# NEWSLETTER

**December 2020**

Association of
Information Security Professionals

## NEWS & UPDATES

The Association of Information Security Professionals (AiSP) has been able to drive initiatives and engage the stakeholders in Singapore's cybersecurity ecosystem with strong support from our members and partners, especially during the current COVID-19 pandemic.

As AiSP enters into 2021, we reflect on what we have achieved so far. We are amazed by our extended reach to more individuals- including students, and companies and secretariat has been able to achieve more with your unwavering support. **We believe we can continue to do more for the ecosystem with your encouragement!**

The Association would continue to foster a collaborative and inclusive ecosystem for all in Singapore, together with our partners as Singapore rides over the COVID-19 pandemic.

Secretariat hopes to see you in person in 2021!

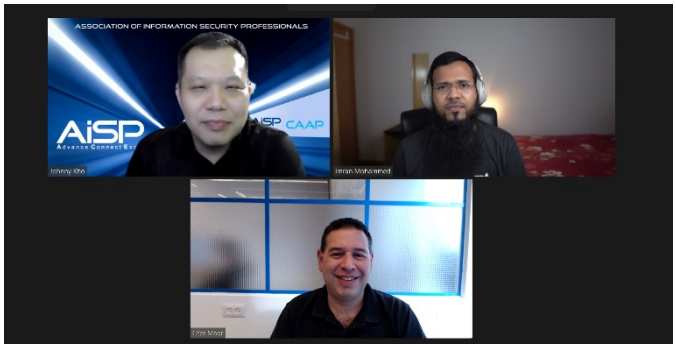
Take care,
Yvonne Wong, MAISP
Associate Director, AiSP

In line with Government's directives on COVID-19 pandemic and AiSP's business continuity plan, AiSP Secretariat is working from home during this period. Please **email us** or **WhatsApp** to our office number (+65 6247 9552), for assistance.

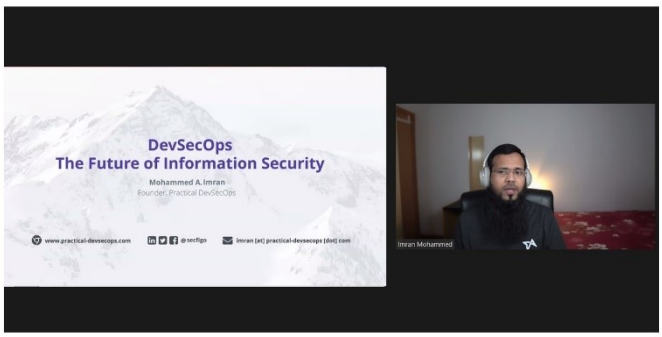
Do check out our **community calendar of events** or follow us on social media for events and updates!

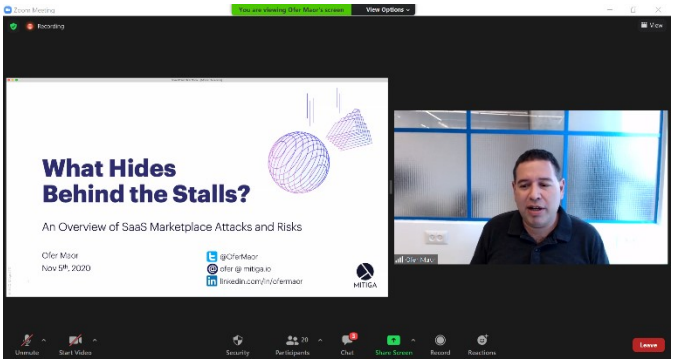
## Knowledge Series Events

### DevSecOps Webinar, 5 Nov 2020



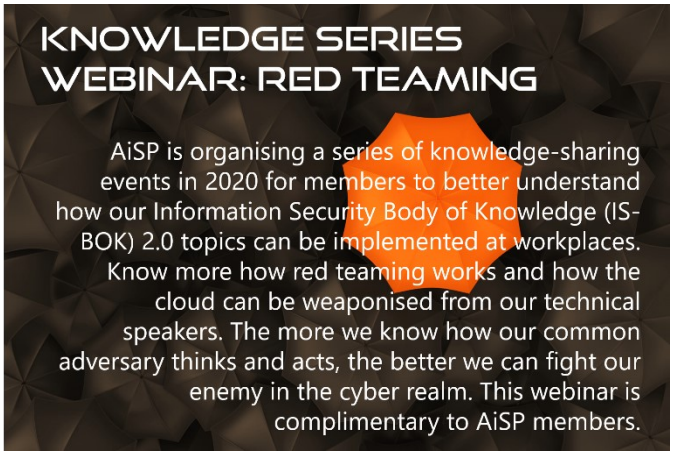

We held our 7th knowledge series webinar- a first for our evening virtual event, focusing on DevSecOps with our speakers from Singapore and Israel, Mr Mohammed Imran, Practical DevSecOps and Mr Ofer Maor, Mitiga.io, representing **Cyber Together**. Our President **Johnny Kho** closed our very first session on this topic and we look forward to *put the Sec in DevOps* in 2021!






