

News & Update

- Knowledge Series
- CAAP
- SVRP
- AiSP Cyber Wellness
- Ladies in Cyber
- Cloud Security Summit
- Special Interest Groups
- The Cybersecurity Awards
- MOU Renewal
- CREST
- Upcoming Events

NEWS & UPDATE

New Partners

AiSP would like to welcome Image Engine, Starhub and Wizlyn as our new Corporate Partners. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem.



Contributed Contents

- IoT SIG: Are you in control of your privacy network?
- CTI SIG: Rantings of a Cyber Security Analyst
- How Data Protection Can Enhance Customer Trust and Improve Competitiveness



Professional Development

Membership

News and Updates

Scantist & OpenSSF's First Community Event on 18 August

It was a great session at the Scantist & OpenSSF's First Community Event on 18 Aug 22 at Red Hat supported by AiSP. Thank you for having our AiSP EXCO Lead for SVRP & IoT Ms Soffenny Yap at the panel discussion on the topic on Doubling Down on Open Source Security on the challenges, solutions and opportunities in the new era.



AiSP x Cybersecurity Agency of Singapore (CSA) Joint Event with CE/CSA on 22 August

On 22 August, AiSP held our first AiSP Validated Information Security Professionals (AVIP) closed door event, where we had the opportunity to invite Mr David Koh, Chief Executive of Cyber Security Agency of Singapore (CSA) to join our AVIP members and discuss on building up a strong cybersecurity workforce core with world class capabilities.



Knowledge Series Events

Security Operation on 24 August

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 24 August, it was an insightful time and engaging session we had for our Knowledge Series on Security Operations. We would like to thank our Corporate Partner, Elastic and Vectra AI for sharing insights with our participants.

Data is at the heart of modern enterprise.

Data is at the heart of modern security.

VECTRA

Enhance Your Network & Cloud Security With **Vectra AI**

Sharat Nautiyal
Regional Security Architect, Asia
CISSP, CISM, CRISC, CDPSE, CCSK, SANS GCIH, AWS SA

CONFIDENTIAL

Lulj Heran (Elastic)

Lulj Sharat (Vectra AI)

Identity & Access Management on 14 September



AiSP Knowledge Series – Identity & Access Management



AiSP Knowledge Series
IDENTITY & ACCESS MANAGEMENT



Lackern Xu
LEAD SOLUTIONS ENGINEER, GLOBALSIGN



Marco Zhang
HEADS - REGIONAL SALES ENGINEERING, APAC, SAVIYNT

 **Wednesday, 14 Sep 22**
3.00PM - 4.30PM

 **Zoom Webinar**



Organised by



Supported by





In support of



In this Knowledge Series, we are excited to have GlobalSign and Saviynt to share with us insights on Identity & Access Management. Based on 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.

Using Certificate-based Authentication for Access Control
Speaker: Lackern Xu, Lead Solutions Engineer (APAC), GlobalSign

Is certificate-based authentication method very different from its traditional counterparts?

Why has certificate-based authentication been widely recognised as the choice solution for a more reliable and convenient way for organisations to authorise devices, users, and applications than the traditional username and password combination?

Let GlobalSign share with you a high-level view of how certificate-based authentication works and its differentiation from other methods. You can also find out about the benefits of such an authentication solution and its role in effective business security operations.

Enabling Modern Workforces with Identity & Zero Trust
Speaker: Marco Zhang, Heads - Regional Sales Engineering, APAC, Saviynt

The modern business landscape demands a new paradigm; one that balances security and accessibility for increasingly remote workforces. By employing an identity-driven approach with Zero Trust principles, enterprises across all sectors can strengthen their IT environments and maintain a productive and secure workforce. With Saviynt's converged, cloud-based platform, getting identity governance off the ground has never been easier.

Key takeaways from the webinar:

- Understanding identity through the Zero Trust lens.
- Empowering remote workers with critical tools, applications, and access.
- How a cloud-based platform streamlines onboarding and access provisioning, identifies and resolves excess permissions, and ensures continuous compliance for any identity, app, or cloud.

Date: 14 September 2022, Wed

Time: 3PM – 4.30PM

Venue: Zoom

Registration:

https://us06web.zoom.us/webinar/register/4316596859661/WN_z2gqLfgBRha5UtwSdefx6Q

Upcoming Knowledge Series

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

1. Identity & Access Management, 14 Sept 22
2. Internet of Things BOK Series, 19 Oct 22
3. 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](#).

