NEWS & UPDATE

In line with Government's directives on COVID-19 pandemic and AiSP's business continuity plan, AiSP Secretariat has commenced partial telecommuting during Phase 3. Please **email us** or **WhatsApp** to our office number (+65 6247 9552), for assistance before you drop by our office.

Do check out our **community calendar of events** or follow us on social media for events and updates!

Annual General Meeting

On 26 March 2021, AiSP held our 13th Annual General Meeting at the Lifelong Learning Institute. We are pleased to announce the following **EXCO members** for 2021/2022:

EXCO Position	**Name of Member**
President	**Mr Johnny Kho**
Vice President	**Mr Alex Lim, Mr Andre Shori, Ms Sherin Lee**
Treasurer	**Mr Boris Choo**
Assistant Treasurer*	**Mr Samson Yeow**
Secretary	**Mr Huynh Thien Tam**
Assistant Secretary	**Mr Cecil Su**
Member	**Ms Faith Chng, Mr Freddy Tan, Ms Soffenny Yap, Mr Tok Yee Ching**
Nominated Committee Members	**Mr Chai Chin Loon, Mr Huang Shao Fei, Mr Martin Khoo, Mr Selwyn Scharnhorst, Dr. Steven Wong**

**New Position*

Please click here to view our Executive Committee (EXCO) 2021/2022 Members.

AiSP New Academic Partner

AiSP would like to welcome Nanyang Polytechnic as our new Academic Partner from 1 April 2021 onwards. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem in 2021.

AiSP New Corporate Partner

AiSP would like to welcome Acronis as our new Corporate Partner from 1 April 2021 onwards. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem in 2021.

MOU SIGNING WITH CYBER YOUTH SINGAPORE (CYS)

On 24 March 2021, AiSP signed a Memorandum of Understanding (MOU) with Cyber Youth Singapore (CYS), a youth-run non-profit organisation that focuses on cybersecurity to provide more targeted skill-appropriate training and development opportunities for students in Singapore. This will facilitate closer collaboration between the two organisations to jointly develop education programmes and outreach activities and increase the number of volunteers from secondary school students.

Working together with CYS, AiSP is aiming to spark the curiosity in cybersecurity among youths at an even younger age, and then sustain their interest throughout their education journey with a wide range of other engagement programmes. This will help encourage more students to choose cybersecurity as an education pathway and eventually as a career when they enter the workforce.

With this partnership, AiSP also aims to evolve the way they engage youths and help them develop their competencies by tailoring their programmes to youths' specific interest and proficiency levels, instead of their age group.

CYBER YOUTH —SINGAPORE—

MOU SIGNING WITH INTERNATIONAL INFORMATION SYSTEM SECURITY CERTIFICATION CONSORTIUM (ISC)²

SINGAPORE

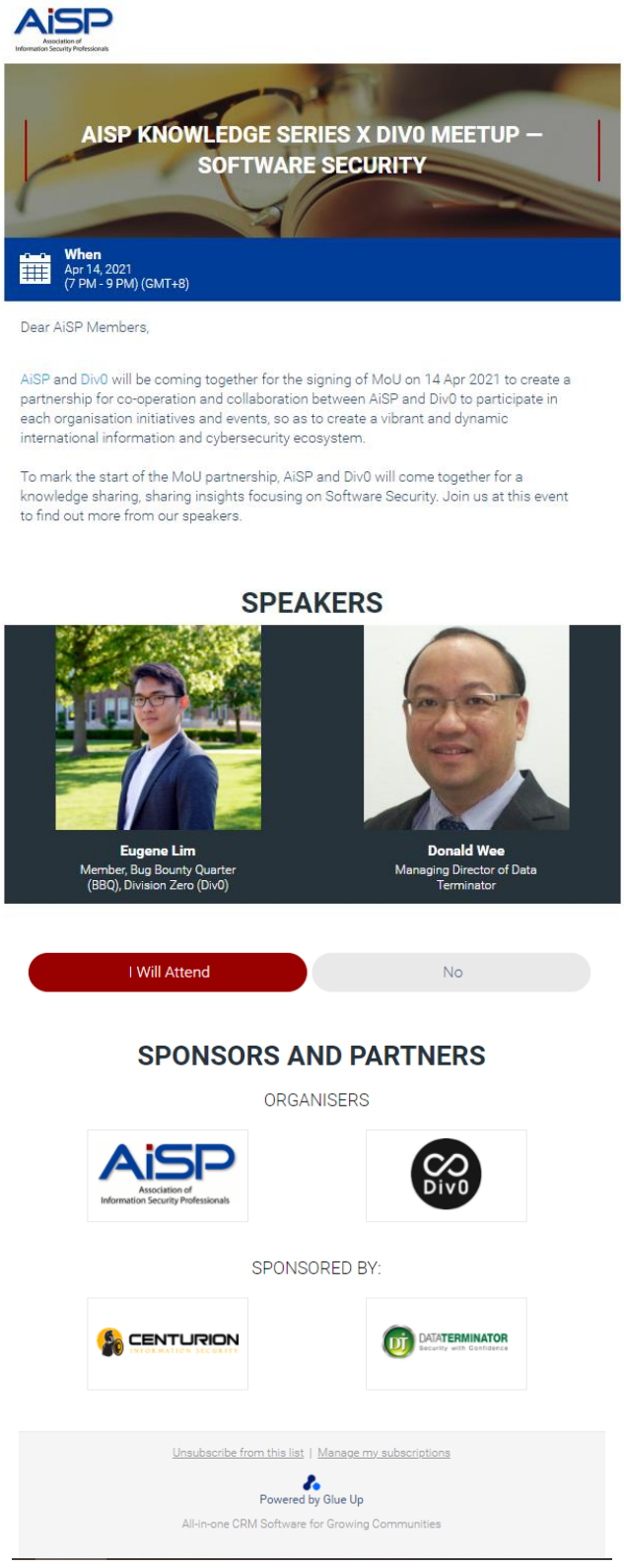
AiSP represented by AiSP President Johnny Kho has renewed the MOU with (ISC)² Singapore Chapter represented by (ISC)² Singapore Chapter President Victor Yeo on 30 March 2021 for another 3 years till 29 March 2024. We look forward to continuous collaboration with (ISC)²!

