NEWSLETTER

October 2022

NEWS & UPDATE

New Partners

AiSP would like to welcome Right Hand Cybersecurity as our new Corporate Partner. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem.

Continued Collaboration

AiSP would like to thank CISCO for their continued support in developing the cybersecurity landscape:

News and Updates

AiSP x IASA Seminar Enhance IT Security With Enterprise Architecture

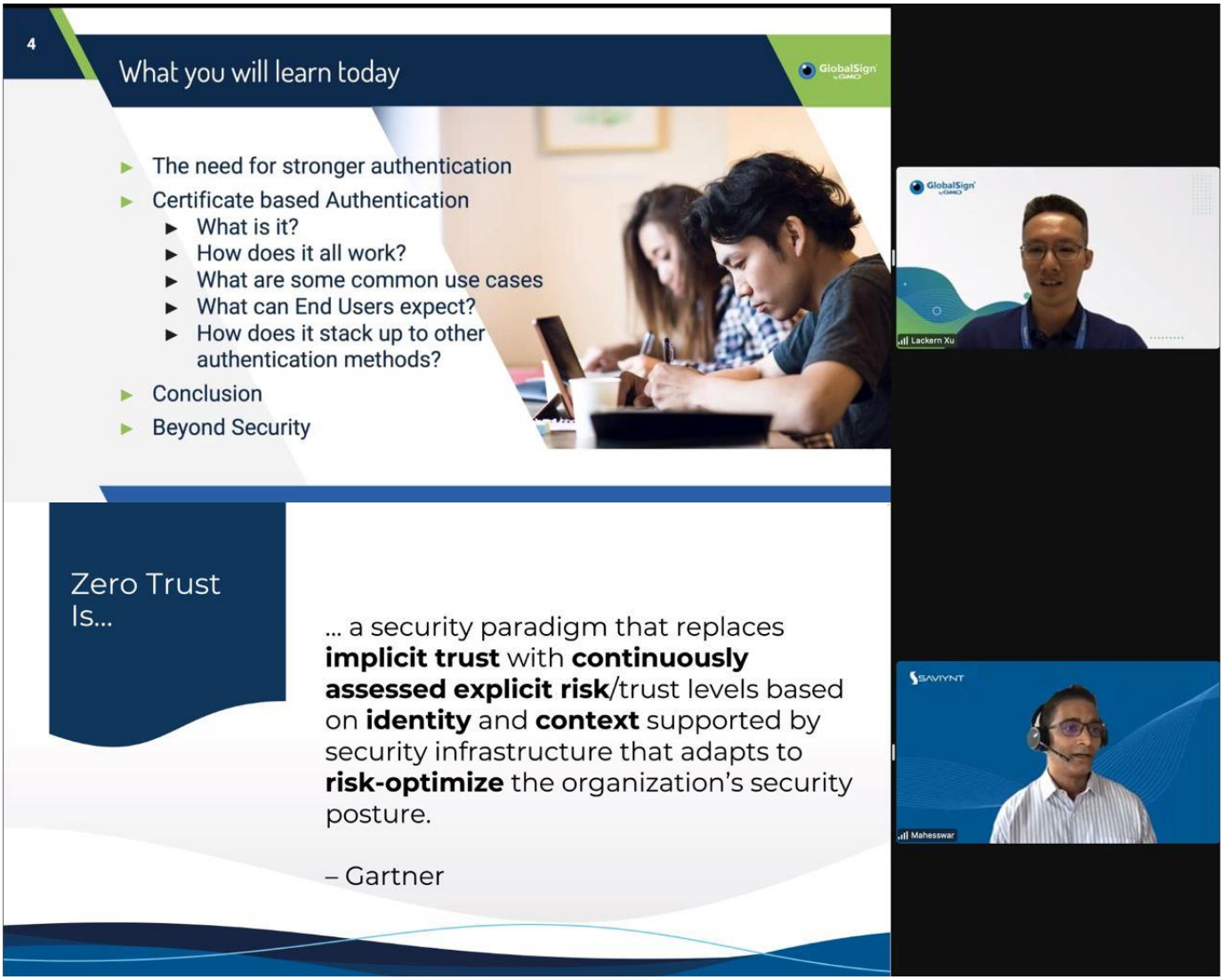
On 20 September, AiSP and International Association of Software Architects (IASA) Asia Pacific did a joint event on Enhance Cybersecurity with Enterprise Architecture. AiSP Immediate Past President, Dr Steven Wong and IASA Asia Pacific co-founder & Chairman, Aaron Tan also signed the renewal of partnership MOU between AiSP and IASA Asia Pacific. A panel discussion on Enhance Cybersecurity with Enterprise Architecture was held and the panel included Mr Jonathan Gardiner (Linfox Logistics) and Mr Edison Tie (Income Insurance Limited) who shared their perspectives and knowledge on this area.

back to top

Knowledge Series Events

Identity & Access Management on 14 September

As part of Digital for Life Movement, AiSP hopes to help Singaporeans of all ages and walks of life to embrace digital learning as a lifelong pursuit. On 14 September, we invited our Corporate Partner, GlobalSign APAC and Saviynt to share insights on Identity & access management with the participants. We hope the participants have gained more knowledge on this aspect of Cybersecurity.



back to top

Upcoming Knowledge Series

Internet of Things on 19 October

AiSP Knowledge Series – Internet of Things

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

Cybersecurity and the Internet of Things
Speaker: Tan Tzen Haw, Senior Consultant & Wong Jia Ping, Consultant, Boston Consulting Group

In this session, you will understand more about IT and OT convergence, the benefits, as well as the best practices for securing OT systems.

- Emerging OT Trends
- Benefits of IT and OT convergence
- Cyber implications of IT & OT convergence
- Best practices for securing OT systems

back to top

Your Classic Cybersecurity IT Skills Will Not Ensure a Smooth IoT Journey
Speaker: Ben Smith, Field CTO, NetWitness

Too many organisations start their IoT journey with the assumption that they can re-use their existing tooling and processes to protect that infrastructure. Join this talk to learn about foundational information security concepts from IoT and the broader CPS (cyber-physical security) space, including the critical importance of visibility and continuous monitoring, data-centric vs. asset-centric security, and even the "people" components of staffing the right skillsets and building an appropriate organisational structure. This talk will close out with a handful of book recommendations for further study, for both the technical and the business professional.

IoT Security, not just a thing "Thing"
Speaker: Gerard De Las Armas, Principal Consultant, wizlynx group

In this presentation, you will get an insight into what an IoT device is and the complex infrastructure needed to operate it.
After that, we'll get into the depths! We will look at the IoT attack surface using real industry cases.

To wrap-up the session, we will show you various examples of IoT/IIoT devices exposed to the Internet and how easy it may be to compromise them by demonstrating a live hack of a connected camera.

Date: 19 October 2022, Wed
Time: 2.30PM – 4.30PM
Venue: Marina Bay Sands, Room GW4 (3412), level 3
Registration: https://forms.office.com/r/GBAWHq21tp
* All attendees to register for the GovWare visitor Pass at https://www.gevme.com/sicw-govware2022 in order to attend the event.

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

1. Internet of Things BOK Series, 19 Oct 22
2. DevSecOps BOK Series, 17 Nov 22

Please let us know if your organisation is keen to provide speakers! Please refer to our scheduled 2022 webinars in our event calendar.

back to top

Cybersecurity Awareness & Advisory Programme (CAAP)

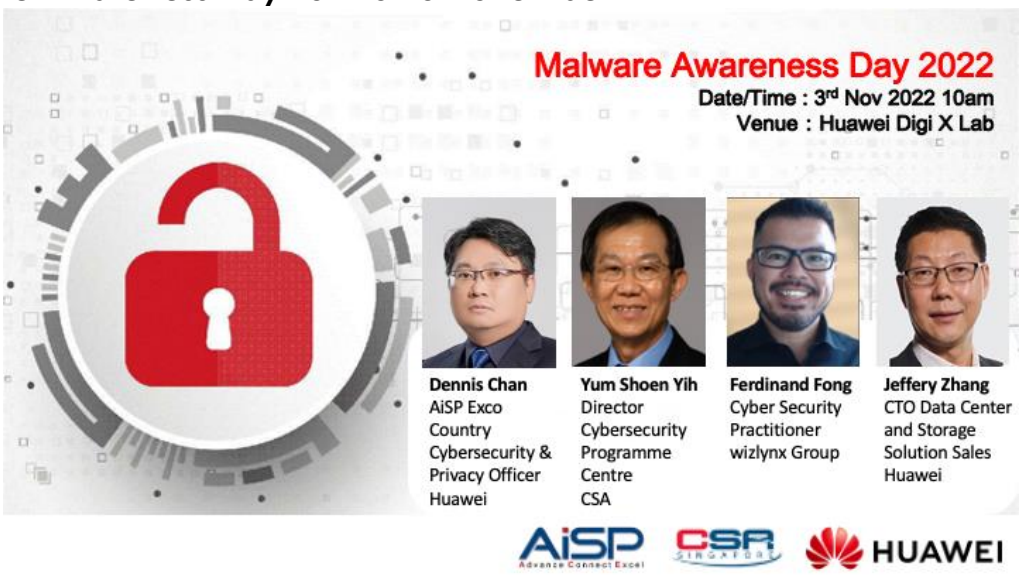
TAC Knowledge Series on Cybersecurity and Data Protection on 26 September