Cybersecurity Awareness & Advisory Programme (CAAP)



AiSP x SIAA - Automation, Robotics & IoT Security Workshop on 25 August

AiSP & Singapore Industrial Automation Association (SIAA) organised a Cybersecurity Awareness & Advisory Programme (CAAP) physical workshop together to provide members knowledge on what solutions are available for securing their solutions in the area of Automation, IoT and Robotics. This event aims to elevate cybersecurity awareness in OT as an integral part of Singapore business fundamentals and establish a self-sustainable support ecosystem where businesses can raise their cyber resilience with the support of agencies, business associations, security communities and service providers.

We would like to thank our Corporate Partner, Cisco , Fortinet and Nozomi Networks who shared insights on security of automation, IoT and robotics. Armis was also invited to share a demo of their solution to the participants.



AiSP Cybersecurity Awareness E-Learning

	
<h3>AiSP Cybersecurity Awareness E-Learning</h3>	
<p>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.</p> <p>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.</p> <p>We will be covering:</p> <ol style="list-style-type: none"> 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 	

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.

Student Volunteer Recognition Programme (SVRP)

Cybersecurity Awareness at Victoria School on 15 August

As part of Digital for Life Movement, AiSP hope to help Singaporeans of all ages and walks of life to embrace digital learning as a lifelong pursuit. On 15 August, AiSP Exco Member and SVRP Lead, Ms Soffenny Yap, did a sharing to over 300 secondary 4 students at Victoria School on cybersecurity awareness.



Learning Journey to Cisco office on 30 August

As part of Digital for Life movement, we hope to help Singaporeans of all ages and walks of life to embrace digital learning as a lifelong pursuit. On 30 August, AiSP brought over 20 secondary 1-3 cyber wellness student ambassdor from Anderson Secondary School for a learning journey to our Corporate Partner - Cisco.

We hope the students have gain insights to share with their classmates back in school.



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. Call for Nomination for Student Volunteer Recognition Programme has ended on 31 July 2022.

AiSP Cyber Wellness Programme

Organised by:



Supported by:



In Support of:



The AiSP Cyber Wellness Programme aims to educate citizens, especially reaching out to the youths and elderly on the importance of Cybersecurity and learn how to stay safe online. There has been an increase in cyber threats, online scams and COVID-19 related phishing activities. With reduced Face-to-Face engagements, the elderly and those with special needs have become more vulnerable to cyber threats. We will reach out to different community groups to raise awareness on the topic of cyber wellness and cybersecurity and participants can pick up cyber knowledge through interactive learning. It is supported by the Digital for Life Fund, an initiative by the Infocomm Media Development Authority (IMDA), that supports digital inclusion projects and activities to help all Singaporeans embrace digital, to enrich lives."

Join us in our monthly knowledge series to learn and pick up tips on Cybersecurity. Visit our website (<https://www.aisp.sg/aispcyberwellness>) to get updates on the latest Cyber tips, Cyber news, activities, quiz and game happenings related to Cyber. Scan the QR Code to find out more.





Scan here for some tips on how to stay safe online and protect yourself from scams



Hear what some of our Professionals have to share. Scan here on Cyber - Use, Identity, Relationship, Citizenship & Ethics.



Have the knowledge and think you are safe? Challenge yourself and participate in our monthly quiz and stand to win attractive prizes. Scan now to take part.



Scan here if you are looking for activities / events to participate in for knowledge exchange / networking / get to know more people / stay protected & helping others.



Want to know more about Information Security? Scan here for some career advice on Information Security.



To find out more about the Digital for Life movement and how you can contribute, scan here.

Contact AiSP Secretariat at secretariat@aisp.sg to find out more on how you can be involved or if you have any queries.

Click [here](#) to find out more!

Ladies in Cybersecurity



Ladies Talk Cyber Series

For the Fourteenth edition of AiSP's 'Ladies Talk Cyber' series, we interviewed Ms Yen Yi Lin, who is currently working as a Security Operations Center (SOC) Analyst at Acronis.

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

Yi Lin is currently working as a Security Operations Center (SOC) Analyst at Acronis. Together with the Security team, they work closely to protect the company's infrastructure, networks and data. SOC analysts monitors for and investigates suspicious events, by analyzing logs from various sources for signs of malicious activities. We also maintain and continuously update our security tools to keep up with the latest attacks.

