AiSP
Association of
Information Security Professionals

NEWSLETTER
August 2021

NEWS & UPDATE

AiSP New Corporate Partners

AiSP would like to welcome BD, Checkmarx and Marsh as our new Corporate Partners. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem in 2021.

AiSP New Collaboration Partner

With effect from 1 Aug 21, AiSP has chosen WebEx as an official collaboration partner, enabling collaboration within the team as well as with its members. WebEx is a leading provider of cloud-based collaboration solutions which includes video meetings, calling, messaging, events, customer experience solutions like contact center and purpose-built collaboration devices.

The WebEx platform will be integrated into the AiSP team's day-to-day activities to drive collaboration, as well as with the AiSP members through webinars and other online engagements.

MOU WITH HTCIA Singapore Chapter

AiSP and HTCIA Singapore Chapter had signed a Memorandum of Understanding (MOU) that provides a foundation to work collaboratively on events that will contribute to the cybersecurity ecosystem. The MOU signed by Mr Pravin P Arvyta (HTCIA Singapore Chapter President) and Mr Johnny Kho (AiSP President) aims to focus on developing cybersecurity talents and providing more opportunities for collective partnerships to benefit members from both AiSP and HTCIA.

AiSP Knowledge Series Events

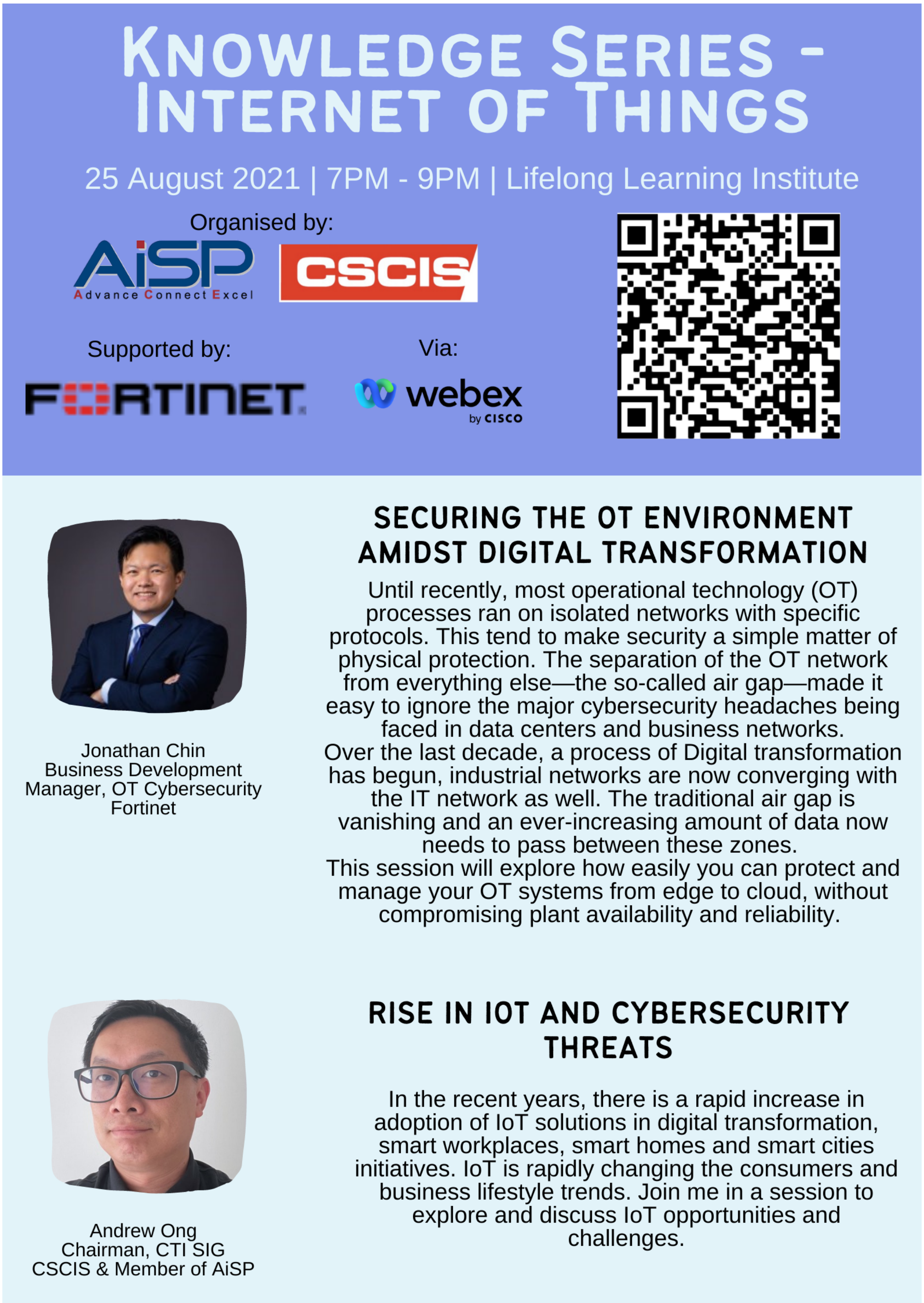
Cyber Defence

In partnership with HTCIA Singapore Chapter and Tufin, AiSP would like to thank all participants who have joined the event on 14 July both virtually and physically. During the event, Mr Henry Pea (Tufin) gave an interesting sharing on the Blueprint for Zero-Trust Networks and Ms Catherine Lee, Mr Darren Cerasi and Mr Bryan Tan from HTCIA Singapore Chapter were the speakers for the topic on Expert Witness Testimony in Digital Forensics.

Blueprint For Zero-Trust Networks
Henry Pea
Sales Engineering Director, APAC
tufin
tufin

Our next Knowledge Series will be on Internet of Things (IOT) on 25 Aug 21

To sign up, please click here



Knowledge Series - Internet of Things

25 August 2021 | 7PM - 9PM | Lifelong Learning Institute

Organised by:

Supported by:

Via:

SECURING THE OT ENVIRONMENT AMIDST DIGITAL TRANSFORMATION

Until recently, most operational technology (OT) processes ran on isolated networks with specific protocols. This tend to make security a simple matter of physical protection. The separation of the OT network from everything else—the so-called air gap—made it easy to ignore the major cybersecurity headaches being faced in data centers and business networks.
Over the last decade, a process of Digital transformation has begun, industrial networks are now converging with the IT network as well. The traditional air gap is vanishing and an ever-increasing amount of data now needs to pass between these zones.
This session will explore how easily you can protect and manage your OT systems from edge to cloud, without compromising plant availability and reliability.

Jonathan Chin
Business Development Manager, OT Cybersecurity
Fortinet

RISE IN IOT AND CYBERSECURITY THREATS

In the recent years, there is a rapid increase in adoption of IoT solutions in digital transformation, smart workplaces, smart homes and smart cities initiatives. IoT is rapidly changing the consumers and business lifestyle trends. Join me in a session to explore and discuss IoT opportunities and challenges.

Andrew Ong
Chairman, CTI SIG
CSCIS & Member of AiSP

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. OT/IOT – IoT Security, 25 Aug (hybrid*)
2. Operation and Infrastructure Security, 15 Sep
3. CTI SIG, 29 Sep (hybrid*)
4. Security Operations – Incident Response Management, 13 Oct
5. 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 & 2022!

AiSP members who registered for the event, can playback the recorded event via their member profile in Glue Up. If you did not sign up for the event, please email secretariat@aisp.sg for assistance. Please refer to our scheduled 2021 webinars in our **event calendar**.

Association of Information Security Professionals
Be Part of Our Events
AiSP Advance Connect Excel
AiSP Advance Connect Excel

THE CYBERSECURITY 2021 Awards

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

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

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

OFFICIAL (ISC)² CHAPTER SINGAPORE

SINGAPORE SCS 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

Centre for Strategic Infocomm Technologies CSIT

DBS

kaspersky

Singtel

wizlynx group

Silver Sponsors

PCS SECURITY

RSA

SIT SINGAPORE INSTITUTE OF TECHNOLOGY

THALES

wsg Workforce Singapore

Cybersecurity Awareness & Advisory Programme (CAAP)

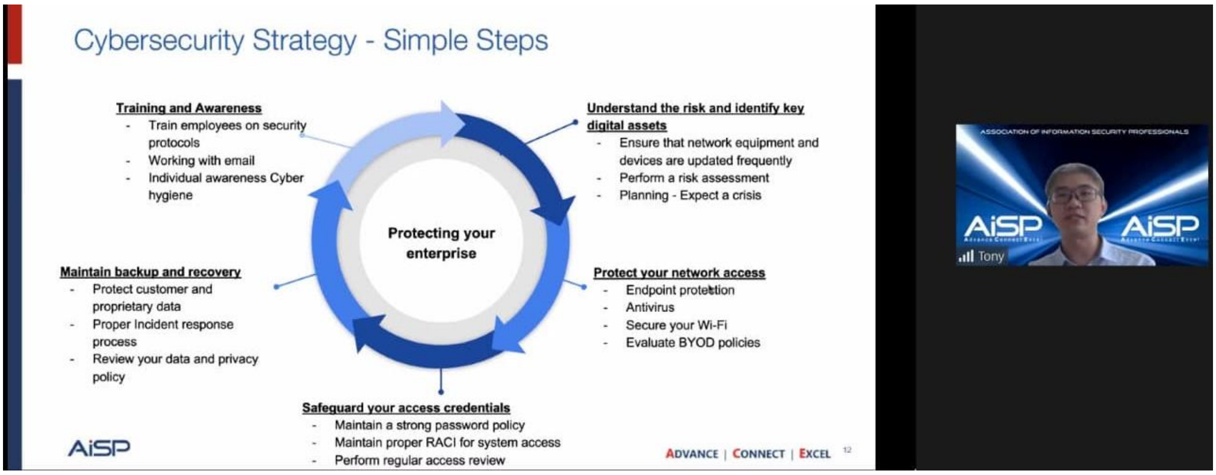
Fortify Your Company's Cyber Security

On 7 July 21, AiSP and SCCCI came together to organise a webinar for SCCCI Members. Fortify your Company's Cyber Security has concluded on a good note with sharing from Mr Tony Low (CAAP Chair, AiSP), Mr Jonas Walker (Security Strategiest, Fortinet), Mr Luke Chung (Senior Manager, VSS Engineering), Ms Tia Asihwardji (SB Commercial Lead, Trend Micro) and Ms Veronica Tan (Director, Safer Cyber Safe of Cyber Security Agency of Singapore). Engaged in the interesting topics that were discussed, participants gained valuable insights which they could apply to their workplaces.

ASSOCIATION OF INFORMATION SECURITY PROFESSIONALS
AiSP Advance Connect Excel
Tony Low
CSA SINGAPORE
SG
CSA - Veronica Tan
VSS - Luke Chung
Fortinet - Jonas Walker
TrendMicro - Tia Asihwardji
SCCCI - Chris Foo

Cybersecurity Awareness Workshop on 27 July

With the current P2HA, the CAAP event has shifted to virtual, but this does not drown the passion of our speakers Mr Tony Low (CAAP Chair) and Mr Collin Chow (Director, Root Security Pte Ltd representing Thales) from sharing their profession and insights in Cybersecurity. Mr Nicholas Yong (Transformist) shared information on Cybersecurity courses during the session which offers participants an avenue to learn more about this field. We would like to thank Thales and Root Security for their strong support to make this talk possible.