AiSP Vice-President & CAAP EXCO Lead, Mr Tony Low joined Cyber Security Agency of Singapore - CSA and Personal Data Protection Commission (PDPC) in the Trade Association Chamber (TAC) Knowledge Series on Cybersecurity and Data Protection organised by Singapore Business Federation (SBF) on 26 Sep 22 afternoon to share more on AiSP and AiSP Cybersecurity Awareness & Advisory Programme (CAAP). Tony also facilitated a group discussion activities for the attendees from the other 29 associations on the importance of Cybersecurity and Data Protection. Thank you SBF for inviting AiSP to the event.

back to top

Upcoming CAAP Event

Anti Malware Awareness Day 2022 on 3 November



3rd November has been dedicated as Anti-Malware Day. On this day we would like to honour all the cybersecurity professionals at the frontline and behind the scene on the collective effort to stamp out on malware. There is no better way to prevent malware than raising awareness hence Huawei together with AiSP will like to present you Malware Awareness Day on 3rd November at Huawei DigiX Lab. Come and hear from our VIP speakers Mr Yum from CSA, Ferdinand Fong from Wizlynx and Jeffery Zhang from Huawei.

Email karen.ong@aisp.sg to RSVP now.

back to top

AiSP Cybersecurity Awareness E-Learning

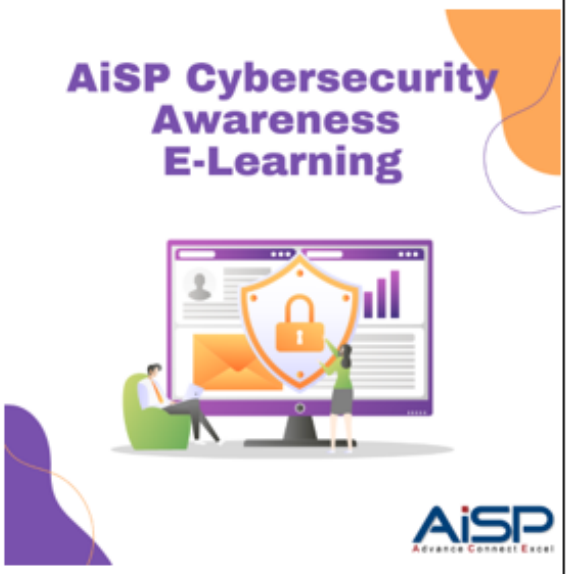
AiSP Cybersecurity Awareness E-Learning

On 7 January 2022, the Association of Information Security Professionals (AiSP) launched the Cybersecurity Awareness E-Learning. It was launched by Ms Gwenda Fong, Assistant Chief Executive (Policy & Corporate Development) of Cyber Security Agency of Singapore.

In this E-Learning, we will bring you through a set of materials that will prepare your Business and your employees to embark on an exciting journey in digital transformation and start your Business to be more secure.

We will be covering:

1. Providing businesses with an understanding of the current digital business landscape
2. Deep dive into understanding the Digital better Transformation Journey
3. Risk and threats for the Business to understand some of the most crucial aspects and assessments.
4. How you can start to explore and secure your Business by handling data securely and setting up your initial cybersecurity framework
5. Providing an understanding of your Business Obligations and the various regulations that will impact your process and impact the Business. Sharing of different policies and guidelines such as PDPA, Cybersecurity Act, Computer Misuse Act
6. Your responsibility to ensure in the event of an incident, how the enterprise should handle



back to top

Why Should You Take This E-Learning & How Will It Help You?

Through this E-learning, we prepare your business and your employees to kickstart your journey in digital transformation and be more cyber safe. With the various contents provided in the E-Learning which will be update consistently, you have be able to have a better understanding on the digital business landscape and how to set up your initial cybersecurity framework.

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

Why Is this E-Learning Special?

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

Subscription Plan

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

*Minimum 1 year subscription

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

Please contact AiSP Secretariat at secretariat@aisp.sg if you have any queries.

SME Cybersafe provides

Enhanced Security Awareness & Training

Cohesive Security Knowledge Resources

Security Solutions & Services Support

Click here to find out more about the E-Learning.

back to top

Student Volunteer Recognition Programme (SVRP)

Student Volunteer Recognition Programme Awards Ceremony on 16 November 2022

SVRP Nomination has officially concluded, and results has been released on our website here. Our student volunteer drive is ongoing till Dec 2022 for those who are interested to volunteer but not sure where to start. Please click here to apply today. The fourth SVRP Awards Ceremony will be held on 16 November 2022 at SIT@Dover.

The Awards Ceremony is sponsored by:

back to top

AiSP Cyber Wellness Programme

Click here to find out more!

back to top

Ladies in Cybersecurity

Ladies Talk Cyber Series

For the Fifteenth edition of AiSP's 'Ladies Talk Cyber' series, we interviewed Ms Lim Shin Yi, who is currently working as a Senior Assistant Director, Economic Development at Cybersecurity Agency of Singapore (CSA).

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

Cybersecurity is an important growth sector in Singapore's economy and digital future. There is a growing need to strengthen Singapore's cybersecurity capabilities so as to protect our cyberspace. Shin Yi is part of a dynamic team that looks into growing a robust cybersecurity talent pipeline through programmes on talent development under SG Cyber Talent, a national initiative by the Cyber Security Agency of Singapore (CSA). She works with internal and external stakeholders such as employers, government agencies, industry associations and training providers to grow and develop the cybersecurity workforce, and create job opportunities for Singaporeans.