Knowledge Series Events

AiSP Knowledge Series Webinar - Cyber Threat Intelligence on 30 Mar 21

We had our first hybrid knowledge series for 20201 where about 40 members joined us physically with another 40 members joining us virtually on the topic on **Cloud Security** with insights from our speakers, **Mr Lim Eng Cheng, from AiSP and Mr Anthony Lim from (ISC)² Singapore Chapter**.

Our upcoming Knowledge Series Hybrid Webinar Event – Software Security will be on 14 Apr 2021 by AiSP & Div0.



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. Software Security, 14 Apr (hybrid*)
2. Physical Security, Business Continuity and Audit, 12 May
3. Security Architecture and Engineering, 16 Jun
4. Data and Privacy SIG, 29 Jun (hybrid*)
5. Operation and Infrastructure Security, 14 Jul
6. OT/IOT – IoT Security, 18 Aug
7. Cyber Defence – Ethnical Hacking, 15 Sep
8. CTI SIG, 29 Sep (physical event* with recording)
9. Security Operations – Incident Response Management, 13 Oct
10. Emerging Trends – Blockchain & AI for Cyber Security, 17 Nov
11. IoT SIG, 8 Dec (physical event* with recording)

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

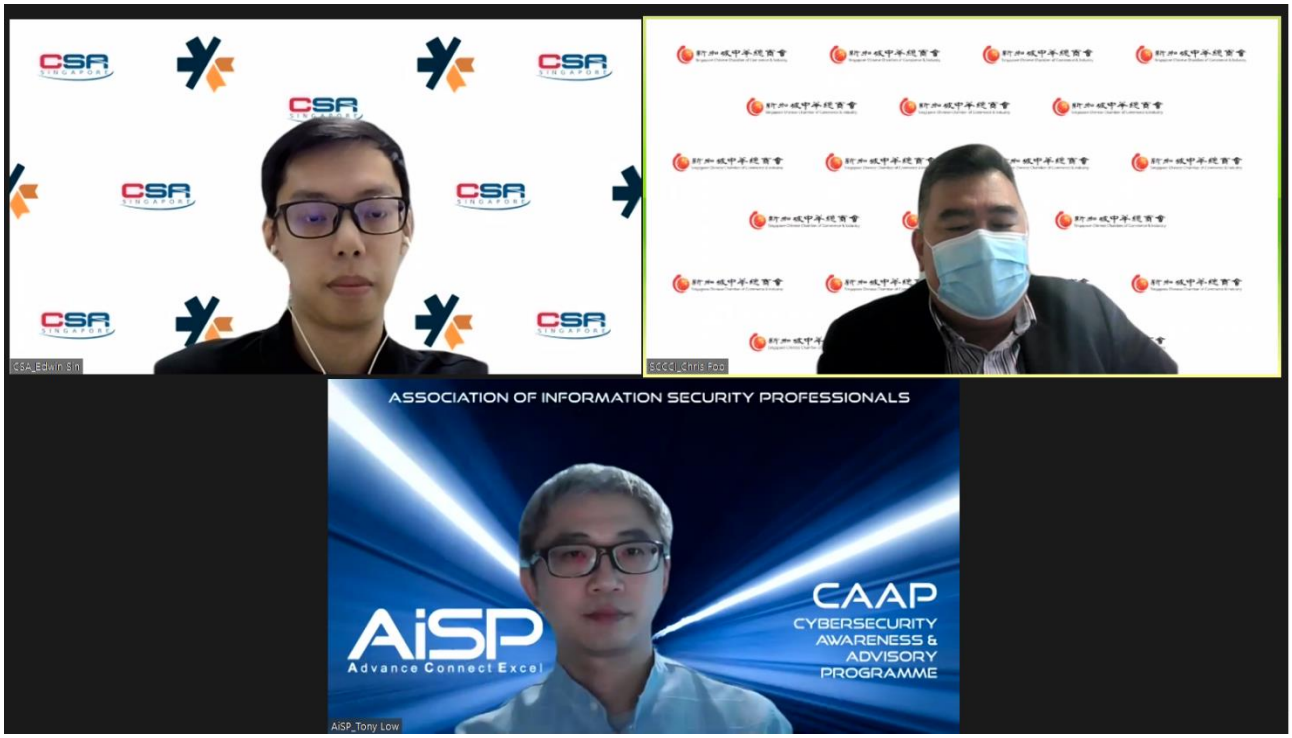
Please let us know if your organisation is keen to be our sponsoring speakers in 2021!

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 event@aisp.sg for assistance. Please refer to our scheduled 2021 webinars in our **event calendar**.

CAAP SCCCI Cybersecurity Outlook 2021

On 31 March 2021, CAAP Co-Chair Mr Tony Low shared on the cybersecurity outlook for 2021. It was an enriching and informative session learning about:

1. Current State: SME in Singapore 2020-2021
2. Budget 2021: Helping SME getting Digital Securely
3. AISP - CAAP: Kickstart Individual and business security awareness



The Cybersecurity Awards 2020 Judges Appreciation was held on 31 Mar 21 at Lifelong Learning Institute. AiSP would like to thank all the judges from the Cyber Security Agency of Singapore and Members of the Singapore Cyber Security Inter Associations (SCSIA) which consists of AiSP, Centre for Strategic Cyberspace + International Studies (CSCIS), Cloud Security Alliance Singapore Chapter, HTCIA Singapore Chapter, ISACA Singapore Chapter, (ISC)² Singapore Chapter, Singapore Computer Society, SGTech, and The Law Society of Singapore for their contributions to make Cybersecurity Awards 2020 a success despite the COVID 19 Situation.