The December 2020 webinar would take place at 7:00 pm to 9:00 pm to accommodate more members to attend after work:

- **Red Teaming Webinar**, 2 Dec 2020 (7:00 pm), registration has since closed.




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. We hope our members can catch up with our eight 2020 webinars over the festive season! Please refer to our scheduled 2021 webinars in our **event calendar**.

## Cybersecurity Awareness & Advisory Programme (CAAP)

AiSP's **CAAP** aims to raise cybersecurity awareness among the stakeholders, including associations in the ecosystem. Please feel free to **contact us** if your organisation wants to raise the cybersecurity awareness and adoption.

### SME Cybersecurity Conference, 5 Nov 2020

We organised our second SME Cybersecurity Conference 2020 - A Safer Cyberspace for Singapore Businesses, today! Our experts and practitioners from Singapore's cybersecurity ecosystem, share their insights and advice on how our Singapore SMEs can better managing cyber risks together—as one united community in 2021.
AiSP wants to thank our speakers and sponsors Acronis RSA Security and Workforce Singapore to make this virtual event possible.

We want to thank our panellists for supporting our event today,

1. Guest of Honour: Ms Gwenda Fong, Assistant Chief Executive, Cyber Security Agency of Singapore

2. Mr Craig Dore, Lead IAM Strategist for RSA APJ

3. Dr Stanislav Protassov, Technology President & Co-founder, Acronis

4. Mr Bay Chun How, Director for Consumer Services & Investigation, Personal Data Protection Commission

5. Mr Yum Shoen Yih, Director for Cybersecurity Programme Centre from the Cyber Security Agency of Singapore

The panel was moderated by CAAP Co-Chair **Tony Low**. This half-day event is fronted by

AiSP's Cybersecurity Awareness and Advisory Programme (CAAP), helps SMEs with plans to digitalise ahead in 2021. The event videos are made available for companies to view and we hope it would be useful for their 2021 planning!


Please reach out to us if your company is keen to adopt cybersecurity practices in 2021!

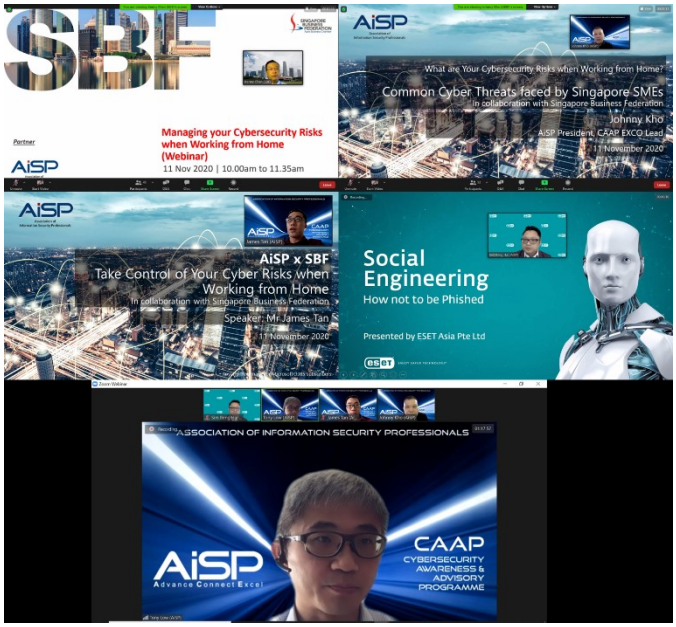
***SME Cybersecurity Conference 2020 Sponsors***

Acronis

RSA

Workforce Singapore

## AiSP x SBF CAAP Awareness Workshop, 11 Nov 2020




AiSP organised its first CAAP Awareness Workshop with the Singapore Business Federation (SBF). As Singapore moves into a Smart Nation, companies are leveraging digitalisation services and products to facilitate digital adoption. Companies adopting work-from-home arrangement during COVID-19 pandemic can be vulnerable to these risks as

their working arrangements are implemented quickly without detailed planning ahead.

