

NEWS & UPDATE

AiSP New Corporate Partners

AiSP would like to welcome ExtraHop, Huawei, Micro Focus and Privasec as our new Corporate Partners. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem in 2021.



AiSP New Academic Partner

AiSP would like to welcome Singapore University of Technology and Design as our new Academic Partner. AiSP looked forward to working with the lecturers and students to contribute to the Cybersecurity Ecosystem.



AiSP Knowledge Series Events

Security Architecture & Engineering

AiSP Knowledge Series Webinar for Best Practices for Enterprise Security Management was held on 16 June together with our MOU Partner IASA with interesting insights from AiSP President, Mr Johnny Kho and Founder and Chairman of IASA Asia Pacific, Mr Aaron Tan. Participants benefitted from the sharing and learned how to create a Digital Enterprise Architecture Map to align Business and IT strategies as well as the fundamental processes in Security Engineering Life cycles.

IASA Presented by Aaron Tan
Chairman of IASA Asia Pacific aarontan@lasahome.org
Chief Architect of ATD Solution aarontan@atdsolution.com
President of Enterprise Architecture Chapter, Singapore Computer Society aarontan@scs.org.sg

A Business-driven Approach for Enterprise Security Architecture

www.atdsolution.com Slide 4

AiSP
Association of Information Security Professionals

SECURITY ENGINEERING LIFE CYCLE

Johnny Kho, AiSP President
16 Jun 2021

CAAP
Cyber Security Advisory & Advisory Programme

Copyright-free image of Microsoft O365 subscribers.

Data & Privacy

On 29 June night, AiSP EXCO Member Ms Yvonne Wong led the panel discussion on “What Cybersecurity Professionals need to take note of GDPR” with panellists Ms Joyce Chua (UOB Group), Mr Bryan Tan (Pinsent Masons LLP) and Mr Ivan Lai (Crypto.com). The sharing session was beneficial to information security professionals who wants to prepare ahead for forward looking data protection practices with the new revisions to the PDPA principles.



Cyber Defence

Our upcoming Knowledge Series Webinar Event – Cyber Defence will be on 14 July 2021 by speakers from HTCIA Singapore Chapter and Tufin. AiSP will also be signing a MOU with HTCIA Singapore Chapter during the sharing too.

Physical Registration: <https://www.eventbrite.sg/e/aisp-x-htcia-sg-chapter-knowledge-series-cyber-defence-tickets-160513904409>

Virtual registration: https://us06web.zoom.us/webinar/register/WN_XYsDQ7SIQ1m_9JYara3pUQ

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 2021 are as follows (*may be subjected to changes*),

1. Cyber Defence – Ethical Hacking, 14 Jul (hybrid*)
2. OT/IOT – IoT Security, 25 Aug (hybrid*)
3. Operation and Infrastructure Security, 15 Sep
4. CTI SIG, 29 Sep (hybrid*)
5. Security Operations – Incident Response Management, 13 Oct
6. Emerging Trends – Blockchain & AI for Cyber Security, 17 Nov

*Subjected to Singapore Government's directives for physical events during COVID-19 pandemic.

Please let us know if your organisation is keen to be our sponsoring speakers in 2021!

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 2021 webinars in our [event calendar](#).



THE CYBERSECURITY Awards 2021

TCA 2021 nomination period has ended on **16 June 2021**. Thank you to all who have submitted the nominations.

Professionals

1. Hall of Fame
2. Leader
3. Professional

Enterprises

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

Students

4. Students

The Cybersecurity Awards 2021 winners will be announced at The Award Ceremony 2021.

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

TCA2021 Sponsors & Partners



Organised by



Supported by



Supporting Associations



Gold Sponsors



Silver Sponsors

Community Partner



Supporting Organisation



Platinum Sponsors



Cybersecurity Awareness & Advisory Programme (CAAP)

AiSP X SFA CAAP Awareness Workshop

On 25 June, Mr Tony Low (AiSP CAAP Co-Lead), Mr Tim Snow (Cisco) and Mr Alvin Tan (Tanium) gave an insightful sharing on how to protect SMEs from cyber threats and adopt digital solutions safely. AiSP would like to thank Singapore FinTech Association (SFA), Cisco and Tanium for supporting the event.



Upcoming CAAP Events

AiSP hope to elevate Cybersecurity 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.

Join our upcoming events below to expand your knowledge on cybersecurity issues.

Jointly organised by:



Fortify Your Company's Cyber Security

Through Endpoint Protection, Managed Detection & Response and Unified Threat Management

Date: 7th July 2021 (Wed) | Time: 3.00pm to 4.45pm | Fees: FREE | *Priority will be given to SCCCI Members

Cybersecurity has become an important consideration in an increasingly digitalised environment. To encourage SMEs to adopt cybersecurity solutions, the government has expanded the range of pre-approved solutions under the SMEs Go Digital programme, to include cybersecurity solutions. Eligible SMEs in need of cybersecurity solutions in the areas of Endpoint Protection, Managed Detection and Response, and Unified Threat Management can get funding support through the Productivity Solutions Grant (PSG). Join us at this webinar to hear more about the importance of cybersecurity and how these solutions can help SMEs to improve their cybersecurity posture.

Key Takeaways:

1. Learn about the importance of cybersecurity in an increasingly digitalised environment from the Cybersecurity Agency of Singapore (CSA), and how CSA's Safer Cyberspace initiatives can support enterprises in raising cybersecurity awareness.
2. Learn how to get the most from your endpoint security.
3. Learn how managed monitoring service will benefit SMEs without IT Resources to safeguard their IT infrastructure and database.
4. Learn how modern attacks have migrated from PC to IoT, Industrial Control Systems, and supply chains to breach organisations effectively.

Webinar Speaker Line-up:



Veronica Tan
Director
Safer Cyberspace
CSA



Tia Asihwardji
SB Commercial Lead
Trend Micro



Luke Chung
Senior Manager
(Sales & Business
Development),
VSS Engineering



Jonas Walker
Security Strategist
FortiGuard Labs



Tony Low
CAAP Co-Chair
AiSP

Sign up now at <https://tinyurl.com/caap070721>



AiSP CAAP Focus Group Discussion – Singapore SMEs' Digital Adoption and Concerns

23 JULY 2021 | 7PM - 9PM | Ensign InfoSecurity
30A Kallang Place, #08-01
Singapore 339213

7:00 PM | Registration & Dinner

7:30 PM - 8:00 PM | Introduction to Cybersecurity Awareness & Advisory Programme and how the focus group discussion would be facilitated

Focus Group Discussion

Area for Discussion:

8:00 PM - 8:45 PM |

1. Immediate concerns arising from rising cyber threats
2. Concerns about cybersecurity incidents in companies
3. Management's and staff's sentiments about the importance of cybersecurity for your business

8:45 PM | AiSP Facilitator to close the session

Facilitated by:



Organised by:



Supported by:



forms.office.com/r/MEFX1RprWn

Sign up now at <https://tinyurl.com/caap230721>

Cybersecurity Awareness Workshop



SIGN UP NOW

| 27 July 2021 | 1.30PM - 5.00PM |
Lifelong Learning Institute

Organised by:



KEY HIGHLIGHTS



Importance of Cybersecurity and Solutions

By Mr Tony Low, CAAP Co-Chair

With the disruption of the pandemic, many cyber threats such as phishing and data breaches has increased over the past 12 months. For 2021, many SMEs in Singapore are looking to increase their cybersecurity to protect against the increased cyber threats.



Beginning your journey on cloud data protection with Thales

By Mr Collin Chow, Managing Director, Root Security

With the rising number of data breaches, it has been proven that data is the new oil. Are you at least on how to secure your critical data that your company holds? Join us to understand how you can easily protect your data anywhere, meet compliance mandates while focusing on your core business needs.

Identity and Access Management 101 with Thales

By Mr Collin Chow, Managing Director, Root Security

With the changes that is happening in the threat landscape for information technology, the importance of cybersecurity has never been more important. Join us in this session to learn how you can implement an effective cloud identity and access management (IAM) strategy in your organization which will help to prevent a cybersecurity attack.



Sharing on Cybersecurity Courses

With the rising cyber threats, SMEs need to continuously enhance their knowledge in cybersecurity to protect themselves. Find out what are the cybersecurity courses available for SMEs to upskill themselves.

Supporting Partners:



THALES



Sign up now at <https://tinyurl.com/caap270721>



CAAP FOCUS GROUP DISCUSSION



FRIDAY, 30 JULY 2021, 10AM - 11.30AM

TOPIC OF DISCUSSION

Companies may not be aware of cyber risks in their digital transformation or when they want to embark on digital initiatives. Through the focus group discussion, participants shares their concerns to our facilitator. Join us to hear from our facilitator on the view of what companies and their staff should be aware of, and what can they do to mitigate risks.

