0 Hour + Skill: 0 Hour + Outreach: 60 Hours



Scan the QR Code for the Nomination Form

The SVRP comprises three broad pillars where IHL students can volunteer:

- + Skills-based: Eg. Conduct cybersecurity workshops or develop related software
- + Events-based: Eg. Provide support at technology or cyber-related events
- + Leadership: Eg. Mentoring younger students and managing teams or projects

The track for Secondary School and Pre-University students comprises three broad pillars where they can volunteer:

- + Leadership refers to how the volunteer leads a team to complete the voluntary activity.
- + Skill refers to how the volunteer applies his/her cybersecurity knowledge to others
- + Outreach refers to how the volunteer is involved in outreach efforts (social media, events) to increase cybersecurity awareness for the public.

Visit www.aisp.sg/svrp.html for more details

Visit www.aisp.sg/svrp.html for more details

AiSP Cyber Wellness Programme

Organised by:



Supported by:



In Support of:



The AiSP Cyber Wellness Programme aims to educate citizens, especially reaching out to the youths and elderly on the importance of Cybersecurity and learn how to stay safe online. There has been an increase in cyber threats, online scams and COVID-19 related phishing activities. With reduced Face-to-Face engagements, the elderly and those with special needs have become more vulnerable to cyber threats. We will reach out to different community groups to raise awareness on the topic of cyber wellness and cybersecurity and participants can pick up cyber knowledge through interactive learning. It is supported by the Digital for Life Fund, an initiative by the Infocomm Media Development Authority (IMDA), that supports digital inclusion projects and activities to help all Singaporeans embrace digital, to enrich lives."

Join us in our monthly knowledge series to learn and pick up tips on Cybersecurity. Visit our website (<https://www.aisp.sg/aispcyberwellness>) to get updates on the latest Cyber tips, Cyber news, activities, quiz and game happenings related to Cyber. Scan the QR Code to find out more.



Scan here for some tips on how to stay safe online and protect yourself from scams



Hear what some of our Professionals have to share. Scan here on Cyber - Use, Identity, Relationship, Citizenship & Ethics.



Have the knowledge and think you are safe? Challenge yourself and participate in our monthly quiz and stand to win attractive prizes. Scan now to take part.



Scan here if you are looking for activities / events to participate in for knowledge exchange / networking / get to know more people / stay protected & helping others.



Want to know more about Information Security? Scan here for some career advice on Information Security.



To find out more about the Digital for Life movement and how you can contribute, scan here.

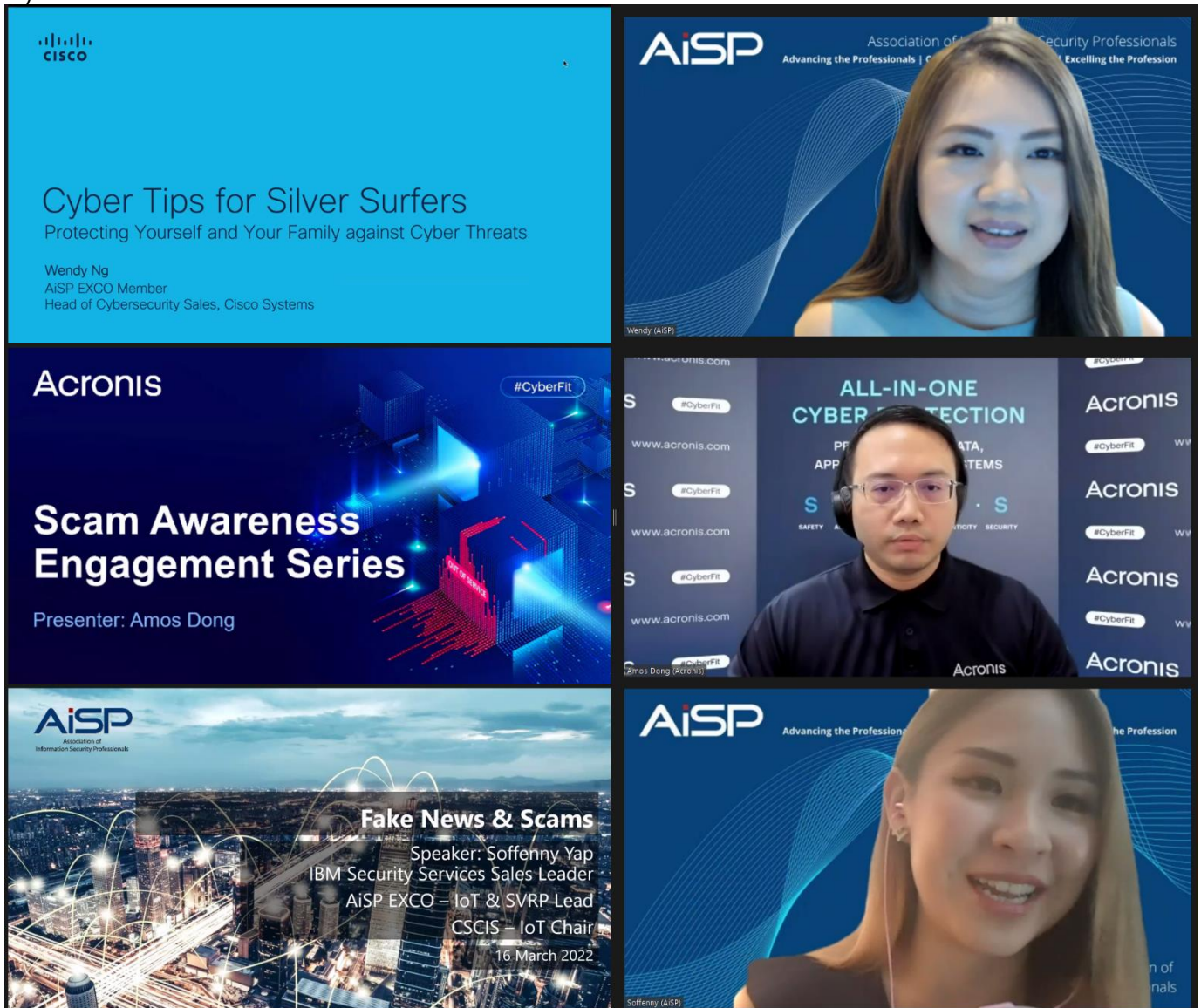
Contact AiSP Secretariat at secretariat@aisp.sg to find out more on how you can be involved or if you have any queries.