We want to thank our speakers for making time to speak at this virtual workshop,

1. Opening and Common Cyber Threats faced by Singapore SMEs by AiSP President, CAAP Exco Lead, **Johnny Kho**

2. Take Control of Your Cyber Risks when Working from Home by **James Tan**, AiSP EXCO Member

3. Social Engineering - how to not to be Phished by Mr Beng Hai Sim, Head of Technical Sales at ESET, Asia Pacific

4. Q&A Panel involving all speakers and moderated by CAAP Co-Chair, **Tony Low**

AiSP has been conducting a series of CAAP events together with industry speakers, with the aim to raise cybersecurity awareness among SMEs. If your organisation is keen to be part of CAAP initiative in 2021, please contact **secretariat** for the membership application today.

Please visit **our website** for update on when the webinar playback is ready in Dec. We have included some useful contents for companies in our **Contributed Contents** as well. Please feel free to tap on them for your cybersecurity journey!

## 2020 APEC SME Cyber Security Forum, 13 Nov 2020

The Asia-Pacific Economic Corporation and the Korea Ministry of SMEs and Startups, organised the 2020 APEC SME Cyber Security Forum to discuss the current status of SMEs, opportunities, and challenges from the Internet and digital economy in APEC region. CAAP Co-Chair **Tony Low** shared about securing cloud environment for SMEs in post-COVID-19 APEC region, at the virtual event.


는 것입니다.
그래서 이런 |


We would like to invite AiSP members to join our **Cloud Security Special Interest Group** as there are exciting activities and projects where our members can deepen their knowledge together in 2021!

## AiSP x TP-SII Focus Group Discussion Workshop for Singapore SMEs offering physical security services, 18 Nov 2020

We collaborated with the Security Industry Institute, Temasek Polytechnic, for 37 participants from Singapore's security industry. Our CAAP Co-Chair Tony Low moderated the focus group discussion (FGD) and covered these areas in the closed-door event,

- What are your experiences in adopting cybersecurity practices in your company?

- Digitalisation has ramped up during this period and many companies have been pushed to do things differently. What would you expect to continue doing in your company in 2021?

- Do you foresee more efforts in implementing cybersecurity practices in your company in 2021?

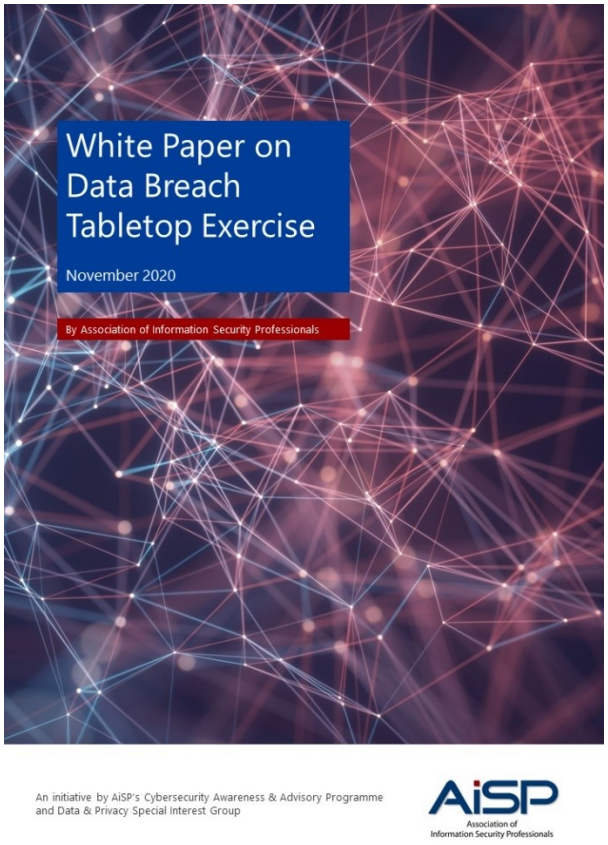
Participants also shared about their plans to enhance their cybersecurity posture, which is the way to go as our companies adapt and improvise their business strategies for 2021.

CAAP plans to conduct more awareness and FGD workshops in 2021, and welcome organisations, partners and associations to collaborate with AiSP! Please **email us** for further discussion.


## White Paper on Data Breach Tabletop Exercise

CAAP conducted AiSP's first virtual Tabletop Exercise (TTX) workshop at PDPC's Privacy Awareness Week in Sep 2020. AiSP has published the white paper on this TTX workshop on its website for companies to access freely.