AREA OF DISCUSSION

FACILITATOR



Mr Tony Low
CAAP Co-Chair
AiSP

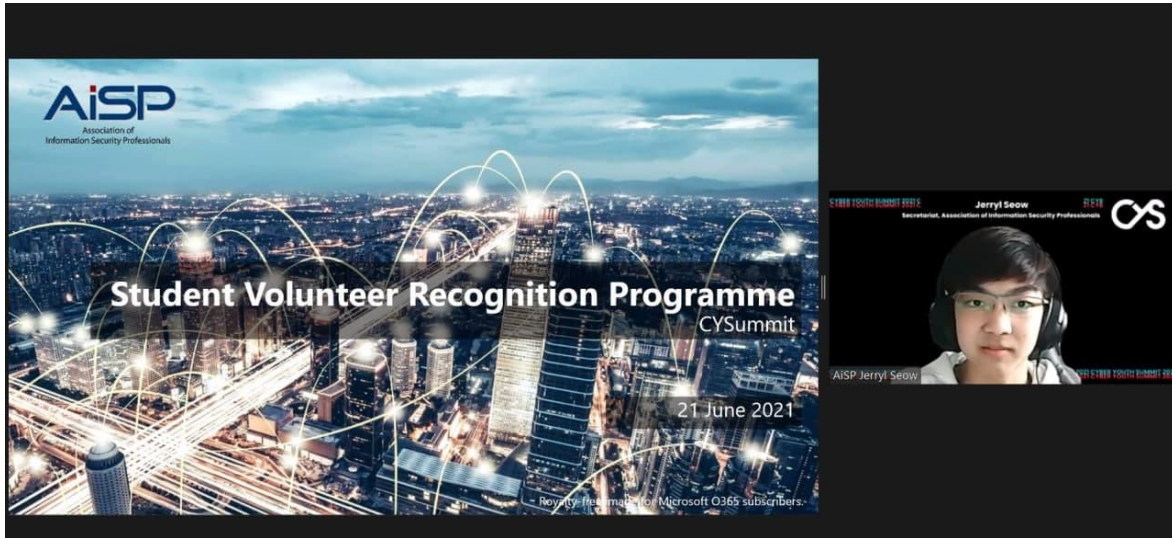
1. Immediate concerns arising from rising cyber threats
2. Concerns about cybersecurity incidents in companies
3. Management's and staff's sentiments about the importance of cybersecurity for your business

Sign up now at <https://forms.office.com/r/pfscNu0rU3>

Student Volunteer Recognition Programme (SVRP)

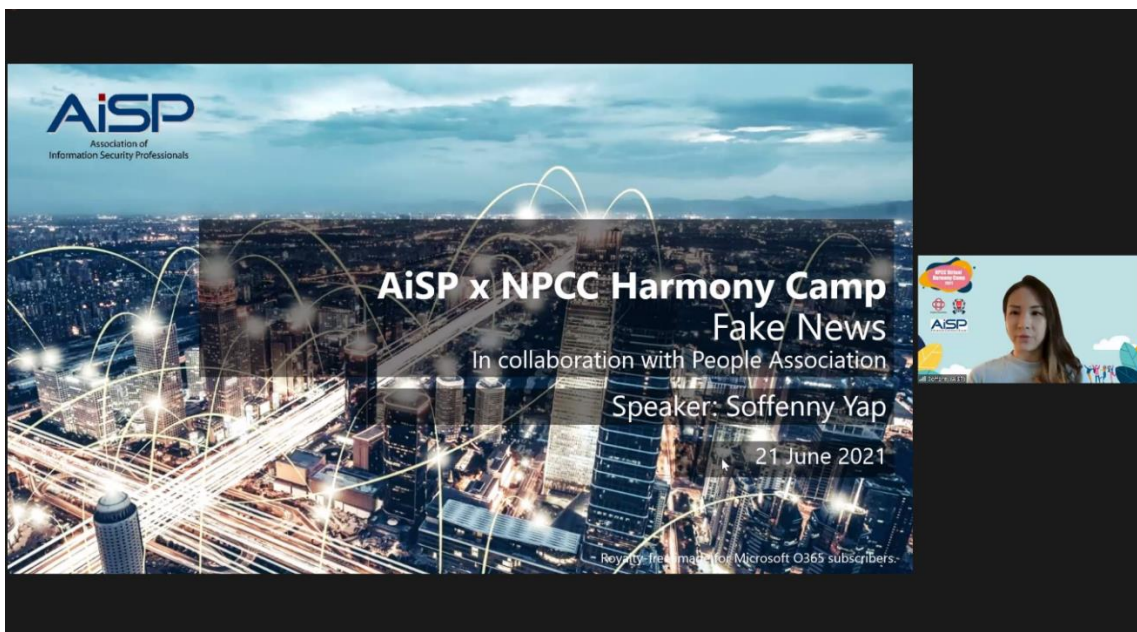
Cyber Youth Singapore (CYS) Summit

CYS Summit has officially launched on 21 June and Mr Jerryl Seow represented AISP to share on the Student Volunteer Recognition Programme (SVRP) benefitting students in the cybersecurity ecosystem.



NPCC Harmony Camp Sharing with Ms Soffenny Yap

On 21 June afternoon, Ms Soffenny Yap (SVRP Co-Lead) gave an interesting sharing to the participants on Fake News in collaboration with National Police Cadet Corps (NPCC) People's Association. At the end of the session, participants tested their knowledge through a game of kahoot.



Our **SVRP 2021 nomination form** is available now for IHL students to apply! To encourage more students to volunteer, secondary school and pre-university students are welcome to participate! Please refer to [SVRP framework](#) and **SVRP 2021 nomination form for secondary school and pre-university students!** We are having a student volunteer drive from now till Dec 2021 for those who are interested to volunteer but not sure where to start. Please **click here** to apply today.



Nomination Period:
1 Sep 2020 to 31 Aug 2021

CALL FOR NOMINATION! STUDENT VOLUNTEER RECOGNITION PROGRAMME

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):

Example A	Example C
Leadership: 10 Hours	Leadership: 0 Hour
Skill: 10 Hours	Skill: 50 Hours
Outreach: 10 Hours	Outreach: 0 Hour
Example B	Example D
Leadership: 0 Hour	Leadership: 0 Hour
Skill: 20 Hours	Skill: 0 Hour
Outreach: 20 Hours	Outreach: 60 Hours



Scan the QR Code for the Nomination Form

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/svvp.html for more details



Nomination Period:
1 Sep 2020 to 31 Aug 2021

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 comprises three broad pillars where IHL students can volunteer:

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

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

Under AiSP's **Academic Partnership Programme (APP)**, the IHLs can include AiSP Student Chapter in their respective institutes. Please refer to our [Student Chapters](#) for the list of current committee members and we look forward to expanding the list in 2021!

SINGAPORE CYBER SECURITY INTER ASSOCIATION (SCSIA) CYBER DAY QUIZ



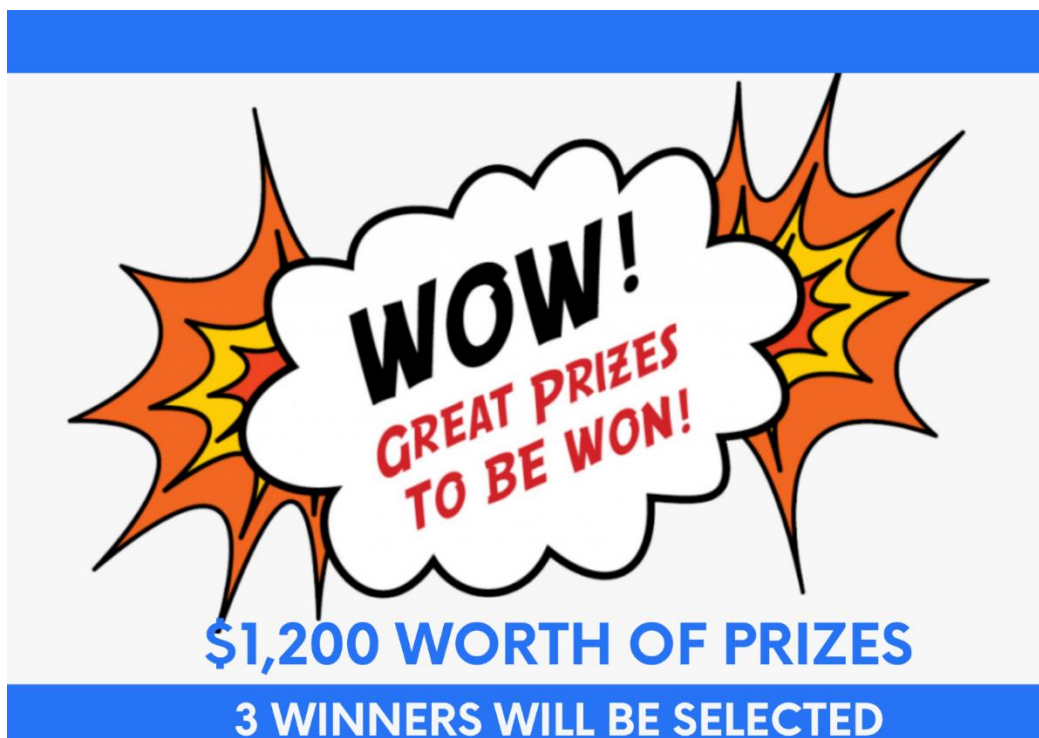
As part of **AiSP's CyberFest 2021** and in conjunction with **Singapore Cyber Day 2021** in November 2021, the **Singapore Cyber Security Inter Association (SCSIA)** is organizing an online quiz competition for primary, secondary and tertiary students (aged 25 years and below) in Singapore with the support from the Cyber Security Agency of Singapore. This competition aims to pique interest in students and equip with knowledge on Cyber Security.