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



Upcoming Ladies in Cyber Events

Learning Journey to Ensign InfoSecurity on 6 Sep

As part of the International Cyber Women Day Celebrations 2022, AiSP will be organising a learning journey to Ensign InfoSecurity on 6 Sep 22 from 2pm to 5pm where we will invite about 50 to 70 female youths (Subjected to COVID restrictions) from our Student Chapters to come together physically for a day of celebration, learning journey and visiting the Ops Centre at Ensign InfoSecurity and interacting with the working personnel at Ensign. Join us for an afternoon of enriching activities ranging from Dialogue Session with our Guest of Honour, Ms Gan Siow Huang, Minister of State in the Ministry of Education and Ministry of Manpower, Recruitment Talk, Internship Opportunities and visit to the Ops Centre. The event is open to all female students in tertiary level. Join MOS Gan, Ms cAsh Chng, Ministry CISO, Ms Jackie Low, Deputy Director and Ms Sherin Y Lee at the event.

The details for the event are as follow:

Date: 6 Sep 22 (Tue)

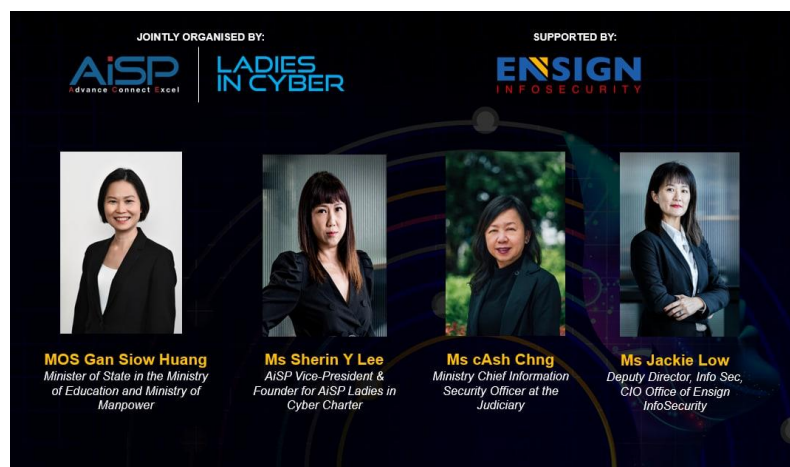
Time: 2pm to 5pm

Venue: Ensign InfoSecurity (Singapore) Pte Ltd located at 30A Kallang Pl, #08-01, Singapore 339213

Dress code: Smart Casual

Guest of Honour: Ms Gan Siow Huang, Minister of State in the Ministry of Education and Ministry of Manpower

*Light Refreshments will be provided at the event



Open to all to join virtually. Register [here](#) by 5 Sep

Cloud Security Summit 2022

Supporting Partners

- CSCIE
- CREST
- cloud security alliance
- CO DIVO
- HTCIA
- IASA
- ISACA Singapore Chapter
- ntuc
- associate
- SINGAPORE BUSINESS FEDERATION
- SFA
- SGTECH
- SIT

Organised by

- AiSP

Co-Organised by

- Tech Talent Assembly

Supporting Agencies

- CSF SINGAPORE
- GOVTECH SINGAPORE

Gold Sponsors

- ARMIS
- NOZOMI NETWORKS
- oneSECURE
- THALES
- netgear

Silver Sponsors

- Lookout
- xcellink.pte.ltd.

Guest of Honour: Mr Tan Kiat How, Senior Minister of State, Ministry of Communications and Information & Ministry of National Development, TTAB Advisor

The inaugural AiSP Cloud Security Summit 2022 is an important event of the year, organised by the AiSP Cloud Security Special Interest Group with partnership and support from NTUC U Associate & TTAB. The programme schedule comprises of key notes, solutions, panel discussion and workshop. The theme for the summit is Accelerate your cloud security Journey. This event is organized for anyone with an interest or wish to find out more or understand more on the landscape of Cloud Security.

Register [here](#)

Special Interest Groups

Cloud Security Summit 2022

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



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.