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

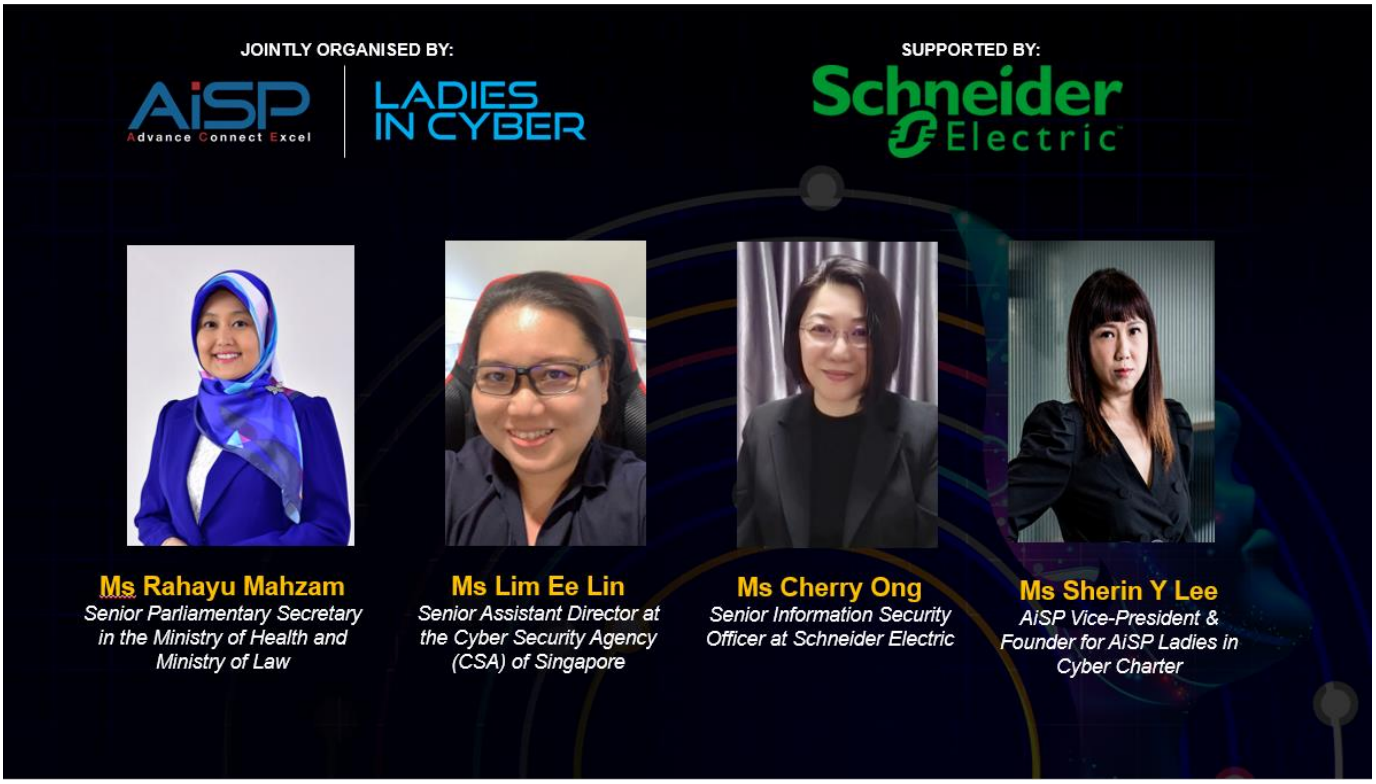
back to top

Learning Journey to Ensign InfoSecurity on 6 Sep

As part of International Women in Cyber Day Celebrations, AiSP and Ensign InfoSecurity organised a learning journey to Ensign on 6 Sep 22. This was followed by a Dialogue Session with Minister of State for Education & Manpower, Ms Gan Siow Huang. More than 100 students attended this hybrid session where they visited Ensign's Executive Briefing Centre and interacted with Ensign's female staff to get to know more about career in Cyber as well as the challenges that the industry faces. We would like to thank our Panellists, Ms. cAsh Chng, MOS Gan Siow Huang, Ms. Jackie Low and our Moderator, Ms. Sherin Y Lee, for sharing their personal experiences with the participants.

back to top

Learning Journey to Schneider Electric on 15 Nov



AiSP will be organising the Ladies in Cyber Learning Journey to Schneider Electric on 15 Nov 22. As part of the Learning Journey, we will be having a dialogue session at the event itself. The dialogue session will be sharing about support ladies in their career in Singapore.

We are honoured to have Ms Rahayu Mahzam (Senior Parliamentary Secretary in the Ministry of Health and Ministry of Law) for the dialogue session together with Ms Lim Ee Lin (Senior Assistant Director at Cyber Security Agency of Singapore), Ms Cherry Ong (Senior Information Security Officer at Schneider Electric). Ms Sherin Y Lee, AiSP Vice-President and Founder for Ladies in Cyber Programme will be the moderator for this event. The event is open to all female students in tertiary level.

The details for the event are as follow:

Date: 15 Nov 22 (Tues)
Time: 6.15pm to 9pm
Venue: Schneider Electric, 50 Kallang Avenue, Singapore 339505
Dress code: Smart Casual (No wearing of shorts and slippers)
Guest of Honour: Ms Rahayu Mahzam, Senior Parliamentary Secretary in the Ministry of Health and Ministry of Law

Click here to register.

back to top

Cloud Security Summit 2022

AiSP organised the inaugural Cloud Security Summit with the partnership and support from NTUC U Associate & Tech Talent AssemBly (TTAB) on 26 September 2022. Participants were intrigued by the speakers who shared insights on the various aspects of cybersecurity such as Operational Technology, Kubernetes, shaping cybersecurity in emerging technologies and more. We would like to thank all our speakers who shared their knowledge with our participants. Thank you SMS Tan Kiat How for gracing the event and AiSP Vice President, Mr Tony Low for the opening address.

We would also like to thank our following sponsors: Armis, Nozomi Networks, ONESECURE Asia Pte Ltd, Thales, Lookout & Xcellink Pte Ltd for making the event possible. This event would not be a success as well without our supporting agencies: Cyber Security Agency of Singapore (CSA) and Government Technology Agency of Singapore (GovTech).

back to top

Special Interest Groups

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

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

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

back to top

AiSP IoT SIG Networking Session on 4 November

Register here

back to top

Digital for Life

Celebrate Digital @ Kreta Ayer-Kim Seng on 18 September

As part of Digital of Life Movement, AiSP and our Corporate Partner, Trend Micro were at Celebrate Digital @ Kreta Ayer-Kim Seng held at Chinatown Point on 18 September. We would like to thank Minister Josephine Teo for visiting our booth. AiSP Secretary and Co-Lead for Cyberwellness, Faith Chng, also conducted a workshop on Scam to over 50 senior citizens on cybersecurity in Mandarin.

back to top

Celebrate Digital @ Chong Pang on 24 September

On 24 September, AiSP went to Celebrate Digital @ Chong Pang to share on cybersecurity tips and knowledge with the residents at Yishun. We would like to thank Minister K Shanmugam for visiting our booth and our AiSP Secretary & Cyberwellness Lead, Ms Faith Chng. Our corporate partner, Trend Micro also supported the event with a series of activities such as spin the wheel, scam awareness quizzes and CyberWatch to win attractive prizes.

back to top

AiSP x PA x Trend Micro Scam Awareness and Dialogue Session on 1 November

back to top

The Cybersecurity Awards

Thank you for all your nominations.
Results will be announced on 11 November 2022

In its fifth year, The Cybersecurity Awards 2022 seeks to honour outstanding contributions by individuals and organisations, to local and regional cybersecurity ecosystems.

Visit www.thecybersecurityawards.sg for more information.

back to top

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

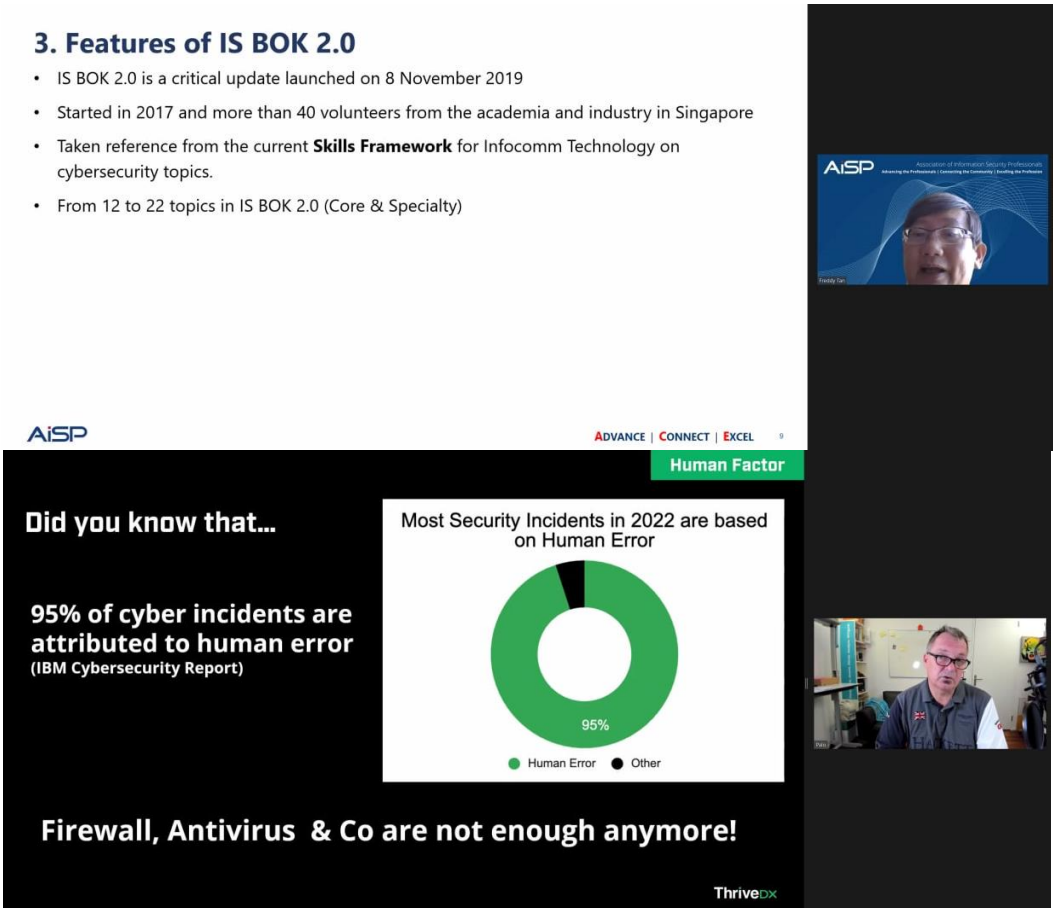
Professionals
1. Hall of Fame
2. Leader
3. Professional

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

Students
4. Students

AiSP x ThriveDX Webinar – The Human Factor Our Weakest link in Cybersecurity

On 15 September, in partnership with our Corporate Partner ThriveDX, AiSP had a webinar where our AiSP Fellow, Freddy Tan did a sharing on our Qualified Information Security Professional (QISP®) Programme. ThriveDX also shared about why human is the main attack vector for cyber criminals, the current trends and how we can prepare ourselves against them.



back to top

Regionalisation

AiSP x CyberTogether Cyber Leaders Series on 26 October

Cyber Leaders Series

In this Cyber Leader Series hosted by AiSP and CyberTogether, we have with us industry experts from Singapore and Israel.