From 25 March onwards, 3 questions will be posted on Facebook and LinkedIn every Thursday. **Answers will be revealed after 30 September** (when the competition ends). Please note that you must complete all **29 weeks of questions** to qualify for the total scoring.

E-Certificate of Participation will be given to all participants. **Attractive Prizes will be given to the top scorers.** You may find the link access below to the past quiz questions. Stay tuned to our [Facebook](#) and [LinkedIn](#) for the upcoming quiz questions!

<p>Week 1 Quiz https://forms.office.com/r/XGHBUPQJJe</p> 	<p>Week 2 Quiz https://forms.office.com/r/gWsMr1ZfLs</p> 
<p>Week 3 Quiz https://forms.office.com/r/ikiwzBiSnV</p> 	<p>Week 4 Quiz https://forms.office.com/r/C0XdFvtqcs</p> 
<p>Week 5 Quiz https://forms.office.com/r/bPYdNn3Ytm</p> 	<p>Week 6 Quiz https://forms.office.com/r/gmgSSn2syS</p> 
<p>Week 7 Quiz https://forms.office.com/r/dV0m8WmvHP</p> 	<p>Week 8 Quiz https://forms.office.com/r/9B9ifeCibI</p> 
<p>Week 9 Quiz https://forms.office.com/r/1fx4XZq8fx</p> 	<p>Week 10 Quiz https://forms.office.com/r/QTgzfkckJ</p> 

<p>Week 11 Quiz https://forms.office.com/r/iKTdAXy4Wc</p> 	<p>Week 12 Quiz https://forms.office.com/r/G60xJEqHpb</p> 
<p>Week 13 Quiz https://forms.office.com/r/FrwapxXVZP</p> 	<p>Week 14 Quiz https://forms.office.com/r/ruKgZ3XaUp</p> 
<p>Week 15 Quiz https://forms.office.com/r/5B4Wq1LqZS</p> 	




WOW!
**GREAT PRIZES
TO BE WON!**

\$1,200 WORTH OF PRIZES
3 WINNERS WILL BE SELECTED

Sharing of Cybersecurity with NTUC Members

Sign up for NTUC Union Membership today and have access to a wide array of benefits from workplace protection to lifestyle benefits (attached below for merchants deals)!














NTUC Membership
Here supporting your needs at work & in life
#hereforyou













Not a member? Receive a FREE OTO Spinal Support worth \$238
when you pay 6 months membership fees and arrange Credit/Debit Card Recurring (CCR) payment

Apply now

In collaboration:

	Union members can sign up for NTUC FairPrice Membership to earn up to \$240 cash rebate* on your groceries, health & wellness products and services as well as purchase shares to earn dividend [^]
	Up to 15% OFF* NTUC Value Meals
 	\$0.50 Hot Kopi/Teh* on Wednesdays at NTUC Foodfare as well as Kopitiam Food courts and coffee shops \$1.80 Breakfast Set*
	Flash NTUC Plus! Card for members' rates
	Enjoy premium rates for as low as \$0.70/day* with LUV Term Life Insurance
	Get \$102 worth of LinkPoints* per year when you enrol your child
	Earn and redeem LinkPoints at over 1,200 merchant outlets!
	NTUC Club – the club for union members! Enjoy special privileges at Wild Wild Wet, Marina Bay Golf Course, Orchid Bowl and more!

	Available on BetterHealth mobile app: • \$10* GP Teleconsultation • \$12* GP Consultation	
	One-year FREE* subscription to access GetDocPlus mobile app	
	Get up to \$60* electricity bill rebates.	
	20% OFF* monthly mobile subscription	
	\$8 OFF* with min. spend of \$15 at foodpanda or pandamart <small>(for new users only)</small>	
	• \$6 OFF* first order <small>(for new users only, capped at the first 2,000 redemptions)</small> • \$8 OFF* with min. spend of \$15 <small>(for existing users, capped at 3 redemptions per user)</small>	
Flash your NTUC Plus! Card for members' rates*		
		
		
And many more!		
Visit ntucmembership.sg to discover more savings!		

Sign up [now](#) and receive an OTO Spinal Support worth \$238

Ladies in Cybersecurity



Ladies Talk Cyber Series

For the Fourth edition of AiSP's 'Ladies Talk Cyber' series, we interviewed Tan Mei Hui, who is the Vice President for Singapore Computer Society (SCS) Cybersecurity Chapter. She shared on her experiences with SCS and how we can encourage more women to enter the field.

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.

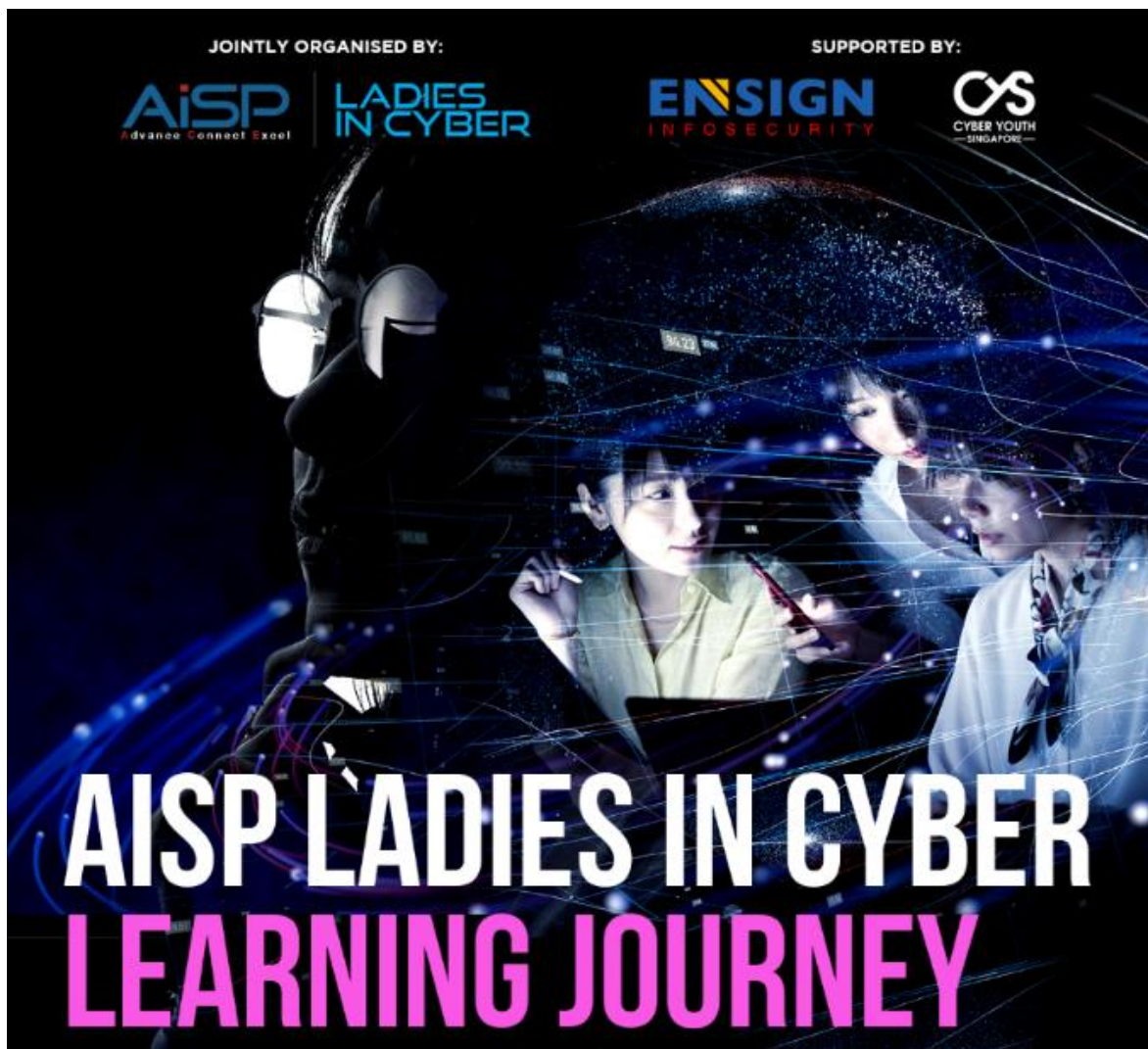
Introducing women with a deep interest in cybersecurity

Mei Hui is currently the Vice-President for Singapore Computer Society Cybersecurity Chapter. She is actively promoting cybersecurity career mentoring for students and work closely with AiSP on various programmes.