THE CYBERSECURITY Awards 2021

We have received new enquires from Singapore and overseas for award nomination after the 2020 call for nomination was closed on 30 Sep 2020. For our nominees to have more time to prepare their submission, we are pleased to commence **TCA 2021** marketing and the nomination period will be from **1 Feb 2021 to 15 May 2021**.

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

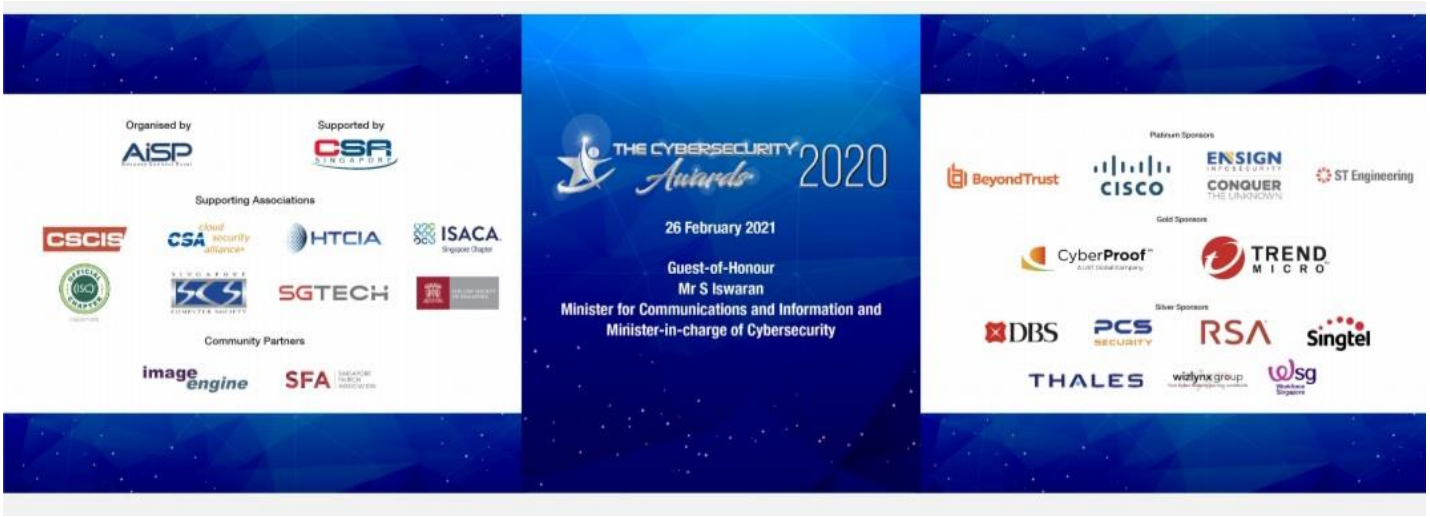
Professionals
1. Hall of Fame
2. Leader
3. Professional

Students
4. Students

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

The Cybersecurity Awards 2021 winners will be announced in October 2021 at the Award Ceremony. The nomination period will be from **1 Feb 2021 to 15 May 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

THE CYBERSECURITY Awards 2021

Organised by

AiSP Advance Connect Excel

Supported by

CSA SINGAPORE

Supporting Associations

CSCIS, CSA cloud security alliance, HTCIA, ISACA Singapore Chapter, (ISC)² Official Chapter Singapore, Singapore Computer Society, SGTECH, The Law Society of Singapore

Community Partner

image engine

Supporting Organisation

SFA Singapore FinTech Association

Platinum Sponsors

BeyondTrust, Cisco, Ensign InfoSecurity, Conquer the Unknown, ST Engineering, Trend Micro

Gold Sponsors

CyberProof A UST Global Company, DBS, Singtel, wizlynx group

Silver Sponsors

PCS Security, RSA, Thales, WSG Workforce Singapore

Student Volunteer Recognition Programme (SVRP)

The SVRP Awards Ceremony was held on 24 Mar 21 at Lifelong Learning Institute Event Hall with Senior Minister of State for Communications and Information and Health, Dr Janil Puthucheary as the Guest of Honour. He presented the awards to the Gold winners. The Award Ceremony is supported by:

A total of 64 winners from ITEs and Polytechnics received the award for the various categories. Our heartiest congratulations once again to all the winners! Please click **here** for the list of winners for 2020.

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.

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** (11 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. 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!

Week	Link Address
Week 1 Quiz	https://forms.office.com/r/XGHBUPQJJe or Scan the QR Code below
Week 2 Quiz	https://forms.office.com/r/gWsMr1ZfLs or Scan the QR Code below

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)!

Sign up now and receive an OTO Spinal Support worth $238!

Be a Global Certified Enterprise Architect for the New Digital Transformation Age

Be a Global Certified Enterprise Architect for the New Digital Transformation Age

Learn how to innovate faster and deliver values with less effort to accelerate digital transformation. With the right skills and capabilities, you can take digital transformation beyond IT and make a positive impact on the business performance through Enterprise Architecture (EA) training.

(IASA Digital Certification Badges)

IASA Certified EA courses:
1. Business IT Architecture Fundamentals
2. IASA Architecture Core (CITA-F)
3. IASA Business Technology Strategy (CITA-A) Part 1

4. IASA Specialisation (CITA-A) Part 2
Infrastructure Architecture
Solution Architecture
Information Architecture
Software Architecture
Business Architecture
(Online Instructor-Led Classes are available)
View **EA Training Roadmap**

Up to *90% funding support available for Singapore Citizens and Permanent Residents

