

News & Update

- Knowledge Series
- CAAP
- SVRP
- AiSP Cyber Wellness
- Ladies in Cyber
- Special Interest Groups
- CREST Singapore
- The Cybersecurity Awards
- IOT Innovation Day
- Upcoming Events

Contributed Contents

- CTI Perspective – Mitigating Data Breaches and Protecting Personal Data
- Huawei
- A Real-World Guide to Modernizing Your IGA Platform
- 2021 Adversary Infrastructure Report
- Let's Grow Singapore's Cybersecurity Talent Pipeline Together!
- The Cybersecurity Awards 2021 Winner – Mr Eugene Lim

Professional Development

Membership

NEWS & UPDATE

New Partners

AiSP would like to welcome Cycognito, Cyfirma and Securecraft as our new Corporate Partner. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem.



SECURECRAFT

Continued Collaboration

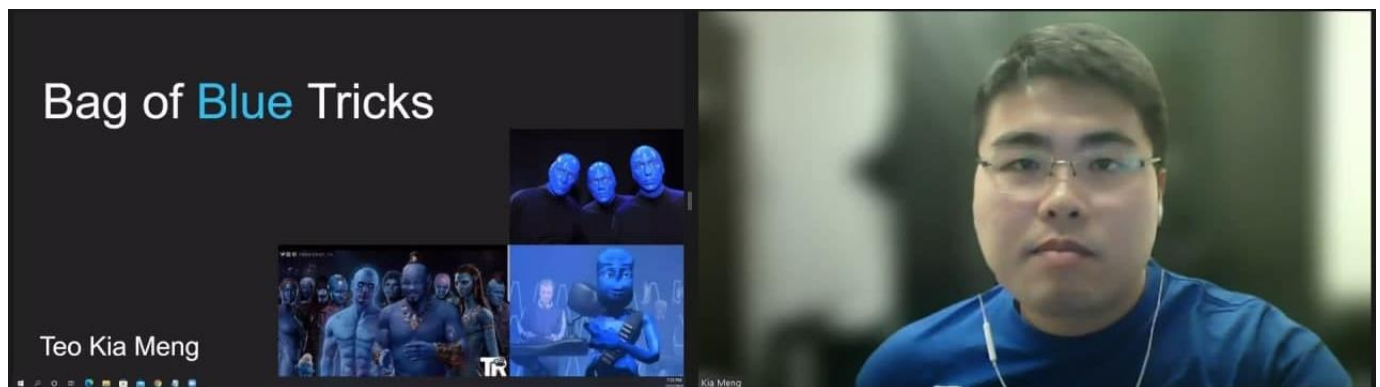
AiSP would like to thank Republic Polytechnic for their continued support in developing the cybersecurity landscape:



Knowledge Series Events

Red Team, Blue Team on 17 Feb

On 17 Feb, Knowledge Series on Red Team Blue Team, it is our pleasure to have our Corporate Partner, Cyber Security Agency of Singapore (CSA), to share with us on the exciting technical information and best practices across domains such as Red Teaming, Threat Intelligence, and incident response. We hope you had fun learning about “Red Tricks, Blue Tricks”.



Cryptography on 31 Mar 22

Based on AiSP Information Security Body of Knowledge (IS BOK) 2.0 content topics, AiSP has been organising a series of knowledge-sharing & networking events to enable AiSP members with a bettering understanding of how IS BOK can be implemented at workplaces.



AiSP Knowledge Series – Cryptography

AiSP Knowledge Series
Cryptography
31 March 2022 | Zoom | 3 PM - 4.30 PM

Ashok Venkateswaran
Vice-President
Mastercard

Magda Lilia Chelly
Managing Director, CISO
Responsible Cyber

Organised by:
AiSP
Advance Connect Excel

Supported by:
INFORM MEDIA DEVELOPMENT AUTHORITY
Mastercard
Responsible Cyber

In support of:
DIGITAL FOR LIFE

In this Knowledge Series, we are excited to have Mastercard and Responsible Cyber to share with us insights on Cryptography. 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.

Introduction to Digital Assets/Cryptocurrency

By: Ashok Venkateswaran, Vice President, Mastercard

Overview of digital assets and why digital assets can be used to solve real world payments issues.

Are your Software Developers set up for Success to Secure your Digital Assets?

By: Magda Lilia Chelly, Managing Director, CISO, Responsible Cyber

Digital Assets are becoming the most valuable assets for companies. However, research shows developers often get password security wrong, confusing hashing and encryption. How do you support your developers to build the right fundamentals, and ensure the security of your Digital Assets?