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

Join us in our next Ladies in Cyber Dialogue Session on 13 Jul 21 (Tue)

AiSP will be organising a Virtual Dialogue Session on 13 Jul 21 for female students. Join Ms Sun Xueling, Minister of State for Ministry of Education and Ministry of Social and Family Development and Dr Tan Mei Hui, Vice-President of Singapore Computer Society Cybersecurity Chapter moderate by Ms Sherin Y Lee, AiSP Vice-President in a closed-door dialogue session on the issues of Supporting women in the workplace and in their career aspirations. **Register now at <https://ensign.global/3uddpl5>**. Please feel free to invite all your female colleagues and friends to join in the session too.



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
- Cyber Threat Intelligence
- Data and Privacy
- IoT

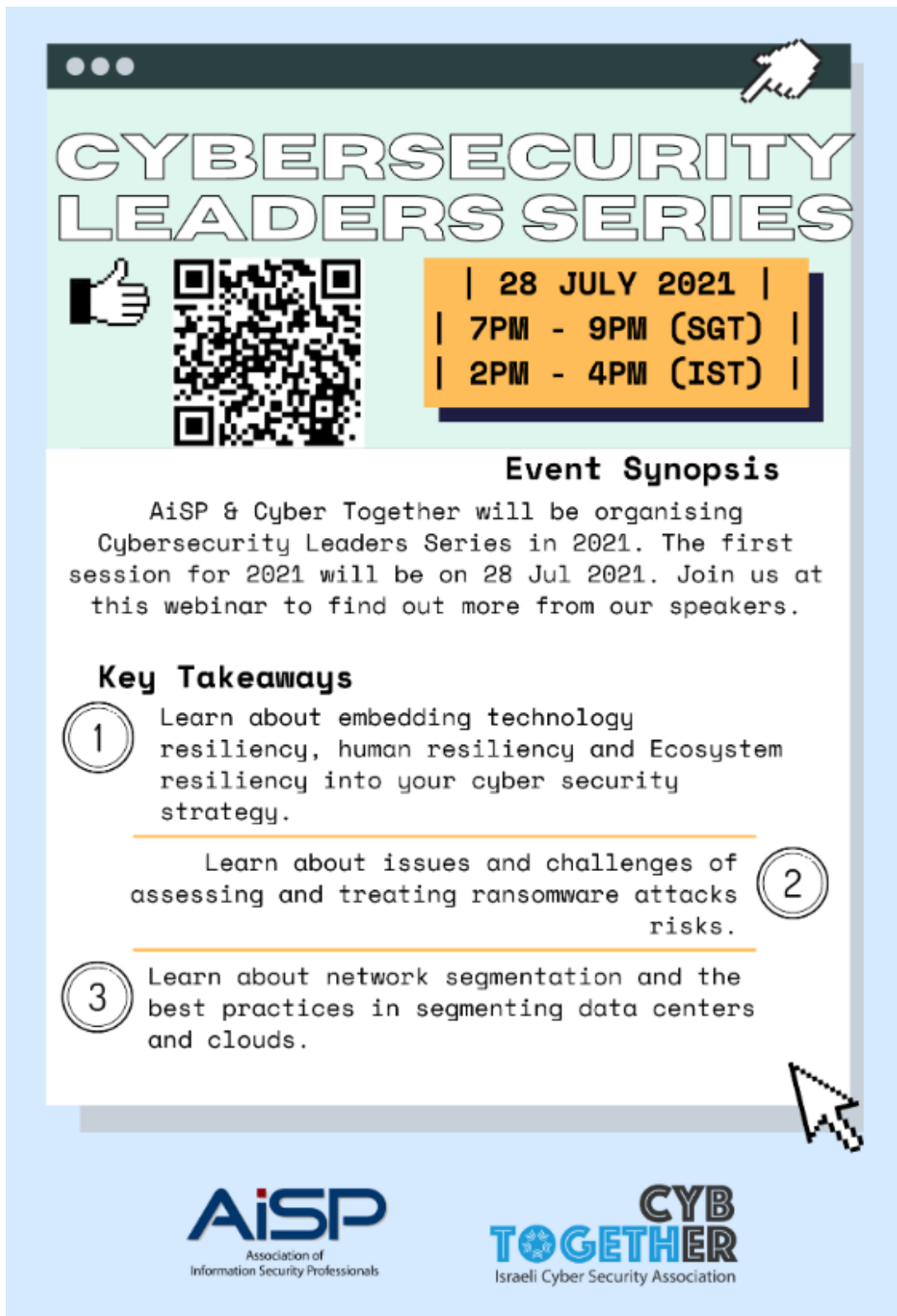
We would like to invite AiSP members to join our [Special Interest Groups](#) as there are exciting activities and projects where our members can deepen their knowledge together in 2021. Please contact us if you are keen to be part of our SIGs as we are actively recruiting members for 2021!



Special Interest Group (SIG) Events



Date	Event
12 August 2021	AiSP SIG Induction Event
14 October 2021	Combined SIG Event Cloud Security & Data & Privacy
03 December 2021	Combined SIG Event CTI & IoT

Cybersecurity Leaders Series



The poster features a light blue background with a dark blue header and footer. At the top, there are three white dots and a white hand cursor icon pointing to the right. The main title 'CYBERSECURITY LEADERS SERIES' is in large, white, outlined letters. Below the title, there is a thumbs-up icon, a QR code, and a yellow box with black text containing the event date and times. The event synopsis and key takeaways are in a white box with a dark blue border. At the bottom, there are logos for AiSP and CYB TOGETHER.

CYBERSECURITY LEADERS SERIES


| 28 JULY 2021 |
| 7PM - 9PM (SGT) |
| 2PM - 4PM (IST) |

Event Synopsis

AiSP & Cyber Together will be organising Cybersecurity Leaders Series in 2021. The first session for 2021 will be on 28 Jul 2021. Join us at this webinar to find out more from our speakers.

Key Takeaways

- 1 Learn about embedding technology resiliency, human resiliency and Ecosystem resiliency into your cyber security strategy.
- 2 Learn about issues and challenges of assessing and treating ransomware attacks risks.
- 3 Learn about network segmentation and the best practices in segmenting data centers and clouds.



AiSP
Association of
Information Security Professionals

CYB TOGETHER
Israeli Cyber Security Association

Sign up now at <https://tinyurl.com/280721>

For AiSP Members only

As we are always looking for new ways to engage our members, AiSP has categorised the various ways for [member-only access](#) as part of our digital engagement during COVID-19 pandemic,

1. Members-only access for [webinar playback](#)
2. [LinkedIn closed group](#)
3. Participate in [member-only events](#) and closed-door dialogues by invitation
4. [Volunteer](#) in our initiatives and interest groups, as part of career and personal development

If you have missed our virtual events, some of them are made available for members' access via [Glue Up](#) platform. Please email (event@aisp.sg) if you need any assistance.

We wish to remind our members to renew their 2021 membership if they have not done so.

Call for Volunteers

As AiSP focuses in raising the professional standing of information security personnel and professions in Singapore since 2008, we have been running various initiatives to address diverse needs and developments. Please [email us](#) for more details!



PROFESSIONAL DEVELOPMENT

Qualified Information Security Professional (QISP®) Course

QISP® is designed for entry to mid-level Information Security Professionals, and any IT Professionals who are keen to develop their knowledge in this field. It will be enhanced to complement AiSP's Information Security Body of Knowledge (IS-BOK) 2.0. Our online examination via Pearson VUE platform would be deployed worldwide in 2021.

QUALIFY YOUR INFOSEC KNOWLEDGE TODAY!

Security is a high priority globally, cyber attacks have increased in frequency, intensity, and severity. It is 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 demanding profession since 2010, the Association of Information Security Professionals (AiSP) has been offering its **Qualified Information Security Professional (QISP®)** Programme. The QISP® examination enables the professionals in Singapore to attest their knowledge in AiSP's IS-BOK domains.

If you want to raise your infosec credentials or your knowledge in cyber security, please sign up for our QISP training or examination today!

Please email us secretariat@aisp.sg if you have any query.

I AM QISP®



Connect with us on LinkedIn, Facebook, Instagram, YouTube and Telegram today.

Please **contact AiSP** if you are keen to leverage the enhanced QISP® for your learning and development needs, or you would like to develop courseware based on AiSP's IS-BOK 2.0 overseas.

BOK 2.0 Knowledge Series

As information security developments are accelerating during COVID-19 pandemic and the trend is expected to be the same for 2021, we have covered the application and implementation of our BOK 2.0 topics at workplaces in our past webinars. This series is useful for working professionals who are preparing for our **QISP®** examination so that their knowledge remains current.

CREST SINGAPORE CHAPTER

The CREST Singapore Chapter was formed by CREST International in partnership with CSA and AiSP to introduce CREST penetration testing certifications and accreditations to Singapore in 2016. Our CREST practical exam will resume on 29 July 2021. Please click [here](#) for the exam schedule for 2021.