ATD Training Subsidy
***Up to 30% off of the course fee for online training.**

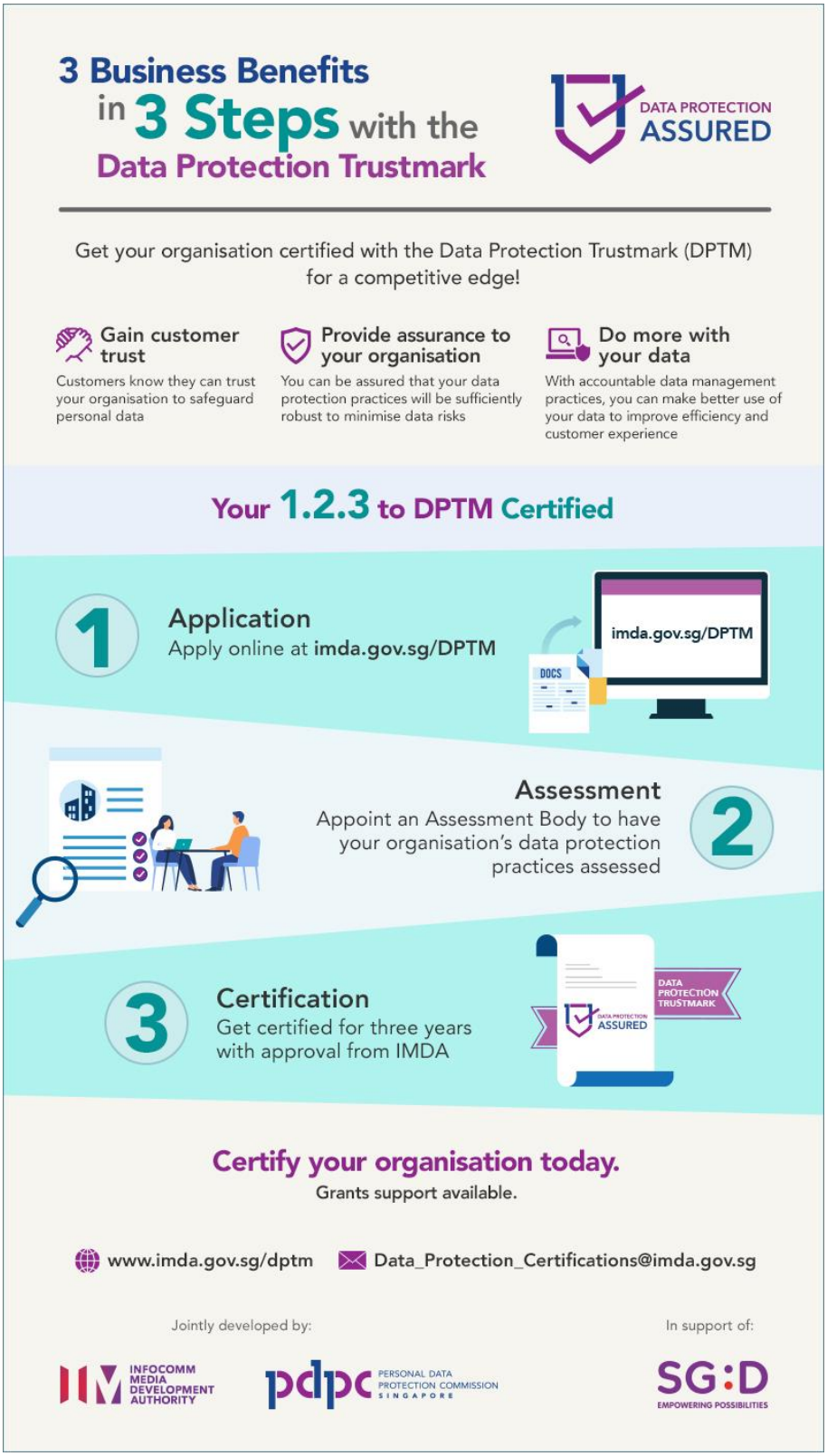
Government Assistance
- * Up to 90% funding support for Enterprise Architecture and ITIL®4 training.
- NTUC Training Fund (SEPs) and SkillsFuture Programs are available.

IBF's Financial Training Scheme (FTS)
Exclusive for Financial institutions, FinTech and Insurance companies.

Training Provider:
***Terms and conditions apply. Please contact** ATD Solution for more information.

For more information, please contact (Ms.) Audrey Loke at (65) 6386 0331 or email to audrey.loke@iasahome.org

Get your organization certified with the Data Protection Trustmark (DPTM)

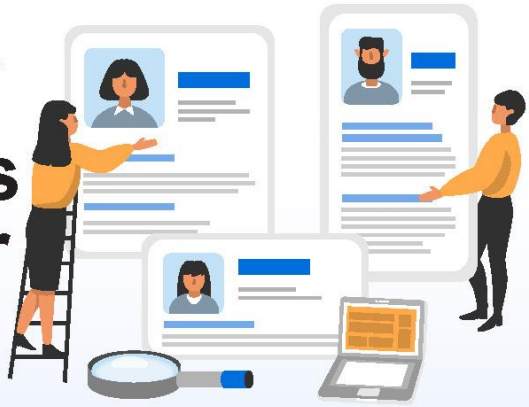


Career & Skills Discovery Fair

Organised by:

新加坡中華總商會 Singapore Chinese Chamber of Commerce & Industry

e2i



#SGUnited Career & Skills Discovery Fair

Virtual Career Fair + Physical Career Fair

In the post-COVID world, what candidates want in a job and what employers require have changed in the New Normal. Faced with skills mismatch and different expectations of candidates, companies need to rebuild their hiring strategy to recruit the right talent.

To provide a platform for companies to establish their corporate presence and meet potential hires, SCCCI and e2i are organising the SGUnited Career & Skills Discovery Fair in a Virtual and Physical format.

Virtual Career Fair

1st - 31st May 2021

uspur.e2i.com.sg

Physical Career Fair

11th May 2021
10am to 4pm

Devan Nair Institute for Employment and Employability
80 Jurong East Street 21 Singapore 609607

How to submit vacancies & participate?

Virtual Career Fair

- No minimum number of job openings required.
- Click here to download and complete the Vacancy Form for job openings to be listed.

Physical Career Fair

- **Minimum number of job openings: 10**
- **2 company representatives must be present during the entire session.**
- Participation is on a first-come-first-serve basis.
- Job openings will also be posted in the Virtual Career Fair.
- Click here to download and complete the Vacancy Form for job openings to be listed.