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

Professionals

1. Hall of Fame
2. Leader
3. Professional

Students

4. Students

Enterprises

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

MOU Renewal



AiSP & IASA Seminar: Enhance
IT Security with Enterprise
Architecture
| 20 September 2022, 9.30a.m

Email not displaying correctly?
[View it in your browser.](#)

AiSP & IASA Seminar
Enhance IT Security with Enterprise Architecture

📅 Tuesday, 20 September 2022
🕒 9.30AM - 12.00 PM (GMT +8)
📍 JustCo (Marina Square) 6 Raffles Boulevard, #03-308, Singapore 039594

Introduction:

Businesses must ensure that their IT security strategies are aligned with and support business objectives, that they consistently comply with regulations through adherence to policies and internal controls, and that they provide accountability in order to manage risk. Enterprise Architecture (EA) framework serves as a standard for aligning business and IT objectives and governs IT security throughout the organisation. To thrive in the digital business, AiSP and IASA have collaborated to provide security professionals with high-impact EA training programmes that are globally certified and supported by IBF and SkillsFuture.

Key takeaways:

- **Introduce the Digital Enterprise Architecture framework.**
- **Learn how to govern IT security and protect its critical assets.**

- Gain an understanding of EA competency skillsets.

[VIEW AGENDA HERE](#)

FEATURED TOPIC

Topic: Qualified Information Security Professional Programme

Speaker: Steven Wong

Security is a top priority globally as cyber-attacks have increased in frequency, intensity and severity. It is critical for businesses and organisations to have qualified information security professionals to manage cybersecurity threats and incidents. To support the development of personnel in this demanding profession since 2010, the Association of Information Security Professionals (AiSP) has been offering its Qualified Information Security Professional (QISP®) Programme. The QISP® examination enables the professionals in Singapore to attest their knowledge in AiSP's IS-BOK domains.

FEATURED SPEAKERS



Johnny Kho

President, Association of Information Security Professionals (AiSP)



Aaron Tan Dani

Chairman, Iasa Asia Pacific /
President, EA-Chapter, Singapore Computer Society



Steven Wong
AiSP Immediate Past President



Jonathan Gardiner
Head of Strategy and
Architecture, Linfox Logistics



Edison Tie
Enterprise Architect,
NTUC Income

EVENT INFORMATION

Date: 20 September 2022 (Tuesday)

Time: 9.30am to 12.00pm (GMT+8)

Address: JustCo (Marina Square), 6 Raffles Boulevard, #03-308, Singapore 039594

[Direction](#)

* Light refreshment will be provided.

[Click Here to Register](#)

Co-organisers:



For any enquiries, please contact Audrey Loke at (65) 6386 0331 or email to audrey.loke@iasahome.org.
Visit [IASA APAC](#) for more info

Copyright © 2022 IASA APAC, All rights reserved.

[Email Preference Center](#)

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.

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/



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
1 Sep	AiSP International Cyber Women's Day Celebrations 2022	AiSP
6 Sep	<u>AiSP Ladies in Cyber Learning Journey to Ensign</u>	AiSP & Partner
6 Sep	PDD Connect Smartness Event	Partner
6- 7 Sep	Identity Week Asia	Partner
6 – 7 Sep	IndoSec 2022	Partner
7 – 8 Sep	Government & Critical Infrastructure APAC 2022	Partner
13 – 14 Sep	SMEICC Conference Series	Partner
14 Sep	<u>Identity & Access Management BOK Series</u>	AiSP
15 Sep	The Human Factor Our weakest link in Cybersecurity	AiSP & Partner
15 Sep	ISACA GTACS 2022	Partner
18 Sep	Celebrate Digital @ Kreta Ayer-Kim Seng (KAKS)	Partner
20 Sep	AiSP x MBOT Ladies in Cyber Joint Webinar	AiSP & Partner
20 Sep	AiSP & IASA Seminar: Enhance IT Security with Enterprise Architecture	AiSP & Partner
21 to 23 Sep	XCION 9th Bali Workshop	Partner
24 Sep	Celebrate Digital event at Chong Pang market Amphitheatre	Partner
26 Sep	Cloud Security Summit	AiSP
26 Sep	AiSP x CSA x PDPC x SBF TAC Knowledge Series on Cybersecurity and Data Protection	AiSP & Partner
12 to 13 Oct	Cloud Expo Asia	Partner
14 Oct	MINDEF Bug Bounty	Partner
15 Oct	ASEAN Student Contest for Information Security 2022	Partner
18 to 20 Oct	SICW & Govware 2022	Partner
19 Oct	IoT Knowledge Series	AiSP
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 October	Data Security with Rubrik and Fortinet	Partner

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

CONTRIBUTED CONTENTS

Article from IoT SIG

Are you in control of your wireless network? Check carefully, cause' you might Have an Evil Twin!