UPCOMING ACTIVITIES/ EVENTS

Ongoing Activities

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

Upcoming Events

Date	Event	By
7-Jul	CAAP Workshop with SCCC1	AiSP & Partner
7-Jul	Demystify Zero Trust	Partner
13-Jul	Ladies in Cyber Learning Journey to Ensign	AiSP & Partner
14-Jul	Knowledge Series – Cyber Defence – Ethical Hacking	AiSP & Partner
14 –16 Jul	ConnecTechAsia	Partner
15-Jul	Sharing on Work Study Diploma in Cyber Security & Forensics by ITE East	Partner
23-Jul	CAAP Focus Group Discussion with PA	AiSP & Partner
27-Jul	AiSP CAAP Workshop	AiSP
28-Jul	Punggol Digital District Industry Event	Partner
28-Jul	Cyber Leaders Series with Cyber Together	AiSP & Partner
30-Jul	AiSP x NTUC CAAP Focus Group Discussion	AiSP & Partner
03-Aug	SBF Cloud Webinar on Cloud optimization and automation	AiSP & Partner
12-Aug	SIG Combined Event	AiSP
17-Aug	CREST Webinar	AiSP
18-Aug	Demystify SASE	Partner
18–19 Aug	ARRC	Partner
24-Aug	Data Security Webinar	AiSP & Partner
25-Aug	Knowledge Series – IoT Security	AiSP

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



CyberFest® is a community-led initiative that would take place from 08 to 12 Nov 2021 in Singapore.

CONTRIBUTED CONTENTS

Insights from The Cybersecurity Awards 2020 Winner – Trustwave, a Singtel Company



Addressing the challenges of cloud security through shared responsibility

The enterprise's role in the shared responsibility model

The cloud plays an increasingly significant role in today's enterprise IT environment, with CIOs coming to a consensus that the combined use of public and private clouds will deliver cost savings and [greater business agility](#), and enable seamless collaboration across the business and its ecosystem partners.

While these offer good reasons for migrating more applications to the cloud, enterprises should exercise caution and adopt a security mindset as they embark on this journey.

Attacks on the cloud environment

According to the [2020 Trustwave Global Security Report](#), attacks on the cloud environment – specifically on software-as-a-service – more than doubled to 20 per cent of overall incidents between 2018 and 2019. The main types of data compromised in these exploits were financial data (42 percent), personal identifiable information (15 percent) and user credentials (15 percent).

In ecommerce environments that include cloud-based infrastructure-as-a-service and platform-as-a-service deployments, attacks also increased from 22 percent to 27 percent, with hackers targeting mainly credit card data.

One factor behind the growing number of exploits is the laissez-faire attitude when it comes to cloud security. In a [2020 Global Encryption Trends Study by the Ponemon Institute](#), more than half of almost 6,500

Shared responsibility model

To address these and other security challenges related to enterprise cloud adoption, the cloud ecosystem has adopted a shared responsibility model which spells out the security obligations of cloud service providers and their enterprise customers to ensure accountability.

Cloud service providers are responsible for securing the infrastructure that runs their applications or services. For example, in supplying infrastructure-as-a-service (IaaS), the cloud provider is responsible for securing basic [cloud infrastructure components](#) such as virtual machines, disks and networks, and the physical security of the data centres that house the infrastructure.

The enterprise's role

For the enterprise, playing its part in the shared security model involves securing the operating system and software stack required to run its applications and manage its data. This will require the enterprise to adopt a holistic approach to security that encompasses the following:

Building an effective strategy to protect its cloud environment and data in the cloud

This includes carrying out security and risk assessments, discovering and classifying sensitive data, vulnerability scanning and penetration testing to better understand the enterprise's security posture, and developing a robust security strategy and policy.

respondents indicated that their businesses use cloud technology to transfer or store data – regardless of whether it is encrypted or protected via any security mechanisms.

Transition challenges

The lack of vigilance is especially worrying during the cloud transition phase, when security challenges are even more complex and harder to tackle.

As enterprises migrate their systems and applications to the cloud, they will be changing connections, permissions and other built-in security functions. This could potentially set off a deluge of security alerts which may be dismissed as false positives as eyes-on-glass fatigue creeps in during the period of environment change, providing the perfect cover for threat actors to strike.

The cloud has also made it easier for attackers to launch exploits that blend into regular, everyday traffic. The ability to create free accounts with no or obfuscated attribution increases hacker anonymity and makes detection that much more difficult for security teams.

This brings us to the challenge of identity and access management (IAM) in the cloud.

IAM vulnerabilities

Whether on-premises, in the cloud or in a hybrid environment, IAM relies on the same fundamental components that have been around for over 20 years, such as Active Directory, permissions and passwords. Businesses today continue to grapple with the known and unknown exploitable vulnerabilities in the use of these IAM mechanisms.

With cloud adoption, there are added [challenges](#) arising from improper service and user provisioning and deprovisioning, the existence of zombie accounts assigned to inactive users, the proliferation of admin accounts and users bypassing enterprise IAM controls – all of which can be exploited by threat actors to carry out privilege escalation and other attacks.

- **Stopping threats from penetrating cloud workloads and executing malicious actions**

Security technologies are implemented to protect people and assets from the constantly evolving threat landscape, stop threats from penetrating cloud workloads and prevent the execution of malicious actions. Examples of these technologies include next-generation firewalls, intrusion detection and prevention systems, cloud access security brokers, secure web and email gateways, web application firewalls, database security and security posture management solutions.

- **Proactively detecting, investigating and responding to threats**

Malicious activity is detected and tracked throughout all phases of the attack kill chain. For example, the Trustwave cloud analysis engine processes all collected events to uncover known threats, anomalous behaviour and suspicious activity and cross references the event data against SpiderLabs Threat Intelligence for indicators of compromise and known bad actors.

- **Empowering staff to respond effectively to threats**

This includes cybersecurity awareness training, executive training, and tactical training programmes and services to equip staff with the knowledge and tools to protect against and respond to threats.





Conclusion

As more and more enterprises embrace the cloud for its elastic capabilities and the ease of spinning up solutions, security challenges will continue to mount. Expectations surrounding the agility of the cloud, set against a backdrop of growing complexity, will continue to add to the difficulty of securing the cloud environment.

Effective management of these challenges will require enterprises to build an effective strategy to secure the data and applications that they are running and storing in the cloud as part of their role in the shared responsibility model for cloud security.

Brought to you by Trustwave, a Singtel company, recognised global and regional leader in managed security services and consulting

Trustwave Cloud Security Services

 <p>Consulting Services</p> <ul style="list-style-type: none"> • Security and risk assessments • Strategy and policy development • Threat and detection workshops • Sensitive data discovery and classification • Vulnerability scanning and penetration testing 	 <p>Security Technologies</p> <ul style="list-style-type: none"> • Next generation firewall • Intrusion detection/prevention system • Cloud access security broker • Security posture management • Endpoint protection • Secure web gateway • Secure email gateway • Web application firewall • Database security 	 <p>Cyber Education</p> <ul style="list-style-type: none"> • Cybersecurity awareness training • Executive training programmes and services • Tactical training programmes and services 	 <p>Managed Security Services</p> <ul style="list-style-type: none"> • Managed detection • Managed security information and event management • Managed detection and response • Digital forensics and incident response
---	--	--	---

Fancy a discussion to advance your organisation's security posture? Contact us now.



g-security@singtel.com



singtel.com/cybersecurity

 **Trustwave**[®]
a Singtel company

Insights from our Corporate Partner Programme (CPP) – Fortinet

Security Is Key for the Success of 5G

By **Ronen Shpirer** | June 03, 2021

5G has been a particularly hot topic lately, sparking significant debates and being considered as polarizing to some extent. However, countries all over the world are rolling out their 5G networks, considering this evolution in mobile connectivity as a strong game-changer for end users, the mobility ecosystem, and many industries.

Two Takeaways that Make 5G Unique

5G differs from 4G and previous mobile generations in two significant and interdependent aspects.

First, 5G breaks away from the gradual evolution from one mobile generation to the other by redefining its technology foundations, to support and drive the ongoing digital transformation businesses, consumers, and even whole societies are undertaking. It means that most of the legacy nature of the mobile network, such as the use of specific protocols and interfaces, is replaced by common IT protocols, **APIs**, and cloud technologies.

Second, 5G brings customized mobile connectivity and added value services both for industrial organizations and mobile network operators (MNOs). Thanks to **5G capabilities**, such as increased bandwidth and low latency, organizations can develop new products, services, and most importantly, best practices, such as significant safety and efficiency in production floors, greater automation in industry 4.0, better proactive maintenance and so much more. This wasn't possible in the days of wired networks or Wi-Fi networks.

When it comes to MNOs, 5G represents a significant growth opportunity. Traditionally, their revenues were heavily dependent on SIM/package sales, as a basic service for a mobile provider. With the 5G capabilities and ecosystem, MNOs can now better address the business segment and deliver added-value services beyond cellular connectivity to their customers, creating new revenue streams and improving margins.

5G Impacts on Cybersecurity

5G “uniqueness” in the mobile generation evolution has had major impacts on many areas, including cybersecurity. With the use of common IT protocols and interfaces in the infrastructure, such as HTTP and API calls, combined with its open and distributed nature, as well as the expanded attack surface, 5G is an attractive target for hackers.