Click [here](#) to find out more!

Scam Awareness Engagement Series

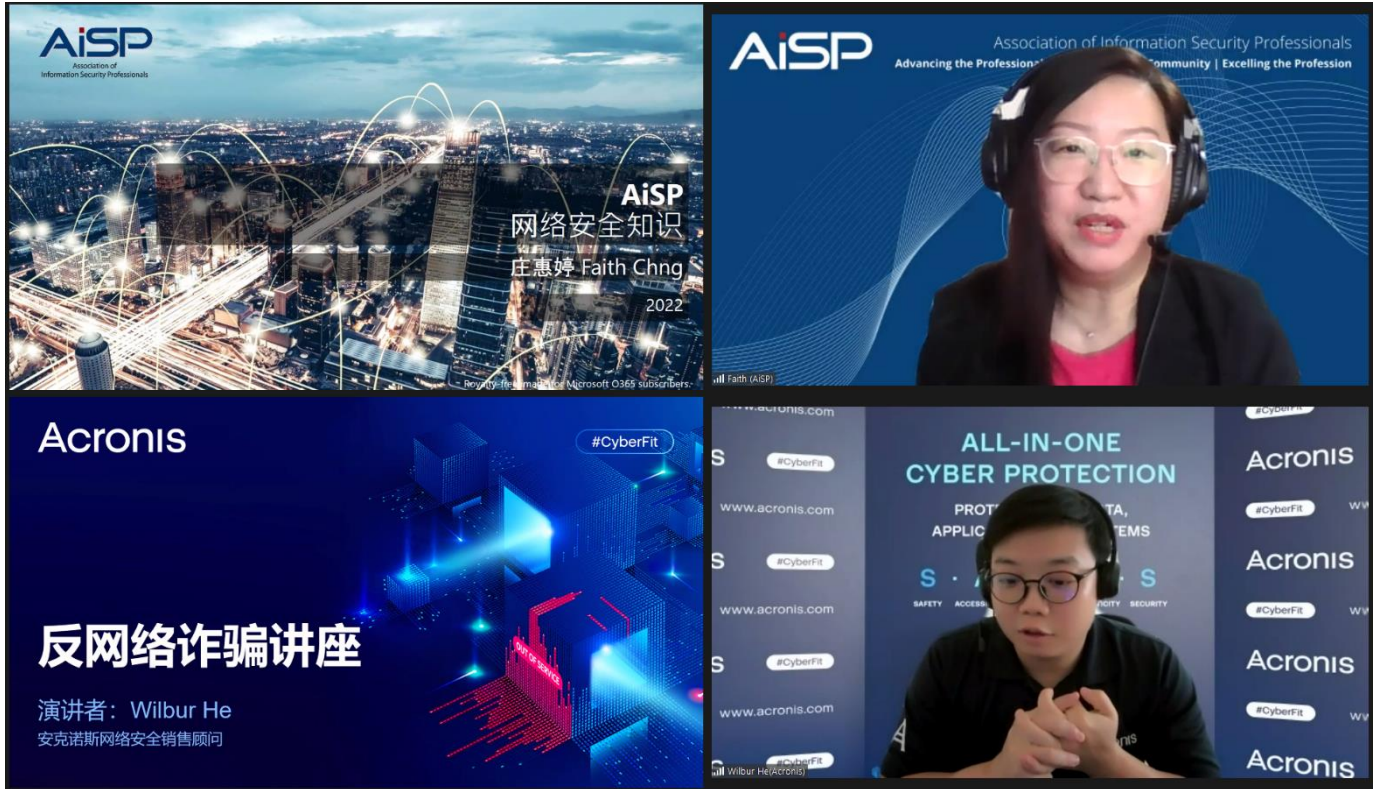
16 March (English)

It was an insightful session on 16 March afternoon for the Scam Awareness Engagement Series (English) with our awesome speakers, Soffenny Yap (AiSP EXCO Member), Wendy Ng (AiSP EXCO Member) and Amos Dong from Acronis. We hoped you have gained insights on how to mitigate scams and how to protect yourself and your family against cyber threats.



17 March (Mandarin)

Scam Awareness Engagement Series was conducted successfully in Mandarin as well on 17 March with Ms Faith Chng (AiSP EXCO Member) and Mr Wilbur He from Acronis. They shared on cybersecurity knowledge in Mandarin for the benefit of our mandarin speaking participants. We hoped they have gained a deeper understanding of cybersecurity and the prevention of digital scams.