Cybersecurity Strategy - Simple Steps

Protecting your enterprise

Training and Awareness
- Train employees on security protocols
- Working with email
- Individual awareness Cyber hygiene

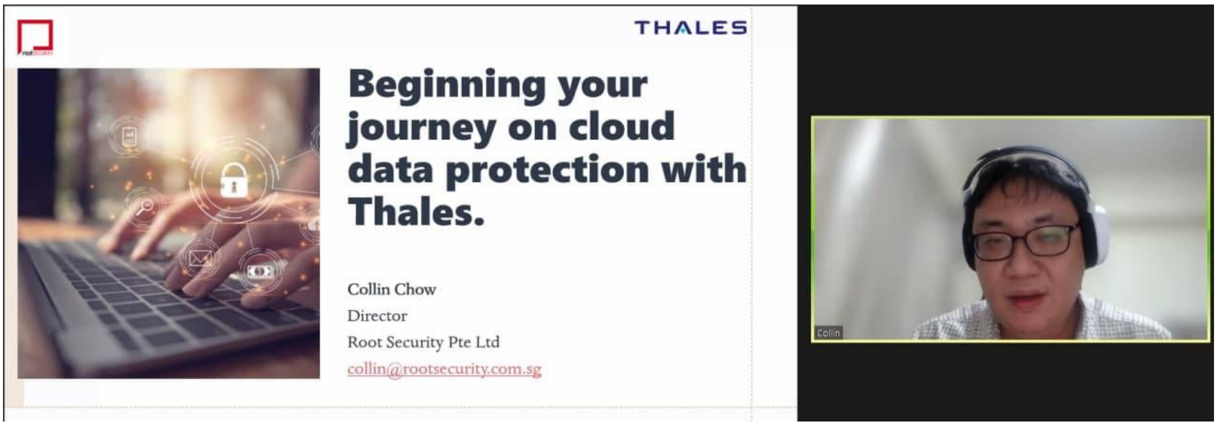
Understand the risk and identify key digital assets
- Ensure that network equipment and devices are updated frequently
- Perform a risk assessment
- Planning - Expect a crisis

Maintain backup and recovery
- Protect customer and proprietary data
- Proper Incident response process
- Review your data and privacy policy

Protect your network access
- Endpoint protection
- Antivirus
- Secure your Wi-Fi
- Evaluate BYOD policies

Safeguard your access credentials
- Maintain a strong password policy
- Maintain proper RACI for system access
- Perform regular access review

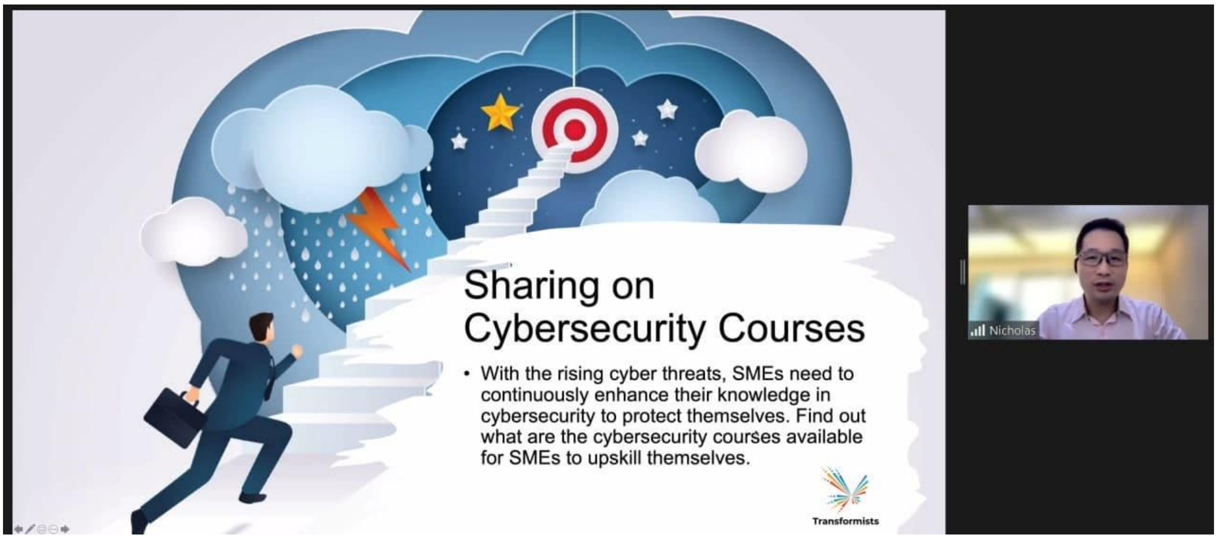
AiSP ADVANCE | CONNECT | EXCEL 12



THALES

Beginning your journey on cloud data protection with Thales.

Collin Chow
Director
Root Security Pte Ltd
collin@rootsecurity.com.sg



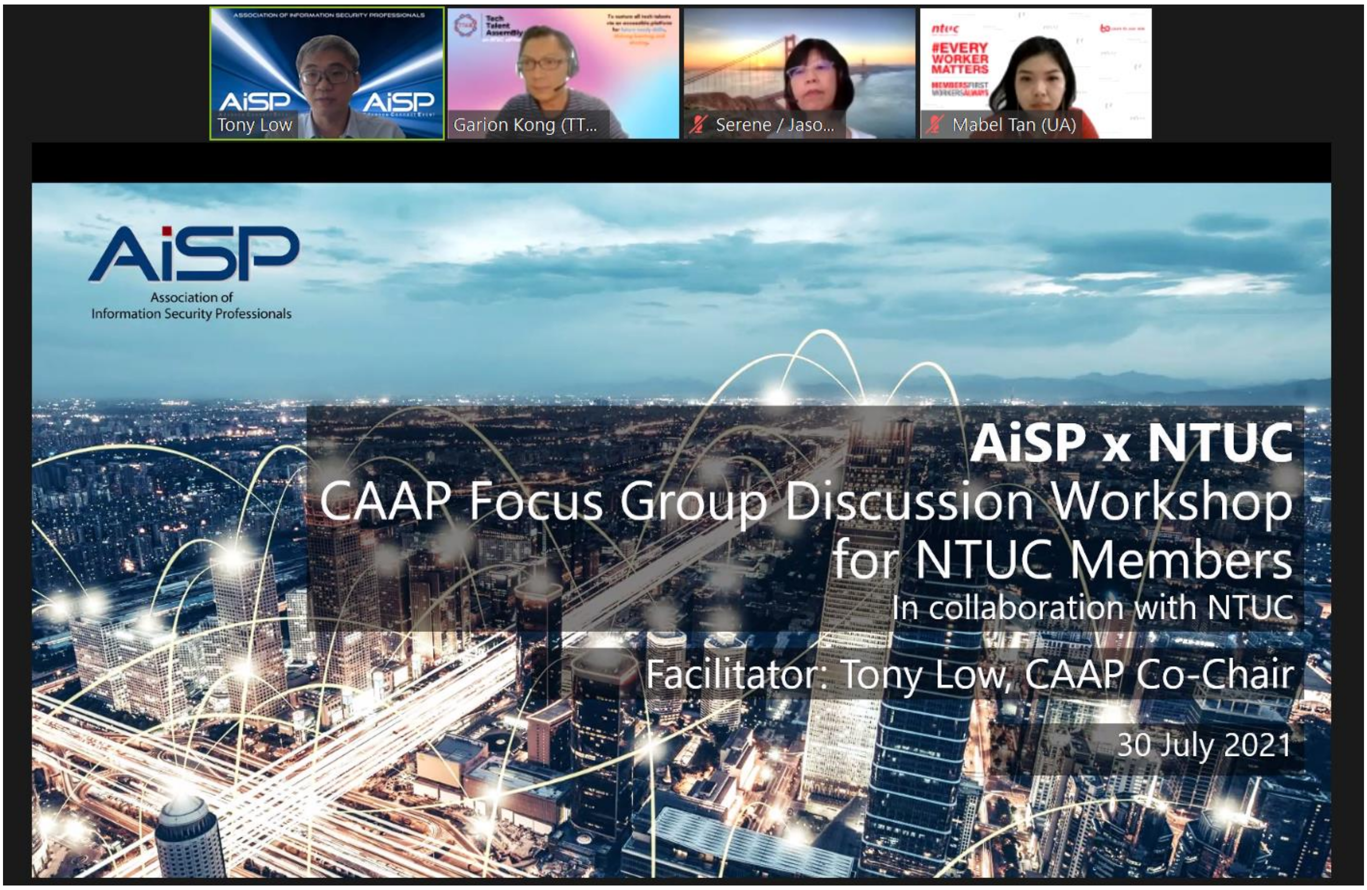
Sharing on Cybersecurity Courses

- 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.

Transformists

AiSP x NTUC Cybersecurity Awareness Programme (CAAP) Focus Group Discussion

On 30 July, CAAP Focus Group Discussion was held for **National Trades Union Congress (NTUC)** and **Tech Talent AssemBly** members in collaboration with NTUC. The workshop was facilitated by **Tony Low** (CAAP Chair) discussed topics such as immediate concerns arising from cyber threats, cybersecurity incidents in companies and importance of cybersecurity for business. We would like to thank all participants who joined us for the discussion.



AiSP x NTUC
CAAP Focus Group Discussion Workshop for NTUC Members
In collaboration with NTUC
Facilitator: Tony Low, CAAP Co-Chair
30 July 2021

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.

1. 8 Sep 21 – AiSP x PA CAAP Focus Group Discussion
2. 9 Sep 21 – AiSP x SCS CAAP Focus Group Discussion
3. 20 Oct 21 – AiSP x ASPRI Cybersecurity Awareness Workshop
4. 11 Nov 21 – AiSP SME Conference 2021

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

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

Singapore SMEs' Digital Adoption and Concerns
| 08 Sept 2021 |
| 7PM - 9PM |
| Ensign InfoSecurity Office |
Sherin Y Lee
Vice Preisdent
AiSP
Organised by:
AiSP
Association of Information Security Professionals
People's Association

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

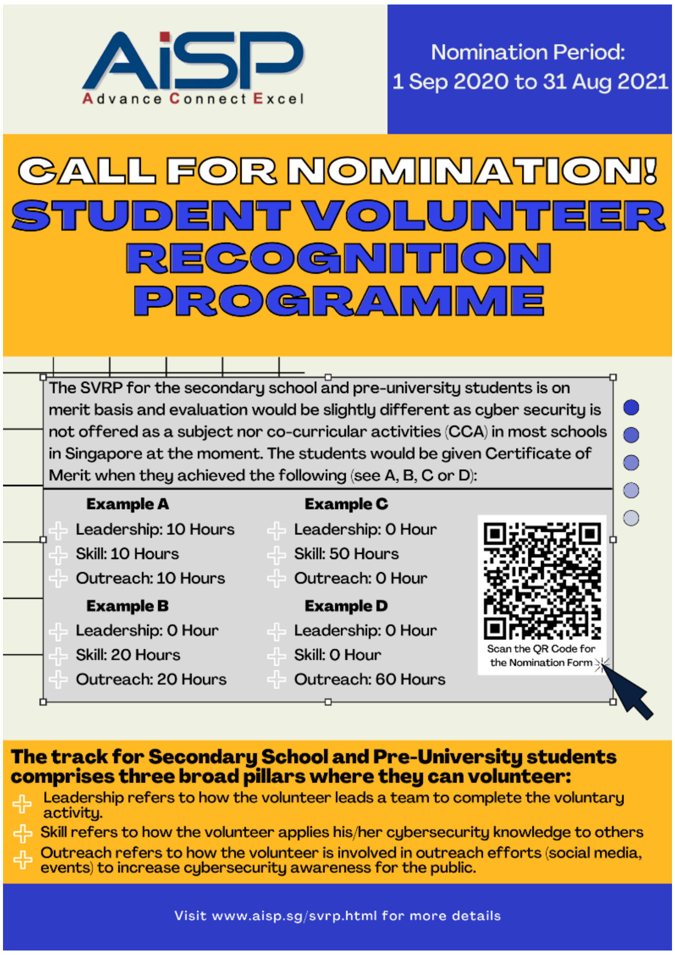
In partnership with PA's Emergency Preparedness Division and Association of Information Security Professionals, this focus group discussion aims at raising SMEs' awareness of cyber risks and adoption of cyber practices. It caters to SMEs across industries, particularly those not in the IT fields to better protect your businesses in the cyber space.

Join us in this focus group discussion as we discuss together about the immediate concerns arising from rising cyber threats, concerns about cybersecurity incidents in companies and sentiments about the importance of cybersecurity for your business from your management and staff.

Date: 08 Sept 2021 (Wed)
Time: 7.00pm to 9.00pm
Venue: Ensign InfoSecurity, 30A Kallang Place, #08-01, Singapore 339213
Registration: forms.office.com/r/msWyEmt7s1

Student Volunteer Recognition Programme (SVRP)

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.