This is an initiative by AiSP's Cybersecurity Awareness & Advisory Programme and **Data and Privacy Special Interest Group**. We look forward to publishing more white papers in 2021 as part of our CAAP engagement with the sectors and companies.



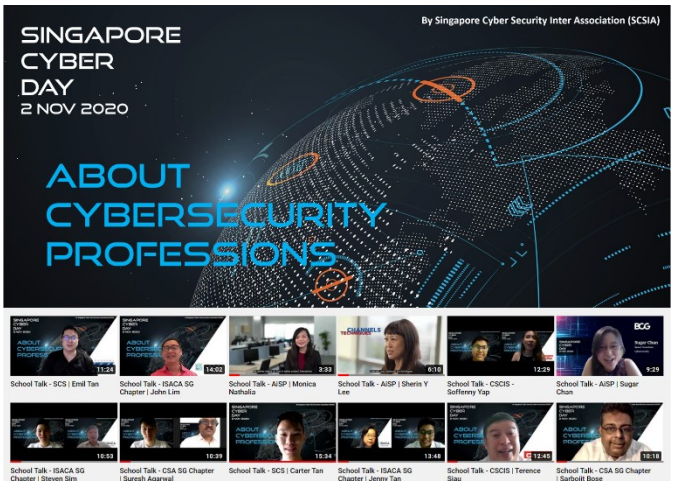

*Please refer to our Contributed Contents as well.*

## Singapore Cyber Day

2 November 2020 is SCSIA's inaugural **Singapore Cyber Day**! The Singapore Cyber Security Inter Association (SCSIA) is organising a series of school talks for secondary school and pre-university students.

The nine members in SCSIA are the Association of Information Security Professionals (AiSP), Centre for Strategic Cyberspace + International Studies (CSCIS), Cloud Security Alliance Singapore Chapter, HTCIA Singapore Chapter, ISACA Singapore Chapter, (ISC)$^2$ Singapore Chapter, The Law Society of Singapore, Singapore Computer Society and SGTech.

### Singapore Cyber Day – SCSIA School Talks, 2 Dec 2020




AiSP wants to thank our 12 volunteers for making time to share their journeys and experiences with our students!

- Sarbojit Bose
- Terence Siau
- Jenny Tan
- Carter Tan
- Suresh Agarwal
- Steven Sim
- Sugar Chan
- Soffenny Yap
- Sherin Y Lee
- Monica Nathalia
- John Lim
- Emil Tan

We hope our youths can learn more about our industry and how they can further their interest in cyber security. Please **contact us** if your schools are keen to organise talks in 2021.

### Singapore Cyber Day – SCSIA School Talks: Q&A session on Cybersecurity Professions, 2 Dec 2020

Secretariat facilitated a Q&A session with our three speakers to address students' queries on cybersecurity professions,

- Ms Jenny Tan who is the Global Internal Audit Leader for Capitaland, and she volunteers in the ISACA Singapore Chapter.

- Ms **Soffenny Yap**, Business Development, Trend Micro, who volunteers in the Centre for Strategic Cyberspace + International Studies, Singapore Computer Society (CSCIS) and AiSP. Soffenny is also one of our mentors for the **Ladies in Cyber** mentorship programme for female IHL students.

- Mr Terence Siau who co-founded TINDO Pte Ltd, and he is the General Manager of CSCIS Singapore chapter.

This segment would be uploaded soon in our **YouTube channel** to benefit more students.

## Regionalisation

AiSP Secretary **Huynh Thien Tam** spoke at MFA-SCP Smart Nation: Strategies, Opportunities and Cybersecurity Management (Civil Service College), on Countering Emerging Technology's Potential for Malicious Abuse, to remote participants worldwide today - including ASEAN countries, Africa, Egypt, Hungary and Seychelles.


We want to work with more overseas partners on adoption of **AiSP Information Security Body of Knowledge 2.0** and the **Qualified Information Security Professional (QISP®)**. Please **contact us** for collaboration.

## CyberFest™ 2021

**CyberFest®** is a community-led initiative that would take place from 1 to 5 Feb 2021 in Singapore. AiSP is awaiting the announcement of Phase 3 in Dec 2020 and would include some virtual events during **CyberFest®** to cater to local and overseas participants.

Our event line-up (tentatively) is as follows:

1. Ladies in Cyber networking seminar, 1 Feb 2021
2. AiSP x NTUC Career Talk on cybersecurity industry, 1 Feb 2021
3. ASEAN Cybersecurity Forum, 2 Feb 2021
4. Student Volunteer Recognition Programme Award 2020 ceremony, 3 Feb 2021
5. CRESTCon Singapore 2020/2021, 4 Feb 2021
6. The Cybersecurity Awards 2020 ceremony, 5 Feb 2021

Please **let us know** if you want to be part of these events as a speaker, sponsor or participant!