This presentation lists common mistakes when implementing cryptographic controls in software development. It sets up best practices to support your developers' team with the right security mindset and security by design approach.

Date: 31st March 2022 (Thurs)

Time: 3PM – 4.30PM

Venue: Zoom

Registration:

https://zoom.us/webinar/register/7216444632711/WN_WI_H84ILTkuRmFEDQlq60w

Cloud Security on 14 April



AiSP Knowledge Series – Cloud Security

In this Knowledge Series, we are excited to have Cisco and SecurID, an RSA Business to share with us insights on Cloud Security. 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.

Evolving Security Strategy for a New World

By: Syed Abdul Rahman Alsagoff, Regional Sales Specialist, Cloud and Endpoint Security, ASEAN & Korea, Cisco

Just as how the pandemic has forever changed the way we work and conduct business, the methods and thinking of how we protect our digital assets need to evolve and change as well. Now more than ever, enterprises need to protect their workforce with security that is scalable and effective but yet simple and adaptive enough to manage. Key concepts like Zero Trust Network Access, SASE, Cloud and As A Service were developed by the industry as an attempt to achieve just that. But where and how do you really start?

In this session, we will look back into the threats that were most prevalent in 2021 and look forward into what Enterprises are investing in a drive to real outcomes organisations need as they accelerate digital transformation in a post-Covid era.

Top Myths About Zero Trust

By: Craig Dore, IAM Specialist for SecurID, APJ

Join the session with our IAM Specialist in APJ on his views around the Top Myths on Zero Trust. Many global security leaders have and are still looking to adopt a Zero Trust model to help reduce cyber breaches in their organisations. For this to be implemented effectively, we need to discuss the misconceptions of Zero Trust.

Date: 13th April 2022 (Wed)

Time: 3PM – 4.30PM

Venue: Zoom

Registration:

https://zoom.us/webinar/register/3216450910823/WN_JpANjQrMTAqIsl3V70astQ

IS Governance on 28 April



AiSP Knowledge Series – IS Governance

AiSP Knowledge Series - IS Governance

28 Apr | MS Teams | 3PM - 4.30PM

Suresh Menon
Sr. Technical Specialist
Cloud-Security & Compliance
Microsoft Singapore



Organised by



Supported by



In support of



In this Knowledge Series, we are excited to have Microsoft to share with us insights on IS Governance. 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.

Fasttrack your Compliance Journey

Speaker: Suresh Menon, Sr. Technical Specialist Cloud-Security & Compliance, Microsoft Singapore

Data breaches are becoming more common than ever before. Yet, nearly 51% of organizations are still unprepared to deal with a data breach.¹ And as your data continues to grow exponentially, so will your risk of breaches and compliance violations.

Afterall, today's employees are often using multiple devices, apps and locations to store and access business-sensitive data. What's more, it can be challenging to keep up with regulatory demands when you're faced with an average of 220 daily updates from global regulatory agencies. The good news is, staying compliant and secure is simpler with the right technologies.

In this webinar, learn how you can reduce risk without compromising productivity by using:

- Machine learning and automation to reduce manual data management tasks
- Microsoft Information Protection to safeguard sensitive data across clouds, apps and endpoints
- Microsoft 365 Compliance to keep up with everchanging privacy regulations, data growth and insider risks

The key to building a more secure and profitable business begins with the way you manage your data. Register now to get started.

Date: 28th April 2022 (Thu)

Time: 3PM – 4.30PM

Venue: MS Teams

Registration: <https://forms.office.com/r/EtSn0UFibu>

About our Knowledge Series

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

1. Cryptography, 31 Mar 22
2. Cloud Security, 13 Apr 22
3. IS Governance, 28 Apr 22
4. Identity & Access Management, 18 May 22

Please let us know if your organisation is keen to be our sponsoring speakers in 2022!

AiSP members who registered for the event, can playback the recorded event via their member profile in Glue Up. If you did not sign up for the event, please email secretariat@aisp.sg for assistance. Please refer to our scheduled 2022 webinars in our [event calendar](#).

Cybersecurity Awareness & Advisory Programme (CAAP)

Upcoming CAAP Event

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

CISCO& SCCC CAAP Event on 10 March

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

In collaboration with:  **AiSP**
Advance Connect Excel

 **CISCO**
DESIGNED

**Shifting the Paradigm in Cybersecurity -
The Next Breach Could Happen to You**

10th March 2022, Thursday | 3:00 PM SGT



The way we work has changed a lot in the last year. This has given an exponential rise in cybersecurity attacks and breaches. The thought of your data being locked away - with the threat of it being destroyed or even released to the general public - is a nightmare for any small business owner. But the reality is that in 2020 alone, ransomware cases rose 154% in Singapore.