The 5G technology impact on security is multi-faceted. While the use of cloud technologies and architectures throughout the 5G infrastructure (**RAN**, core, and edge) enables enhanced agility, scalability, efficiency, and customization, securing that environment is also a key element to consider. Security must be integrated into the virtual infrastructure as well as the orchestration layer and embedded into the end-to-end network to ensure both security and business continuity.

Hyperscalability, ultra-low latency, support for machine communications, predictability, agility, and high precision are some of the capabilities that will drive 5G adoption and use cases in vertical industries and for consumers. It is mandatory that the cybersecurity approach and solutions will support, and not hinder, these capabilities.

Security visibility, automation, threat intelligence, and control are critical to protect the 5G infrastructure and the 5G-enabled use case ecosystem (OT/IIoT/IoT devices, 5G public and private networks, MEC and **public cloud** environments, applications and APIs).

Cybersecurity: A 5G Enabler for Widespread Adoption

5G is the most natively secured mobile generation. But the security foundations laid out in the 5G standards can only be a starting point for a security blueprint that secures end-to-end 5G-enabled innovation and use cases.

In 2020, Fortinet conducted a survey around security in enabling 5G adoption in business verticals, and the results are very clear:

Almost 90% of respondents stated that the MNO's security capabilities are either critical or very important for success in vertical industry use cases. More than 80% consider native 5G security features as important, but only a baseline for the security needed to serve the 5G market.

Another interesting data point arising from the survey is that 54% of respondents believe operators should offer a shared responsibility model. However, nearly all those who support this approach believe that a shared responsibility model should be offered as an option alongside the alternative of comprehensive, full-stack, end-to-end security. True to the traditional telco business model, fully 86% of respondents believe operators should offer full-stack security.

In previous mobile generations, security was all about protecting the network itself, creating a walled-garden environment for the core of the network by securing all external exposure points, such as the internet/PDN, roaming, RAN to core access, external partners, etc. This is also valid to 5G, with the appropriate integration and compatibility to 5G technologies and architectures. But the unique nature of 5G and its role and criticality in the business segment means that security's role is changing and expanding, and should encompass the following main roles:

- Protect the 5G mobile infrastructure from attacks to ensure service continuity and availability. This is similar to the traditional security role in previous mobile generations.
- Protect the larger 5G ecosystem required to deliver 5G-enabled use cases for enterprise verticals to meet security and regulatory requirements.
- Enable monetization via a wide range of 5G security services to organizations through managed security services as part of service/use case offerings.

The Success of 5G

The benefits of 5G far outweigh its potential risks—but only when security is an integrated part of the process and solution. Although 5G has some built-in security, organizations will still need to integrate a larger cybersecurity strategy to confidently move to 5G applications. They need a solution that will provide comprehensive protection at 5G speeds without compromising end-to-end visibility, automation, and enforcement throughout the ecosystem's attack surface. And to do that most efficiently and securely, the solution must also be part of a coherent, integrated, and self-healing security platform. This will enable organizations all over the world to confidently distribute 5G services from the core of their network out to its furthest reaches, while allowing them to continue developing and deploying critical digital innovation.

Learn more about how the Fortinet Security Fabric protects 5G ecosystems.

More about Fortinet at www.fortinet.com

Insights from our Partner – Kaspersky

Filling the gaps: The story of APAC's cyber capacity building

By Genie Sugene Gan, Head of Public Affairs & Government Relations for Asia Pacific at Kaspersky

The recent cyberattack incidents involving the largest pipeline system for refined oil products and one of the world's biggest meat producers in the United States serve as yet another reminder that countries will continue to deal with cyberattacks. And the number is growing. Globally, the percentage of attacked industrial control systems in the second half (H2) of 2020 was 33.4 percent --- an increase of .85 percentage points compared with the first half of the year.

For cybercriminals, countries in the Asia Pacific (APAC) region have not fallen off the radar. If anything, cyber gangs are stepping up their campaigns in a region, which continues to attract more and more investments in supply chains and logistics.

Unfortunately, not all countries have the capacity to tackle cyber threats adequately. Laying the foundation for an organization's cyber-resiliency starts with having a cyber-capacity-building program in place and cultivating a culture of cooperation among all stakeholders.

Stages of Cyber-Resiliency

Cybersecurity education and capacity-building begins with a recognition of the vast diversity that exists in the region.

Looking at APAC, we can categorize countries into three groups, according to the stages that they are at in dealing with cyberattacks:

- **Advanced:** Leaders in the cybersecurity field that have a clear strategy in place and are already doing more in terms of development
- **Intermediate:** Those that have identified cyberattacks as an area they need to look into and have attempted to make some inroads;
- **Initial:** Countries which have just begun paying attention to this area for various reasons, including more pressing domestic needs.

The state of APAC

Let me give you some (non-exhaustive) examples of good national cybersecurity efforts in the region.

Singapore is an example of a country that is putting a lot of effort into boosting its national cybersecurity capabilities. When Singapore launched its \$30-million, five-year project called the ASEAN-Singapore Cybersecurity Centre of Excellence in 2019, it opened up an opportunity to offer policy and technical programs for member state participants to help bolster regional cybersecurity capabilities. The project also pushed for collaboration among ASEAN member countries to conduct research, share knowledge and train to respond to cyber threats.

Placing data security high on the national list is what we saw when Australia's Cyber Security Strategy 2020 kicked off last year with an investment of A\$1.67 billion allocated over 10 years. The government's three-pronged strategy of building a stronger digital ecosystem, growing a skilled workforce and protecting Australians shows us that they are taking cybersecurity very seriously.

Japan has also gradually integrated cybersecurity into boosting capacity-building in ASEAN, offering platforms for collaboration with individual Southeast Asian countries as well as the United States through additional coordination. Through mechanisms such as the annual ASEAN-Japan Cybersecurity Policy Meeting first held in 2009, Tokyo has gradually broadened its engagement with Southeast Asian states to include a range of areas such as mutual notification for incidents, joint industry-government-academic collaboration, the construction of new facilities such as the ASEAN-Japan Cybersecurity Capacity Building Center in Thailand, and the holding of U.S.-Japan training workshops on areas like industrial control systems.

In today's landscape, a key focus area of cybersecurity education and capacity-building is enabling countries in the intermediate category to move towards the advanced group.

Vietnam in particular has been actively reinforcing regulations and standard-setting across the government and in partnership with the private sector. Among the pivotal measures it has established include a national cybersecurity law, standards and blueprints across government and private organizations.

In its twin five-year cybersecurity master plans, the private sector is encouraged to collaborate with the government in cascading materials to customers, granting scholarships and co-organizing campaigns and training. One of the prominent campaigns in the country was the government-led National Malware Detection and Removal Campaign launched in 2020 and supported by 18 local and foreign cybersecurity firms, including Kaspersky.

Both India and Indonesia are on the cusps of releasing their national cybersecurity strategies, highlighting the awareness that these markets have on the importance of the issue.

While India may have grappled with an unprecedented spike in cyberattacks since the pandemic, it has made headway in training thousands of government officials and critical sector companies, initiating cybersecurity investments and establishing agreements outside ASEAN such as with Japan, Israel and more recently with Bahrain to boost cooperation in cybersecurity in capacity-building, research and development and the protection of critical information infrastructure.

Efforts to promote cybersecurity education and capacity-building should also build on or integrate ongoing initiatives. India is a case in point, with New Delhi having several individual efforts but facing challenges in integrating them into a coherent strategy and promoting cyber awareness across society at large.

Indonesia, which is in a similar spot as India, is counting on firming up its cybersecurity education and capacity-building initiatives to achieve its national interests including political stability and economic growth. Through its National Cyber and Crypto Agency (BSSN), the country has involved its key stakeholders including the public for cybersecurity awareness to address the shortage of local cybersecurity experts.

Cybersecurity education and capacity-building initiatives would help Indonesia's government agencies to address concerns on data leaks and data-sharing practices. Data leaks continue to occur often in Indonesia, most recently with its state health insurer, and government agencies have taken the necessary steps to ramp up prevention and mitigation measures in a bid to protect Indonesia's information security and critical infrastructure. Meanwhile, data-sharing initiatives may also create beneficial spill over effects, where data can be reused by government agencies safely to open up significant growth opportunities or to generate benefits across society in ways that could not currently be seen.

Asian states are actively thinking about cybersecurity, while some may still be lacking behind due to not being well-equipped to either advance thinking or practice or provide timely opportunities for ideas to be shaped in a meaningful manner.

It is important that each country's strategy is cohesive enough to enable them to understand where to bridge their own internal gaps. Regional and international organizations provide additional platforms that countries can leverage.

Regional Cooperation on Cybersecurity

As countries look towards formulating and implementing their strategies, regional cooperation between countries and with the industry is essential to help with knowledge and capacity building.

While there are already conversations on cybersecurity in Asian multilateral institutions, there are opportunities for expansion both horizontally and vertically. This includes not only channels within ASEAN engagements, but also in APEC where there may be links between cybersecurity issues and wider subjects being discussed such as data flows and digital transformation.