## The Cybersecurity Awards

**The Cybersecurity Awards (TCA) 2020** seeks to honour outstanding contributions by individuals and organisations, to local and regional cybersecurity ecosystems. In view of COVID-19 pandemic and well-being of our guests at the award ceremony, AiSP has moved the physical event on 6 Nov 2020 to **5 Feb 2021**.

We would like to give a shout-out to our 2020 sponsors and look forward in publishing the knowledge-sharing articles by our partners in 2021!

***TCA2020 Sponsors***














## Student Volunteer Recognition Programme (SVRP)

The SVRP working committee would be reviewing our nominees' submission in Dec 2020 ahead of its award ceremony in Feb 2021.

Our student volunteers have not taken a backseat during COVID-19 pandemic and we want to recognise those who hold leadership positions in their student chapters and student interest groups. Under AiSP's **Academic Partnership Programme (APP)**, the IHLs would 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 expand the list in 2021!

We would be having a student volunteer drive in Dec 2021 during the Inter-poly CTF and CYSummit 2020! Please **email us** if you are keen to be part of this initiative.

## Ladies in Cybersecurity Charter

Under our **Ladies in Cybersecurity Charter**, AiSP's volunteer team of female cybersecurity professionals have been mentors to female students through our Ladies in Cyber Mentorship Programme. We welcome female volunteers and students to join our programme as **mentors** and **mentees** (please see online forms).

### Ladies in Cyber ITE School Talk, 6 Nov 2020

Our Ladies in Cyber Mentors shared about their cybersecurity journey with 30 ITE female students via a virtual school talk today. Some of the topics covered include how did they join the cybersecurity industry, and the subjects or

topics that would be helpful to students interested in cyber security.

We want to thank our five mentors for making time to share their experiences,

- **Alina Tan**
- **Catherine Lee**
- **Eileen Yeo**
- **Faith Chng** and
- Tan Mei Hui

The ladies shared how they joined the cybersecurity industry, with ITE students. The session also covered their work experience in private and public sectors and the subjects and skillsets students could take up to further their interest in cyber security.

To benefit more students, the recording is made available on **AiSP YouTube channel**. We encourage IHLs to get in touch with us to plan out school talks in 2021, please **email** us today!

ITE is one of our **Academic Partners**, where our partnering IHLs' current full-time students in all schools are offered complimentary Affiliate membership, not limited to just information security or cybersecurity disciplines. Please visit email us at secretariat@aisp.sg if you have any query.

AiSP hopes to work closer with our industry partners to attract more female cyber professionals in Singapore. Please **contact us** if your organisation would like to take this conversation further.

## Special Interest Groups

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

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

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

We wish to remind our members to renew their 2021 membership by **12 Dec 2020**, before the expiry date of 31 Dec 2020.


## 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 Jan 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 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 and hybrid events in 2021 are as follows (*may be subjected to changes*),

1. Data Security – PDPA Amendments, 12 Jan
2. Cyber Threat Intelligence (CTI), 10 Feb
3. Governance and Management, 17 Mar
4. Cloud Security SIG, 30 Mar 2021 (hybrid)
5. Software Security, 14 Apr
6. Physical Security, Business Continuity and Audit, 12 May
7. Security Architecture and Engineering, 16 Jun
8. Data and Privacy SIG, 29 Jun (hybrid*)
9. Operation and Infrastructure Security, 14 Jul
10. OT/IOT – IoT Security, 18 Aug
11. Cyber Defence – Ethnical Hacking, 15 Sep
12. CTI SIG, 29 Sep (physical event with recording)
13. Security Operations – Incident Response Management, 13 Oct
14. Emerging Trends - Blockchain, 10 Nov
15. Emerging Trends – AI for Cyber Security, 8 Dec
16. IoT SIG, 22 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!**

**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.

## 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.

### Temporary suspension of CCT Info and CCT App exams till early 2021

As of 3 Sep 2020: Further to CREST International's previous updates on 12, 17 and 20 Aug 2020, CREST has been conducting an investigation into the recent deposit of confidential exam material into the public domain.

### CRESTCon Singapore 2020/2021

The CREST Singapore Chapter is organising the **first CRESTCon Singapore 2020/2021** on 4 Feb 2021 and has invited presenters to submit their topics by **31 Dec 2020**. Please **email secretariat** if your organisation is keen to submit paper or sponsor the event!