With employees working from home and applications moving to cloud, the old ways to secure the network are becoming obsolete. That is why it costs less for small businesses to prevent ransomware rather than pay-up. In this session we are going to cover how Cisco is helping Small Business's prepare and prevent from potential cybersecurity breaches with security that follows the user no matter where they work from.

Agenda:

1. Welcome Address by AiSP
2. Evolution of Singapore Cyber Threats
3. Understand how to plug common security gaps easily
4. Q&A

Guest Speakers

Aseem Javed
Small Business
Architecture
Leader ASEAN
Cisco Systems






Wendy Ng
EXCO Member
AiSP



Click [here](#) to register.

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 	 <p style="text-align: center;">AiSP Cybersecurity Awareness E-Learning</p> 
<p>Why Should You Take This E-Learning & How Will It Help You?</p> <p>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</p>	

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 to sign up for the E-Learning or if you have any queries.

Payment Details

Bank	:	DBS Bank 12 Marina Boulevard DBS Asia Central @ Marina Bay Financial Centre Tower 3 Singapore 018982
Bank Code	:	7171
Branch Code	:	012
Account Name	:	AISP (GLOBAL) PTE LTD
Account No	:	072-033821-9

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)

Millenia Institute School Talk on 3 and 4 February

On 3 and 4 February, more than 200 students from Millenia Institute had the opportunity to hear from SVRP Lead, Ms Soffenny Yap on the importance of Cyber Hygiene, how to stay safe online, AiSP Cyber Wellness Programme, Volunteering in the Cyber Ecosystem and the different careers in Cyber as part of the Digital for Life programme. It was an insightful session for the students as they also learned about cybersecurity career, challenges faced in the industry and our very own Student Volunteer Recognition Programme (SVRP).



Questions for Speaker

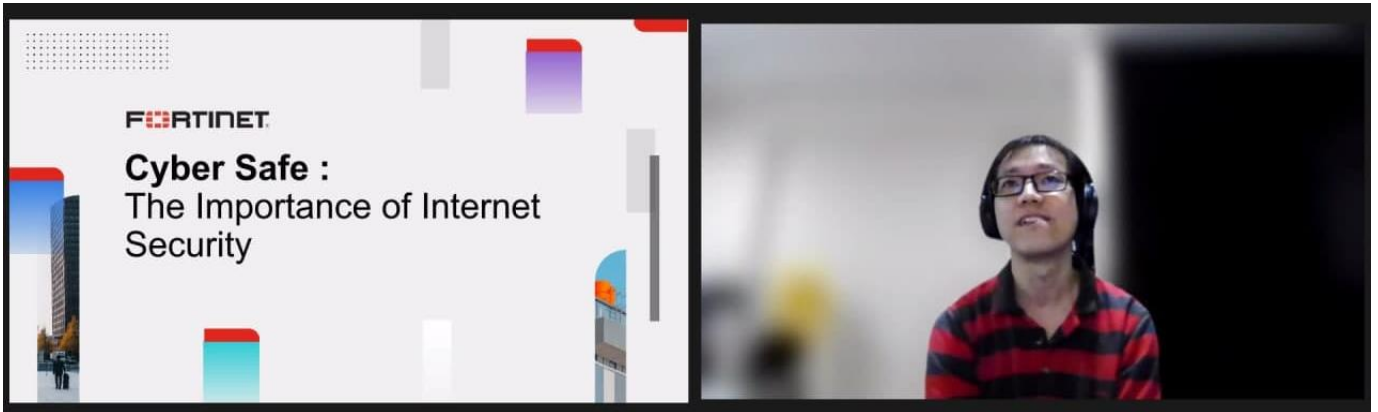
1. What is necessary for a person working in the cybersecurity to excel in?
2. What is the drives you to become what you are right now
3. What's the toughest thing about your job?
4. How did you choose your desired course?
5. How difficult was it on your way up in your career?
6. How does it feel to work in your industry?
7. How did you cope during the pandemic?
8. What challenges did you face in your job?
9. How did you get into cyber security? What motivates you to join?
10. What does your course of study or line of profession entail? What are your responsibilities at work?
11. How to join a cyber security MNC?
12. How would you describe the work environment in your industry?
13. What words of advice would you give our students who aspire to work in this industry?
14. What do you think students can do in planning their future pathways?