Staying Ahead of Email-based Attacks
Speaker: Itay Glick, VP of Products, IT Security, OPSWAT

OPSWAT presentation will introduce the challenges of sophisticated email attacks, and enables some insights how organizations can advance their email security with OPSWAT solution.
Itay Glick is VP of Products for IT Security in OPSWAT, in this role he is responsible for the vision, strategy, and GTM for OPSWAT IT products. Itay is excited about Zero-days, Vulnerabilities, and malwares and well experienced in building enterprise security products. Prior to OPSWAT, at Allot, Itay was VP Products for Cyber Security, where he provided protection to 10s of millions of consumer customers via carrier service provider. At Dell Technologies, as a Senior Manager, Established the Cyber Security Services, provides hands-on security services for F100 customers. An expert on cyber security product development, system architecture and go-to-market, Itay has played an instrumental role in securing several multi million-dollar contracts with global enterprises and established his own cyber-security company (VOTIRO). He is also a regular speaker at industry events and the Executive Briefing Programme on how organisations can take a proactive approach to

back to top

mitigating risk. Itay holds a BSc in Electrical and Electronics Engineering from the Israel Institute of Technology and an MBA from the University of Bar-Ilan, as well as a CISP and CEH.

We will review the challenges of protecting against advanced email attacks and provide insights into how organizations can move their security posture to a higher level. OPSWAT's mission is to reduce cybersecurity risk for critical infrastructures and enterprises by filling security gaps, with technologies such as Deep CDR and Multiscanning. We can enable organizations to better protect themself from sophisticated attacks featuring sub-zero, zero-day exploits and malware commonly used today.

Building a Cyber Resilient Business
Speaker: Philip Ng, Co-founder and CEO, BitCyber

Modern day cyber attacks are getting ever quicker and more sophisticated at exploiting zero day vulnerabilities. It is no longer a question of "IF" your environment will be breached but "When". And when you are breached, is your environment resilient enough to withstand the attack and keep your business running? What are some strategies that you can adopt to build cyber resilience into your business?

Cybersecurity to Cyber Resilience: A Paradigm Shift
Speaker: Dr. Fene Osakwe, Forbes Technology Council Member & Director IT-GRC IHS

As the world becomes more digitally connected, corporate systems are becoming increasingly vulnerable to evolving cyber security threats. 2021 was yet another year in which high-profile security incidents dominated news headlines. Notably, we saw an alarming spike in incidents of ransomware-related data leaks, which climbed 82% in 2021. Software supply chain attacks increased by 650% during the year as bad actors proactively moved upstream to wreak havoc by infiltrating open-source software.

It is becoming increasingly difficult to completely prevent a cyber-attack from happening as the threat landscape and actors are constantly changing and evolving. Cyber and IT leaders need to begin to consider how their systems will respond and recover from an incident to prevent the wheels of their organization from grinding to a complete halt. This is where the concept of cyber resilience moves to the fore. Dr Fene will be speaking briefly on how cyber leaders can approach cyber resilience for their organisations and how this differs from just traditional cybersecurity thinking.

My Cyber Resilience Goal
Speaker: Tzer Yeu, Pang, Head, Information Security Office, Mediacorp Pte Ltd

For some time, the industry had acknowledged that a cyber breach is matter of “when” and not “if”. Cybersecurity while necessary, is no longer sufficient. Companies must be cyber resilient.

Are we resilient enough with backup and restoration plans? BCP/DRP? Well documented and well-rehearsed plans? Well, it depends.

I’ll share my goal and why, so that we can have a conversation.

Panel Discussion
Moderator: Alon Refaeli, Founder, CyberTogether & Malcolm Rowe, Vice President APAC, OPSWAT
Malcolm leads Asia Pacific & Japan sales and distribution for OPSWAT. In this role, Malcolm is responsible for driving sales revenue growth, ensuring the improved effectiveness of the

back to top

sales organization and for optimizing the ongoing sales strategies in light of constantly changing competitive pressures, markets demands and evolving products and services.

Malcolm has over 30 years of IT industry experience, including more than 15 years in the Cybersecurity business. Malcolm has been living and working in Singapore since 1997 and prior to joining OPSWAT, Rowe held senior leadership roles IBM, Tenable and Akamai, before which his formative career years were spent in London after graduating with honours in 1988.

Panellists:
Tzer Yeu, Pang, Head, Information Security Office, Mediacorp Pte Ltd
Dr. Fene Osakwe, Forbes Technology Council Member & Director IT-GRC IHS
Philip Ng, Co-founder & CEO, BitCyber
Itay Glick, VP of Products, IT Security, OPSWAT

Date: 26 October 2022, Wednesday
Time: 5PM - 7PM (SGT) / 12PM - 2PM (IST)
Venue: Zoom
Registration: https://us06web.zoom.us/webinar/register/2916635774699/WN_-EPrSAF2Q26v0mu-ba4oXA

South East Asia Cybersecurity Consortium on 23 – 24 November

Cybersecurity is borderless and the COVID-19 crisis has pushed many individuals and organisations to leverage the digital economy for sustainable development and growth. AiSP setup the Southeast Asia Cybersecurity Consortium (SEA CC) to:

1. Create a consortium of like-minded individuals and organisations that have a part to play in the Southeast Asia.
2. Drive initiatives and events that bring together a community of stakeholders for knowledge exchange, communication, and strategy.
3. Drive the cybersecurity strategy for the Southeast Asia region.

The inaugural Southeast Asia Cybersecurity Consortium (SEA CC) Forum 2022 is an important event of the year, organised by the AiSP. The programme schedule comprises of key notes, discussions and sharing by the various South-East Asia country's cyber security associations on their cybersecurity programmes and initiatives on developing technical competence, innovation, talent development and spreading of cyber security knowledge amongst its citizens.

This event is organized for anyone with an interest or wish to find out more or understand more on the Cyber Security landscape and work with cyber security associations from Brunei, Cambodia, Indonesia, Malaysia, Myanmar, Thailand and Vietnam. We are expecting 150 attendees, subject to COVID restrictions, at this physical event. We will be inviting a Political Office Holder (POH) to be our distinguished Guest of Honour for the opening and witness the MOU signing between Brunei, Cambodia, Indonesia, Malaysia, Myanmar, Singapore, Thailand and Vietnam Cyber Security Associations.

back to top

23 Nov 22 – Day 1 (Open to All including AiSP members for 150pax)
Venue : Life long Learning institute
Signing of MOU between the 8 Associations
Sharing by the 8 Associations
Key-Note Sharing

24 Nov 22 – Day 2 (Closed Door Discussion for 50pax)
Venue : Justco Marina Square
Harmonisation of Certification
Cybersecurity Labelling Scheme
Key Activities for the next 5 years

Participating Association

CREST

An update from CREST

CREST AGM & Future Plans

It was great to have an opportunity to engage with so many CREST members at our AGM in June. This provided a great platform for us to share a strategic update on our plans and aspirations for the next 24 months.

There is a significant focus on increasing our member benefits, and the AGM provided a great opportunity to share some of the plans we are working on to deliver additional value to members in all corners of the globe.

CREST OVS Programme

As most of you will recognise, cyber security never stands still. There are a huge number of initiatives and programmes we are working on to help shape and enhance the ecosystem. A significant amount of our discussions is focused on defining and raising standards across the key programmes we operate.

back to top

We are planning to release a series of new programmes throughout the next 12 months, and the first of these launched recently through the CREST OVS programme.

Read more about this initiative in consultation with OWASP –
https://www.crest-approved.org/membership/crest-ovs-programme/

Skilled Person Register

We hope these programmes will help buyers of cyber security services identify suitably skilled and competent organisations to engage with. As a result, you can expect further updates to our accreditation process and our Skilled Persons Register throughout the quarter ahead.

Read more here about how to register your employees -
https://www.crest-approved.org/membership/registering-your-skilled-professionals/

Updating Examinations

Examinations are a major focus for CREST, and several updates are taking place to certified level assessments.

We have listened to the feedback from recent exam takers, and we are using this insight to shape and enhance the exam experience. We hope to be able to communicate more tangible details about the planned changes this year.

International Events

It was great to see and meet many of you at recent events in the Middle East, Singapore, Malaysia, RSA and Infosec. We are delighted that so many people attended our recent CRESTCon; the CREST team was delighted to speak to you in person after so many months of virtual events and virtual meetings. We thank all our sponsors for helping to support CRESTCon.

CREST Communications

Make sure you follow us on LinkedIn and keep an eye out for some email-based member communications.

It is exciting times, and with your support and engagement, CREST hopes to materially enhance cyber security standards across large swathes of the cyber security landscape.