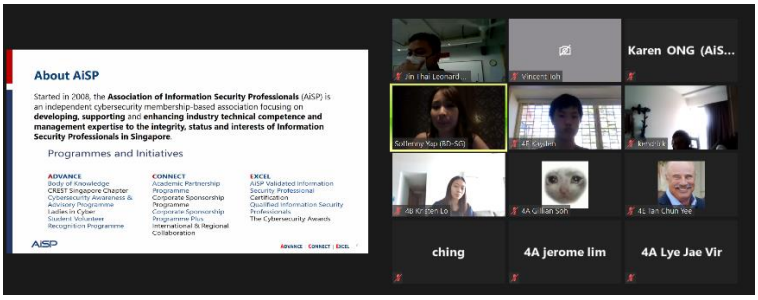
Completed Vacancy Form + High Resolution Company Logo
to be submitted through email **by 10th April 2021.**

For enquiries, please contact your respective Trade Association Representative.

Career Talk & Sharing in Schools

On 8 March 2021, our AiSP EXCO Co-opted Member, Mr David Siah shared with 25 students from Regent Secondary School on the information Technology & Cybersecurity Product Commercial roles as well as the career prospects and Singapore Cyber Youth Programme.

On 8 March 2021, our AiSP EXCO Co-opted Member & Co-Lead for Student Volunteer Recognition Programme (SVRP), Ms Soffenny Yap shared with 40 students from Fairfield Methodist Secondary School during the school Career Day Talk on Cybersecurity Roles and the career prospects as well as Singapore Cyber Youth Programme.



On 10 March 2021, our AiSP EXCO Co-opted Member & Co-Lead for Student Volunteer Recognition Programme (SVRP), Ms Soffenny Yap shared with students from Bedok Green Secondary School on the need for cybersecurity and the career prospects as well as Singapore Cyber Youth Programme.

Interested to have us in your school to share on the Professional in Cybersecurity or on the Student Volunteer Recognition Programme (SVRP). Please **email us** for more details!

Ladies in Cybersecurity

Ladies Talk Cyber Series

For the first edition of AiSP's 'Ladies Talk Cyber' series, we interviewed Sherin Y Lee, a specialist in one of Asia's largest pure-play cybersecurity services firm about her perceptions of the industry and how we can encourage more women to enter the field. Sherin was the founder for AiSP's Ladies in Cyber Charter launched in November 2018 and is currently serving in AiSP's Executive Committee as Vice President.

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

In our first edition, we sit down with Sherin, a marketing specialist from a Singapore headquartered pure-play cybersecurity services firm serving enterprises in Asia. Sherin is the Asia Pacific Head of Marketing, Brand and Communications for one of Asia's largest pure-play end-to-end cybersecurity service providers. As a Marketing Director, Sherin is passionate about bringing to market new cyber technologies and knowledge that can help solve problems in today's digital economy. She currently spearheads cybersecurity brand marketing initiatives aimed at capturing the audiences' imagination to achieve brand differentiation, as well as measurable results, for the company's cyber security services.

Please click here to view the full details of the interview.

Ladies in Cyber Fireside Chat with TrendMicro

As part of the International Woman Celebration 2021, AiSP organised the Ladies in Cyber Fireside Chat on 18 March 2021 held at TrendMicro office with students from various IHLs.

The panellists for the event were Ms Tin Pei Ling (Member of Parliament of MacPherson SMC), Ms Veronica Tan (Director, Safer Cyber Space of Cyber Security Agency of Singapore), Dr Ong Chen Hui (Cluster Director, Technology Development, Information Media and Development Agency), Ms Myla Pilao (Head of Technical Marketing, Core Technology, TrendMicro) moderated by Ms Sherin Y Lee (AISP Vice-President & Founder for Ladies in Cyber Charter Programme).

We had about 40 students that joined us physically for the session and about 50 mentors & students that joined us virtually in this hybrid event. We would like to thank our Sponsors Ensign InfoSecurity and TrendMicro for their kind sponsorship to make this event possible.

Our next AiSP Ladies in Cyber Event will be held on 31 May 21 where we will have 2 of our mentors and 2 speakers from Israel Cyber Together sharing on the Technical and Non-Technical issues of Cybersecurity. Contact secretariat@aisp.sg for more details on how you can be involved and be part of the event.

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!

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.

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.

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.

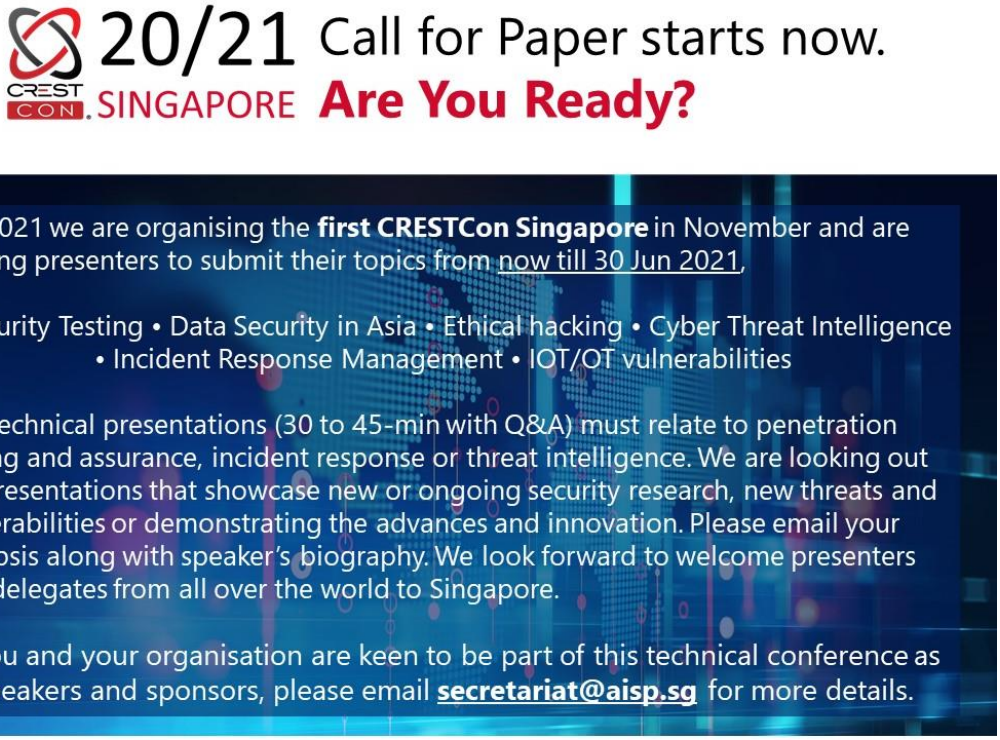
CREST SINGAPORE CHAPTER

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 had resume since February 2021. Please click here for the exam schedule for 2021.