AiSP ADVANCE | CONNECT | EXCEL



Sharing with Horizon Primary School on 7 February

On 7 February, we had the opportunity to do a cybersecurity awareness sharing with over 1500 students from Horizon Primary School. We would like to thank our Corporate Partner, Fortinet, for sharing with the students on the importance of Internet Security.



SVRP Nomination has officially concluded, and results have 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. Nomination period is from 1 Aug 2021 to 31 Jul 2022.

Nomination Period:
1 Aug 2021 to 31 Jul 2022

Nomination Period:
1 Aug 2021 to 31 Jul 2022

CALL FOR NOMINATION! STUDENT VOLUNTEER RECOGNITION PROGRAMME

Tier	Requirements
Bronze	Completion of one of three pillars or complete three of three pillars with minimum 50% attained hrs. + Skills: 30 Hours or more + Events: 60 Hours or more + Leadership: 30 Hours or more
Silver	Completion of two of three pillars + Skills: 30 Hours or more + Events: 60 Hours or more + Leadership: 30 Hours or more
Gold	Completion of all three pillars + Skills: 45 Hours or more + Events: 60 Hours or more + Leadership: 45 Hours or more

Scan the QR Code for the Nomination Form

The SVRP for the secondary school and pre-university students is on merit basis and evaluation would be slightly different as cyber security is not offered as a subject nor co-curricular activities (CCA) in most schools in Singapore at the moment. The students would be given Certificate of Merit when they achieved the following (see A, B, C or D):

Example A	Example C
+ Leadership: 10 Hours	+ Leadership: 0 Hour
+ Skill: 10 Hours	+ Skill: 50 Hours
+ Outreach: 10 Hours	+ Outreach: 0 Hour
Example B	Example D
+ Leadership: 0 Hour	+ Leadership: 0 Hour
+ Skill: 20 Hours	+ Skill: 0 Hour
+ Outreach: 20 Hours	+ Outreach: 60 Hours

Scan the QR Code for the Nomination Form

The SVRP comprises three broad pillars where IHL students can volunteer:

- + Skills-based: E.g. Conduct cybersecurity workshops or develop related software
- + Events-based: E.g. Provide support at technology or cyber-related events
- + Leadership: E.g. Mentoring younger students and managing teams or projects

The track for Secondary School and Pre-University students comprises three broad pillars where they can volunteer:

- + Leadership refers to how the volunteer leads a team to complete the voluntary activity.
- + Skill refers to how the volunteer applies his/her cybersecurity knowledge to others
- + Outreach refers to how the volunteer is involved in outreach efforts (social media, events) to increase cybersecurity awareness for the public.

Visit www.aisp.sg/svvp.html for more details

Visit www.aisp.sg/svvp.html for more details

AiSP Cyber Wellness Programme

[back to top](#)

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 Tenth edition of AiSP's 'Ladies Talk Cyber' series, we interviewed Ms Tham Mei Leng, Ministry Chief Information Security Officer (MCISO) in the Ministry of Sustainability and the Environment (MSE). Her role involves providing cybersecurity leadership to the Agency CISO in MSE HQ and the agencies in the MSE family (namely PUB, NEA and SFA) in charting the development of cyber and data security goals, strategies and action plans.

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

Ms Tham is the Ministry Chief Information Security Officer (MCISO) in the Ministry of Sustainability and the Environment (MSE). Her role involves providing cybersecurity leadership to the Agency CISO in MSE HQ and the agencies in the MSE family (namely PUB, NEA and SFA) in charting the development of cyber and data security goals, strategies and action plans.

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



AiSP International Women Day Celebrations – 08 March 2022

AiSP Ladies in Cyber International Women Day 2022 Learning Journey with Trend Micro & Fireside Chat

Panelists

Moderator



Ms Yeo Wan Ling
Member of Parliament
for Pasir Ris-Punggol GRC
& Director of U SME and
Women & Family Unit



Ms Tham Mei Leng
Chief Information
Security Officer (CISO),
Ministry Family



Ms Veronica Tan
Director of the Safer
Cyberspace Division,
Cyber Security Agency of
Singapore



Ms Jessie Chong
Director of Marketing, SEA
Trend Micro



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



SUPPORTED BY



With men in tech outnumbering women by 3 to 1, Cybersecurity industry has always had an undeserved reputation of being a man's world. And there are quite a few reasons for the disproportionate number but arguably the main reason for it, is the lack of understanding of what women can do in an industry that's perceived to be tough and unforgiving. Yet, recent studies show that women are more likely to hold high-level roles in cybersecurity industry. It has also been proven that organizations advocating gender diversity tends to be more profitable.