Rowland Johnson, CREST President

Keep up-to-date with CREST:
www.crest-approved.org
www.linkedin.com/company/crest-approved/

back to top

Upcoming Activities/Events

Ongoing Activities

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

Upcoming Events

Date	Event	Organiser
12 to 13 Oct	Cloud Expo Asia	Partner
12 to 13 Oct	Cyber Security World Singapore	Partner
13 Oct	Learning Journey to CISCO with ITE West	AiSP & Partner
14 Oct	MINDEF Bug Bounty	Partner
14 Oct	Digital Government Conference & Expo @ Hai Phong, Vietnam	Partner
15 Oct	ASEAN Student Contest for Information Security 2022	Partner
18 to 20 Oct	SICW & Govware 2022	Partner
19 Oct	Internet of Things Knowledge Series	AiSP
20 Oct	ISC2 Cyber Secure Singapore 2022	Partner
21 Oct	MFA-SCP Smart Nation Strategies, Opportunities and Cybersecurity Management	Partner
26 to 27 Oct	ADS & ARTC 2022	Partner
26 Oct	Cyber Leaders Series	AiSP & Partner
27 Oct	Data Security with Rubrik and Fortinet	Partner
27 Oct	ElasticON	Partner
28 Oct	Archer Workshop	AiSP
1 Nov	AiSP x MBOT Ladies in Cyber Webinar	AiSP & Partner

back to top

1 Nov	AiSP x PA x TrendMicro Scam Awareness Event with MOS Sun Xueling	AiSP & Partner
2-4 Nov	Singapore FinTech Festival	Partner
3 Nov	Anti Malware Day with Huawei	AiSP & Partner
4 Nov	IoT Special Interest Group Recruitment Drive	AiSP
9 Nov	Learning Journey to Trend Micro	AiSP & Partner
9 to 10 Nov	CDIC @ BITEC Bangkok Thailand	Partner
11 Nov	The Cybersecurity Awards 2022 Gala Dinner	AiSP
15 Nov	Ladies in Cyber Learning Journey to Schneider Electric	AiSP & Partner
16 Nov	SVRP 2022 Awards Ceremony	AiSP
17 Nov	Knowledge Series – DevSecOps	AiSP
23 to 24 Nov	South East Asia Cybersecurity Consortium (SEACC)	AiSP
30 Nov	SME Cybersecurity Conference 2022	AiSP

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

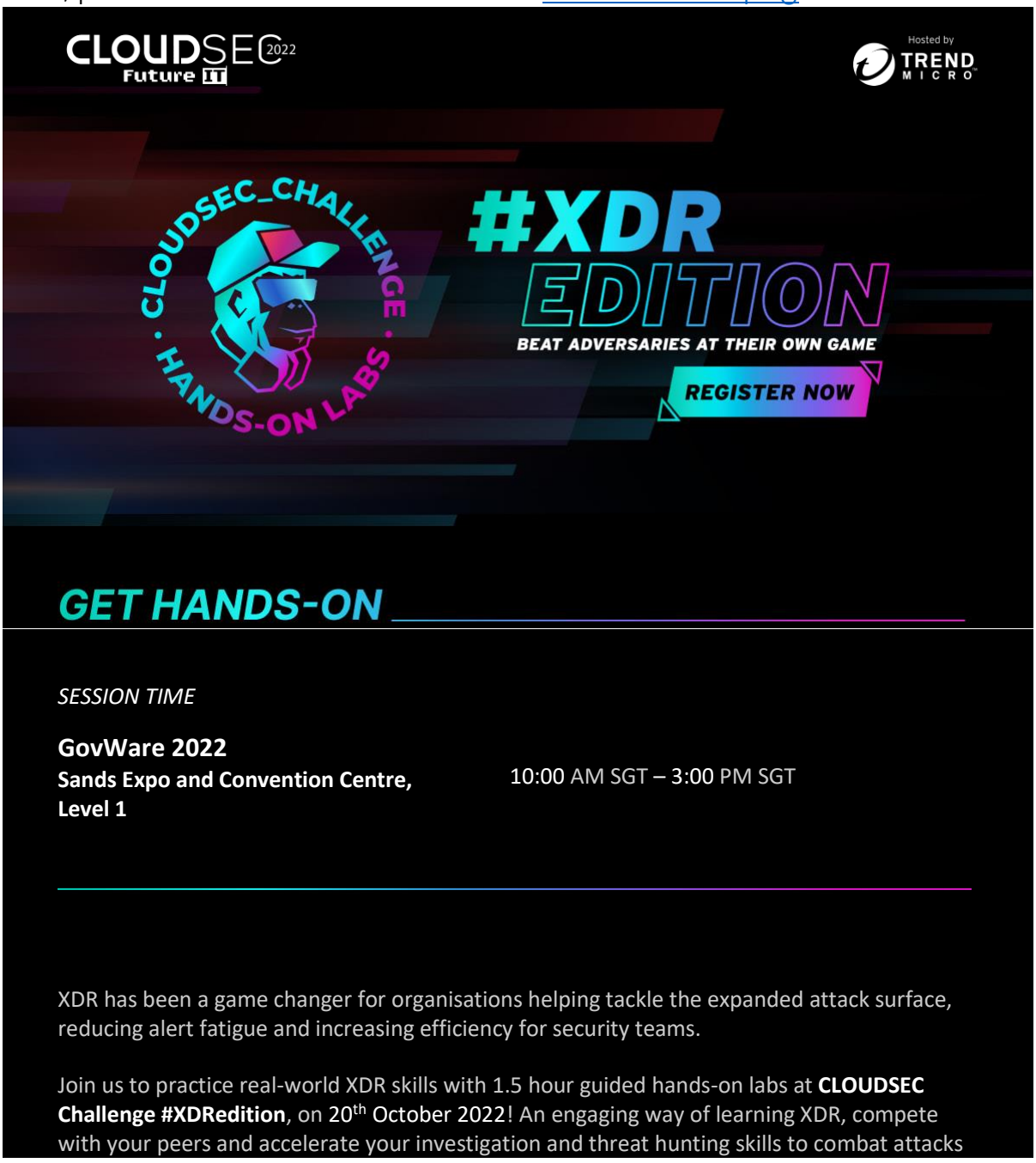
AiSP is excited to share that we are an official event partner of Cyber Security World, Singapore! Join us at Asia's most exciting cyber security event on 12-13 October 2022 at Marina Bay Sands Expo and Convention Centre. AiSP will be at B50 booth at the Singapore Pavilion.

back to top

Registering for one FREE ticket allows you to source from over 400 exhibitors including **Barracuda Networks, BeyondTrust, CrowdStrike, Darktrace, Illumio, Pacific Tech, Radware, Sophos** and more. Plus, get to learn from over 600 international speakers from organisations such as **Arascina®, Fusion Bank, IT Standards Committee, Singapore, Institute for Infocomm Research (A*Star), MUFJ, Mediacorp, Sekuro,** and **Tokopedia** just to name a few.

Register for your FREE ticket here: https://www.cybersecurityworldasia.com/partneraisp

Any issues, please contact AiSP Secretariat at secretariat@aisp.sg



back to top

efficiently. Choose from 2 sessions: Session 1 at 10am and Session 2 at 1230pm on 20th October.

Don't miss out, register today!

SAVE MY SPOT

WHAT TO EXPECT IN 2 HOURS

EXCITING PRIZES

Participants who successfully complete the challenge will receive an exclusive CLOUDSEC Challenge swag bag (worth $100).

Top scorer across both sessions walk away with Apple Watch Series 8!

Ideal for : Chief Information Security Officers, Information Technology Managers, Cyber Security Operations Managers, Cyber Security Operations Analysts, Incident Responders, Threat Hunters, and Cyber Security Engineers.

There's never a better time to invest in yourself and expand your threat detection and response skills. All players will earn a **CLOUDSEC Challenge certificate** for successful completion of hands-on labs.

REGISTER NOW

Registered at: https://cloudsec.com/SEA/HOL/

back to top

CONTRIBUTED CONTENTS

Article from Data & Privacy SIG

Understanding and Operationalizing Singapore's Mandatory Data Breach Regime

Steve Tan†, Professor (Adjunct)
Partner, Rajah & Tann Singapore
Director, Rajah & Tann Technologies
Director, Rajah & Tann Cybersecurity

A. Introduction

1. Concomitant with the digitalisation of the world economy, organisations have in the last several years pivoted their operations and business practices to one focused on the leveraging of technology. This has brought about a tsunami of data, being generated and relied upon by organisations. Much of such data comprise personal data, i.e. in simplified words, data that directly or indirectly identifies an individual. Without a doubt, the digital economy is in essence a data driven economy.