Now that cybercriminals are upping their game like never before, cyber infections are not going away, even for the APAC region whose threat landscape is as diverse as it is rapidly evolving. Against the backdrop of the pandemic and geopolitics, government organizations will continue to be natural targets for a whole array of cyberattacks, be it espionage or politically-motivated attacks.

The respective situations of certain countries in the region shared above, while still in flux, should nonetheless give all other countries a few ideas to explore strategies and evolve their cybersecurity implementation if they want to achieve cyber resilience and mitigate catastrophic risks.

To remain ahead of the game, a multifaceted approach is required. From Kaspersky's experience, the most effective formula is to have constant improvement of security awareness. This includes engagement with the wider cybersecurity community and stakeholders, including cybersecurity providers to validate and verify the trustworthiness of its products, internal processes and business operations - an important pillar upheld by Kaspersky. To help improve incident response capabilities and ensure the safety and wellbeing of their citizens, countries should also continually promote skills training and enhanced collaboration.

For more information or to get connected, please visit www.kaspersky.com or contact Genie at genie.gan@kaspersky.com.

Insights from our Partner – Thales Group



IDC TECHNOLOGY SPOTLIGHT

Sponsored by: Thales

The phenomenal power of quantum computing has major implications for data privacy and security, and managing crypto keys to ensure they are quantum safe is an imperative for Asia/Pacific organisations.

Quantum-Safe Crypto Key Management: Why Now!

June 2021

Written by: Simon Piff, Vice President Trust and Security Research

1. Introduction

Data privacy legislation is extending its reach beyond the basic requirements of personally identifiable information to include information that could be detrimental to the critical infrastructure of a city or country.

Businesses also host an array of information that they desire to keep confidential – intellectual property, contract details, pricing agreements to name a few – as well as the primary tool used to safeguard the confidentiality of data across all technology types, be it on- or off-premises encryption.

Encryption needs managing, and it has an event horizon threat in the form of quantum computing: quantum computers have the potential to break encryption keys due to their phenomenal computing power¹.

IDC has already identified that 26% of organisations globally² are already in the process of operationalising their quantum computing plans, or will do so in the next 18-24 months.

So, while there is one school of thought that believes the cost is potentially too prohibitive and is a deterrence to adopt this for cybercrime, the reality is that many threat actors are nation-states

AT A GLANCE

KEY STATS

- » 26% of organisations globally are in the process of operationalising their quantum computing plans.
- » 37.4% of Asia/Pacific organisations, vs 47.2% globally, have adopted hardware security modules. The low adoption shows a lack of concern about the impact of quantum computing on security.

WHAT'S IMPORTANT

Encryption, as we know it, especially asymmetric key schemes, will be under threat from quantum computing and Asia/Pacific, with some of the highest levels of ecommerce globally, is an ongoing target for cyber criminals.

KEY TAKEAWAYS

Asia/Pacific organisations need to possess a clear understanding of their systems, have a definitive inventory of all keys and certificates, and improve their key protection and management by practising crypto agility now.

¹ <https://csrc.nist.gov/publications/detail/white-paper/2020/05/26/getting-ready-for-post-quantum-cryptography/draft>

² IDC Survey Erosion of Classical Computing and the Impact of Quantum Computing on Workloads: 2020 Survey Findings n=520

with both high levels of motivation and almost limitless funding to invest in this area – regardless of how nefarious it may be – under the guise of national security and pro-active counter-espionage. However, across Asia/Pacific, the concerns around this issue are lower than other regions³, which, in IDC's opinion, is more an indication of a lack of understanding than anything else.

At the heart of encryption is the encryption key – the part of the puzzle that creates the encryption. Should a threat actor be able to decipher what the key is, all data encrypted using this key can be easily unlocked and the information made broadly available – clearly not a good thing. Therefore, quantum-safe crypto-key management, the ability to create, manage and store keys that will not fall foul of quantum computing, needs to be implemented as an imperative as this technology can help companies avoid the current and future challenges of quantum computing.

To address these concerns, the National Institute of Standard and Technology (NIST) in the United States is working on a range of encryption algorithms that will be implemented as “quantum-safe standards” for public-key encryption and key-establishment algorithms.

Establishing a relationship with an encryption vendor that can support these, as yet undefined, new algorithms should be a focused priority for all organisations that rely on digital commerce or communication – which is pretty much everyone!

Encryption use cases under threat

- » Encryption today is as invisible as electricity, and equally critical. It is used in simple messaging applications from messaging and email, to web-browsing (if you have the right browser or extension), military-grade secure communication, and, critically, every online financial transaction. But its implementation remains a dark art of the security teams. With different types of encryption algorithms, different approaches to implementing encryption and, from a lay person's perspective, an almost impossible grasp of the mathematics behind, it has suffered from being considered a “set and forget” technology.

Implemented in the early days of the internet to secure web servers, then ecommerce, its use is so invisible to most that its existence is often forgotten – until something goes wrong. And when something does go wrong with encryption, it is monumentally catastrophic – just like when the electricity supply is disrupted unexpectedly. Compounding matters, we are about to enter a phase where the longevity of encryption is going to become part of its weakness. Since it is used to identify many devices that exist both on and offline, its longevity has been a useful characteristic, which has led to this “set and forget” attitude. However, with the advent of quantum computers, we are going to have to locate how and where encryption is being used and assess how we will address the concerns that are on the horizon.

- » Encryption is used to:
 - Secure data at rest
 - Secure data in transit
 - Assure the integrity of identities, data, and devices through the use of digital signatures
 - Manage digital rights and protect copy
 - Assure the integrity of software code through code signing technology

³ IDC-Thales Data Threat Report 2020 n=1723

II. Definitions

Symmetric-key encryption involves a single key to encrypt and decrypt data. Due to the performance of symmetric encryption in both hardware and software, this mechanism is quite useful for bulk encryption of data at rest and in motion. However, the complexities involved in securely distributing the symmetric keys make them a poor choice for authentication and authorisation. This is where asymmetric cryptography plays a key role.

Asymmetric encryption uses different keys, one to encrypt and another to decrypt data. Each user generates a key pair, made from both a public and private key. The public key is shared openly, while the private key is kept secret as a password. Due to a complex mathematical relationship between the two keys, once data has been encrypted with a public key, it can only be decrypted by its matching private key. This is also known as public key encryption (PKI).

While both types of encryption are at risk to the creation of a scalable quantum computer, the asymmetric algorithms are particularly at risk due to the quantum algorithms' ability to attack their underlying mathematical properties.

III. Benefits

Addressing the issue of quantum-safe crypto-key management means understanding how and where keys are generated, managed, and stored, and considering the best approach for the most important issues. As outlined in the NIST paper, [Getting Ready for Post-Quantum Cryptography](#), what is required is crypto agility.

Hardware security modules (HSM) are potentially the best way to address the issue of crypto agility in a post-quantum world. An HSM is a dedicated device that is specifically designed for the protection of the cryptographic keys.

Equally important are certifications and compliance with local regulations such as FIPS 140-2, [Common Criteria for Information Security Evaluation](#), and in Singapore, being compliant with the National IT Evaluation Scheme (NITES), where NITES provides the assurance that the security measures provided by the product to safeguard the highly classified information in the intended deployment scenarios are suitable.

An HSM is a computing device that safeguards and manages digital keys, performs encryption and decryption functions for digital signatures, and provides strong authentication and other cryptographic functions. These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server.

An HSM contains one or more secure crypto-processor chips. Physical and logical protection of the appliance is supported by a tamper resistant/evident shell, and protection from logical threats, depending on the vendor's products, is supported by integrated firewall and intrusion prevention defenses. HSMs are also available in the cloud as a service, and dedicated HSMs through cloud service providers.

Organisations need to easily and efficiently identify how and where encryption is being used...and understand how to quickly swap out those algorithms in order to respond to incidents.

IV. Trends

Quantum computing will, ultimately, place all current encryption algorithms at risk. Even new algorithms will need updating in a world with quantum computing, and this is the core of the issue. Organisations need to easily and efficiently

identify how and where encryption is being used across their environment, understand what cryptography is being used today, know the whereabouts of their keys and certificates, and understand how to quickly swap out algorithms in order to respond to incidents.

Now is the time for organisations to prepare for the quantum era, since we know this issue is on the horizon. Asia will likely be slow to start as HSM adoption in Asia/Pacific is amongst the lowest globally – only 37.4% of organisations (vs 47.2% worldwide) have implemented HSM. This will result in a sudden increase in adoption as the reality of the situation becomes apparent, and potentially a bottleneck in supply as demand will spike for latecomers.

Whilst legislation around privacy will drive encryption to a degree, it has to be the concern about financial transactions that captures the attention of CEOs and CFOs globally. Calculate how much of your revenue is being driven via online commerce – that is the extent of your risk should encryption fail.

V. Vendor Profile

Today's enterprises depend on the cloud, data, and software in order to make decisive decisions. Thales aims to help organisations protect and secure access to their most sensitive information and software wherever it is created, shared or stored – from the cloud and data centers to devices and across networks. Thales' solutions are designed to enable organisations to move to the cloud securely, achieve compliance with confidence, and create more value from their software in devices and services used by millions of consumers every day.