AiSP Advance Connect Excel

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
- Leadership: 10 Hours
- Skill: 10 Hours
- Outreach: 10 Hours

Example B
- Leadership: 0 Hour
- Skill: 20 Hours
- Outreach: 20 Hours

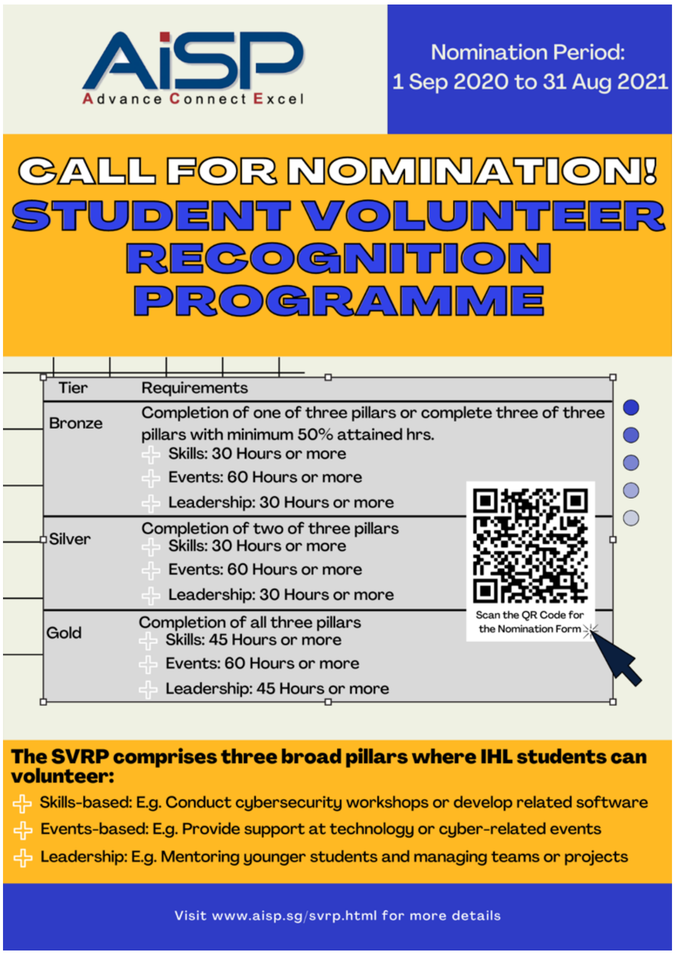
Example C
- Leadership: 0 Hour
- Skill: 50 Hours
- Outreach: 0 Hour

Example D
- Leadership: 0 Hour
- Skill: 0 Hour
- 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/svrp.html for more details



AiSP Advance Connect Excel

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/svrp.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!

Week 1 Quiz https://forms.office.com/r/XGHBUPQJJe	Week 2 Quiz https://forms.office.com/r/gWsMr1ZfLs
Week 3 Quiz https://forms.office.com/r/ikiwzBiSnV	Week 4 Quiz https://forms.office.com/r/C0XdFvtqcs
Week 5 Quiz https://forms.office.com/r/bPYdNn3Ytm	Week 6 Quiz https://forms.office.com/r/gmgSSn2syS
Week 7 Quiz https://forms.office.com/r/dV0m8WmvHP	Week 8 Quiz https://forms.office.com/r/9B9ifeCibT
Week 9 Quiz https://forms.office.com/r/1fx4XZq8fx	Week 10 Quiz https://forms.office.com/r/QTgzkfkckJ

Week 11 Quiz https://forms.office.com/r/iKTdAXy4Wc	Week 12 Quiz https://forms.office.com/r/G60xJEqHpb
Week 13 Quiz https://forms.office.com/r/FrwapxXVZP	Week 14 Quiz https://forms.office.com/r/ruKgZ3XaUp
Week 15 Quiz https://forms.office.com/r/5B4Wq1LqZS	Week 16 Quiz https://forms.office.com/r/x880GsNhNs
Week 17 Quiz https://forms.office.com/r/TnfYnVEWhc	Week 18 Quiz https://forms.office.com/r/PUuZKeK7xa
Week 19 Quiz https://forms.office.com/r/AKLFC1HGay	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)!

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

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: associate an NTUC initiative | AiSP Association of Information Security Professionals

FairPrice Unity	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^
Foodfare	Up to **15% OFF*** NTUC Value Meals
Foodfare KOPITIAM	**$0.50 Hot Kopi/Teh*** on Wednesdays at NTUC Foodfare as well as Kopitiam Food courts and coffee shops **$1.80** Breakfast Set*
Health	Flash NTUC Plus! Card for **members' rates**
income	Enjoy premium rates for as low as **$0.70/day*** with LUV Term Life Insurance
my first skool	Get **$102 worth of LinkPoints*** per year when you enrol your child
plus!	Earn and redeem LinkPoints at over 1,200 merchant outlets!
Club	NTUC Club – the club for union members! Enjoy **special privileges** at Wild Wild Wet, Marina Bay Golf Course, Orchid Bowl and more!

MHC A BetterHealth Company	Available on BetterHealth mobile app: • **$10*** GP Teleconsultation • **$12*** GP Consultation
GetDocPlus	One-year **FREE*** subscription to access GetDocPlus mobile app
sembcorp	Get up to **$60*** electricity bill rebates
StarHub	**20% OFF*** monthly mobile subscription
foodpanda	**$8 OFF*** with min. spend of $15 at foodpanda or pandamart *(for new users only)*
WhyQ	• **$6 OFF* first order** *(for new users only, capped at the first 2,000 redemptions)* • **$8 OFF*** with min. spend of $15 *(for existing users, capped at 3 redemptions per user)*

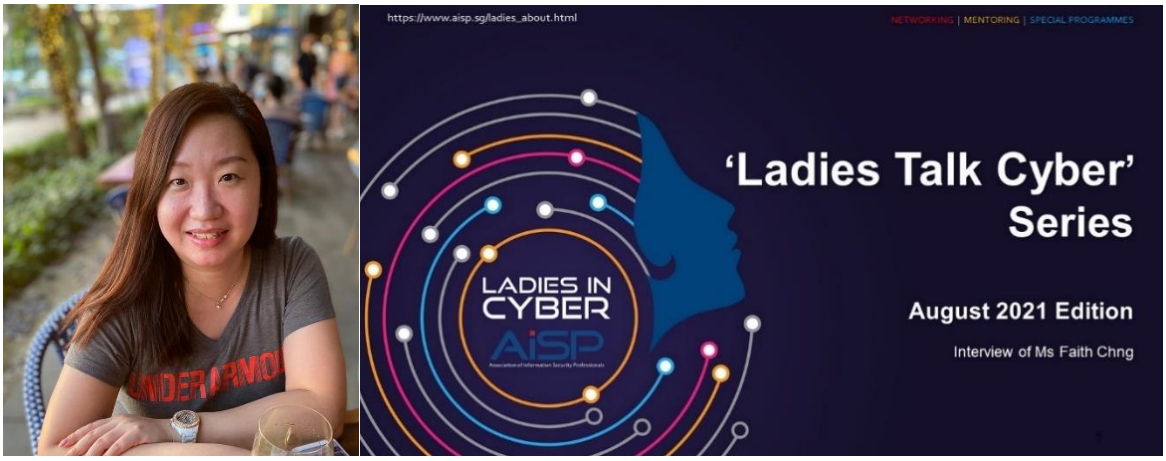
Flash your NTUC Plus! Card for members' rates*

FULLERTON HEALTH · Healthway Medical · Parkway Shenton · RafflesMedical · THOMSON PARENTCRAFT CENTRE · unity denticare

And many more!

Visit **ntucmembership.sg** to discover more savings!

Ladies in Cybersecurity


https://www.aisp.sg/ladies_about.html
NETWORKING | MENTORING | SPECIAL PROGRAMMES
'Ladies Talk Cyber' Series
August 2021 Edition
Interview of Ms Faith Chng
LADIES IN CYBER
AiSP

Ladies Talk Cyber Series

For the Fourth edition of AiSP's 'Ladies Talk Cyber' series, we interviewed Faith Chng, who is the Associate Director at Trustwave. She shared on her experiences with Trustwave 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

Faith is an associate director handling product management in APJ. The product management role includes conceptualising, developing and launching new services for that will be useful and beneficial to enterprises. She also developed Go-To-market strategies to target the right audiences to grow sales leads and revenue for Trustwave. In short, she manages the whole lifecycle of a product or service offering from beginning to end-of-life.

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

Join Faith on 1 Sep 21 at 7pm via Zoom as part of International Women in Cyber Day - Spill the Tea session with prominent speakers in a insightful sharing on what our speakers have to say on their personal experience in cybersecurity and working life and the reason why they are still in this industry and how they are coping between work and their personal life in the current situation and what they hope to achieve.

Contact AiSP secretariat@aisp.sg if you wish to be part of it.

AiSP Ladies in Cyber Learning Journey at Ensign InfoSecurity on 13 July 2021

Gender diversity benefits most industries, and it's especially important in the cybersecurity sector. To encourage more women to join this field, AiSP's Ladies in Cyber Charter and Ensign InfoSecurity organised an event: AiSP's Ladies in Cyber Dialogue Session and Learning Journey.

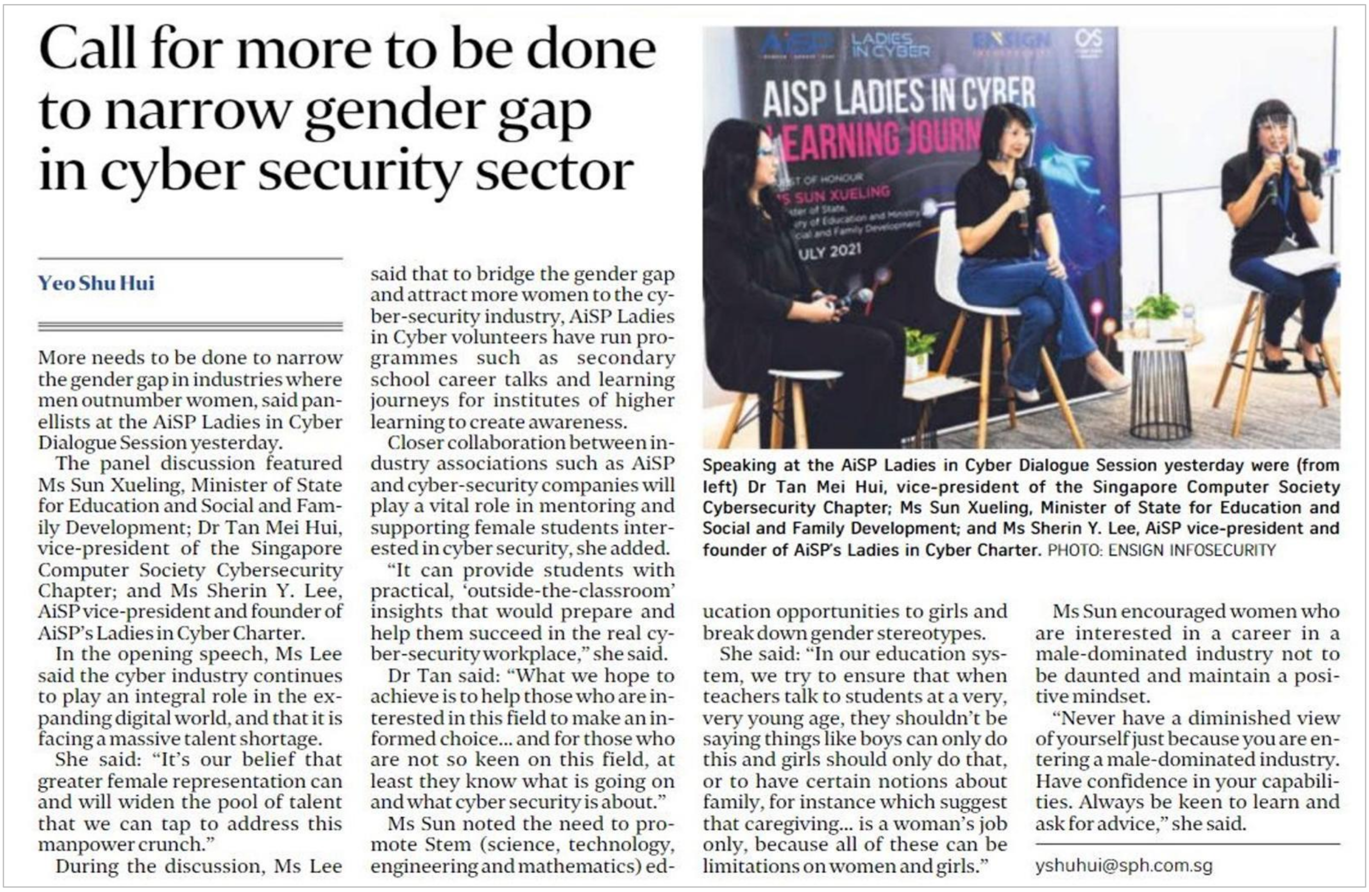
The event aims to give women an in-depth understanding and a feel of the cybersecurity workplace. More than eighty female professionals and students join in the event virtually and thirty-five of our female students that join in physically get to tour Ensign's office and speak with their HR personnel and cyber professionals about what they do daily as part of the learning journey.

The event's panellists, Minister of State in the Ministry of Education and Ministry of Social and Family Development Ms Sun Xueling and Dr Tan Mei Hui, Vice-President of Singapore Computer Society Cybersecurity Chapter shared their thoughts and expertise on how women can thrive in the cyber workplace and realise their career aspirations. Ms Sherin Lee was the panel moderator for the session.

AiSP would like to thank Ensign InfoSecurity for organising the session and provide a platform for the female students to know more about Cybersecurity and discuss gender diversity issues.