2. As and from 1 February 2021, organisations subject to Singapore's overarching data protection law, the Personal Data Protection Act [1] ("**PDPA**"), are mandatorily required to notify Singapore's data protection regulator, the Personal Data Protection Commission ("**PDPC**") and/or affected individuals, upon the occurrence of a data breach if certain conditions are met.

3. This effectively means that organisations can no longer sweep data breaches under the carpet, as they have been accustomed to doing, in years past. The significance

† Partner and Deputy Head, Technology, Media and Telecommunications/Data Privacy practice group, Rajah & Tann Singapore. Steve has been appointed Adjunct Professor of the National University of Singapore, teaching "Privacy & Data Protection Law" at the law faculty. Steve co-founded and is Director of Rajah & Tann Technologies Pte Ltd. Steve also co-founded and is Director of Rajah & Tann Cybersecurity Pte Ltd. Highly regarded for his expertise in data privacy and technology law work, Steve has pioneered several data-protection-related services which organisations have found valuable. Steve has been recognised as a leading lawyer in *PLC Cross-border Media and Communications Handbook*, *Asia Pacific Legal 500*, *AsiaLaw Profiles*, *Practical Law Company Which Lawyer*, *Chambers Asia Pacific*, *Best Lawyers*, *The International Who's Who of Telecoms and Media Lawyers*, and *Who's Who Legal: Data*. Steve has been named Communications Lawyer of the Year in the Corporate Livewire 2015 Legal Awards and in Corporate Insider Business Excellence Award 2019. Steve is cited as "one of the best in the field of personal data protection" in *Legal 500* 2017 and as being "one of the gurus in the field of data protection" in *Legal 500* 2019 and as "*an icon in the data privacy arena. Has a great depth of knowledge as the subject matter expert and one of the sought after authorities in this field*" in *Legal 500* 2021. In 2022, Steve was awarded ALB Asia's Top 15 TMT Lawyers. Steve is a Certified Information Privacy Professional (Asia) (CIPP/A).

[1] Personal Data Protection Act 2012 (Act 26 of 2012).

back to top

of this mandatory data breach notification requirement under the PDPA is even more pronounced considering the fact that statutory fines under the PDPA[2] is one of the highest in Asia, and enforcement of the PDPA has been strong and efficient.

4. Any sort of data incident can befall an organisation at any point in time. No organisation is immune from suffering a data incident. It could be as simple as an employee accidentally sending an email with an attachment containing personal data of its customers or employees to a wrong recipient, a simple disclosure of email addresses of multiple recipients in the sightable 'cc' or 'to' field of an email, throwing documents containing personal data of customers in the dustbin without shredding, to a sophisticated hack by a third party threat actor. The operational question that every organisation needs to know would be whether any data incident, even the simplest, needs to be notified to the PDPC and/or affected individuals.

5. In assisting many organisations in dealing with data incidents, I have seen many organisations being befuddled by the above. This is exacerbated by the fact that the mandatory data breach notification regimes of different jurisdictions have significant differences and Singapore is no exception. Singapore's is markedly dissimilar from the European Union's General Data Protection Regulation[3] ("**GDPR**").

B. What is a data breach?

6. To answer the above, let us consider the expansiveness or otherwise of the mandatory data breach notification regime under the PDPA.

7. The first question that an organisation needs to consider would be whether the data incident falls within the definition of a 'data breach' under the PDPA. The PDPA defines a 'data breach' as :

> "*(a) the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data; or*
>
> *(b) the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur.*"

8. This definition is rather expansive and will undoubtedly capture many incidents which may not fall within the definition of a data breach in other jurisdiction(s)' data protection laws. For example, under the GDPR, a data breach[4] is defined as :

[2] The increased fining formula is scheduled to come into force on 1 October 2022. This means that hitherto maximum fines of up to S$1 million, will be changed to the following : the higher of (i) S$ 1 million or (ii) up to 10% of the annual turnover in Singapore of the organisation where the organisation's annual turnover in Singapore exceeds S$10 million.
[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
[4] The GDPR defines it as a 'personal data breach'.

back to top

"*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*".

9. By comparing the 2 different laws' definitions of what constitutes a data breach, one can ascertain that the definition under the GDPR is qualified and limited by the fact that there must have first been a '*breach of security*'. There is no such qualifier under limb (a) of the definition of 'data breach' under the PDPA (see paragraph **7** above), which renders the coverage of what constitutes a data breach under the PDPA wider than under the GDPR. This is just one of the differences.

10. The expansiveness of limb (a) of the definition of 'data breach' does leave some uncertainty though. For example, this limb captures a situation where there has been unauthorised 'use' of personal data. Read literally, could it be argued to include a situation where existing personal data of individuals that had been lawfully collected by an organisation, is being used for a purpose which is not covered by the consent previously provided by the individuals or for which no exception to the requirement of consent under the PDPA applies? If this interpretation were to be adopted, it could make the definition of 'data breach' under the PDPA even wider than as described above, as it covers not only incidents where there is the element of a breach or compromise but one where it is simply a breach of the Consent Obligation under the PDPA. Was this intended by the parliamentary drafter of the mandatory data breach notification regime?

C. Notification thresholds

11. Setting aside the uncertainty described at paragraph **10** above, there is a zone of certainty with respect to certain types of data incidents that would clearly fall within the definition of 'data breach' under the PDPA. Hence, this therefore means that many data incidents would be captured by the PDPA's definition of a data breach. Certainly, the examples given at paragraph **4** above would be captured by the definition of a 'data breach' under the PDPA, so long as the data that has been affected includes personal data. Fortunately, regardless that a simple data incident may fall within the definition of a 'data breach' under the PDPA, there is a second step to be satisfied before the requirement to notify the PDPC and/or affected individuals kicks in. This is that the data breach must meet one of the two notification thresholds under the PDPA.

12. The two notification thresholds are :

    (a) Where the data breach results in, or is likely to result in, significant harm to an affected individual ("**Notification Threshold X**"); or

    (b) Where the data breach is, or is likely to be, of a significant scale ("**Notification Threshold Y**"). Significant scale looks at how many individuals have been

back to top

impacted by the data breach. Where the number of individuals impacted by the data breach is 500 or more, it is deemed to be of significant scale.

(Notification Threshold X and Notification Threshold Y shall be collectively referred to as the "**Notification Thresholds**")

13. Notification Threshold X does not look at the number of individuals affected by the data breach. It focuses on the nature of the personal data that has been the subject of the data breach. The fact that there is only 1 individual affected by the data breach is sufficient to trigger Notification Threshold X if the nature of the personal data impacted falls within the Notification Threshold X formula of significant harm. The Personal Data Protection (Notification of Data Breaches) Regulations 2021 provides for a list of situations as to which significant harm is deemed to have occurred. It is important to bear in mind that this list is non-exhaustive. Hence, despite the following not being mentioned in the said list, this author would posit that the mere compromise of an individual's identification number (such as his/her NRIC number) alone would suffice to trigger Notification Threshold X.

14. Notification Threshold Y casts the net wide in capturing data breaches that arguably cause no or little harm to an affected individual. This is because the focus of Notification Threshold Y is the number of individuals affected and not the nature of the personal data that has been compromised. Various other jurisdiction(s)' mandatory data breach notification regimes are triggered only where there has been or there is likely to be harm caused to the affected individual. Notification Threshold Y means that a data breach which may not be notifiable under another jurisdiction's mandatory data breach notification regime, would be captured by the PDPA's mandatory data breach notification regime. This triggering difference is one of the reasons why the Singapore subsidiary of a multinational conglomerate must not simply adopt the data breach management plan or policy that it has issued for its European entities but instead require a standalone or supplementary data breach management plan to deal with the PDPA.

15. Many data breaches can therefore trigger Notification Threshold Y, so long as the number of individuals affected is at least 500. As an example, a simple list headlined as VIP members of a consumer facing company, who are attending the company's cocktail event on a specific date with 600 individuals listed, comprising their full names and the type of membership tier each member has, such as Gold, Silver or Black (assuming there are these 3 membership tiers) could trigger Notification Threshold Y if such list was inadvertently disclosed or lost.

D. Timelines

16. There are two spheres of timelines that an organisation needs to implement operationally. The first is when it is established that a data incident is a 'data breach' as defined in the PDPA. The second is after it has been established that the data breach meets one of the two Notification Thresholds.

back to top

17. Let us consider the first timeline. Where the organisation has reason to believe that a data breach affecting personal data in the organisation's possession or control has occurred, the organisation must conduct, in a reasonable and expeditious manner, an assessment of whether the data breach meets any of the Notification Thresholds, and the PDPC has taken the position that this assessment should not exceed 30 calendar days[5].

18. This does not mean that an organisation can take its time to wait out the full 30 calendar days to deal with the triggering of one or both of the Notification Thresholds. Should it establish at an early stage (shorter than the 30 calendars) that indeed one of the Notification Thresholds has been met, that would mean that the next timeline of dealing with a triggered Notification Threshold would kick in.