Sharing on Scam Awareness to Yio Chu Kang Residents on 19 March

On 19 March, AiSP EXCO Member, Faith Chng and Huawei Singapore Head of Marketing & Strategy, Norman Kuo did a sharing on Scam Awareness to over 70 Yio Chu Kang Residents. It was an enjoyable session with the senior citizens as they asked many questions during the event. AiSP would like to thank Mr Yip Hon Weng 叶汉荣 for gracing the event and the following partners for supporting the event: Acronis, Huawei Singapore, Trustwave & UOB.





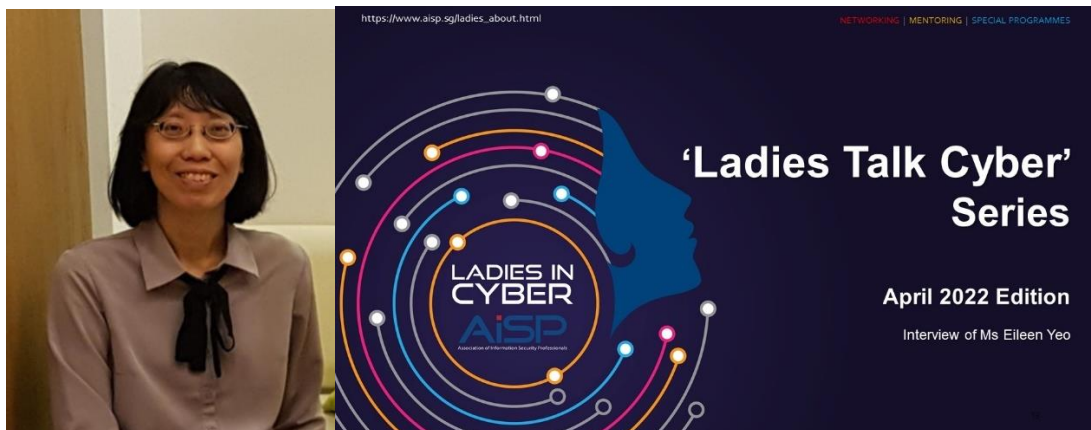
Sharing on Scam Awareness at Tampines East CC on 19 March

The journey did not end as on the same day, AiSP EXCO Member, Faith Chng did a sharing on Scam Awareness to over 40 Tampines East Residents who comprise of mostly senior citizens (in Mandarin) on the importance of cybersecurity and equip them with basic cybersecurity knowledge.





Ladies in Cybersecurity



Ladies Talk Cyber Series

For the Eleventh edition of AiSP's 'Ladies Talk Cyber' series, we interviewed Ms Eileen Yeo, Senior Lecturer in the School of Computing, Singapore Polytechnic. She is currently teaching cybersecurity modules to the students of the Diploma in Infocomm Security Management in Singapore Polytechnic and is constantly inspired by the enthusiasm of her students.

How to be successful in cybersecurity field

In celebration of [SG Women year](#), AiSP's secretariat decided it was timely to launch a series of interviews of female leaders across industries who fulfil high impact roles, and learn about their journeys, experiences and insights. The initiative aims to shed some light on what it takes to make it in this field. The interviews can be source of invaluable career insights as well as opportunities

for those in the field to get a deeper understanding of the industry, and how its leaders are innovating to disrupt the cyber landscape.

Introducing women with a deep interest in cybersecurity

Eileen is a Senior Lecturer in the School of Computing, Singapore Polytechnic. She is currently teaching cybersecurity modules to the students of the Diploma in Infocomm Security Management in Singapore Polytechnic, and is constantly inspired by the enthusiasm of her students.

Please click [here](#) to view the full details of the interview.



AiSP International Women Day Celebrations – 08 March 2022

Gender diversity benefits most industries, and it's especially important in the cybersecurity sector. To encourage more women to join this field, and in celebration of The International Women's Day 2022, AiSP's Ladies in Cyber Charter organised the AiSP's Ladies in Cyber Fireside chat. We would like to thank the event's moderator and the founder of Ladies in Cyber Charter, Sherin Y Lee, along with our panellists Yeo Wan Ling, Veronica Tan, Jessie Chong & Tham Mei Leng for sharing their time and expertise with us. We would also like to thank Trend Micro for hosting us in their beautiful office and be part of the celebration with us.



AiSP Ladies in Cyber Inaugural Symposium – 22 March 2022

AiSP Ladies in Cyber Symposium was launched on 22 March with more than 150 female tertiary students and young cybersecurity professionals joining physical and virtually online. Mrs Josephine Teo, Minister for Communications and Information and Minister-in-Charge of Smart Nation and Cybersecurity, was the Guest-of-Honour for the event. We would like to thank all panellists Ms Tammie Tham, Co-Chair of the AiSP Advisory Council & Group CEO of Ensign InfoSecurity, and Ms Teo Yi Ling, Senior Fellow, Centre of Excellence for National Security, S Rajaratnam School of International Studies at Nanyang Technological University for taking their time off to join us for the symposium.

This was AiSP's inaugural Ladies in Cyber Symposium, bringing together a stellar lineup of female leaders in their respective cyber and technology fields. It featured a panel session and breakout sessions with subject matter experts in IoT, AI and cybersecurity operations. Attendees got a chance to network and learn from these industry mentors, gaining for themselves valuable insights into the real world of the cyber and tech industry. We would like to thank Acronis, Checkmarx, CISCO, Cyber Youth Singapore, DBS, Fortinet, Huawei, IBM, Mastercard, Responsible Cyber, Singtel, ST Engineering, Tanium, and TrendMicro for sponsoring the event.