The walls around us have completely disappeared. What is the meaning of a protected perimeter when a 30 cm concrete wall can be penetrated by a 35\$ pineapple device?

Unlike wired networks, wireless networks can be easily accessed by anyone. Even restricted wireless environments can be penetrated from nearby. Wireless networks host a wide variety of mobile and IoT devices that are difficult to secure. They often have vulnerable interfaces, unprotected storage, hardcoded backdoors, unencrypted communications and insecure pairing procedures that hackers can exploit. This combination of unmonitored access, poor device security and lack of controls leaves enterprises exposed to attacks that lead to data loss, ransomware, and denial of service.

Here are top five wireless threats not detected by traditional security controls:



Evil Twin

A malicious access point masquerades as a legitimate network. It copies another network's SSID to look exactly like an existing network. Users and devices are tricked into connecting to the malicious AP.



Karma

Attacker sends fake probe responses to devices that sent directed probe requests. For example, if the target is at work and his device probes for its coffee shop network, the attacker replies and the target device automatically connects.



Rogue Hotspot

Corporate devices connected to an external secure/insecure network pose a risk as these hotspots are not monitored by the organizations' cyber defenses and the external devices connected to these networks are able to compromise them.



Suspicious AP

The presence of an access point with a similar SSID to the corporate network can indicate an attempt to fool unsuspecting users into connecting to a malicious access point.



Insecure IoT Device

Some IoT devices like smart printers and smart TVs are physically connected to the corporate network (via a cable) but also host a wireless network, thus acting as a bridge between the two networks. These devices can be used to exfiltrate sensitive data from devices by activating sensors (camera, microphone, screen recording, keyboard sniffing, etc.)

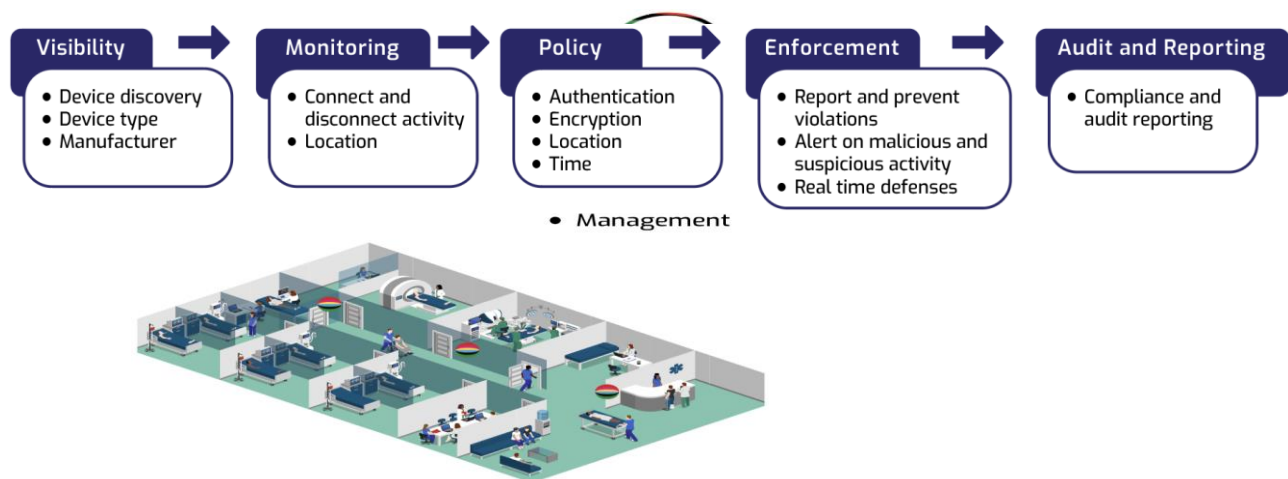
Unmanaged and IoT devices outnumber managed devices in 69% of the organizations surveyed • 84% of respondents believe that unmanaged and IoT devices are more vulnerable to cyber-attacks than corporate-managed devices.

82% of healthcare organizations have experienced an IOT-focused cyberattack

The problem with traditional network access controls (NAC) is they only see what is connected to the network. Wireless attackers operate in the airspace but do not need to connect to the network to do damage.