19. Let us consider the second timeline. Once it has been established that one of the Notification Thresholds is met, the affected organisation has to notify the PDPC of the data breach within 3 calendar days. In the case where the data breach has triggered Notification Threshold X, the organisation has to additionally notify the affected individuals. The timeline for doing so is "*on or after*" notifying the PDPC.

20. It is pertinent to note that the PDPA provides for 2 exceptions whereby even though Notification Threshold X has been triggered and the organisation needs to notify both the PDPC and the affected individuals, there is no need for the organisation to notify the affected individuals[6]. The 2nd exception is subject to debate. It provides that there is no need to notify the affected individual if the organisation :

> "*had implemented, prior to the occurrence of the notifiable data breach, any technological measure that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual.*"

One cannot but contend that if indeed the organisation had prior to the occurrence of the data breach falling within Notification Threshold X, implemented a technological measure that prevents significant harm to the affected individual, then surely Notification Threshold X would not have been met and hence not triggered; and in such a case, there would not even be a need to notify the affected individual.

E. Operationally dealing with a data breach

21. From the foregoing, it should be clear to an organisation that navigating statutory requirements of a mandatory data breach notification regime, whether of Singapore or any other country's, is not a 'walk in the park'. When a data incident occurs, the organisation would need to deal with many substantive issues including but not limited to determining whether the data incident is considered a data

[5] Advisory Guidelines on Key Concepts in the Personal Data Protection Act
[6] Section 26D(5) of the PDPA.

back to top

breach under the PDPA, dealing with the statutory timelines of handling the data breach, assessing whether the data breach meets one of the Notification Thresholds, and reporting it to the PDPC. It is therefore in the interest of the organisation to seek external assistance from specialist lawyer(s) with expertise on dealing with a data breach, to handhold the organisation in meeting its statutory requirements. In fact, it may be the case that the specialist lawyer could very well assess that the data breach does not meet a Notification Threshold, thus obviating the statutory need to notify the PDPC or affected individuals. The specialist lawyer could also commission a technical forensics specialist to investigate the cause of the data breach in order to obtain key facts of the types of personal data and number of individuals, involved in the data breach. By involving the specialist lawyer to commission the technical forensics specialist, the report from the technical forensics specialist procured by the specialist lawyer could be endowed with legal privilege; a benefit that an organisation would not be able to obtain if engaging the technical forensics specialist directly.

F. Conclusion

22. This article has been written with the objective of providing a brief overview of the subject in question, and does not purport to cover all the issues and requirements under the PDPA's mandatory data breach notification regime.

23. The contents of this article does not constitute legal advice - In particular, each data incident has its own peculiarities and specificities and upon a data incident happening, the organisation should immediately seek legal advice on it.

About Rajah & Tann Cybersecurity
Rajah & Tann Cybersecurity, member of Rajah & Tann Technologies Group, is uniquely placed to help clients protect, mitigate against attacks, minimise disruptions from a security breach and effectively deal with a data breach. Email us at info@rtcyber.com for enquiry.

Article from Cyber Threat Intelligence SIG

Rantings of a Cyber Security Analyst

Layered Defense. I am sure many in the security field has heard this term. Most understand this as having different solutions to protect different portions of the infrastructure. A firewall for networking, endpoint protection for the devices, some form of Multi Factor Authentication for better verification of access… the list goes on.

What I personally feel goes wrong is treating this as a checklist. Do I have a firewall? Check. Endpoint Security? Check. Once all these requirements are checked, my security is good. Right?

back to top

Not completely in my opinion.

During the time when I was still new to cyber security, I got into a meeting with a bank's security team. One of the team members said "We can buy all available solutions, block everything, but is that feasible? If it is not, what is the risk of this and how do we minimize or control the risk?"

This statement stuck with me and really made sense. Another, more general statement that should always be remembered is, "if it's too good to be true, it probably is". Let's use a simple example of a house.

Let's say you just built a house and naturally you would want to secure it. Maybe fence up the entire property? What is the crime rate like in the area? What would be the risk of not having a fence? Even with a fence, you would still have a door into your home. If the risk is high or you are just paranoid, you may even consider having a gate before the door. As you shop for locks, this salesperson comes over and tells you the lock he sells is unpickable and you need not even bother to get an additional gate. Too good to be true?

Now you look around your house and notice it is possible to climb through the windows on the first floor. Solution would be to get grilles, but what about the second-floor windows? What are the chances of someone climbing and reaching the second-floor windows? Do I want to spend my budget on getting grilles for the second-floor or invest in some alarm system?

In the example, the planning and design of the security is based on risk. Ideally, I think it would be great if all cyber security personnel planned their security in this way. As the term "Layered Defense" states, you build layers to reduce risk. There is no silver bullet solution and there should be decisions on what product should be purchased and even how it is configured with the goal of reducing risk in mind. But remember, there is no such thing as zero risk. It simply does not exist and there is no way to reduce risk to zero.

Back to the cyber world, a common example that I hear is companies using legacy operating systems due to the business-critical software not designed to run on the newer supported operating systems. With that, there is no way to patch should there be any vulnerabilities and there is a security risk involved. So how do you secure these systems? Do you still treat them as your other servers running on supported operating systems? Slap on an anti-malware solution and call it a day? Now use a risk management approach to deal with this. Must this server be public facing? Is it possible to restrict access and even protocols to these servers? For the service to function, must it be part of the domain? It is possible to have the important data store on another server which can be better secured? All that thought process helped to create a feasible security for the legacy systems, with risk that is much more manageable. Even if the server is compromised, the access to other systems have been considered.

back to top

So where does Cyber Threat Intelligence come into play here? Remember there is no silver bullet to security, and Cyber Threat Intelligence is just another layer. As the name implies, it is not a product, but information. The value of CTI is having the capability to learn of methods used to breach environments. One common way is to monitor for intelligence of threats against companies of the same industry.

For example, monitoring the healthcare industry, if the company I am securing is a hospital. Understanding how a threat actor is currently targeting exposed MSSQL servers, for example, allows the team to firstly check if they do have an exposed MSSQL server. If they do, the next step will be to check if they see similar traits, such as build version of the MSSQL service, signs of attempts to remotely exploit and run commands on the system. Even if all these are secured (server is patched, XDR in place to monitor the system and perform threat hunts on related indicators), the 5 Ws 1 H, which I talked about in the last article, should be asked. Why is this server public facing? What other services is this server running? How can I reduce the risks of this exposed server? Should this MSSQL server, holding data which poses risk if stolen, be exposed to public or is there a way to restrict access, such as restricting access through a VPN or only allowing a specific remote IP to access it?

This entire process is a cycle as threats will always evolve and continuous understanding of these threats will allow the security team to learn of the risks and adapt a strategy to defend against the new threat.

Another common mistake I often experience is companies getting a NAS and backing up data to it. That is a great first step towards having data resiliency in the event of hard disk failure, but that does not reduce the risk of a breach.

"I have data backed up, so if I get hit with ransomware, I can recover from the NAS."

That's the statement I often hear, but when hit with an actual ransomware attack, failure to realize this is a human adversary whose goal is to make sure all your business-critical data is encrypted, including the backups is devastating. Adversaries easily realize there is a NAS in place; through mapped drives, applications on the server itself or looking at the scheduled tasks. And often, for convenience, access to the NAS from the server is unhindered. The result is data in the NAS gets encrypted too. I have also seen cases of adversaries simply resetting the NAS to factory default, wiping out all data in the process.

In a risk management approach, questions such as "What if the NAS gets compromised?", "How do I secure the NAS?", "Do I have another copy of the data, maybe a week old, stored offline?", should be asked.

This is the reason many security practitioners say, "Assume breached". Daunting as it may sound, companies need to understand this is the way to design their security and for smaller organizations, they should approach a security advisor who plans, using the same risk management approach.

back to top

Harvey Goh is a cyber security specialist having been in the cyber security industry for over 15 years as a technical personnel. Currently he is working as part of Sophos' Managed Threat Response team. He is also a member of AiSP CTI SIG, EXCO and volunteer at CSCIS CTI SIG.

Views and opinions expressed in this article are my own and do not represent that of my places of work. While I make every effort to ensure that the information shared is accurate, I welcome any comments, suggestions, or correction of errors.

Article from our Cloud Security Summit Sponsor, Lookout

Attaining Freedom of Control
Security Service Edge (SSE) transforms your Cloud Security

The Covid 19 pandemic has turned the traditional enterprise inside out. As the new normal of hybrid work takes shape, the cloud has become the primary location for businesses to store data. These days, more and more enterprise data is moving outside the network perimeter, beyond the reach of traditional firewalls, on-premises web proxies, and DLP appliances that aren't equipped to read cloud traffic. Couple this with the growing number of remote endpoints connecting to enterprise networks and you have a recipe for unreliable oversight of company data.