The Symposium is supported by partners from the government, industry and community such as, the Government Technology Agency of Singapore (GovTech), Ensign and Cyber Youth Singapore (CYS). It is part of the Cyber Security Agency of Singapore (CSA)'s SG Cyber Women X Series. The event is also organised as part of AiSP Cyber Wellness Programme which is supported under the Digital for Life (DfL) movement and Fund. Through the DfL movement, like-minded partners across private, public and people

[back to top](#)

sectors work together to help Singaporeans embrace digital as a lifelong pursuit, so as to enrich their lives and build a safe and inclusive digital society for all.



JOINTLY ORGANISED BY



AS PART OF



SG CYBER WOMEN X SERIES

SUPPORTED BY



IN SUPPORT OF



SPONSORS



Special Interest Groups

AiSP has set up four **Special Interest Groups (SIGs)** for active AiSP members to advance their knowledge and contribute to the ecosystem are:

- Cloud Security
- Data and Privacy
- Cyber Threat Intelligence
- IoT

We would like to invite AiSP members to join our **Special Interest Groups** as there are exciting activities and projects where our members can deepen their knowledge together. If you are keen to be part of a SIG, please contact secretariat@aisp.sg



AiSP x Recorded Future Capture The Flag Session on 25 March

On 25 March, AiSP and Recorded Future co-hosted the Capture the Flag (CTF) session at Marriott Tang Plaza Hotel. AiSP would like to thank the panellists who had a discussion on the rapidly evolving and intertwined geo-political and cyber threat landscape and how organisations are using threat intelligence to enable themselves to become proactive with a variety of security risks.

Congratulations to all the winners who have won the CTF competition!



The Cybersecurity Awards



The Cybersecurity Awards has three (3) award categories: Professionals, Enterprises and Students -a total of eight (8) awards:

Professionals

1. Hall of Fame
2. Leader
3. Professional

Students

4. Students

Enterprises

5. MNC (Vendor)
6. MNC (End User)
7. SME (Vendor)
8. SME (End User)

Please email us (secretariat@aisp.sg) if your organisation would like to be our sponsors! Limited sponsorship packages are available.

Nominations details will be announced shortly.

THE CYBERSECURITY 2022 Awards

Organised by



Supported by



Supporting Associations



Community Partner



Supporting Organisation



Platinum Sponsors



Gold Sponsors



Silver Sponsors



IOT Innovation Day

The AiSP IoT Innovation Day & Exhibition is the can't-miss event of the year as professionals come together for a day of sharing on Smart City, Driverless Transportation and Health Technology Ecosystem connect for the education, innovation, and collaboration they need to reimagine as part of innovation and smart nation for everyone, everywhere. This event which will be held on 11 May 2022 is targeting at professionals from CIOs and senior executives to providers and payers to IT consultants and entrepreneurs to join in and attend this influential to get the information and solutions they need to reimagine on a Smart City for everyone, everywhere.

Sponsors:

CISCO, ExtraHop, Elastic, Recorded Future and SecureCraft



**AiSP IoT
Innovation Day**
11 May 2022 | 10AM - 3.30PM
Suntec Convention Centre

Reimagining a Smart City
for everyone, everywhere

Organised by:
AiSP
Association of
Information Security Professionals

Register Now!

Click [here](#) to register

Upcoming Activities/Events

Ongoing Activities

Date	Event	Organiser
Jan – Dec	Call for Female Mentors (Ladies in Cyber)	AiSP
Jan – Dec	Call for Volunteers (AiSP Members, Student Volunteers)	AiSP

Upcoming Events

Date	Event	Organiser
1 Apr	AiSP x Huawei CAAP Roundtable	AiSP & Partner
1 Apr	Thrivex Cybersecurity Webinar	Partner
7 Apr	Fortinet OT Summit	Partner
12 to 13 Apr	SMG's Virtual Cybersecurity Summit South East Asia-2022	Partner
13 Apr	Knowledge Series – Cloud Security	AiSP & Partner
19 to 20 Apr	Cloud Security Summit APAC 2022	Partner
26 to 27 Apr	Cyber Security for Critical Assets APAC Summit	Partner
26 to 27 Apr	Cyber Security for Financial Services Asia Part II	Partner
28 Apr	Knowledge Series- IS Governance	AiSP & Partner
29 Apr	CTI SIG Event	AiSP

***Please note events may be postponed or cancelled due to unforeseen circumstances.*

CONTRIBUTED CONTENTS

Article from Cloud Security SIG

Success in the Cloud: Three Common sense Principles

Three commonsense principles to guide cloud strategy and decision-making help ensure an organization's success—even in times of rapid, dramatic change. With unprecedented challenges disrupting organizations' cloud strategies—and with the race to the cloud continuing to accelerate—three commonsense principles can help businesses stay on track: seeing cloud as an enabler; expecting the unexpected and adapting; accordingly and relying on vendors who are eager to partner to deliver exactly what's needed.