So, who's protecting your unmanaged devices??

Harmony IoT from Orchestra Group creates a protective Cyber Iron dome around your organization, monitoring all airspace activity, detecting and protecting your network from these top threats and many more. Our lightweight, AI based cloud managed out of bound solution delivers end to end **real time, actionable** security that is non-invasive and non-disruptive.



Harmony IoT delivers complete, proactive, end to end security for your wireless airspace.

Learn more at www.orchestragroup.com/#hiot

About Orchestra Group

Orchestra Group is a privately held company led by top cybersecurity and data-science experts. Our Harmony IoT solution protects retail, financial institutions, banks, data centers, governments, healthcare organizations, manufacturing facilities, defense contractors, and SCADA companies. Visit us at www.orchestragroup.com

About SecureCraft

SecureCraft is a distributor of Orchestra Group. With a team of committed and skilled security professionals, solely focused on Information Security, SecureCraft fully understand the challenges that businesses are facing in today's information-driven world. Our vision is to be the preferred, best-of-breed cyber security and network performance, solutions' distributor for end-to-end security products. Visit us at www.securecraftasia.com or contact us at sales@securecraftasia.com

Article from Cyber Threat Intelligence SIG

Rantings of a Cyber Security Analyst

Who, What, When, Where, Why & How. The Five Ws and one H are questions whose answers are considered basic in information-gathering. As quoted from multiple sources, they are often mentioned in journalism, research, and police investigations. According to the principle of the Five Ws and one H, a report can only be considered complete if it answers these questions starting with an interrogative word: -

- **Who** is it about?
- **What** happened?
- **When** did it take place?
- **Where** did it take place?
- **Why** did it happen?
- **How** did it happen

Each question should have a factual answer and importantly, none of these questions can be answered with a simple "yes" or "no".

In Cyber Security, I feel the above concept needs to be applied to events. Many times, I am called in to assist to investigate on an incident and most of the time, the details of the logs were ignored or were not further investigated.

Imagine a scenario where you hear someone continuously jiggling the door handle of your home. Would you react or just think your door and lock is working and preventing the person from entering and just ignore this? You would want to know **who** this person is, **why** is this person trying to enter and **what** is he trying to do.

Let me use a breach that I recently investigated, where a company was hit with ransomware and called in for assistance, as an example. As with all such breaches, it is understandable that it is a stressful situation to be in and being swarmed with statements like "the product failed me" is not a great feeling.

The first lead in my investigation was the endpoint security logs itself. Prior to the encryption phase, there were detection of tools like PsExec and Mimikatz. These were blocked, but going with the Five Ws and one H, I dug into this detection, found the time stamp, and noticed the tools were detected on C:\Users\Administrator\Pictures\
Now, if the internal security team were investigating, this should raise red flags. Even though the threat at that time was blocked, **why** were these tools dropped into that folder? **Who** was it who dropped these tools into this folder? Was it really a legitimate user of the Administrator profile? Looking at **when** this happened with the time stamps, it happened at 6am, before any IT staff was on site. So of course, the next questions would

be **how** it is possible for someone to be using the Administrator account and **how** was this done remotely.

As this customer did not have any XDR or EDR tools at that point of time, I had to manually go through the Windows Event Logs and hoped the threat actor has not wiped them. Fortunately, they were not wiped and through significant manual sieving of the logs, it was found that Remote Desktop Protocol was used to access the server and was also used to laterally move to other servers.

Not going to share the rest of the investigation, but this should be clear that asking questions helps with investigations. XDR are just tools to help answer these questions quickly through queries to the entire environment.

Just from this initial, high-level investigation, we identified the Administrator credential was compromised and the servers had RDP enabled.

In fact, threat actors are, in a way, using the same Five 5s and one H concept in their attacks.

Why is my payload being blocked? **What** type of privileges do I have? **Where** are the payloads being blocked? **How** do I overcome this control? **When** should I execute the activities to not arouse suspicion?

On the defender side, the same concept also applies for incidents, not just breaches. Take for example, you noticed the server security is blocking PowerShell execution and this process is spawned from sqlservr.exe. Instead of answering “yes, the threat is blocked”, start asking questions. **How** is this possible? **What** is this server, and does it require MSSQL? **Why** is this database public facing?