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

This coming International Women Day 2022 on 8 Mar 22 (7.30pm to 8.30pm), **AiSP Ladies in Cyber** is organizing a hybrid fireside chat together with our Corporate Partner Trend Micro. Join **Ms Yeo Wan Ling, Ms Tham Mei Leng, Ms Veronica Tan, Ms Jessie Chong and**

Ms Sherin Y Lee - our female leaders from Cybersecurity industry as they share their experience, advice and provide guidance on career in IT industry for females.

Sign up virtually at:

https://zoom.us/webinar/register/3016429005761/WN_EDPpwcSGRViZ55PwJjt4nw.

Physical registration is open to students only and they can email to secretariat@aisp.sg to sign up or sign up through their lecturers.

AiSP Ladies in Cyber Inaugural Symposium – 22 March 2022

AiSP Ladies in Cyber Symposium

“How Can Women In Tech Define The Future Of Cyber & Tech?”
Dialogue Session



Minister Josephine Teo
Minister for Communications and Information and
Minister-in-Charge of Smart Nation and Cybersecurity



Ms Tammie Tham
Chief Executive Officer of
Ensign InfoSecurity
Co-Chair of the AiSP
Advisory Council



Ms Teo Yi Ling
Senior Fellow, Centre of
Excellence for National
Security - S Rajarajam
School of International
Studies



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

Attend Breakout Sessions By Female Cybersecurity Experts



Dr Tan Mei Hui
AiSP Mentor
Director at Tencent
Speaker for AI in Cybersecurity /
Threat Modeling



Ms Soffenny Yap
AiSP IoT SIG Lead
Security Services Sales
Leader of IBM
Speaker for IoT



Ms Sugar Chan
AiSP EXCO Member
Manager at Boston
Consulting Group (BCG)
Speaker for Risk



Ms Daisy Radford
AiSP Mentor
Head of Operations & Delivery
APAC at BAE Systems
Speaker for Security
Operations

JOINTLY ORGANISED BY:  AS PART OF:  SUPPORTED BY:    IN SUPPORT OF: 

30 CYBER WOMEN X DIGITAL

SPONSORS:
















AiSP will be organising the inaugural Ladies in Cyber Symposium for the female Youths that highlights 4 different topics on cybersecurity, including the importance of cybersecurity, and how women can play a role in it. We are expecting 150 Youths and professionals (Subject to COVID-19 restrictions) at the event on 22 March 2022 at Life-Long Learning Institute. The theme for this year Symposium is “**How can Women in Tech define the future of Cyber & Tech**”. Visit https://www.aisp.sg/ladies_symposium.html for more details of the event or sign up below using the below URL.

Physical Registration: <https://forms.office.com/r/QiyQi4QvWP>

Virtual Registration: https://zoom.us/webinar/register/WN_aVmzPp8aS96ll63whBEfog

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



AiSP
Advance Connect Excel

AiSP x Recorded Future Capture The Flag Session

**AiSP x Recorded Future
Capture The Flag Session**

25 March | 2PM - 5PM
Singapore Marriott Tang Plaza Hotel

REGISTER NOW

Organised by **AiSP** Advance Connect Excel

Supported by **Recorded Future** **Infocomm Media Development Authority** **Digital For Life**

Do you find it time consuming to prioritize threats at your enterprise? Are you overwhelmed by the long list of threats every morning when you start your day?

We would like to extend the opportunity to take Recorded Future's security intelligence solution for a test drive with your peers on **March 25, 2:00PM – 5:00PM at Singapore Marriott Tang Plaza Hotel.**

See for yourself how easy it can be to implement real-time intelligence into your existing security workflows.

This is a focused opportunity to experience a real-time, hands-on capture the flag (CTF) event with Recorded Future to learn how you can make faster and more informed security decisions.

What to Expect at the CTF:

A security intelligence experience (CTF) where you'll learn how to:

- Effectively identify and profile threats from the dark web, open web, and technical sources
- Proactively prevent attacks by prioritizing vulnerabilities based on real-life exploitability
- Quickly triage alerts with external, real-time threat intelligence, and monitor for and alert on relevant threats to your business
- Easily research and report on trending malware and threat actors
- The winner of the CTF walks away with a prize and bragging rights!