Over the past couple of years, the pace of cloud adoption has [accelerated](#). For some organizations, moving to the cloud during this time has been out of an obvious necessity to enable remote work in the pandemic. Those that were already planning a “someday” cloud presence also likely had to push up the timing of cloud rollouts. Organizations operating in the cloud long before early 2020 benefited from having the

[back to top](#)

technology in place—but had to quickly rethink strategy. Could the cloud help them solve some of the dilemmas posed by new operating models, like no longer being able to conduct all business face to face?

These scenarios remind us that the cloud is perhaps best thought of not as a goal, but as a journey. There will always be those at the very beginning of that journey, who are considering whether operating in the cloud is something they can or should do—as well as those much further down the path, who are seasoned SaaS veterans. But no matter where your organization may be on the continuum of [cloud maturity](#), an event like the pandemic can lead you to question everything about your cloud strategy: why you're doing what you're doing, whether you're on the right path, what to do next.

1. At a recent [event](#), Chief Product Officer Jim Taylor discussed how to think through, set and adapt an organization's cloud strategy. He outlined three commonsense principles that—no matter where you are on your journey—can guide your thinking and decision-making and ensure that you're headed in the right direction:

Remember it's not about the cloud. It's about what the cloud enables.

For all its power to simplify operations and reduce costs, cloud computing isn't about those benefits per se; it's about what simpler operations, lower costs and other lifts enable organizations to accomplish. The cloud helps you pursue whatever it is you want to pursue and achieve what you set out to achieve—whether that's empowering a productive, agile workforce, for example, or growing a flexible global supply chain—and do it in more effective, efficient ways. When your decisions about cloud operations are informed by that reality, you'll stay on track even when circumstances—a pandemic, a meteorite, an invasion from Mars—threaten to throw you off.

2. Expect the unexpected and be prepared to adapt. The cloud is there to help.

As you think about how the cloud can enable your organization to achieve its goals, know that those goals will constantly change. The changes may be forced by external events (see #1, above) or driven by internal initiatives—or both, as is the case when the former impacts the latter. (In the pandemic, for example, carefully planned strategic cloud initiatives to simplify and drive down the cost of infrastructure gave way to the tactical need to stand up entire remote workforces fast.) No matter how much or how suddenly you need to [adapt](#), or whether you need to re-prioritize certain steps, the constant should be that the cloud continues enabling you to do it quickly, cost-efficiently and at the right scale.

3. Find a vendor who wants to partner with you to deliver exactly what you need in the cloud.

This may sound obvious, but it's never a good idea to invest in technology with the intention of figuring out how to apply it to your particular situation as you go along. Yet that's exactly what happens in the cloud when your vendor does not have a clear and specific understanding of the business issues you're trying to address or the problems

you're trying to solve in the cloud. Make it a priority to identify and work with a vendor who wants to be a true partner—learning your business, understanding your strategic direction and building solutions to meet your specific needs. A strong vendor relationship based on these goals can benefit both parties for years. After all, your first trip to the cloud won't be your last—just like your first car won't be your last. As your needs change and the technology advances, make sure you have someone working alongside you who will help you get the most from the cloud throughout your organization's journey.

For more information, please visit <https://securid.com/en-us/solutions/cloud/>

About SecurID

SecurID, an RSA business, is the trusted identity platform for 13,000 organizations around the world, managing 50 million identities and providing secure, convenient access to 30 million users. SecurID empowers organizations to thrive in a digital world, with complete capabilities for modern authentication, lifecycle management and identity governance. Whether in the cloud or on-premises, SecurID connects people with the digital resources they depend on everywhere they live, work and play. For more information, go to [SecurID Identity and Access Management](#)

Article from our CPP Partner, IBM



IBM Security X-Force Threat Intelligence Index

Each year, IBM Security X-Force – IBM's in-house team of cybersecurity experts and remediators – mines billions of data points to expose today's most urgent security statistics and trends.

This year's IBM Security X-Force Threat Intelligence Index presents an uncomfortable truth: as businesses, institutions and governments continue to adapt to a fast-changing global market – including hybrid and cloud-based work environments – threat actors remain adept at exploiting such shifts.



Scan to read
the full report

Article from our CPP, Cyfirma

How To Defend Against Hackers: Three Cyber Intelligence Viewpoints

By Kumar Ritesh
Founder and CEO
CYFIRMA

Imagine you are in a boxing ring. Your opponent is masked and in a fighting stance. You have been training for this day. The boxer throws a punch, aiming for your jaw, and then a jab, and then another and another. Then, when you raise your hand to a high guard, the boxer suddenly executes an uppercut — this time straight into your belly.

In many ways, cyber defense is similar to boxing. You gauge the risk, anticipate the attack, decide how you'd defend and try to outsmart the hackers. What if you have a special technique where you can hear the hacker's thoughts, smell his or her fear and predict the next move? You'd likely emerge the winner.

Cyber intelligence would help you do just that — you receive signals on an impending breach with insights on questions like: Who are the hackers? Why are you on their target list? What is their motive? When do they plan to strike? How will they do it?

With those answers, you can have clarity on your external threat landscape, and you can adjust your defense strategies to counter the unseen enemy. To do so, you need to blend cyber intelligence into cyber strategy, policy, security operations and people development.

You can accomplish this goal by analyzing intel across three lenses: strategic, management and tactical.

Strategic Cyber Intelligence

Strategic Cyber Intelligence should answer a key question: Do you have the right information and insights to provide to the senior leadership to help them evaluate cyber risk?

Strategic intelligence seeks to understand who the adversaries are, their motive, intention and potential impact.