All these questions eventually help close the security gaps, identifying unpatched systems, servers with unnecessary services or access and so on. Of course, to be fair, on the vendor side of things, there must be improvements to assist on filtering out the noise and presenting detections that should be investigated.

However, it must be noted that the investigation still needs to be done by the security team. Products are not able to magically investigate and produce the results for you. Like a crime investigation, the investigator must collect leads, but it is up to the investigator to see if these leads are part of the case, when do these leads fit into the timeline of the crime and build the complete investigation.

Without asking questions, the team will never learn about the weaknesses or risks the environment has. Simply restoring systems after a breach without going through the Five Ws and one H will simply lead to a repeated breach which could have even worst outcomes on the next attack.

Let's start asking questions and stop ignoring the “door jiggles”. Having a static approach to security is not going to cut it against dynamic adversaries.



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 Youth Symposium Partner, Huawei

How Data Protection Can Enhance Customer Trust and Improve Competitiveness

By Yu Xian Ming, Dennis Chan

Huawei as a global ICT company is committed to bring digitalisation to every person, family and organisation, hence building a connected, intelligent world. It is our responsibility and obligation to protect the data of our customer, partner, and employee. To address this, Huawei appointed a data protection officer, set up a data protection team and developed personal data protection policies to ensure that all data assets including both personal and business are secured. Furthermore, we have identified the potential risks and incorporated data protection measures into our daily business and operation processes where the specifications are according to laws and regulations and guidance given by PDPC. In addition to conducting training to raise awareness among our colleagues, we also manage our third-party partners via regular checks on compliance to ensure that our partners are also doing their part to ensure proper data protection.

To demonstrate Huawei's commitment in protecting customers' privacy, Huawei has data protection measures and best practices in place. We will continuously improve the governance of data protection to build confidence and trust among our consumers, customers, suppliers, partners, and employees, hence improving our business competitiveness.

[back to top](#)

For assurance, we will perform risk assessment and adopt certification from local authoritative organisations like IMDA Singapore who advocates Data Protection Trustmark (DPTM) as the most appropriate localised personal data protection certification standard.

In February 2022, Huawei International have achieved DPTM certification from IMDA Singapore. To prepare for the certification, we have conducted assessment and made improvement based on the DPTM standard/guidelines released by IMDA, together with guidance of Huawei team of personal data protection experts. Despite the delay caused by COVID-19, Huawei passed the certification in one attempt within the scheduled timeline. The key success factors for achieving DPTM certification are as follows: 1) teamwork, 2) minimisation of personal data, 3) external regulations and internalisation policies and processes, 4) IT information system security control, 5) third-party supplier management, and 6) routine self-check, inspection and improvement.

1. Teamwork

Obtain CEO's endorsement to appoint a data protection workgroup led by the Data Protection Officer (DPO). The DPO will be responsible for the overall personal data protection of the company. Appoint a primary owner of each department or section (preferably departmental director/section leader), and designate appropriate team members of the department to take charge of data protection. The DPO and the assigned team members will work together to ensure data security, hence building a well-coordinated team is an important factor to effective personal data protection.

2. Minimisation of personal data

There is a need to mobilise the respective DPO of each business department to list out their respective business processes and operational scenarios, identify and record all involved personal data assets, summarise and output a data asset map based on business scenario. Both business experts and data protection experts may jointly identify and review the involved data items that are required by services, work on principles such as the non-collection of unnecessary data, deletion of unnecessary personal data collected in the past from the IT system, minimising the need of personal data and reducing risks from the source of data, etc.

When there are any changes in business process or a new business been introduced, review the data asset map of the business, identify and analyse risks, update the operation guide, and check list.

During DPTM assessment, we adopt the improvement suggestions provided by the assessor, we consolidate and optimise the data asset map, this will greatly reduce any similar and duplicate Data Inventory, also will facilitate organisations to formulate targeted risk control measures based on category of data.

3. Policy and process regulations for external regulation and internalisation

Today, there are numerous employees working on some form of data in accordance with the various business operation processes daily. Hence, it is critical to ensure that proper

governance on collection and processing of personal data in their daily work, both legal requirements and PDPC guidelines are incorporated into the processes and workflow relating to personal data.