Thales Luna HSM – the foundation of digital trust

Digital security is dependent on cryptographic keys that encrypt and decrypt data, and perform functions such as signing and verifying signatures. Ensuring the integrity of those keys and the cryptographic functions within a secure environment, such as an HSM, is paramount, especially as we creep towards the quantum era. Furthermore, organisations preparing for a post-quantum world require crypto agility, integrating quantum algorithms on the fly.

Luna HSMs are designed to play a critical role in protecting applications that are vulnerable in the quantum era. They act as trust anchors, protecting the cryptographic infrastructure of some of the most security-conscious organisations in the world by securely managing, processing, and storing those keys inside a hardened, tamper-resistant device. Thales' keys in hardware approach ensure that an organisation's devices, identities, and transactions always remain protected in the FIPS 140-2 Level 3 certified, and Common Criteria (CC) EAL4+ validated, secure foundation of digital trust.

Designed to integrate quantum technologies as they emerge, Luna HSMs' crypto agility provides the ability to quickly react to cryptographic threats by implementing alternative methods of encryption. As a result, organisations will:

- » have the agility to respond to incidents;
- » have a definitive inventory of all certificates and keys from all issuing authorities;
- » know how they are using their keys;
- » be able to automate management of server/appliance trust stores and key stores;
- » allow for remote updating of device roots, keys, and certificates; and
- » ensure their PKI can be quickly migrated to new post-quantum resistant PKI root and new algorithms.

Additionally, Thales has partnered to integrate not only quantum-safe algorithms, but also quantum random number generation (QRNG) into the Luna HSMs to generate the entropy, or randomness, into a powerful combination to secure an enterprise.

Thales also offers quantum-safe, high-speed encryptors that provide QRNG, quantum key distribution, and the framework to support quantum resistant algorithms as they become available.

Challenges

The quantum threat, whilst well documented, has no defined timeline and will be the single biggest challenge Thales and enterprises will face. The unknown, coupled with IT security investments that rarely take place in a timely or well-funded manner, pose a great risk to cyber security as a whole. IDC sees a range of ad hoc implementations in response to a real or perceived threat, and frequently after the fact. Overcoming this unwillingness of line of business (LoB) leaders to make an early and strategic investment in an inevitable solution is the key challenge.

Overcoming this unwillingness of LoB leaders to make an early and strategic investment in an inevitable solution is the key challenge.

VI. Conclusion

Encryption is a complex, technical process that requires careful management and oversight. When designed and implemented properly, it is a critical component of a layered defense.

Some of the encryption use cases that will be affected by the impact of quantum computing are:

- » Root Certificate Authorities (CAs). Root CA keys generally have longer lifetimes, and consequently, the certificates that are signed using those keys are at risk from the development of a quantum computer.
- » Data Retention Requirements. An enterprise that stores and keeps data safe for a determined period of time for compliance or business reasons must take into account the post-quantum era.
- » Code Signing Certificates. Code signing is on the increase with the explosion of the DevOps world. Whilst largely targeting cloud-based apps, there are other areas where compromised code signing could be disastrous. Firmware exists in a range of devices beyond traditional computers. Cars are the most obvious use, and the impact of malicious firmware can have life and death implications. Similarly, (software) driver signing is another area that could be under threat in a quantum world.
- » Any data transferred over transport layer security (TLS) will be potentially decryptable with perfect forward secrecy.
- » Document Signing Solutions. Anything signed now will not have integrity in the post-quantum era.

Encryption is an incredibly important control, but leaders should also realise that it is not a silver bullet. For encryption to be effective, it must be applied in an appropriate manner and implemented well. Additionally, organisations must also safeguard their encryption keys to ensure that they maintain control of their information. The advent of quantum computing is going to put all existing encryption, especially asymmetric key schemes, at risk unless the organisation steps up to becoming crypto agile and, consequently, well positioned to implement a quantum-safe encryption strategy prior to the creation of a quantum computer.

Thales is a provider of encryption technology and has crypto-agile solutions and partnerships in place to help organisations address this issue. The key challenge will be educating business users that their operations could easily become transparent, or even halt should they fail to become quantum safe, and that now is the time to address this issue, and not after the fact.

About the Analyst



Simon Piff, Vice President Trust and Security Research

Simon Piff is Vice President for IDC's Asia/Pacific region based in Singapore. He advises both technology and business leaders, as well as IT suppliers on Digital Transformation, the CIO Agenda and Digital Trust, as they relate to the ability of organisations to gain improved returns on their IT investments around hybrid cloud infrastructure, mobile productivity, the value of analytics and artificial intelligence (AI).

Sharing by our Cybersecurity Awareness Alliance Partner - AIG



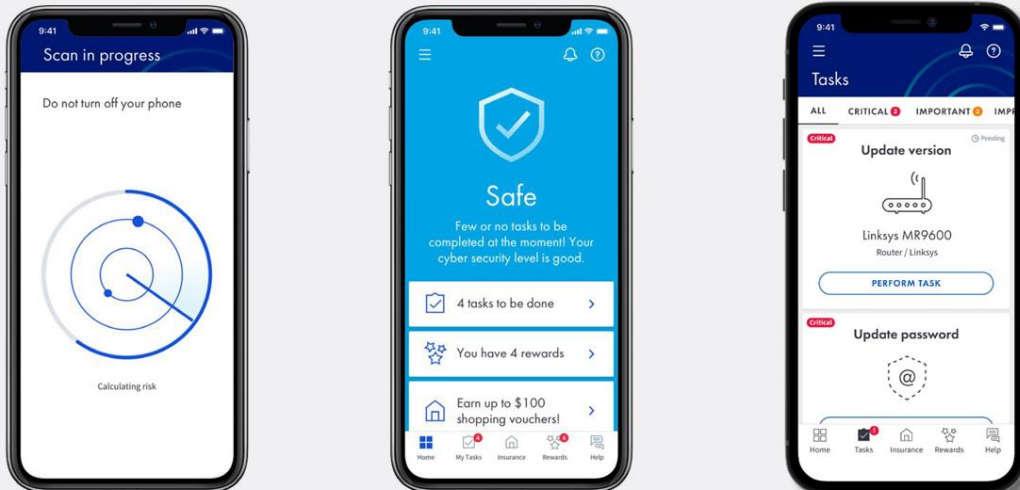
Although you have secured the physical doors and windows of your home, have you secured the doors and windows that are invisible to you?

Cyber criminals are aware that many of us fail to secure our home network and smart devices. And these digital entry points serve as ways to intrude into our homes and lives.

48%* of respondents experienced at least one cybersecurity lapse within a year, which means almost half of us were victims of a cybersecurity lapse.

That's why we created the **AIG CyberPal** app to help strengthen your cybersecurity.

How It Works:



Download AIG CyberPal app to help strengthen the security of your home network and smart devices today

Scan the QR code below to Download Now



*<https://www.csa.gov.sg/news/press-releases/csa-public-awareness-survey-2018>

For more Contributed Contents please visit this [link](#) on our website

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: 2020 to 2021) from 1 Sept 2020 to 31 Aug 2021. 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 moved its digital membership to Glue Up, previously known as Event bank, an all-in-one cloud platform for event and membership management. You can access your digital membership via the [web portal](#) or the mobile application ([App Store](#), [Google Play](#)), using the email address you have registered with AiSP.

The platform allows our members to sign up for events and voluntary activities, and check membership validity.

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

Be part of the Cybersecurity Ecosystem, JOIN AiSP!

AVIP MEMBERSHIP

Limited to 1st
100 sign-ups
For 2021

BENEFITS OF MEMBERSHIP

- Recognition as a **Trusted Infocomm Security Professional**. You can use the designation of **AVIP (AiSP Validated Information Security Professionals Member)** as your credentials.
- Special Invite to **Exclusive Activities & Events**.
- AVIP members enjoy the **Professional Indemnity Coverage in Singapore and Overseas (FIRST in Asia)!**
- AVIP members will be invited for **key dialogue sessions with national & industry leaders** for their opinions on cyber security.
- AVIP members will be **invited to represent AiSP for media interviews** on their opinions on cyber security.



CORPORATE PARTNER PROGRAMME
Registration Fee
(One Time): \$321*
Annual Membership Fee: \$267.50*



ORDINARY MEMBER (PATH 1)
Registration Fee
(One Time): \$481.50*
Annual Membership Fee: \$267.50*

**Price includes GST*

Email membership@aisp.sg to sign up and for enquiries.

AiSP CORPORATE PARTNERS

Acronis



HUAWEI CLOUD



Privasec



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

Visit https://www.aisp.sg/corporate_benefits.html if you wish to join our AiSP Corporate Partners Programme (CPP).

AiSP ACADEMIC PARTNERS



OUR STORY...



 www.AiSP.sg
 secretariat@aisp.sg
 +65 6247 9552
 116 Changi Road
#04-03 WIS@Changi
Singapore 419718

*Our office is closed.
We are currently
telecommuting.*

*Please email us or
message us via
Telegram
at @AiSP_SG*



Please contact secretariat@aisp.sg on events, membership, partnership, sponsorship, volunteerism or collaboration.

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.