Here are a few things you can expect from strategic cyber intelligence:

- A deep understanding of emerging external threats and their impact on business continuity.

- The cybersecurity risk spectrum the organization is currently operating in (for example, critical, high, medium, low).
- Awareness of key assets and prioritizing their value to the organization.
- Ability to identify confidentiality, integrity and availability risks on your data and systems.
- Legal liability in case the risk materializes.

And here are a few tips about how to apply strategic cyber intelligence strategies:

- Embed a risk-based approach in business decision-making by quantifying the organization's digital asset, data and information flow.
- Use real-time insights to ensure your cybersecurity strategy stays agile and always relevant to the current business climate.
- Have a deep knowledge of the external threat landscape. This should be at the core of an organization's business risk management and can be a tool to trigger a change in business priorities and drivers.

Management Cyber Intelligence

Management intelligence will give you insights into the readiness of your cyber perpetrators to launch an assault and inform you if you have the right controls to fend off the attack. Intel here will address what are the crown jewels and assets which are of interest to hackers. Here, the intelligence provided will answer this question: Do you know your crown jewels and the core processes supporting them?

Here is what you can expect from management cyber intelligence:

- Mature cyber processes to meet business objectives.
- Controls, process maturity and gaps identified to protect against cyberattacks.
- Validation of the effectiveness of security controls.
- An understanding of the digital assets, data and information that you need to protect.
- Knowledge of attack vectors that can compromise your crown jewels.
- The people, process, technology and policy needed to defend against cyberattacks.

Here are a few ways to apply management cyber intelligence:

- Enable the organization's business leaders to gain an understanding of the risk and impact of a potential breach.
- Identify remedial controls needed to contain risk and track its effectiveness.
- Support your cybersecurity program and provide a path forward to cybersecurity maturity.
- Be aware of the potential impact due to changes in your external threat landscape.
- Optimize resources and capabilities.

Tactical Cyber Intelligence

Tactical intelligence will help you drive security controls efficiently. You need to be aware of the latest cyber criminals attack methods, tools and techniques. The questions that this view of cyber intelligence needs to answer

[back to top](#)

are: Do you know your attack surface? Are your cybersecurity controls effective against the external threat landscape?

Here are a few things you can expect from tactical cyber intelligence:

- An understanding of which individuals and digital assets could be at risk and their corresponding impact on the organization.
- An understanding of the path of attack that an adversary can use to launch a campaign targeting you.
- Insights into tactics, techniques and procedures cybercriminals would use to execute cyber attacks.
- Knowledge of your security controls and their effectiveness and efficiency.

Here's how to apply tactical cyber intelligence:

- Guide threat analysis by ensuring intel can be ingested into the SIEM and SOAR to bolster the organization's cyber defenses.
- Help the security operations center make "real-time" or "near real-time" decisions to defend against cyberattacks.
- Enhance security controls and improve operational efficiency by providing technical specifics around a cyberattack.
- Validate the effectiveness of security controls and of processes.
- Optimize resources to solve the most critical vulnerabilities.

The cybersecurity boxer uses all three types of intelligence so that even if a southpaw attack occurs, he or she is ready to return with a right hook, followed by an uppercut. Our boxer would have gathered insights into the

opponent's strengths and weaknesses, predict the next move and adapt defense on the fly. Our boxer is ready to take the championship with a resounding knock-out.

To build a strong cyber posture, let's remember to float like a butterfly and sting like a bee.

For any enquiries, please contact Ms Anna Koh at anna.koh@cyfirma.com

Article from The Cybersecurity Awards 2021 Winner – Ms Shamane Tan



I was simply blown away when I heard my name announced as the winner of the Cybersecurity Awards 2021 (Professional Category). Borders still wasn't fully opened yet, and it has been 2 years since I was able to return to Singapore. As I went up the stage at Marina Bay Sands, my heart was warmed as Minister Josephine smiled and handed me a beautiful glass award with my name engraved on it.

This award is incredibly meaningful to me because of what it represents. Having lived in Australia for the last 7 years while driving industry awareness for the global communities, contributing to Singapore's ecosystem has always remain a key and intentional priority of mine.

Born and bred here in Singapore, graduated with my honour's degree in Computer Engineer from NTU more than a decade ago, and now as Sekuro's Chief Growth Officer, working with the C-execs in their mission of building and uplifting their business resilience with cyber, all these different experiences have shaped my journey in cyber security.

I first founded Cyber Risk Meetup in 2017 in Sydney with a raw desire to bring security expertise together in a room and provide a platform for the hungry and aspiring leaders to learn. Never would I imagine that over the years, the meetup would grow to more than 5,000 professionals with chapters set up in Sydney, Melbourne, Perth, Adelaide, Singapore and Japan. I find that there are always two distinct groups; the experienced leaders who have been doing the CISO role (but under a different title) for decades, and then we have the newer leaders who are either finding the shoes big to fill, or they're realising that it can be very lonely at the top.

I started running the CISO tribe where a room full of CISOs and senior security leaders get together every few months to discuss their challenges and approaches that have worked for them. It was behind this closed door and in this exclusive setting that a safe space was created, and the leaders were able to confide and soundboard with one another across the industry.