Our next AiSP Ladies in Cyber learning journey will be on 24 Sep 21 at CISCO office.

To find out how you can sponsor, volunteer, or play a part in our programmes, please contact us at secretariat@aisp.sg today.



Call for more to be done to narrow gender gap in cyber security sector

Yeo Shu Hui

More needs to be done to narrow the gender gap in industries where men outnumber women, said panellists at the AiSP Ladies in Cyber Dialogue Session yesterday.

The panel discussion featured Ms Sun Xueling, Minister of State for Education and Social and Family Development; Dr Tan Mei Hui, vice-president of the Singapore Computer Society Cybersecurity Chapter; and Ms Sherin Y. Lee, AiSP vice-president and founder of AiSP's Ladies in Cyber Charter.

In the opening speech, Ms Lee said the cyber industry continues to play an integral role in the expanding digital world, and that it is facing a massive talent shortage.

She said: "It's our belief that greater female representation can and will widen the pool of talent that we can tap to address this manpower crunch."

During the discussion, Ms Lee said that to bridge the gender gap and attract more women to the cyber-security industry, AiSP Ladies in Cyber volunteers have run programmes such as secondary school career talks and learning journeys for institutes of higher learning to create awareness.

Closer collaboration between industry associations such as AiSP and cyber-security companies will play a vital role in mentoring and supporting female students interested in cyber security, she added.

"It can provide students with practical, 'outside-the-classroom' insights that would prepare and help them succeed in the real cyber-security workplace," she said.

Dr Tan said: "What we hope to achieve is to help those who are interested in this field to make an informed choice... and for those who are not so keen on this field, at least they know what is going on and what cyber security is about."

Ms Sun noted the need to promote Stem (science, technology, engineering and mathematics) education opportunities to girls and break down gender stereotypes.

She said: "In our education system, we try to ensure that when teachers talk to students at a very, very young age, they shouldn't be saying things like boys can only do this and girls should only do that, or to have certain notions about family, for instance which suggest that caregiving... is a woman's job only, because all of these can be limitations on women and girls."

Ms Sun encouraged women who are interested in a career in a male-dominated industry not to be daunted and maintain a positive mindset.

"Never have a diminished view of yourself just because you are entering a male-dominated industry. Have confidence in your capabilities. Always be keen to learn and ask for advice," she said.

yshuhui@sph.com.sg

Speaking at the AiSP Ladies in Cyber Dialogue Session yesterday were (from left) Dr Tan Mei Hui, vice-president of the Singapore Computer Society Cybersecurity Chapter; Ms Sun Xueling, Minister of State for Education and Social and Family Development; and Ms Sherin Y. Lee, AiSP vice-president and founder of AiSP's Ladies in Cyber Charter. PHOTO: ENSIGN INFOSECURITY

Photo Credits: Ensign's InfoSecurity and Singapore Press Holding (Straits Time)

Join our next AiSP Ladies in Cyber Learning Journey & Fireside Chat at Cisco on 24 Sept 21

Cybersecurity industry has always had an undeserved reputation of being a man's world. And there are quite a few reasons for the disproportionate number but arguably the main reason for it, is the lack of understanding of what women can do in an industry that's perceived to be tough and unforgiving. Yet, recent studies show that women are more likely to hold high-level roles in cybersecurity industry. It has also been proven that organizations advocating gender diversity tends to be more profitable.

AiSP has continuously initiate activities to inspire more women to join the force by engaging and educating students early, holding role-model pairings and hosting dialogues with notable women leaders and cybersecurity practitioners who can provide guidance and inspiration to the younger generation.

This September, **AiSP Ladies in Cyber** is organizing a hybrid fireside chat together with our Corporate Partner Cisco Systems. Join **SMS Sim Ann, Wendy, Catherine and Sherin** - our female leaders from Cybersecurity industry as they share their experience, advice and provide guidance on career in IT industry for females.

Female students can choose to attend the event either physically or virtually. Physical registration is limited to the **first 50 females,** and it consist of an Office & Lab Tour, Dinner, Fireside Chat and Photo-taking with our speakers. **Please email to secretariat@aisp.sg to find out more details on the event.**

Date & Time: 24 Sept 2021 (Fri) from 6.30pm to 9.00pm
Venue: 80 Pasir Panjang Rd, Building 80, Level 25 Mapletree Biz City, Singapore 117372

Ms Sim Ann
Senior Minister of State in the Ministry for Foreign Affairs and Ministry for National Development

Ms Wendy Ng
Head of Cyber Security Sales, Singapore Cisco Systems

Ms Catherine Lee
Senior Specialist, Regional IT Risk Management & Security

Ms Sherin Y Lee
AiSP Vice-President & Founder for AiSP Ladies in Cyber Charter

Special Interest Groups

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

- Cloud Security
- Data and Privacy
- Cyber Threat Intelligence (CTI)
- Internet of Things (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!

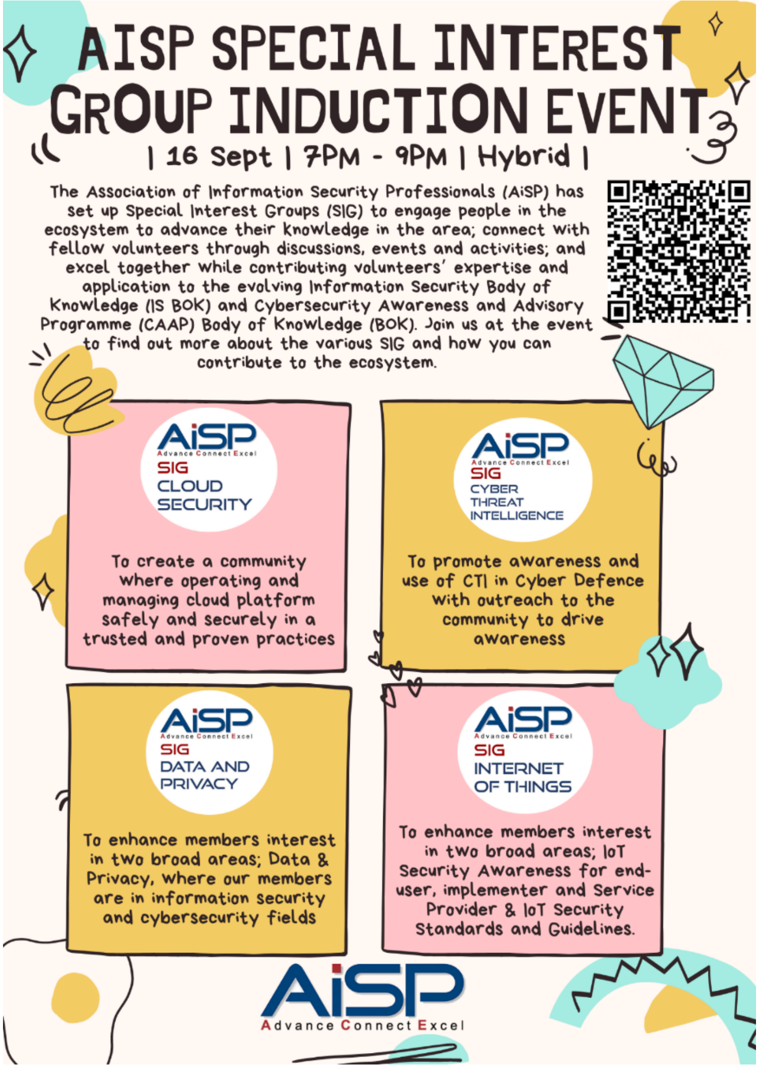
AiSP Advance Connect Excel SIG CLOUD SECURITY

AiSP Advance Connect Excel SIG CYBER THREAT INTELLIGENCE

AiSP Advance Connect Excel SIG DATA AND PRIVACY

AiSP Advance Connect Excel SIG INTERNET OF THINGS

Sign up here: AiSP Special Interest Group Induction Event



AISP SPECIAL INTEREST GROUP INDUCTION EVENT

| 16 Sept | 7PM - 9PM | Hybrid |

The Association of Information Security Professionals (AiSP) has set up Special Interest Groups (SIG) to engage people in the ecosystem to advance their knowledge in the area; connect with fellow volunteers through discussions, events and activities; and excel together while contributing volunteers' expertise and application to the evolving Information Security Body of Knowledge (IS BOK) and Cybersecurity Awareness and Advisory Programme (CAAP) Body of Knowledge (BOK). Join us at the event to find out more about the various SIG and how you can contribute to the ecosystem.

AiSP Advance Connect Excel SIG CLOUD SECURITY

To create a community where operating and managing cloud platform safely and securely in a trusted and proven practices

AiSP Advance Connect Excel SIG CYBER THREAT INTELLIGENCE

To promote awareness and use of CTI in Cyber Defence with outreach to the community to drive awareness

AiSP Advance Connect Excel SIG DATA AND PRIVACY

To enhance members interest in two broad areas; Data & Privacy, where our members are in information security and cybersecurity fields

AiSP Advance Connect Excel SIG INTERNET OF THINGS

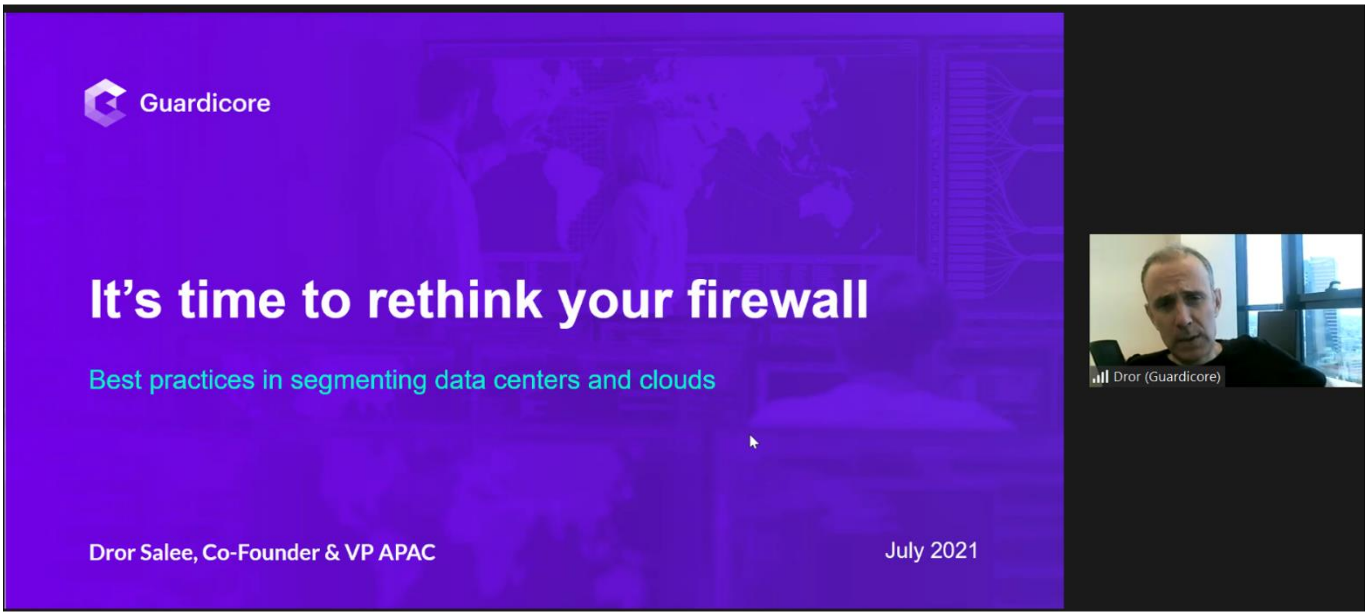
To enhance members interest in two broad areas; IoT Security Awareness for end-user, implementer and Service Provider & IoT Security Standards and Guidelines.

AiSP Advance Connect Excel

Cybersecurity Leaders Series on 28 July

On 28 July, Cybersecurity Leaders Series was successfully launched with panel speakers Mr Chim Chin Kiat (Dyson), Mr Kevin Reed (Acronis)and Mr Dror Sal'ee (Guardicore) moderated by AiSP President, Mr Johnny Kho. More than 90 C-Suite level Professionals joined in the Webinar with the speakers sharing topics on Technology Resilience and how Cybersecurity can protect us. We would like to thank our speakers for taking time to join us in this community talk.

Our next Cybersecurity Leaders Series Webinar will be on 23 Nov 21. Contact AiSP secretariat@aisp.sg if you wish to be part of it.