According to Gartner, by 2025, ***80% of enterprises will have adopted a strategy to unify web, cloud services, and private application access*** *from a single vendor's SSE platform.*

With the traditional perimeter all but disappearing, the inspection point must move out of the centralized data center as close as possible to where the data is accessed, whether that's a cloud service (CASB), private application access (ZTNA), or the web (SWG). A **unified SSE platform** with a common intermediary "proxy" and a cohesive package of advanced data security controls provides all the security tools needed to secure the transition to the cloud.

back to top

Download complimentary copies of the **2022 Gartner® Magic Quadrant™ for SSE** and **Critical Capabilities** reports to learn:

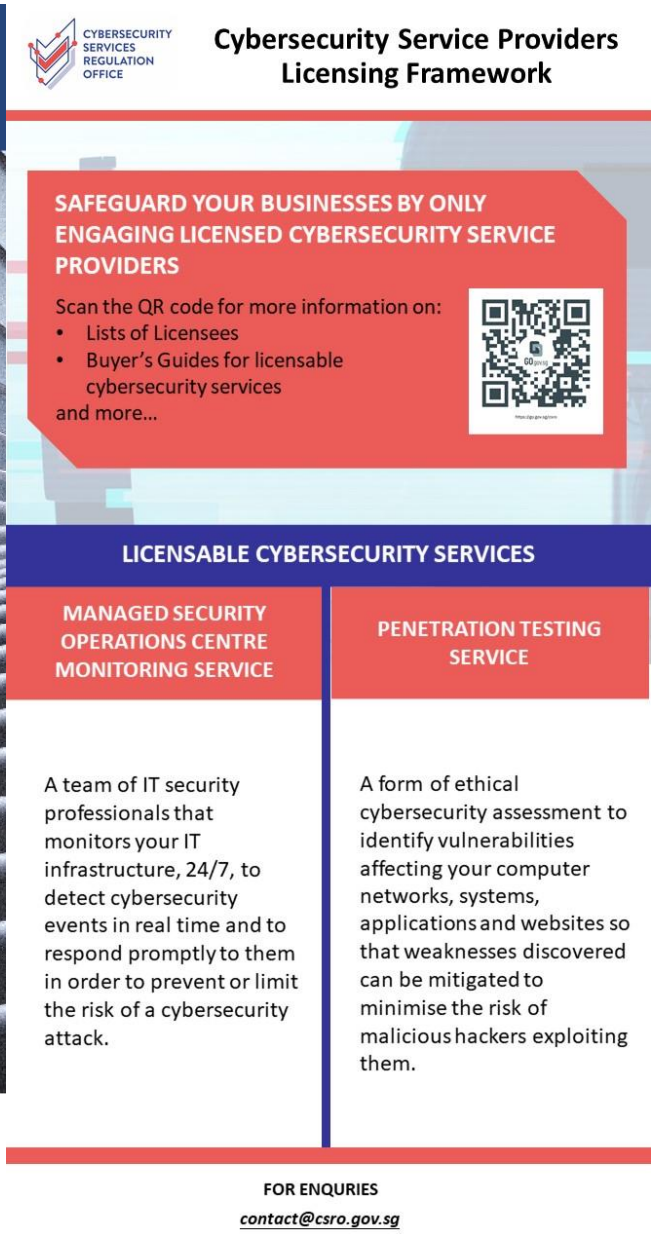
- How SSE can help you reduce complexity, costs, and management overhead
- Which SSE Gartner Critical Capabilities to focus on
- Which Use Case/s could be applied to your organization and what to look for in an SSE vendor

SCAN ME

For any enquiries, please contact Ms Sheila Chan at sheila.chan@lookout.com

back to top

Consumers of Licensable Cybersecurity Services



For enquiries, please email contact@csro.gov.sg

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

The content and information provided in the document do not constitute the opinions and views of the Association of Information Security Professionals. AiSP remains neutral to the products and/or services listed in the document.

back to top

PROFESSIONAL DEVELOPMENT

Listing of Courses by Wissen International

EC-Council, creator of the Certified Ethical Hacker (CEH) program, has launched the Certified Cybersecurity Technician (CCT) certification to help you transition from an IT career or take the first step toward a rewarding future in cybersecurity.

The CCT program includes comprehensive lab-based exercises to verify and expand your practical skills, it offers a multidisciplinary education in core security skills to help participants gain a broader perspective on the cybersecurity industry.

Start your cybersecurity career with EC-Council's CCT certification - the only baseline-level cybersecurity program that offers 85 performance-based labs, Capture-the-Flag challenges, and multidisciplinary training in a variety of cybersecurity skills.

SPECIAL PRICE OF S$917 for AISP MEMBERS!
CCT iLearn Kit - includes videos, e-book, cyber range labs and exam.
Email aisp@wissen-intl.com now!

Brought to you by Wissen International - EC-Council Exclusive Distributor

Advertisements placed on the AiSP website is in no way intended as endorsements of the advertised products and services. No endorsement of any advertisement is intended or implied by AiSP.

back to top

Listing of Courses by ALC Council

Stand out from the crowd

Cyber security offers one of the best future-proof career paths today. And ALC – with our industry-leading program of cyber certifications - offers you one of the best ways to advance your cyber career.

We offer the most in-demand cyber certifications including:

- CISM®, CRISC®, CISA®, CGEIT®, CDPSE®
- SABSA®, NIST®, ISO 27001
- CISSP®, CCSP®
- CIPM, CIPT, CIPP/E

The right training makes all the difference

Lots of things go into making a great course, but the single most important is always the trainer: their knowledge of the subject; their real-world experience that they can draw upon in class; their ability to answer questions; their communication skills. This is what makes the difference.

ALC works only with the best. That has been the core of our business model for the past 28 years. You can see the calibre of our trainers on our Faculty page.

back to top

AiSP Member Pricing – 15% discount

AiSP members receive 15% discount on all ALC training courses. To claim your discount please enter the code **ALCAiSP15** in the Promotion Code field when making your booking.

Upcoming Training Dates

Click this link to see upcoming Course Dates. If published dates do not suit, suggest an alternative and we will see what we can do.

Special Offers.

We periodically have special unpublished offers. Please contact us aisp@alctraining.com.sg to let us know what courses you are interested in.

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

Thank you.

The ALC team

ALC Training Pte Ltd
3 Phillip Street, #16-02 Royal Group Building, Singapore 048693
T: (+65) 6227 2883 | E: learn@alctraining.com.sg | www.alctraining.com.sg

back to top

Qualified Information Security Professional (QISP®) Course

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

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

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

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

COURSE DETAILS

back to top

2022 Course dates can be found on https://www.aisp.sg/qisp_training.html
Time: 9am-6pm
Fees: $2,800 (before GST)*
**10% off for AiSP Members @ $2,520 (before GST)*
***Utap funding is available for NTUC Member**
*** SSG Funding is available!**

TARGET AUDIENCE

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

COURSE CRITERIA

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

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

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

Program Partner

Transformists NETWORK

Delivery Partners

Ai Network 360 | OPUS ACADEMY | NETASSIST

back to top

Cybersecurity Essentials Course

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

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

Course Objectives

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

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

back to top

- Cloud Computing
- Cybersecurity Operations

COURSE DETAILS

Training dates for year 2022 can be found on
https://www.aisp.sg/cyberessentials_training.html
Time: 9am-6pm
Fees: $ $1,600 (before GST)*
**10% off for AiSP Members @ $1,440 (before GST)*
***Utap funding is available for NTUC Member**
*** SSG Funding is available!**

TARGET AUDIENCE

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

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

back to top

MEMBERSHIP

AiSP Membership

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

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

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

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

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

back to top

Sign up for AVIP MEMBERSHIP

AVIP membership is the FIRST in Asia to bundle the Professional Indemnity for professionals involved in cybersecurity related work, to give them greater assurance undertaking projects in Singapore and worldwide.

BENEFITS

- 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.

PRICE

Application Fee : $481.50 (1st 100 applicants),
$321 (AiSP CPP members)
Annual Membership: $267.50
*Price includes GST

EMAIL MEMBERSHIP@AISP.SG TO SIGN UP AND FOR ENQUIRIES

back to top

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

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

Be Plugged into Cybersecurity Sector – Join us as a Member of AiSP!

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

AiSP Corporate Partners

back to top



back to top

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

AiSP Academic Partners

back to top

Our Story…

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

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

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

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

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

www.AiSP.sg
secretariat@aisp.sg
+65 8878 5686
6 Raffles Boulevard, JustCo, Marina Square, #03-308, Singapore 039594
Please email us for any enquiries.

back to top