I saw how many have gained comfort in knowing they're not alone in their challenges, and that they've found a community hub where they can bounce off ideas with one another. When I first published '*Cyber Risk Leaders*', the vision was to equip our security leaders with a guidebook, where they can have access to more than 70 over C-executives' insights, voices and perspectives. The purpose was to bridge the knowledge and experience gap in our community. Writing a book took a lot of discipline and courage. I even became a victim of the imposter syndrome, a topic I later ended up giving a TEDx talk on, '*The Imposter Syndrome of the Tall Poppy*'.

However, throughout my journey, I would never forget the people who have cheered me on and encouraged me to use my voice. I ended up writing my next book '*Cyber Mayday and the Day After*' together with my co-author Dan Lohrmann (who was the former CSO for the State of Michigan, and previously from the US national security agency), which global publisher Wiley took up. Shortly after its release this year, I found out that it became an Amazon best-seller in the US, UK and Australia.

My achievements today are largely attributed to the previous generation of cyber security leaders, who firstly, gave me the opportunity to learn from them, but also took the time to share their experiences with me - the authenticity and support provided from our senior leaders have deeply accelerated my growth. Thank you also to all of my mentors, peers, industry leaders and my security community and collaboration partners who have poured in and imparted into our ecosystem; this award belongs to all of you. Thank you AiSP for all of the work that you are doing for our society, while advocating and supporting our cyber leaders as well.

I have always believed that it takes a community to build a community. And now, my personal experiences have inspired me to contribute back, and continue enriching our community *especially in Singapore*, in bringing together groups of diverse leaders. We are better, stronger, and more impactful as a group together, than as an individual.

Visit <https://www.aisp.sg/publications> for more contributed contents by our partners.

PROFESSIONAL DEVELOPMENT

Listing of Courses by Wissen International

New course by
EC-Council
www.eccouncil.org

A First of its kind
Vendor Neutral and
Vendor Specific Certification

The **Next Dimension**
in Cloud Computing

CCSE
Certified Cloud Security Engineer

Become a **Certified Cloud Security Engineer (CCSE)**

The **CCSE Program Advantage**

- 50+ Hands-on Intensive Labs
- Mapped to 20 Cloud Job Roles
- Mapped with Real-Time Industry Job Roles

AWS AWS Cloud

Azure Azure Cloud

Google Cloud Google Cloud Platform

REGISTER NOW

Brought to you by Wissen – EC-Council Exclusive Distributor APAC

WISSEN
Cyber Security Competency Development

Email us for more info
aisp@wissen-intl.com

Introducing new course by EC-Council
Certified Cloud Security Engineer (CCSE)

Organizations need cloud security engineers to help them build a secure cloud infrastructure, monitor vulnerabilities, and implement incidence response plans to mitigate cloud-based threats. CCSE, with its unique blend of vendor-neutral and vendor-specific concepts, trains candidates in the fundamentals while equipping them with job-ready practical skills.

Email us to find out more aisp@wissen-intl.com

[back to top](#)

Listing of Courses by ALC Council



“The global standard for Cyber Security Architecture”

SABSA Foundation 23-27 May 2022

Live Virtual training 9:00 am – 5:00 pm SGT

Special 15% discount for AiSP members

Getting your architecture right is the critical success factor for robust and effective cyber security in business and government.

SABSA represents the world standard for cyber security architecture. When you get your SABSA accreditation you become a member of an exclusive group positioned strategically between two domains – that of top management and that of the technical subject matter expert.

SABSA mandates the most highly-qualified instructors

Fully-accredited SABSA training is conducted only by instructors who hold the SABSA Master certification - the most demanding certification in the industry. Accredited SABSA trainers have to pass three exams – SABSA Foundation and two Advanced courses - with a minimum mark of 75%. They then have to attain the SABSA Master certification by preparing a university-style thesis

demonstrating experience and understanding, subject to review by two assessors. That is what you get from ALC.

[SABSA Certification >>](#)

ALC is the only accredited SABSA provider in Singapore

ALC Training Pte Ltd is the only accredited provider of SABSA cyber security architecture training in Singapore.

Start your SABSA journey with the globally recognised **SABSA Foundation Certificate**. Next course to be held in the Singapore time zone on 23-27 May 2022.

[Full course details and registration >>](#)

ALC Training Pte Ltd is proud to be an AiSP Partner.

Take a look at our full [Singapore training program](#).

You can claim your AiSP 15% member discount against any course. All you have to do is copy-paste **ALCAiSP15** on the Promotion Code field on the registration form.

Any questions, don't hesitate to contact us at customerservice@alctraining.com.sg

Thank you.

The ALC team



ALC Training Pte Ltd

3 Phillip Street, #16-02 Royal Group Building, Singapore 048693

T: (+65) 6227 2883 | E: learn@alctraining.com.sg | www.alctraining.com.sg

Qualified Information Security Professional (QISP®) Course



Companies around the world are doubling down on their security as cyber attacks see an increase in frequency, intensity and severity. It is thus critical for businesses and organisations to have Qualified Information Security Professionals to manage cybersecurity threats and incidents.

To support the development of personnel in this profession, the Association of Information Security Professionals (AiSP) is offering the Qualified Information Security Professional (QISP) Programme.