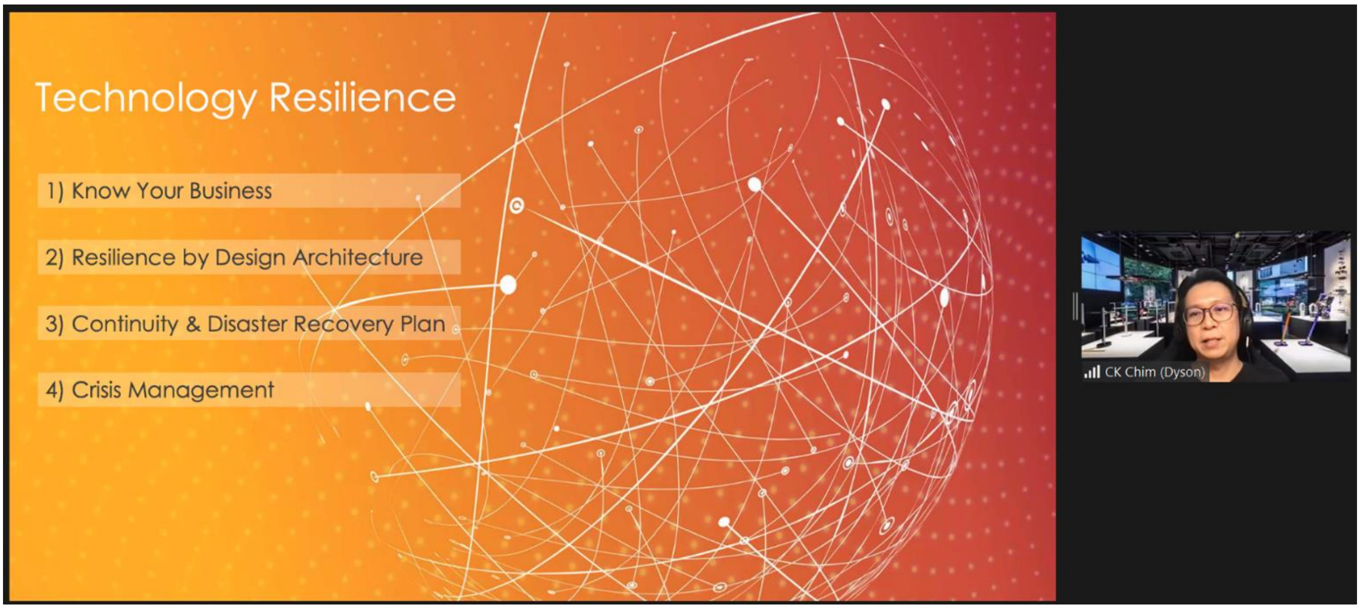
Guardicore

It's time to rethink your firewall

Best practices in segmenting data centers and clouds

Dror Salee, Co-Founder & VP APAC

July 2021



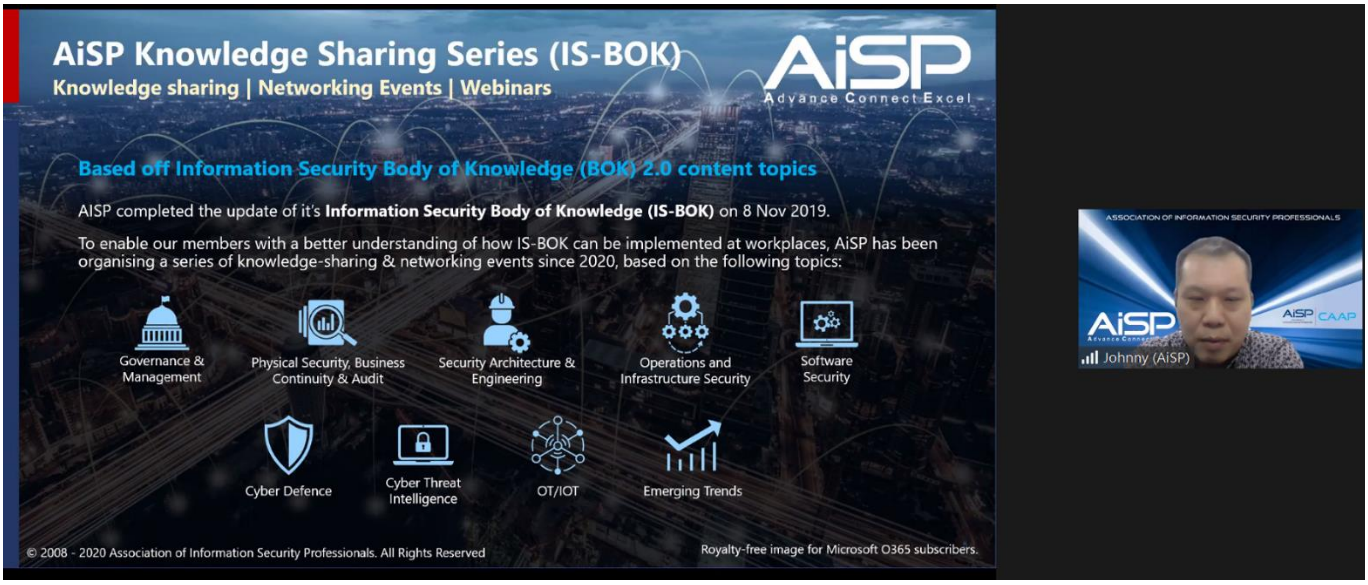
Technology Resilience

1) Know Your Business

2) Resilience by Design Architecture

3) Continuity & Disaster Recovery Plan

4) Crisis Management



AiSP Knowledge Sharing Series (IS-BOK)

Knowledge sharing | Networking Events | Webinars

Based off Information Security Body of Knowledge (BOK) 2.0 content topics

AISP completed the update of it's **Information Security Body of Knowledge (IS-BOK)** on 8 Nov 2019.

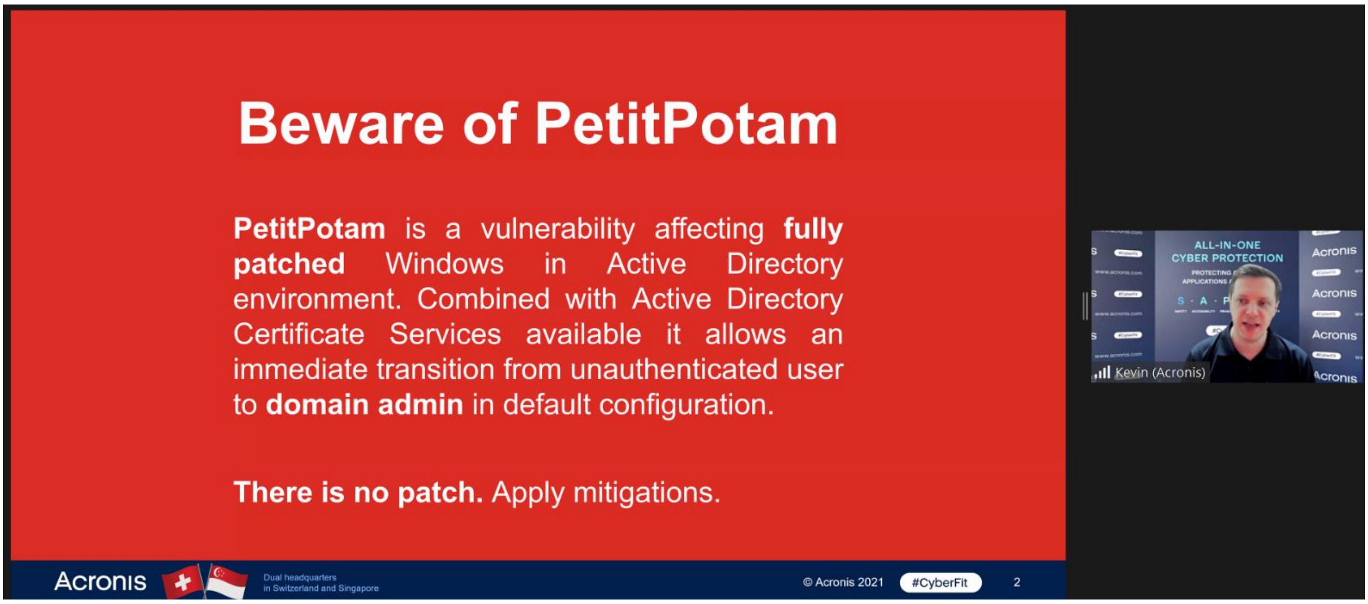
To enable our members with a better understanding of how IS-BOK can be implemented at workplaces, AiSP has been organising a series of knowledge-sharing & networking events since 2020, based on the following topics:

- Governance & Management
- Physical Security, Business Continuity & Audit
- Security Architecture & Engineering
- Operations and Infrastructure Security
- Software Security
- Cyber Defence
- Cyber Threat Intelligence
- OT/IOT
- Emerging Trends

© 2008 - 2020 Association of Information Security Professionals. All Rights Reserved

Royalty-free image for Microsoft O365 subscribers.

AiSP Advance Connect Excel
ASSOCIATION OF INFORMATION SECURITY PROFESSIONALS
AiSP CAAP
Johnny (AiSP)

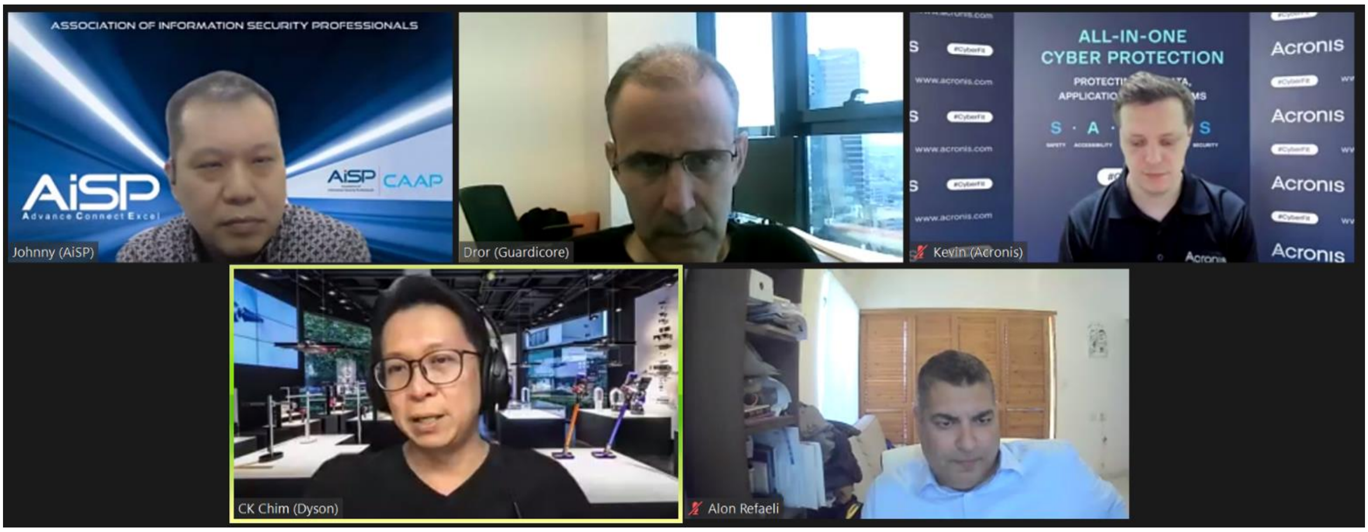


Beware of PetitPotam

PetitPotam is a vulnerability affecting **fully patched** Windows in Active Directory environment. Combined with Active Directory Certificate Services available it allows an immediate transition from unauthenticated user to **domain admin** in default configuration.

There is no patch. Apply mitigations.

Acronis Dual headquarters in Switzerland and Singapore © Acronis 2021 #CyberFit 2



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 (secretariat@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

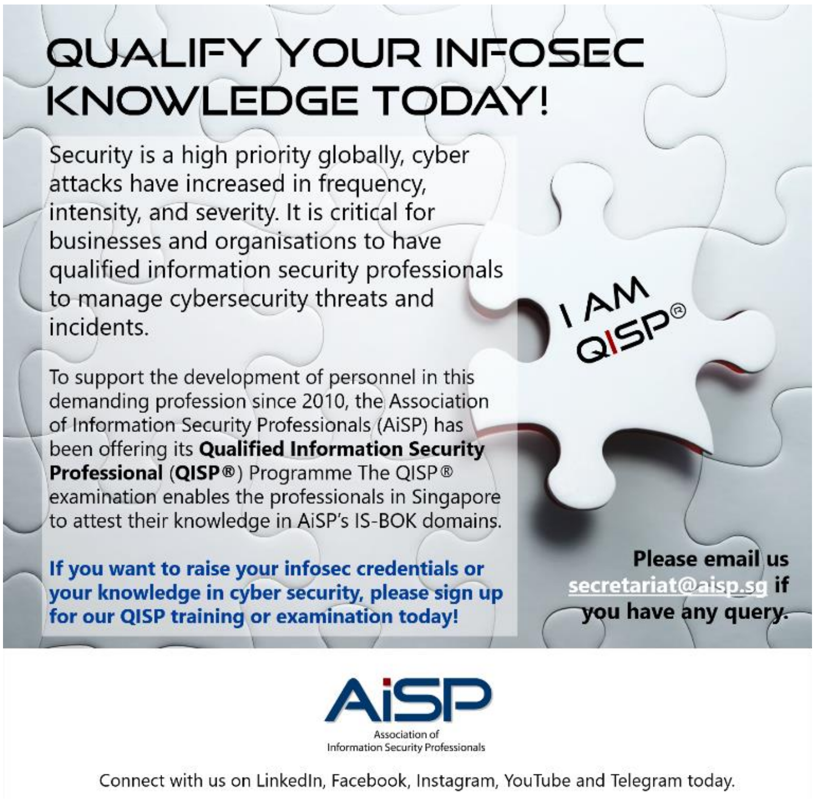
As AiSP focuses in raising the professional standing of information security personnel and professions in Singapore since 2008, we have been running various initiatives to address diverse needs and developments.