CRESTCon Singapore 2020/2021

The CREST Singapore Chapter is organising the **first CRESTCon Singapore 2020/2021** in November 2021 and is now calling for paper submission till 30 Jun 2021. Please **email secretariat** if your organisation is keen to sponsor the event!



AiSP Association of Information Security Professionals | CYBER FEST

The AiSP **CyberFest™** is a series of cybersecurity events and initiatives that take place from 8 to 12 November 2021 in Singapore.

Connect with us on LinkedIn, Facebook and Instagram today.

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**
Feb-May	Call for Nomination for The Cybersecurity Awards 2021	**AiSP**
Feb-Jun	Call for Paper Submission for CRESTCon Singapore 20/21	**AiSP CREST SG**

Upcoming Events

Date	Event	By
7-Apr	Tanjong Katong Secondary School Talk	Partner
9-Apr	Greenridge Secondary School Talk	Partner
14-Apr	**Knowledge Series – Software Security & MOU signing with Div0**	**AiSP & Partner**
16-Apr	Cyber Attack 2021- Panel	Partner
20-Apr	**Job opportunities in the Cybersecurity Sector (Facebook Live)**	**AiSP & Partner**
1 – 31 May	SGUnited Career & Skills Discovery Fair by SCCCI	Partner
4 - 7 May	Black Hat Asia Virtual	Partner
12-May	**Knowledge Series – Physical Security, Business Continuity and Audit**	**AiSP & Partner**
21-May	**SBF Focus Group Discussion**	**AiSP & Partner**
25-May	**Punggol Digital District Industry Event**	**AiSP & Partner**
28-May	Focus Group with People Association Leaders	Partner
31-May	**Ladies in Cyber Session with Cyber Together**	**AiSP & Partner**

***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 our new Corporate Partner Programme (CPP) – FireEye

"The invisible risk to supply chain and why it is a top security priority"

By Yuh Woei Tan, Vice President, ASEAN, FireEye

In December 2020, FireEye revealed the details of a sophisticated threat actor that took advantage of SolarWinds' Orion Platform to orchestrate a wide-scale supply chain attack and deploy a backdoor we call SUNBURST. This attack impacted organizations worldwide, leading executives to question whether their environment fell victim. Many rushed to quickly identify SolarWinds assets within their environment and determine potential impact.

Working from our first-hand experience, we observed the threat actors' techniques and quickly moved to identify similar activities within our customers' environments. This is a natural progression of threat intel leading to actionable direct threat hunting missions daily within our Managed Detection and Response (MDR) service offerings. Mandiant is on the front lines of incident response around the globe, and our investigative findings quickly make their way into the workflow of our hunting team.

Today, organizations are struggling to catch up to ever-increasing demands for new services, new capabilities and better customer facing goodness, teams are looking to leverage and integrate more third-party developed offerings in order to meet tight deadlines. The risk to internal systems is higher than it was in the pre-COVID world.

As these components become fully intertwined with internal systems, it becomes harder to identify individual sources that impact their security. More importantly, it clearly highlights dependencies and risks from this supply chain.

Ultimately, while organizations have many formalized partnerships, there may be many more that are not reviewed and are not part of a centralized procurement. These completely circumvent any security audit or even basic identification. Even approved vendors and technology partners can be exposed to an undocumented supply chain, since they also leverage solutions and code from other third parties in their own hopes to better serve us and do so more quickly. This process is further exacerbated as organizations look to leverage more cloud-based capabilities and code.

How can we protect these internal systems?

It is practically impossible to review and exhaustively test every single line of code that has been introduced in application or service. This is like the alert overload problem most security teams experience in their day-to-day operation.

However, like the security teams who use an intelligence-based approach, it's also important to streamline the process of critical threat identification and take steps ahead to minimize supply chain risk. As a starting point, there are many fewer vendors, partners and third-party sources of code and services than there are lines of code. While documenting these relationships will not be a simple task that can be achieved in a few days, it is a human-scale task and it can be improved over time as awareness of the need to document these relationships becomes more prevalent and integrated in various activities.

Once these relationships begin to be documented, they can be monitored for issues, reputation, brand and other concerns by scanning for news stories, articles and mentions in forums and other sites about the organization itself, the third parties that are part of their supply chain, their key executives, contributing personnel and more.

While this effort can be a tedious undertaking if performed manually, service providers are available that offer this insight. While organizations use these brand monitoring and threat detection services internally for their brands and key personnel, it can be extended to partners, third parties and few vendors to establish top security for the entire internal system.