This special five-day training programme is based on AiSP's Information Security Body of Knowledge (IS BOK) 2.0. This course will prepare participants for the QISP examinations. After attending this course, participants will also be able to understand and attain knowledge in these areas:

- Enterprise Governance
- Risk Analysis and Management
- Security Controls
- Security Principles and Lifecycle
- Business Continuity Planning
- Develop and Implement Security Goals, Objective and Strategy and Programs

- Maintain and Review Security Operations

COURSE DETAILS

2022 Course dates can be found on https://www.aisp.sg/qisp_training.html

Time: 9am-6pm

Fees: \$2,500 (before GST)*

*10% off for AiSP Members @ \$2,250 (before GST)

*Utap funding is available for NTUC Member

TARGET AUDIENCE

- Professionals who wish to learn more or embark into Cybersecurity
- Security Professionals who will be leading or taking on a senior management/technical role in ensuring Enterprise Governance is achieved with Corporate, Security and IT Governance

COURSE CRITERIA

There are no prerequisites, but participants are strongly encouraged to have:

- At least one year of experience in Information Security
- Formal institutional training in cybersecurity
- Professional certification in cybersecurity

For registration or any enquiries, you may contact us via email at secretariat@aisp.sg or Telegram at **@AiSP_SG**.

Program Partner



Delivery Partners





This course is suitable for people who are new to information security and in need of an introduction to the fundamentals of security, people who have decided to make a career change to take advantage of the job opportunities in information security and need formal training/certification. Professionals who are in need to be able to understand and communicate confidently about security terminology.

To support the development of personnel who are new to information security and wish to pursue career in this profession, the Association of Information Security Professionals (AiSP) is offering the Cybersecurity Essentials Course. With the completion of this course, participants will have an overview on cybersecurity. The course will build on the foundation to prepare participants for Qualified Information Security Professional (QISP) course.

Course Objectives

This 3-day training program is for those who have very little knowledge of computers & technology with no prior knowledge of cyber security. After attending this course, participants will also be able to understand and attain knowledge in these areas:

- Introduction to Security
- Risk Management
- Cybersecurity IT Platform
- Securing the Server
- Securing the Network
- Cloud Computing
- Cybersecurity Operations

COURSE DETAILS

Training dates for year 2022 can be found on https://www.aisp.sg/cyberessentials_training.html

Time: 9am-6pm

Fees: \$ \$1,600 (before GST)*

*10% off for AiSP Members @ \$1,440 (before GST)

*Utap funding is available for NTUC Member

TARGET AUDIENCE

- New to cybersecurity
- Looking for career change
- Professionals need to be able to understand and communicate confidently about security terminology

Please email us at secretariat@aisp.sg to register your interest.

Program Partner



Delivery Partners



MEMBERSHIP

AiSP Membership

Complimentary Affiliate Membership for Full-time Students in APP Organisations

If you are currently a full-time student in the IHLs that are onboard of our [Academic Partnership Programme \(APP\)](#), AiSP is giving you complimentary Affiliate Membership during your course of study. Please click [here](#) for the application form and indicate your student email address, expected graduation date and name of your institution in the form.

Complimentary Affiliate Membership for NTUC Members

AiSP offers one-time one-year complimentary Affiliate Membership to all active NTUC members (membership validity: 2021 to 2022) from 1 Sept 2021 to 31 Dec 2022. The aim is for NTUC members to understand and know more about information security and Singapore's cybersecurity ecosystem. [This does not include Plus! card holder \(black-coloured card\), please clarify with NTUC on your eligibility.](#)

On [membership application](#), please do not email your personal data to us via email if your information or attachment is not password-protected. Please send us your password via [Telegram](#) (@AiSP_SG).

Once we receive confirmation from NTUC on the validity of your NTUC membership, AiSP would activate your one-year complimentary AiSP Affiliate membership.

AVIP Membership

AiSP Validated Information Security Professionals ([AVIP](#)) membership helps to validate credentials and experience for IS-related work including cybersecurity, professional development and career progression for our professionals. Interested applicants should be qualified [AiSP Ordinary Members \(Path 1\)](#) to apply for AVIP.

Your AiSP Membership Account

AiSP has ceased its digital platform, Glue Up and are currently exploring other options to provide our members a better and user-friendly experience.

Membership Renewal

Individual membership expires on 31 December each year. Members can renew and pay directly with one of the options listed [here](#). We have GIRO (auto - deduction) option for annual auto-renewal. Please email secretariat@aisp.sg if you would like to enrol for GIRO payment.

[Be Plugged into Cybersecurity Sector – Join us as a Member of AiSP!](#)

Please check out our website on [Job Advertisements](#) by our partners.
For more updates or details about the memberships, please visit
www.aisp.sg/membership.html

AiSP Corporate Partners



Acronis





Visit https://www.aisp.sg/corporate_members.html to know more about what our Corporate Partners (CPP) can offer for the Cybersecurity Ecosystem.

AiSP Academic Partners



Our Story...

We are an independent cybersecurity association that believes in developing, supporting as well as enhancing industry technical competence and management expertise to promote the integrity, status and interests of Information Security Professionals in Singapore.

We believe that through promoting the development, increase and spread of cybersecurity knowledge, and any related subject, we help shape more resilient economies.

Our Vision

A safe cyberspace supported by a strong and vibrant cybersecurity ecosystem.

Our Mission

AiSP aims to be the pillar for Information Security Professionals and the overall Information Security Profession through:


- promoting the integrity, status and interests of Information Security Professionals in Singapore.
- enhancing technical competency and management expertise in cybersecurity.
- bolstering the development, increase and spread of information security knowledge and its related subjects.



 www.AiSP.sg

 secretariat@aisp.sg

 +65 8878 5686

 116 Changi Road, #04-03 WIS@Changi, S419718

Please [email](#) us for any enquiries.