## UPCOMING ACTIVITIES/ EVENTS

### Ongoing Activities

| Date | Event | By |
|---|---|---|
| Jan-Dec | Call for Female Mentors (Ladies in Cyber) | **AiSP** |
| Mar-Dec | Call for Volunteers (AiSP Members) | **AiSP** |
| Jan-Dec | CRESTCon Call for Paper | **AiSP** |

### Upcoming Events

| Date | Event | By |
|---|---|---|
| 1 Dec | SCSIA School Talks – Q&A session on Cybersecurity Professions | AiSP & Partners |
| 2 Dec | [BOK] Knowledge series webinar – Red Teaming | **AiSP** |
| 4-6 Dec | STACK the Flags 2020 CTF | Partner |
| 4 Dec | Webinar for DPO/CISO – Securing Personal Data for Organisation | Partner |
| Dec | Inter-poly CTF: Lag and Crash | Partner |
| 18-21 Dec | CYSummit 2020 | Partner |
| 2 Jan 2021 | SINCON 2020 Conference | Partner |
| 12 Jan | [BOK] Knowledge series webinar – Data Security: PDPA Amendments | AiSP & Partner |
| 1 Feb | [Ladies in Cyber networking seminar | **AiSP** |
| 1 Feb | AiSP x NTUC Career Talk on cybersecurity industry | AiSP & Partner |

| Date | Event | By |
|---|---|---|
| 2 Feb | ASEAN Cybersecurity Forum | **AiSP** |
| 3 Feb | SVRP Award 2020 ceremony | **AiSP** |
| 4 Feb | CRESTCon Singapore 2020/2021 | **AiSP & CREST SG Chapter** |
| 5 Feb | The Cybersecurity Awards 2020 ceremony | **AiSP** |
| 10 Feb | [BOK] Knowledge series webinar – Cyber Threat Intelligence | **AiSP** |

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

## Contributed Contents

*Insights from our Data and Privacy SIG*

The Data and Privacy SIG's founding members shared their views on the recent amendments to Singapore's Personal Data Protection Act (PDPA). Lim Ren Jun is a Principal at Baker McKenzie Wong & Leow and Honorary Legal Advisor on AiSP EXCO, while Yvonne Wong is the Associate Director and the Data Protection Officer at AiSP.

*Note: Hyperlinks are underlined for reference.*

***Based on the amendments to the PDPA, do you think Singapore companies are more prepared in their data protection measures?***

**Ren Jun (RJ):** Broadly, yes. The introduction of new obligations under the Personal Data Protection (Amendment) Bill (the "Bill") such as the requirement to notify the PDPC and individuals in the event of a data breach, can help companies develop more comprehensive data protection plans. This is supported by additional measures such as the development of the Data Protection Starter Kit or by offering organisations the opportunity outsource their data protection functions via the Data-Protection-as-a-Service initiative.

Moving forward however, further clarity on the PDPA amendments would be helpful. The new Data Portability Obligation for example, would need to be supplemented by further Regulations to address matters such as the categories of data that should be portable, alongside other technical and consumer protection details (see Mr. S Iswaran's Opening Speech at the Second Reading of the Personal Data Protection (Amendment) Bill 2020 at [29] and his Closing Speech at [47]).

Terms that have remained unaffected by the Bill may also warrant future scrutiny**.** For example, the meaning of "an individual acting in a personal or domestic capacity" (s4(1)(a) PDPA) may have to be re-examined in light of the increasingly amorphous nature of employment relationships caused by developments like the gig economy and the shift towards WFH arrangements to help companies determine to whom the PDPA applies to.

**Yvonne Wong (YW):** I have a different view.

Prior to COVID-19 pandemic, most SMEs are starting to embark on their PDPA compliance. I noticed most of them do so as they are concerned about fines, negative publicity or if their customers required them to do so. It is common to see that not many of them have a data protection notice in place nor a contact person (i.e. data protection officer or DPO) for

enquiries. COVID-19 pandemic has caused extensive business disruptions where companies are facing survival issues. They do not have the bandwidth to embark on or enhance their compliance efforts.

However, the move for the amendments has to take place as Singapore's economy and companies are closely intertwined with regional and global commerce links. After the General Data Protection Regulation (GDPR) went into effect on 25 May 2018, countries and companies with close ties with the European Union have moved quickly to incorporate the GDPR to their data protection framework and implementation.

If Singapore lags behind this global development, our companies would not be able to capture a wider market share confidently when the COVID-19 situation improves.