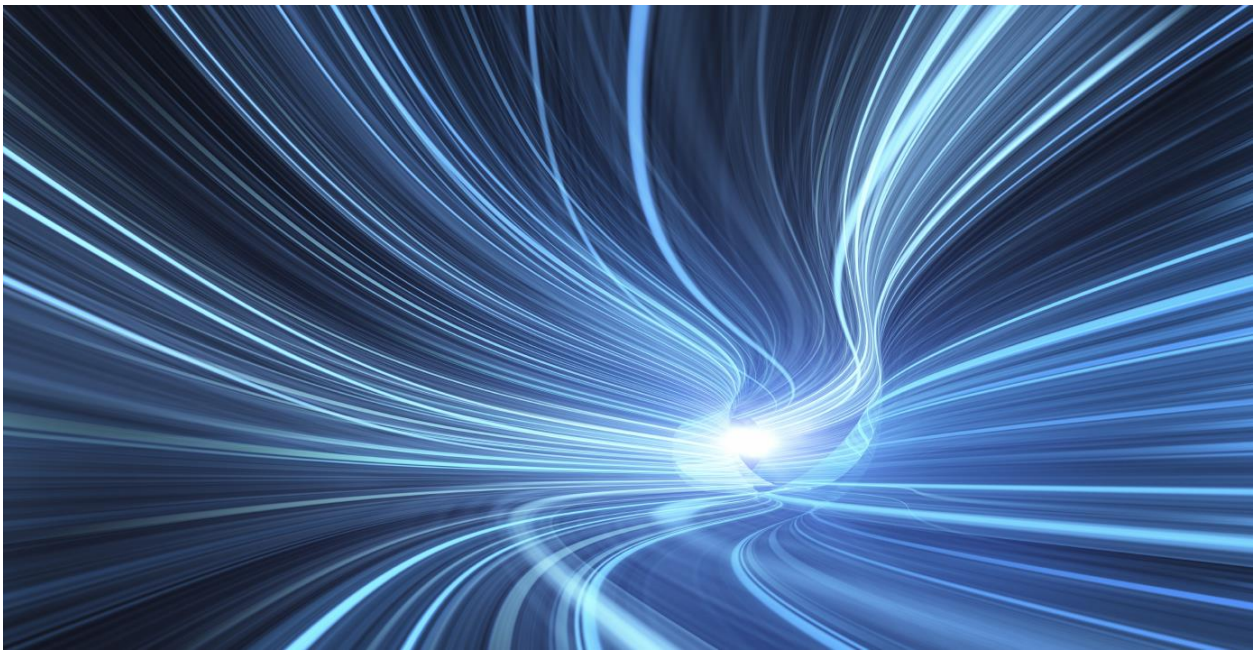
The combination of threat intelligence data and monitoring issues by placing all the components in line will help organizations develop a 360-degree view of any potential threat across the system. It will provide ease to regularly update the risk score and quickly identify any concerns before they hit to a critical level. This is a scalable approach to mitigate and work towards the potential risk landscape.

Conclusion

As the world is gearing towards preparing itself for the adversaries caused by the global pandemic every single day, securing these internal systems, the supply chain networks including externally connected vendor systems will be a tedious but scalable approach to protect the entire supply chain ecosystem of the organization.

CONTRIBUTED CONTENTS

Insights from our Sponsor for The Cybersecurity Awards 2020 – Thales



CryptoAgility to take advantage of Quantum Computing

Authors:

	
Mr. Welland Chu *Ph.D, CISA, CISM* (Welland.Chu@thalesgroup.com) Business Development Director, Asia Pacific	Mr. Rana Gupta (Rana.Gupta@thalesgroup.com) Vice President, Asia Pacific Sales & Services, Thales

Threat or Opportunity?

Every change brings along the aspect of disrupting the current set of ecosystem and practices and hence providing an opportunity to doing something differently and hopefully in a better way. The key lies in being able to sense the change on the horizon and getting ready to embrace the change.

The same goes with the advent of Quantum Computing that is supposed to bring exponential computing power that shall not only bring endless benefits but also raises question marks on the current state of cryptography that is the bedrock of all information security as we know today.

What is quantum computing and what changes will it bring?

While classical computers use "0" and "1" to represent 2 distinctive states of a bit of information, quantum computers leverages the properties of the "Uncertainty Principle", "Superposition", "Entanglement" of quantum bits (Qbit), so that their respective "0" and "1" can exist at the same time, with a different probability and in a correlated fashion. When a few Qbit interact together, the probability of each bit being a "0" or "1" can be expressed as a vector. When a measurement is taken, the function collapsed according to the applied programmed condition and you end up with the most likely result. (You'd probably do the computation a few times, supplemented by further checking using a classical computer, to make sure you arrive at the same result). To put into context, a 3-bit classical computer can express 1 value out of 8 combinations. A 3-Qbit quantum computer, however, can express 8 different possible combinations all at once. A 300-Qbit quantum computer (if and when it becomes a reality), you'd end up with a number of possibilities that is larger than the number of atoms in the observable universe (estimated to be 10^{78} to 10^{82} atoms).

This vast amount of new computing power is useful for many applications, eg. from modeling how molecules interact with one another, thus speeding up the development of new drugs and materials, to predicting traffic, weather and possibilities of the earthquakes occurrence, etc. One particular application of quantum computer is to solve some hard mathematical problems, like finding the prime factors of large numbers. Take for example, if you are asked to calculate the factors of the current year "2021", you may do this by dividing 2021 with 2, then 3, … until you reach the number 43, which gives you the result of 43 x 47 = 2021. A 4-digit number "2021" may not sound too difficult for a classical computer to factorize, but you may start to push to the limit of most classical computers if the number to be factorized is as large as 1.3×10^{154} (which represents a 512-bit number). This kind of hard mathematical problem is exactly what our traditional public key cryptography such as RSA (which works with prime factors) and DSA, Diffie-Hellman, and Elliptic-Curve (which work with discrete logarithm problems) has been based upon, and there lies the security foundation of today's of e-Commerce, digital identities, etc. By using a sufficiently powerful quantum computer running Shor's algorithms, named after the mathematician, you may be able to solve these traditionally hard mathematical problems in a matter of days or even hours. With the advent of quantum computing, the security that protects the digital identities and internet communications (SSL/TLS) of our modern society is thus significantly weakened.

What risks will this entail?

When access to this computing power falls to the wrong hand, what we have taken for granted, such as mobile banking, e-Shopping, IOT, traffic light control, electricity distribution will become vulnerable to device take-over as they are not strong enough to resist a quantum attack.