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.

AiSP Association of Information Security Professionals

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. 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
03 Aug	SBF Cloud Webinar on Cloud optimization & automation	AiSP & Partner
17 Aug	**CREST Webinar**	**AiSP**
18 – 19 Aug	ARRC	Partner
24 Aug	Data Security Webinar	AiSP & Partner
24 – 25 Aug	ISMG's Virtual Cybersecurity Summit Asia: Healthcare	Partner
25 Aug	**Knowledge Series – IoT Security**	**AiSP**
27 Aug	Digital Transformation Summit Asia	Partner
31 Aug	Niche & Hot InvestTech Talks Series -Venture Capital Investing: Mainstream vs. Technology Platform	Partner
1 Sep	**Ladies in Cyber Webinar – Spill the Tea**	**AiSP**
2 Sep	ISACA Singapore Annual GTACS 2021	Partner
8 – 9 Sep	OT-ISAC Summit 2021	Partner
8 Sep	AiSP x PA CAAP Focus Group Discussion	AiSP & Partner
9 Sep	AiSP x SCS CAAP Focus Group Discussion	AiSP & Partner
15 Sep	**Knowledge Series – Operation & Infrastructure Security**	**AiSP**
15 – 16 Sep	CIISec Live by CII SEC	Partner
15 Sep – 30 Nov	SMEICC Conference Series 2021	Partner
16 Sep	**SIG Combined Event**	**AiSP**
18 Sep	ASEAN Students Contest on Information Security 2021	Partner
24 Sep	Ladies in Cyber Learning Journey & Dialogue Session at Cisco	AiSP & Partner
29 Sep	**Knowledge Series – CTI**	**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.

Sign up now at https://app.glueup.com/event/crest-webinar-17-aug-2021-39996/

CREST WEBINAR

17 August 2021 | 3 PM - 4.30PM

| Webex |

JOURNEY TO THE CENTER OF CLOUD: THE ESSENTIAL APPROACH TO GOVERNANCE AND SECURITY IN THE POST-COVID ERA

Enterprises are contending with challenges as they attempt to manage multiple Cloud-adoption approaches. From the simple: "LIFT and SHIFT" of legacy systems to a Cloud service;

Or, other approaches by replacing or rebuilding entire and new Cloud-native systems;

Or, on the other hand, some organisations still maintain on-premises systems with traditional enterprise architecture, yet, still a hybrid mixed-in with Cloud-based SaaS.

Clearly, for any businesses transforming into the digital economy, two-thirds (2/3) of them are making this journey to digitalise assets in the Cloud, yet have to choose how to do it wisely.

These same businesses need to keep in mind the key challenges to maintain governance and security, and to be successful in doing it safely and securely in the post-COVID era.

Peter Gwee
Principal Consultant
ST Engineering

CONTENT MANAGEMENT SYSTEMS AND THE IMPORTANCE OF VULNERABILITY MANAGEMENT

A demystification of dangerous and widespread myths on the security of Content Management Systems. A technical presentation and demonstration of a vulnerability affecting the most popular CMS will highlight the risks associated with these systems. The presentation will also put the spotlight on existing defences and best practices to protect Content Management Systems against the latest threats.

Tom Philippe
Cyber Security Consultant
Responsible Cyber

Organised By: AiSP Advance Connect Excel

Supported By: Responsible Cyber | ST Engineering

Via: webex by CISCO

CONTRIBUTED CONTENTS

Insights from The Cybersecurity Awards 2020 Winner – Alina Tan

THE CYBERSECURITY Awards 2020
26 February 2021
Guest-of-Honour
Mr S Iswaran
Minister for Communications and Information an
Minister-in-charge of Cybersecurity
BeyondTrust
DBS

I am incredibly humbled and honoured to have won The Cybersecurity Awards 2020 (Professional Category).

When I started in cybersecurity, I was extremely fortunate to be plugged into two amazing cybersecurity communities — AiSP and Division Zero (Div0). I got myself involved in many activities such as AiSP Ladies in Cyber and AiSP's IoT Security Interest Group (SIG).

Inspired by many community leaders, I founded an automotive security interest group — called Car Security Quarter (CSQ) — in Div0 community. CSQ sets out to promote and facilitate automotive security learning through technical talks and workshops, and CTFs.

Having observed a lack of techno-centric activities in Singapore's women in cybersecurity scene, I co-founded Div0's Women In Cybersecurity (WICS) initiative.

I am thankful that my efforts were recognised by the ecosystem to be awarded this incredible honour. I hope that this award will inspire more people to step up and contribute further to Singapore cybersecurity ecosystem.

I'm definitely not going to let up. This award has inspired me to push harder in promoting automotive security and inspiring more women to join the cybersecurity industry.

Thank you AiSP & SCSIA for organising The Cybersecurity Awards and thank you to the esteemed panel of judges for recognising my contributions to the ecosystem.

Last but not least, thank you Div0 for the nominations and empowering individuals like me to run an automotive security interest group like CSQ. And, of course, a big thank you to my team at CSQ for the consistent support and effort in building the knowledge bank on automotive security.

Insights from our Corporate Partner Programme (CPP) – Checkmarx

Considerations for Open Source and Proprietary Application Security Solutions

The process of writing code (and the code itself) has changed dramatically: functionality and end-goals for code execution are lightyears ahead of where we began. The software development tools to support the magic of coding have spurred a new process with a fancy name, DevOps, which has enabled developers to deploy code faster than ever before.

However, code vulnerabilities live on the other side of this magic and there's an increasing need to release secure code. It is not enough to write code quickly and not consider security. You must make sure it does not expose vulnerabilities that can have a critical impact on the organization. Despite commercial and open source tools that perform Application Security Testing (AST) becoming available to help development teams write secure code, not all developers and organizations have adopted security best practices and made the subsequent shift from DevOps to DevSecOps.

Learn how to take an integrated approached to embedding security into DevOps here. >>

AST tools span the software development life cycle (SDLC) – from code-writing to production environments. Naturally, there's a market divide between open-source AST, developed in software communities, typically available free of charge, and commercial AST vendors. Teams might want to use either open source or proprietary application security solutions for different reasons. We're going to shed light on similarities and difference between open source and proprietary AST so you can gain a better understanding of which will support your development, security, and operations needs and goals.

Let's explore these two types of code-scanning solutions, and which is right for your team right now.

The Power of Community

One of the most significant advantages of any open-source project, and not just regarding AST solutions, is the community. Open source is, to the benefit of the end-user, powered by an entire, hidden developer community that happily contributes code to a given project. Open source code projects took us to Mars – what could be a stronger tribute to the developer community's power? NASA and Microsoft back this popular project, ensuring that committed code is vetted, issues receive due attention, and the community is properly supported in reaching and setting new goals. It's wise to research who orchestrates community efforts and understand if the people or organization will continue to prioritize the projects for the next five plus years, ensuring that you have a product that you may rely on for the foreseeable future.

Open source projects that provide the foundation for a commercial offering, where the core of the commercial product is available as open source but a vendor layers 'value-add' features like reporting, enhanced capabilities, or integrations into a comprehensive platform, are arguably the safest bet. Projects like this are better supported because an organization's revenue stream relies on it. The downside? Some developers might be less inclined to contribute to a project that is also generating commercial revenue for a company.

However, if an open source project isn't backed by an organization that doesn't continuously reinvest its resources in fostering the community, developers might lack a real commitment to the project, so the results aren't as impressive. It turns out that shepherding a successful open source project can be as much work as writing the code itself, and often less rewarding. Sometimes the work of maintaining a project becomes just that – work. That's when things can go wrong: bugs and features often go neglected. Over time, users search to look for other solutions, which isn't simple if the deployment process requires a lot of effort.

Look at how many years of market leadership, vision, and development is behind an AST solution. Also check out Gartner and other analyst reports that evaluate these solutions based on the engine accuracy and performance, and roadmap, reassuring the users both for today and the future.

The Premium of Freemium

While the accuracy, dedicated support, and R&D teams provide a clear win for commercial solutions, it wouldn't be a fair debate unless we mentioned the price. Open source projects have a forever free or freemium usage model, so the cost of commercial AST solutions may sway a smaller development team's decision. As such, open source can be either an excellent way to either support complimentary AppSec solutions within your pipeline or an ideal entry-point for a smaller development team to start an AppSec program. Yet we, also, encourage to do your due diligence regarding who and how open source projects are supported. Then, depending on the reliability of the tool, crunch the numbers to see what's the hidden cost of an implementation full of friction and the ultimate cost of a breach? If you're in this position, remember that most companies also offer basic packages or code scanning functionality that scales as you scale.

Develop-Centric for Accelerated Time to Market

Developers' ability to focus is paramount for companies hitting their release targets. If you're juggling point-products, developers will need to toggle between multiple UIs and spend considerable time making sense of the different security scan reports before remediation.

As someone involved with the procurement of application security solutions, you need to make sure the following is covered in either a commercial or open source tool:

1. Accuracy
2. Extensive language coverage
3. Vulnerability prioritization based on severity or exploitability
4. Scans for different types of code in the various stages of the SDLC
5. Ability to customize and tune

If you find that any of the five factors above are lacking, you might find yourself piecemealing multiple open source solutions together, getting tangled in a web of remediation that will surely decelerate DevOps. That workflow alone doesn't provide a positive developer experience, but even each tool as a standalone project won't support developers' focus and accelerating time to market, either.

Accuracy

Regarding the accuracy of the engines, this is, also, highly variable between engines and languages. There are open source engines that boast excellent results with impressive accuracy. For example, every Application Security Engineer and vendor will recognize the open source SAST solution "Brakeman" as a leading SAST solution for Ruby code. Other open source engines are less accurate than their commercial counterparts for all the reasons mentioned above. Typically, at best, the results will show false positives, requiring additional monitoring by the user. At worst, scans may contain false negatives, opening the possibility of known vulnerabilities exposure in the application production environment. So, what was now a free solution is costing you more in the long run.

Even if you don't decide on open source AST, you'll most likely leverage OSS in some way, so you'll need to secure it. **Learn more about Software Composition Analysis to scan third party and open source code in "The Ultimate Guide to SCA." >>**

Integrations throughout the SDLC

Accuracy, performance, and data insights that bring together results from multiple scans (SAST, SCA, IAST, IaC scanning) will help you insert security and shift left without slowing down the SDLC but asking developers to toggle to another UI or work around a clunky integration is a friction point. Solid integrations throughout the SDLC are the name of the game. To enjoy the benefits of AST without slowing DevOps, meet the developers where they are.

Most proprietary solutions have extensive integrations that streamline DevSecOps workflows. For example, you can automate scans, whether by GIT events as part of the CI process, or you can automate reporting to a system like JIRA. But you could also find an open source solution for which you can build custom scripts.

Language Support
Additionally, there is typically much more robust support for multiple languages. Most open-source scanning engines know how to work with a limited list of languages, and legacy languages have almost no place in open-source projects. Consequently, you must accumulate a stack of open source scan engines to support all the languages that your development team uses in your own proprietary code and open source libraries – each with different syntax, formats, reporting structure, and learning curves. If you can, look for solutions that are built to be extensible.

Choose a Solution and *Use* It

Today we are witnessing more attacks that the production of secure code could avoid. Companies and organizations developing software are coming to a fuller understanding that releasing secure code is not just a box to check for compliance. It is the additional barrier against the next attack. As we detailed, there are advantages to both open source and proprietary solutions. Regardless of what is suitable for your team at this point, do your research, do your due diligence. Choose *and use* one of them, and do not give up on it.