***What are the three key things you feel the companies need to prepare ahead for implementation?***

**RJ:** First and foremost, companies should focus on strengthening their data protection practices and developing a coherent data breach management plan if they have not done so in light of the new data breach notification obligations and harsher penalties for PDPA non-compliance. This is an especially critical step, given that these two amendments do not appear to have a sunrise or transitional period.

Second, I believe that companies must review and amend their existing privacy policies in order to ensure compliance with the brand-new obligation to preserve copies of personal data ("Preservation Obligation"). This should be accompanied by the relevant infrastructural changes such as the development of a data retention schedule.

Third and more generally, companies should keep abreast of any new guidelines or developments that may be released by the PDPC which would offer clarity on how the new PDPA provisions will apply in practice. In particular, Mr. Iswaran indicated the future release of Regulations and/or Advisory Guidelines relating to (i) data protection (Closing Speech at [24]); (ii) compliance with the new Data Portability Obligation (Closing Speech at [47]); and (iii) the offence rendering an individual liable for the egregious mishandling of personal data (Closing Speech at [58]).

**YW:** In addition to what Ren Jun has shared on breach responses, policies and importance to stay ahead on PDPA developments, I feel it is important for companies to consider from the risk management perspective,

1. If you cannot protect the personal data entrusted to you, it is risky to collect and retain it. Do consider data minimisation where applicable.

2. Identify your gaps in your current data protection practices, and if they are sufficient to reduce risks in unauthorised disclosure and malicious activities. For instance, an information security audit.

3. Plan-Test-Update your processes. For companies to demonstrate accountability, they should have tried-and-tested workflows to ensure confidentiality, integrity and availability of companies'

critical data in a realistic and practical manner. Testing such as tabletop exercise, is important to ensure you know the vulnerabilities.

***In your opinion, what is the most common issue our companies experienced on their data protection practices during COVID-19 pandemic?***

**RJ:** Cyber attacks seem to be the most common problem; with the education (see here) and healthcare sectors (see here) being heavily impacted. In my view, this is unsurprising. Given the pressure the COVID-19 pandemic exerted on companies to move their services online, companies, in their haste, may have not paid enough attention to cybersecurity and data protection arrangements.

More generally, there were also a number of recent high profile data breaches affecting platforms such as Grab, Eatigo, and Lazada.

**YW:** The fact that malicious actors have increased phishing attacks significantly during the WFH arrangement worldwide, underscores how vulnerable and unprepared we are as remote workers.

This means technical controls in devices and platforms, may not be updated before WFH arrangement is deployed on short notice. Personnel's Internet connection and router setup in home environment are likely not to be very secured as compared to workplaces. Coupled with remote IT support and users' limited understanding of the threat scenarios, these conditions create a perfect storm for WFH personnel to be susceptible to frauds, cyber attacks and social engineering.

***What you hope to see in Singapore's data protection practices and trends in 2021?***

**RJ:** First, I hope to see companies capitalise on the expanded (i) exceptions to the consent requirement and (ii) definition of "deemed consent" as these amendments were made to support data use for business innovation and to accommodate the realities of modern commercial arrangements (Opening Speech at [33]).

Next, I would like to see more active private enforcement of the PDPA (i.e. by seeking relief via civil proceedings under s 32 PDPA or by raising a complaint to the PDPC). While the Bill's harsher penalties and new offences for the egregious mishandling of personal data may go some way towards incentivising compliance with the PDPA, I believe this must be accompanied by an increased likelihood that would-be offenders are actually caught and punished. More active private enforcement to this end, may increase the detection of potential PDPA non-compliance by increasing the number of entities scrutinising/monitoring the market for potential breaches.

Finally, I hope to see further guidance on how to discharge the PDPA's data protection obligation. In my view, "reasonable security arrangements" remain an open textured term as what is "reasonable" will depend on a factors such as the sensitivity of the data in question (Aviva Ltd [2017] SGPDPC 14 at [16]). Consequently, further guidance by the PDPC on this would provide clarity and potentially, best practices to help companies tailor their data protection practices based on their business needs. This may be especially helpful

to companies operating in emerging sectors, such as telemedicine providers.

**YW:** I hope more companies start to reflect on their role as custodians for the personal data entrusted under their care and adopt a security-by-design approach as they digitalise their businesses. There should be proactive efforts to minimise the harm and impact arising from data breaches, to affected individuals.

DPOs should be encouraged to deepen their understanding and contextualise their knowledge for various scenarios as there is no quick nor simple answer on data protection practices, and cyber threats evolve. Thus, we hope to encourage more AiSP members in building their knowledge on a continuous basis, through their involvement in the **Data and Privacy SIG**.