Starting from the data asset map, we derive a data life cycle flowchart to identify potential risks, analyse risk impacts, develop risk control measures that meet the requirements of personal data protection laws and regulations, and incorporate them into business processes to form Huawei Personal Data Protection Compliance Operation Guide for all business domains. Review and update on yearly basis. Normalising external legal requirements into corporate policy could be a lengthy and heavy workload but it is necessary. Personal data can be protected without any dead end only when legal requirements for personal data protection are implemented in all operational processes.

4. IT information system security control

IT systems are handling an increasing load of various data, especially in this digital era. As such, control of the IT systems is crucial to ensure overall security. As part of daily routine, there will be scans for viruses and malware, performing security checks, and continuous security monitoring and protection for all IT systems and applications. Strict control on system access rights, routine review of authorised access list, and prompt change/removal of access rights for employees who have transferred out or resigned. At the same time, regular check on data retention to ensure that personal data in the IT system is deleted or desensitised according to the regulatory compliance and legal obligations of data retention.

5. Third-party supplier management

Huawei focuses on three aspects in managing the personal data protection of third-party suppliers. First, we evaluate the supplier's personal data protection mechanism, set the introductory threshold level, and reject suppliers with inadequate or unqualified data protection. Secondly, the responsibilities and obligations of data protection should be specified in contract terms and conditions according to the service scope. Thirdly, during fulfillment phase, we will evaluate the suppliers' compliance to cyber security and personal data protection regularly, conduct due diligence (DD) checks on the fulfillment, rectify any identified issues, and eliminate suppliers who do not perform meet our contract obligations.

It is our responsibility to properly manage third-party vendors and to collaborate with them to protect any personal data; this is a key focus of DPTM certification evaluation. Before DPTM assessment, Huawei will prepare a list of suppliers involved in personal data processing, including the involved personal data types, personal data protection agreement template and signed clauses (desensitisation), DD performance check template, and actual check report.

6. Self-check, inspection, and improvement

Huawei conducts compliance self-check for data protection based on all business scenarios annually. We also implement semi-annual self-check and inspection for businesses that involve large amount of personal data or sensitive personal data

collection and processing. Self-check will help to ensure legal requirements are met, on-site inspection could also be performed by the Personal Data Protection Working Group. In the event that any item is found to be non-satisfactory during the self-check, rectification will be enforced within given time. Self-check will also allow for optimisation and improvement on control measures that may be found to be not aligned with the actual business scenario.

In addition to the above 6 key factors leading to successful DPTM certification, establishing a well implemented framework with control mechanism for data retention, protection of data subject rights, data breach response and handling are the indispensable elements.

Personal data protection will evolve as data subjects' requirements for privacy protection are increasing and facing ever-changing cyber-attacks, Huawei will continue to acquire new knowledge and technologies, learn from peer best practices, and comply with legal requirements and DPTM certification standards. Continuously improve the data protection framework to ensure that personal data is continuously protected, hence maintaining the trust of consumers, customers, suppliers, partners, employees, and regulatory agencies, continuously improve competitiveness, to ensure stable business development of the company.

About Huawei

Founded in 1987, Huawei is a leading global provider of information and communications technology (ICT) infrastructure and smart devices. We have approximately 195,000 employees and we operate in over 170 countries and regions, serving more than three billion people around the world.

Huawei's mission is to bring digital to every person, home and organization for a fully connected, intelligent world. For more details, please visit <https://www.huawei.com/sg/>
The End

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

PROFESSIONAL DEVELOPMENT

Listing of Courses by Wissen International



EC-Council

CCT
Certified
Cybersecurity Technician

EC-COUNCIL, CREATOR OF THE CERTIFIED ETHICAL HACKER CERTIFICATION,
launches the only entry-level cybersecurity program in the world

- WITH 85 HANDS-ON,
- STATE-OF-THE-ART LABS:
- REAL LIFE PERFORMANCE BASED EXAM

Register Now!

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 \$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.

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

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.

Qualified Information Security Professional (QISP®) Course

QUALIFIED INFORMATION SECURITY PROFESSIONAL (QISP)

- 5 DAYS -

\$840*

~~**\$2800**~~

*70% funding for Singaporeans 40 and above.
50% funding for all Singaporeans below 40 & all PRs.

Call us: +65 8839 0071
Email us: training@opusit.com.sg

AiSP Advance Connect Excel

OPUS ACADEMY

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

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



Delivery Partners



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

- 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.

Program Partner



Delivery Partners



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.

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

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



Acronis







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



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.