Unsure which is right for your team? **Click here to schedule time with an AppSec expert. >>**

For any enquiries, please contact:
Kevin Tham
Marketing Manager, APAC
+65 6955 9633
kevin.tham@checkmarx.com
https://www.checkmarx.com/

Insights from our Corporate Partner Programme (CPP) – Tanium

The Role of Hygiene in Cyber Security

Alvin Tan, Regional Vice President, Tanium

Cybersecurity is in the spotlight. The recent Microsoft Exchange server attacks sent ripples across the world with hundreds of thousands of organizations impacted. An estimated 30 million Dell computers are affected by several vulnerabilities that may allow an attacker to remotely execute code in the pre-boot (BIOS) environment. More recently, Kaseya VSA vulnerabilities were used in the REvil ransomware attack.

Meanwhile, the business landscape has changed drastically in the last two years. Digitalization has been placed at the core of almost every business and government, with transformation occurring at unprecedented scale and speed. As businesses thrive and technology proliferates, the threat of a digital attack grows. Reports of cyberthreats are rising across the region, and businesses and governments are looking at ways to address the security challenges present in our increasingly digital world.

No company wants to be the next headline, spiralling into crisis mode to remediate a breach and manage reputational fall-out.

It's time for all of us to ensure our cyber doors are locked.

With digital transformation, many businesses have experienced growth leading to expansion, both physical and virtual, in multiple locations across the region. This growth however can see good cyber hygiene practices fall away at a time when organisations are expanding, increasing vulnerabilities that are yet to be patched, and for regulated businesses, experiencing compliance drift that is hard to manage at scale.

Malware can spread rapidly before it is detected. Real-time visibility is vital because it allows any intrusion to be quickly discovered, mitigating the spread – and providing heightened situational awareness for rapid response.

Going back to basics and focusing on hygiene is fundamental to mitigating your cyber risk. Because it is impossible to control the unknown, and unaccounted. Research shows that 80% of cyber breaches would not have been successful if cyber hygiene was practiced correctly.

The seven cyber hygiene principles described in Tanium's endpoint article, Cyber Hygiene 101, will make your enterprise a simpler, cleaner, and less-inviting target for cybercriminals.

At Tanium, we partner with businesses and governments to detect anomalies in real time—protecting your organisation and preventing it from becoming the next big headline.

With businesses in Southeast Asia exposed to the highest rate of data breaches globally, cybersecurity will continue to be in the regional spotlight for the foreseeable future.

Simply put, businesses can no longer ignore the risk and the need for cyber hygiene. The costs – in dollars, reputation and recovery – are too high.

For more enquiries, please contact Charis.Oh@tanium.com

Insights from our Corporate Partner Programme (CPP) – Privasec

Updates To ISO 27002 And Its Impact

Written by Angela Yuen, Privasec's GRC and Security Consultant

Introduction

In the cybersecurity landscape today, there are many information security frameworks to help organisations protect their information assets. These frameworks serve as a common language that allows all staff within an organisation, as well as relevant stakeholders to develop a shared understanding of information security risks. It is thus important for organisations to choose the right framework that suit their environment. Broadly speaking, there are three types of information security frameworks:

1) Control frameworks which contain a set of baseline control to be implemented.
2) Program frameworks which define the requirements for building an effective information security system.
3) Risk frameworks which describe the process to manage risks.

ISO 27001 sits within the program framework as it mandates the design and implementation of an Information Security Management System (ISMS). Nonetheless it makes references to the risk management framework to help organisations identify, evaluate, and treat risks surrounding information assets.

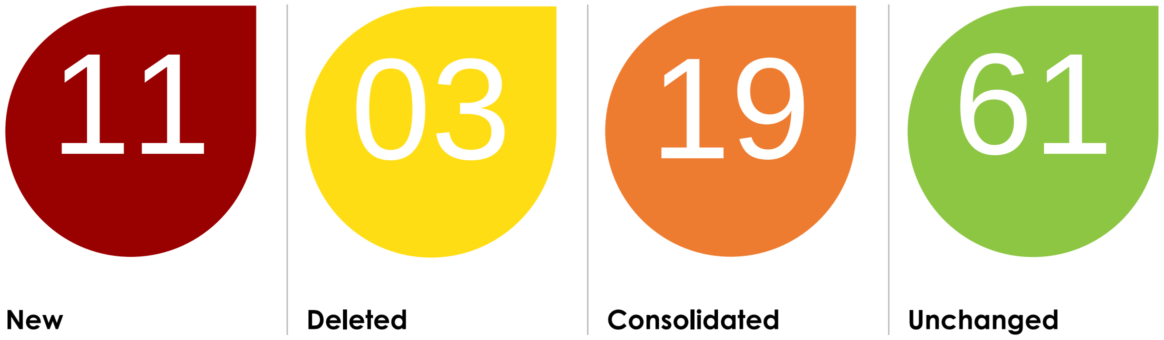
What is ISO 27001/ISO 27002?

ISO 27001 is the central framework of the ISO 27000 series and takes a risk-based approach to help organisations manage information security. It provides organisations the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS). The core requirements of the standard are supported by a set of security controls, known as Annex A. While organisations are not required to implement all the controls within Annex A, it serves as a catalogue for organisations to select appropriate controls to tackle the information security risks identified, based on business objectives and risk assessment.

ISO 27001 has become the go-to standard for information security as it can be adopted by any organisations regardless of size and sectors who are keen to establish and maintain a working ISMS. There has been increasing pressure, by regulators, clients and other stakeholders, for organisations to proof the robustness of their security controls. Conforming to an international standard shows that organisations are putting in effort and commitment towards security and improving their security posture through a well-defined continual improvement process. Although ISO 27001 certification remains non-mandatory for most organisations, organisations are beginning to recognise the value and benefits it brings in certifying the strength of its ISMS as it becomes the new norm for best practice in information security.

You might be wondering if ISO 27002 is a separate standard in the ISO 27000 series. Well, not exactly. Annex A provides an outline for each control, ISO 27002 delves into the details on how the controls can be implemented. The ISO 27002 standard, like all other ISO standards, is subject to a review every 5 years to determine whether updates are required. Since its last revision in 2013, ISO 27002 has been set for a refresh, and is slated to be published by end 2021.
Unlike ISO 27001, organisations cannot certify against ISO 27002. It is to be used as a reference for control implementation. Organisations can select additional controls from other standards such as PCI DSS, NIST or MITRE ATT&CK framework and so forth.

What has changed in ISO 27002?



The main difference between the Draft International Standard (DIS) and the 2013 version is the structure of the control set. While majority of the ISO 27002 controls remains unchanged, the controls have been regrouped from 14 categories to 4 broad categories that include Organisational, People, Physical and Technology. The number of controls has also been reduced from 114 to 93 in the DIS, with the introduction of 11 new controls, deletion of 3 existing controls and consolidation of 48 controls into the current 19 controls.

For example, controls pertaining to user endpoint devices was distributed across different domains (A6 and A11) in the 2013 version, when it could be combined under one broad category (i.e., user endpoint devices) in the DIS. Some other individual controls in the 2013 version were also integrated into a single control in the DIS as they are work on the same fundamental principles. For example, controls A.12.4.1 to A.12.4.3 in the 2013 version which concerns logs have been categorised under Logging in DIS to minimise duplication. The wider structure eliminates redundancy between controls across multiple domains as well as within the same domain. It allows users to examine the subject based on themes and direct implementation efforts effectively. The new structure is less prescriptive and gives organisations the autonomy to explore its options to meet control objectives.

Digital transformation, together with a worsening cyber threat landscape, has accelerated the change in ISO 27002. ISO 27002 will include new controls relating to threat intelligence, cloud services and secure coding to reflect the rapidly evolving technology.

We can see similar updates to other industry standards and guidelines, such as the Monetary Authority of Singapore (MAS) Technology Risk Management (TRM) Guidelines in 2021 and the Association of Banks in Singapore (ABS) Cloud Computing Implementation Guide in 2019. The new MAS TRM guidelines has been updated to include best practices on cyber security operations and software application development and management while the ABS Cloud Computing Implementation Guide revised to place more emphasis on the safe adoption on cloud; all three topics new in ISO 27002 DIS. At a broader level, there are changes to regulations concerning data, especially personally identifiable information on the international field. Threat intelligence has also been included in industry guidelines published across several bodies, signalling an industry wide recognition of its value as part of a cyber defender's arsenal.

With the pending updates to the ISO 27002, it is now more well-rounded for tackling information security risks. What remains a constant, is the purpose of the standard to provide implementation guidance on security best practices for compliance to ISO 27001.

The differences are summarized in the tables below:

Consolidated Controls			
5.1 – Policies for information	5.1.1, 5.1.2	8.1 – User endpoint devices	6.2.1, 11.2.8
5.9 – Inventory of information and other associated assets	8.1.1, 8.1.2	8.8 – Management of technical vulnerabilities	12.6.1, 18.2.3

5.14 – Information transfer	13.2.1, 13.2.2, 13.2.3	8.15 – Logging	12.4.1, 12.4.2, 12.4.3
5.15 – Access control	9.1.1, 9.1.2	8.24 – Use of cryptography	10.1.1, 10.1.2, 18.1.5
5.16 – Identity management	9.2.1, 9.4.3	8.25 – Secure development lifecycle	14.1.1, 14.2.1
5.17 – Authentication information	9.2.4, 9.3.1	8.26 – Application security requirements	14.1.2, 14.1.3
5.18 – Access rights	9.2.2, 9.2.5, 9.2.6	8.29 – Security testing in development and acceptance	14.2.8, 14.2.9
5.22 – Monitoring, review and change management of supplier services	15.2.1, 15.2.2	8.31 – Separation of development, test and production environments	12.1.4, 14.2.6
5.29 – Information security during disruption	17.1.1, 17.1.2, 17.1.3	8.32 – Change management	12.1.2, 14.2.2, 14.2.3, 14.2.4
7.10 – Storage media	8.3.1, 8.3.2, 8.3.3		

New Controls	
5.7 – Threat intelligence	8.11 – Data masking
5.23 – Information security for use of cloud services	8.12 – Data leakage prevention
5.30 – ICT readiness for business continuity	8.16 – Monitoring services
7.4 – Physical security monitoring	8.22 – Web filtering
8.9 – Configuration management	8.28 – Secure coding
8.10 – Information deletion	

Deleted Controls	
8.2.3 – Handling of assets	11.2.5 – Removal of assets
16.1.3 – Reporting information security weaknesses	

How does the new revision of ISO 27002 impact ISO 27001?

Since ISO 27002 is essentially expanding on Annex A of ISO 27001, an update to ISO 27002 will inevitably affect the control set in ISO 27001. These changes are expected to be reflected in Annex A of ISO 27001 after the official release of the updated ISO 27002 to ensure that information from both standards is consistent.

How does it impact organisations that are already ISO-certified?

There is currently no impact on organisations that are already maintaining a certified ISMS until the ISO 27002 DIS has been finalised and the new ISO 27001 Annex A released. Typically, organisations will be given a grace period before they are required to adopt the revised ISO 27001 standard and it is likely for organisations to address the changes in conjunction with the next recertification audit cycle once the revised standard is published.

Although further modification is possible prior to formal publication, it might still be worthwhile for organisations to obtain a copy of the ISO 27002 DIS and access the impact of the changes to their existing ISMS implementation and the additional effort required to meet the updated requirements, so to better prepare themselves for the upcoming changes than to struggle with the implementation thereafter.

For organisations that intend to certify their ISMS, this should not be a showstopper. Organisations should familiarise themselves with the draft control set and with the help of the mapping to the 2013 version, make-ready for the certification.

What is the extended impact to other ISO standards?

Extended standards such as

- ISO 27017 – *Code of practice for information security controls based on ISO/IEC 27002 for cloud services;*
- ISO 27018 – *Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*; and
- ISO 27701 – *Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management*

will be affected by the revision of ISO 27002. At this stage, there is limited information on other standards that rely on ISO 27002 controls. However, this should not hinder organisations who are currently planning on obtaining certification or those who are operating and maintaining a certified ISMS.

About the Author
Angela Yuen is a Security GRC Consultant at Privasec. She is a technology governance, risk and compliance professional who has worked on several industry verticals in organisations around compliance towards regulatory requirements, and management of technology and operation risks. She is also a certified ISO 27001:2013 Lead Auditor and Certified Information Systems Auditor (CISA).

About Privasec
Privasec is one of the fastest growing independent security, governance, risk and compliance consulting firms in South East Asia and Australia. We are driven by business outcomes bridging the gap between the technical and business worlds to create meaningful business cases and enhance decision making.

We have two lines of businesses across GRC and RED servicing Government, Financial Services, Legal, Retail, IT, Health, Entertainment and Not-for-Profit sectors.