AiSP welcomes our Associate and Ordinary Members' **contribution and participation to knowledge-sharing activities** in the information security domains. **Please write to us (membership@aisp.sg) if you want to volunteer!**

**New Corporate Partners for 2021**

We would like to welcome our new partners **BitCyber** and **ST Engineering** for 2021!

BitCyber
Securing Your Business

BitCyber's mission is to target the complexity out of cybersecurity, making cyber defence accessible to every business, securing organisations against cyber attacks, data breaches and business disruptions.

ST Engineering

ST Engineering is a global technology, defence and engineering group specialising in the aerospace, electronics, land systems and marine sectors. Under its Defence & Public Security, it will be driving thought leadership and next-generation products and solutions for customers in defence, public security and critical infrastructure segments.

As all stakeholders have a part to play in Singapore's ecosystem, AiSP offers three types of group members for companies:

- Startups
- Companies
- Large organisations

AiSP has since included two more benefits for both Academic and Corporate Partners in 2020,

- Complimentary Affiliate membership to all full-time students from the Academic Partners (i.e. IHLs). This would be extended to all current students in all schools, not just for information security or cybersecurity disciplines.

- Listing of relevant cybersecurity events organised by our corporate partners, on AiSP Community Events webpage.

Please refer to the benefits and rates for **our partners**, and be plugged into Singapore's cybersecurity ecosystem today!

**Keen to share your organisation's initiatives, updates and insights to the cybersecurity community?** Please email to secretariat@aisp.sg if you would like to be our event sponsors or corporate partners!

## MEMBERSHIP

**AiSP membership cycle starts on 1 Jan, this means all members on annual fee should pay 2021 membership by Nov 2020.** This is to ensure there is no disruption to your membership and benefits.

We encourage Ordinary and Associate Members to pay for 3-year membership for the convenience and there is saving as compared to repetitive annual fee payment.

**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.

**Your AiSP Membership Account on Glue Up**

AiSP has moved its digital membership to EventBank, now known as Glue Up, an all-in-one cloud platform for event and membership management. You can access the web portal or the mobile application (App Store, Google Play), **using the email address you have registered your AiSP membership for**.

**There is no need to create another profile if you are using a different email address; you can just update your alternative email address in your membership profile.** 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!**

| 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.<br>▪ Regular updates on membership activities.<br>▪ Free and discounted rates for events organised by AiSP and partners.<br>▪ Priority for activities, talks and networking events.<br>▪ AVIP members enjoy Professional Indemnity coverage in Singapore and overseas. |

| Type | Benefits |
|---|---|
| **Corporate Partner Programme (CPP)** | ▪ Listing on AiSP website as a Corporate Partner<br>▪ Free and discounted rates for events |

| | |
|---|---|
| | organised by AiSP and partners.<br>▪ Complimentary AiSP Affiliate membership for organisation's personnel.<br>▪ Special invite as speakers for AiSP events.<br>▪ 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). |

| Type | Benefits |
|---|---|
| **Academic Partnership Programme (APP)** | ▪ Inclusion of an AiSP Student Chapter for the Institute.<br>▪ Ten (10) complimentary AiSP Affiliate membership for personnel from the Institute.<br>▪ Complimentary AiSP Affiliate membership for all existing full-time students in the Institute, not limiting to cyber/infosec domains.<br>▪ Listing on AiSP website as an Academic Partner.<br>▪ One annual review of Institute's cybersecurity course curriculum. |
| | ▪ AiSP speakers to speak at Student Chapter events, including briefings and career talks.<br>▪ Free and discounted rates for events organised by AiSP and partners.<br>▪ One complimentary info/cybersecurity or internship post in AiSP website per month. |

**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.

**AVIP Membership**

AiSP Validated Information Security Professionals (**AVIP**), the 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.

## CONTACT US

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

AiSP outreach and programmes are made possible by our Partners.

## Corporate Partners

## Academic Partners


Association of Information Security Professionals

+65 6247 9552 (**WhatsApp**)

secretariat@aisp.sg

www.aisp.sg

116 Changi Road
#04-03 WIS@Changi
Singapore 419718


The Association of Information Security Professionals (AiSP), formed in 2008, is an independent cybersecurity association that believes in developing, supporting and enhancing industry technical competence and management expertise to promote the integrity, status and interests of Information Security professionals in Singapore.

We believe that in promoting the development of cybersecurity and increasing and spreading of cybersecurity knowledge can shape more resilient economies.

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

- promoting the integrity, recognition 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.