- If communications in electronic banking are compromised, thus leaking customers' transactions to the public, that can trigger a bank run as few customer would put their trust and their money in a bank that cannot keep their secret
- The situation may soon turn into a life-and-death situation if some medical IOT devices have their identities compromised and allowed malware to take control of the devices. Receiving a ransomware demand from one's pacemaker is certainly the last thing a patient would want to hear.
- Government and defense sectors should be alarmed most by the threat. While an adversary may not be able to crack the cryptographic codes that are used to protect communications at present, these actors can hoard the information now and analyse the encrypted data when the means to crack the cryptography is available. Compromising such secrets will jeopardize national security.

How much time do we have?

Current advancement in quantum computing is restrained by the delicate operation required of the quantum device. To reduce the noise of the device, the operation needs specialized environments that will be cooled to 0.015 Kelvin (colder than outer space) and the device be placed in a high vacuum to 10 billion times lower than atmospheric pressure. So if you want to operate a 1,000 logical Qbit computer in a stable condition, you may need to build a quantum computer with 1 million physical Qbits. Experts in this field predict that it may take another 5-20 years before quantum computing can become practically useable. While there is no need to panic – the proper path to take is not to stop advancement in Quantum Computing but to challenge the frontiers of Cryptography and Information Security as we may know today.

What shall we do to get ready?

There are 3 areas that risk owners, CISO and system architects should look into:

1. **Crypto-Agile Implementation with Quantum-safe algorithm**: Components relying on digital certificates and have a life-span extending into the quantum era should safely migrate from the current cryptography to the use of quantum-safe algorithms. In the imminent anticipation of Quantum Computing's arrival, you would want to be in a position to be able to make quick changes that forces the applications to switch over to either using quantum-safe algorithms or larger sized keys (this is in line with the crypto-agility requirements as stated in Cybersecurity Labelling Scheme of Cyber Security Agency of Singapore). A drop-in replacement for RSA, ECDSA, ECDH and ECIES is an option to consider.
   Thales recommendations: Becoming crypto-agile is critical to protecting and securing data and fending off new threats. The Luna HSM Post Quantum Crypto Functionality Module (FM) utilizes the ISARA Radiate™ Quantum-safe Toolkit and allows for quantum-safe signatures to be used for code-signing today. This implementation includes mechanisms for key compression that are optimized for either speed or for size to help ensure that the

private key is optimally stored and used in an operational environment with different requirements. Certificate authorities, document signing and firmware code signing that have a longer life-span than 5 year (lower-limit of quantum arrival) should start the migration.

2. **Quantum random number generation**: It has to be stressed that random number generators based on a quantum process are not normally used on its own, partly because few certification scheme accept the output of a QRNG device to be used directly. Rather, the resulting high entropy of the random number generated by a quantum source is suitable to re-seed a certified Deterministic Random Bit Generator algorithm on a frequent basis.
   Thales recommendations: Luna HSM provides an API which can mix in external entropy and there is an out of the box integration where an iDQ device can be used to provide additional entropy to the HSM which will be mixed with internal entropy sources.
3. **Quantum key distribution**: It is envisaged that the arrival of Quantum Computing will have much more impact on the Public Key Cryptography as compared to the Symmetric Cryptography. Public Key Cryptography is mostly used for the purpose of Key Distribution and hence securing Key Distribution mechanisms shall be considered as first priority. There is a possibility that the encrypted data streams are being recorded and stored NOW to have those interpreted as and when the Quantum Computing power becomes available in order to decrypt the data in future. This can be highly problematic for those scenarios whereby the information must remain confidential for 20-years or more.
   Thales recommendations: Thales High-Speed network encryptors incorporate both quantum random number generation and quantum key distribution. These quantum-ready encryptors should be specified for use in all networks where highly sensitive data are in transit.

Conclusions: Preparedness is the key

Although post-quantum is projected to be a few years away, any enterprises or government agencies that rely on digital trust must start planning today to be post-quantum ready. The authors would encourage the readers to take our free risk assessment to learn if your organization is at risk of a post-quantum breach. Having gained the situational awareness, users can then start to strategise their post-quantum implementation plan.

The authors would like to acknowledge valuable discussions with Michael Gardiner of Thales.
Readers are also welcome to share thoughts on the subject with the authors.

MEMBERSHIP

Type	Benefits
Individual Membership	▪ Recognition as a Trusted Infocomm Security Professional. You can use the designation of AVIP (AiSP Validated Information Security Professionals) or MAISP (Ordinary Member) as your credentials. ▪ Regular updates on membership activities. ▪ Free and discounted rates for events organised by AiSP and partners. ▪ One-time discount for QISP® examination fee for Affiliate members who are working professionals. ▪ Priority for activities, talks and networking events. ▪ AVIP members enjoy Professional Indemnity coverage in Singapore and overseas.
Corporate Partner Programme (CPP)	▪ Listing on AiSP website as a Corporate Partner ▪ Free and discounted rates for events organised by AiSP and partners. ▪ Complimentary AiSP Affiliate membership for organisation's personnel. ▪ Special invite as speakers for AiSP events. ▪ One complimentary job advertisement or knowledge-sharing article on AiSP platform per month (i.e. a total of 12 ads or articles in a year).
Academic Partnership Programme (APP)	▪ Inclusion of an AiSP Student Chapter for the Institute. ▪ Ten (10) complimentary AiSP Affiliate membership for personnel from the Institute. ▪ Complimentary AiSP Affiliate membership for all existing full-time students in the Institute, not limiting to cyber/infosec domains. ▪ Listing on AiSP website as an Academic Partner. ▪ One annual review of Institute's cybersecurity course curriculum. ▪ AiSP speakers to speak at Student Chapter events, including briefings and career talks. ▪ Free and discounted rates for events organised by AiSP and partners. ▪ One complimentary info/cybersecurity or internship post in AiSP website per month.

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 Jul 2020 to 30 Jun 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 **WhatsApp** (+65 6247 9552).

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 Eventbank, 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

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 during Phase 3. We are currently telecommuting.

Please email us or message us via WhatsApp at +65 6247 9552.

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.

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