- Privasec GRC are the specialists in Governance, Risk and Compliance which covers ISO27001, NIST CSF, PCI DSS, SOC2, GDPR, PDPA, Data Protection Trustmark Certification and other key regulations required to operate in today's market.
- Privasec RED are leaders in Security and Penetration Testing, Cloud Security Testing, Drone Security, Red Team Attack simulations, Purple Teaming, Physical Intrusions, Theft simulations, Open Source Intelligence Gathering (OSINT), Social Engineering, and Phishing.

To learn more about us and our services, visit: www.privasec.com.

Insights from our Corporate Partner Programme (CPP) – FireEye

RANSOMWARE EVOLVES INTO MULTIFACETED EXTORTION

The Problem Statement : Terminology is not keeping pace with the threat landscape.

When business leaders and risk managers today hear the term "ransomware" they often envision scenarios of malware encrypting files, making them inaccessible to legitimate users, and ultimately resulting in some level of business disruption. They also see that the best protection against these sorts of attacks is solid offline backups. This understanding of ransomware was appropriate for 2019 but is now no longer appropriate. The way ransomware attacks are executed today, the business consequences that these attacks bring, and the protections that need to be in place are totally different.

The problem itself is fundamentally different. However we still refer to the problem as "ransomware". Mischaracterizing these attacks as ransomware is not serving organizations well. Often they are unprepared for the attack when its true nature is revealed in the midst of a real incident. It's time to adopt a new name to characterize these attacks to more adequately describe what they are. At Mandiant we refer to them as "Multifaceted Extortion".

The first extortion facet is the deployment of ransomware encryptors. Organizations files are encrypted and made unavailable. The attacker demands a payment for the decryption tool and key. This is traditional ransomware.

The second extortion facet is threatening to make stolen confidential data public. Organizations' files are stolen, and the attacker demands a payment not to publish the sensitive data. This extortion is much more consequential than the first as it may give the attacker more leverage. With a multifaceted extortion, the attacker turns a "service disruption" into a "data breach".

Data breaches may have more serious business consequences than service disruptions do. A data breach can result in greater reputational damage, regulatory fines, class action lawsuits, and derailed digital transformation initiatives. These are consequences that were typically not seen with traditional ransomware prior to 2019 and may be consequences that come as unexpected if organizations continue to think of modern multifaceted extortion attacks simply as ransomware.

The third extortion facet is shaming the victim by publishing stolen data on a “victim shaming website”, which many multifaceted extortion groups operate on the Tor network. Additionally, they may engage security and technology media organizations to amplify their attacks and attempt to coerce victims into paying.

One important point to highlight is that with multi-faceted extortion, in addition to deploying ransomware encryptors and disrupting business operations, the threat actors steal data, publish it, and shame victims. Having good backups only address part of the problem.

With multifaceted extortions, the attacks are not targeting IT systems and data, they are targeting the business itself. These threat actors are hitting businesses where it hurts the most, and their extortion demands are now in the millions or tens of millions of dollars. These attacks are high volume, high impact, and they don't discriminate based on geography or industry.

Call To Action

There are so many layers of preventative security controls in place already, what more is reasonable for organizations to do to address the multifaceted extortion threat?

There are actually many things that organizations could do but likely have not yet done to bolster a stronger defense. Many of these may not require technology purchases but rather just some time and effort to adopt.

1) Don't have a mindset of fighting ransomware as if it was malware.
With multifaceted extortion attackers 1) break into a network 2) identify and get access to critical servers 3) steal the data on those servers 4) deploy ransomware on those servers 5) threaten to make the stolen data public. By treating ransomware like malware defenders are giving steps 1-3 to the attacker for free, and only starting or trying to defend themselves when the attacker is already on step 4. It's important to recognize that with multifaceted extortion, there is a network intrusion preceding the ransomware deployment. Defenders are better served by defending themselves starting on step 1 rather than on step 4 of the attack.

2) Premediate your environment against multifaceted extortion threats.
When Mandiant responded to victims of these attacks, they observed that there were non-optimal configurations and architectural decisions which weakened the overall defense. Had best practices been in place before the attack, it would have greatly reduced the likelihood of the attacker's success. These misconfigurations are commonplace and not the exception. Defenders can put up significant hurdles for the attackers by putting in these best practices as a premediation rather than as a remediation. See the whitepaper and webinars referenced below for specific premediation steps, which often don't require any additional purchases, but can bear significant returns in preventative efficacy.

3) Assess yourself specifically against multifaceted extortion both strategically and technically.
Of late the industry has come to realize that prevention alone is not enough. Organizations need to be prepared for the inevitable prevention failure and be armed with a plan and capabilities to detect and respond to those failures. The same mindset applies to multifaceted extortion. In addition to trying to prevent it from happening in the first place, organizations need to think through what to do if it happens despite their best efforts to prevent it. Response plans, communication workflows, and stakeholder identification all should be thought through ahead of time, not in the heat of a crisis. "Ransomware Defense Assessments" are available on the market to help organizations work through both the strategic and technical aspects organizations need to have in place to consider themselves resilient.

References and Resources

White Paper: Ransomware Protection and Containment Strategies Practical Guidance for Endpoint Protection, Hardening and Containment (22 pages)
Sep 05, 2019
https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/wp-ransomware-protection-and-containment-strategies.pdf

On Demand Webinar: Vigilance in An Era When Ransomware Is Big Business (59m)
Apr 13, 2021
https://www.brighttalk.com/webcast/10469/475967

On Demand Webinar: Proactive Solutions to Stop Modern Ransomware in its Tracks (58m)
Jun 20, 2020
https://www.brighttalk.com/webcast/10469/403414

Ransomware Defense Assessment
Evaluate your ability to prevent, detect, contain, and remediate a ransomware attack
https://www.fireeye.com/mandiant/ransomware-defense-assessment.html

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.

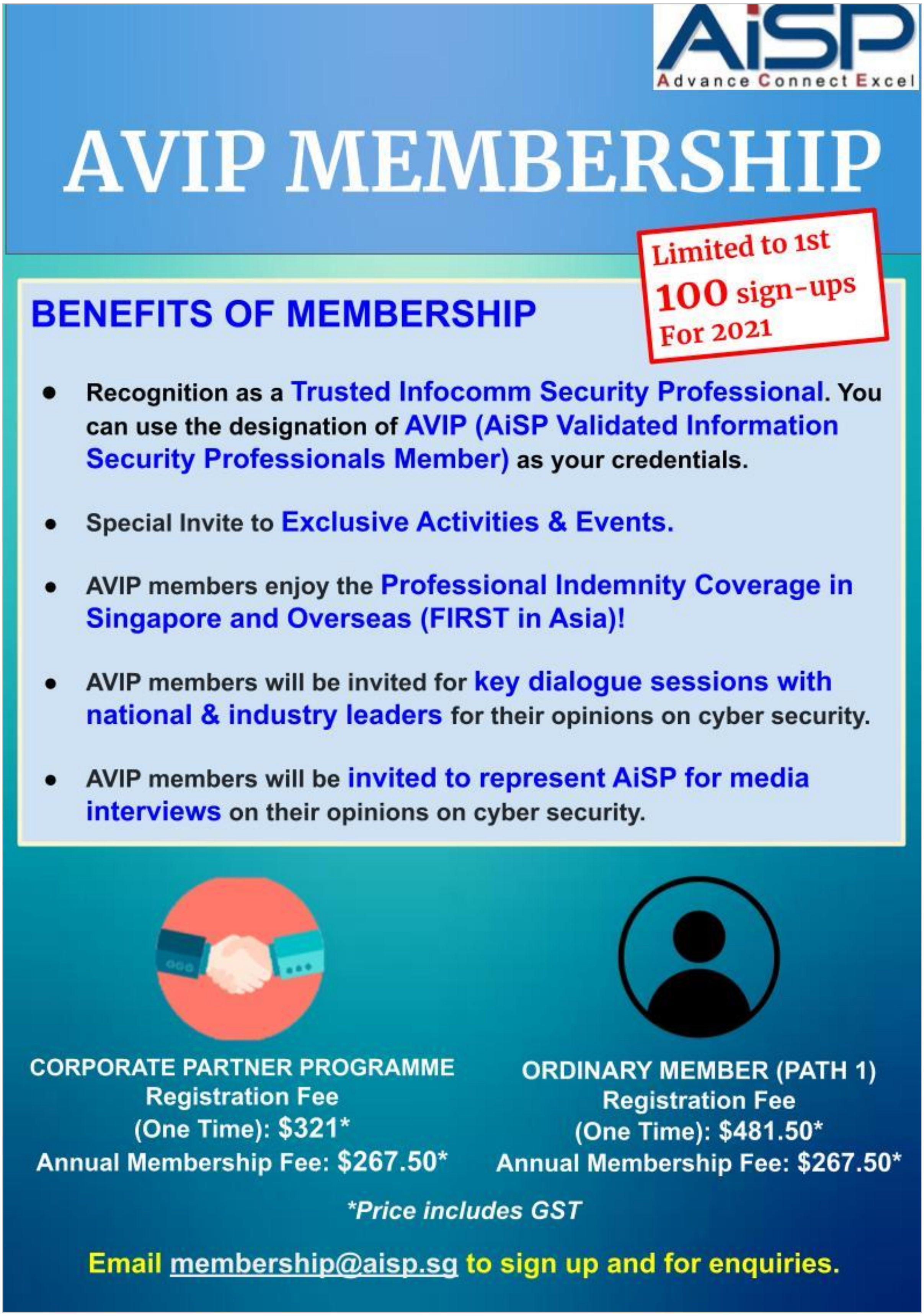
Your AiSP Membership Account

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!



AiSP Advance Connect Excel

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

BCG

BitCyber
Securing Your Business

BD

Checkmarx

cisco

DBS

ENSIGN
INFOSECURITY
CONQUER
THE UNKNOWN

ExtraHop

FIREEYE™

FORTINET®

GOVTECH
SINGAPORE

HUAWEI
HUAWEI CLOUD

ITSEC
ASIA

Marsh

MICRO FOCUS®

YANG PERTAMA DAN UTAMA
MINDEF
SINGAPORE

Privasec

Responsible Cyber

ST Engineering

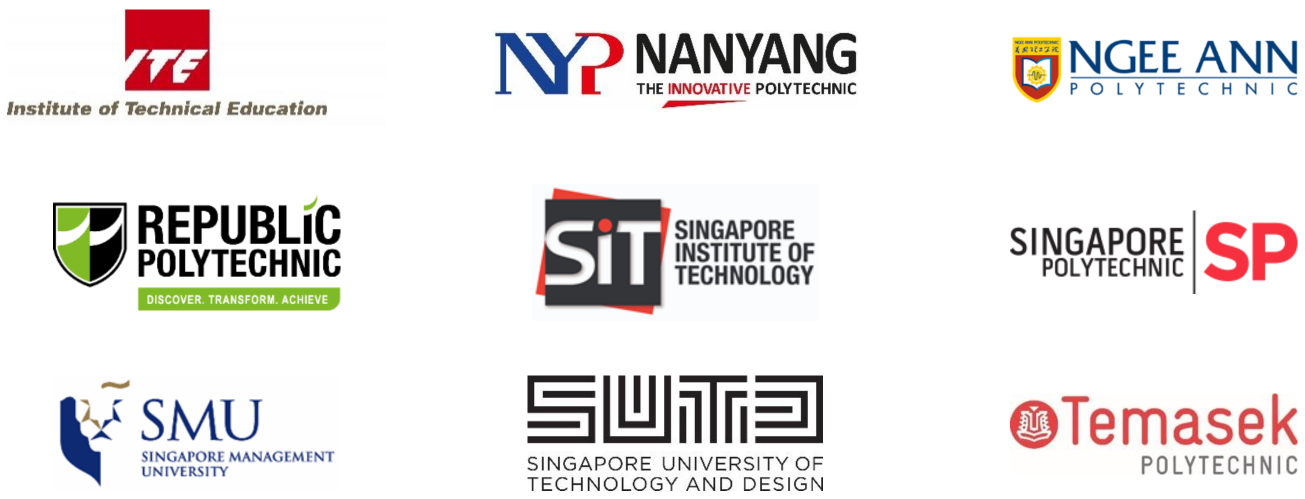
TANIUM.

TREND
MICRO™

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


ITE
Institute of Technical Education
NYP NANYANG
THE INNOVATIVE POLYTECHNIC
NGEE ANN POLYTECHNIC
REPUBLIC POLYTECHNIC
DISCOVER. TRANSFORM. ACHIEVE
SIT SINGAPORE INSTITUTE OF TECHNOLOGY
SINGAPORE POLYTECHNIC SP
SMU
SINGAPORE MANAGEMENT UNIVERSITY
SUTD
SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
Temasek POLYTECHNIC

OUR STORY…

AiSP
Advance Connect Excel

🌐 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

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.