Date: 25th March 2022 (Friday)

Time: 2PM – 5PM

Venue: Singapore Tang Marriott Plaza Hotel

Registration: <https://www.eventbrite.sg/e/275465162717/>

AGENDA

2:15 PM: **Welcome Address by AiSP CTI SIG Lead**

2:30 PM: **Panel Discussion- Discussion on the rapidly evolving and intertwined geo-political and cyber threat landscape and how organisations are using threat intelligence to enable themselves to become proactive with a variety of security risks**

3:00 PM: **CTF Orientation and CTF by Recorded Future Intelligence Specialists**

4:30 PM: **Results and Prize Presentation for top winner followed by F&B**

5:00 PM: **End**



AiSP CTI SIG Event

AiSP Cyber Threat Intelligence SIG Event

29 April | 10AM - 12PM | Hybrid



Michael Tan

Michael Tan, Regional VP
APAC
CyCognito



Kok Kiat Han

Systems Engineer (Cyber
Intelligence Analyst)
Cyber Security Agency of
Singapore



Sukhdev Singh

SIG Member
CTI SIG



Organised by



Supported by



In support of



AiSP has set up a Special Interest Group (SIG) – Cyber Threat Intelligence. Our SIG covers the following topics broadly, with an open view that the emerging trends that should feed into AiSP’s Information Security Body of Knowledge and CAAP Body of Knowledge. As part of the CTI SIG engagement, AiSP will be organising a series of events to engage AiSP members and share more insights of Cyber Threat Intelligence.

You can’t protect what you don’t know. That is why visibility and protection of your entire Attack Surface is of utmost importance. In this session, we will talk about what is External Attack Surface Management, why CyCognito EASM platform can help you to manage your Attack Surface effectively, easily with automation and integration to your existing adjacent security portfolio.

AGENDA

- 10:00 AM: **Welcome Address by AiSP CTI SIG Lead**
- 10:30 AM: **Attack Surface Visibility – The Foundation of Effective Cybersecurity**
- 11:00 AM: **Defending your digital surface. VAPT vs EASM**
- 12:00 PM: **End**

Join us in our panel discussion as we discuss further on defending your digital surface.

Date: 29th April 2022 (Friday)

Time: 10AM – 12PM

Venue: Hybrid

Registration: <https://www.eventbrite.sg/e/aisp-cti-sig-event-tickets-282631126307>

CREST Singapore

CREST is an international not-for-profit accreditation and certification body representing and supporting the technical cybersecurity market.

CREST has a network of approaching 300 accredited member companies operating in many countries worldwide. In addition, thousands of cybersecurity professionals globally hold one or more CREST certifications. CREST also has links to governments, regulators and partner organisations in numerous countries.

CREST has a proud history of working with organisations in Southeast Asia, including AiSP. Indeed, AiSP ran a project in partnership with CREST between 2016 and 2021 to help establish the CREST Singapore Chapter. The project concluded successfully in March 2021 and CREST began a process of transition to a fully autonomous chapter.

Thanks to the work of AiSP, and others around the world, CREST now has a truly international structure covering Southeast Asia, Australasia, the Americas, the EU and the UK. Members in each of these regions are represented on elected CREST Regional Councils.

The CREST Southeast Asia Council was elected in December 2021 and comprises of 11 members. It is chaired by Emil Tan, Chief Operating Officer of cybersecurity talent development company Red Alpha. Emil founded Singapore's largest cybersecurity community group, Division Zero (Div0), and he previously worked for the Infocomm Media Development Authority (IMDA).

Emil, and the Chairs of the other Regional Councils, sit on the CREST International Council, ensuring our governance structure is representative and reflects CREST's global reach.

The broad objectives of CREST in Southeast Asia are to support members to grow their businesses, grow the CREST membership, and support governments and regulators as they seek to enhance and elevate cybersecurity for their infrastructures and businesses.

CREST recently contributed to the Consultation on the Licensing Framework for Cybersecurity Service Providers, issued by the Cyber Security Agency of Singapore

(CSA), at the end of 2021. CREST is committed to working in partnership to support the development of the cybersecurity industry in Singapore and the wider region.

CREST President Rowland Johnson also welcomed the CSA's updated Cybersecurity Strategy, launched in October 2021, saying: "CREST welcomes the strategy's focus on supporting organisations to adopt appropriate and high-quality cybersecurity solutions, underpinned by a skilled cybersecurity workforce linked to strong professional communities.

"CREST and its members look forward to working with the CSA to help to implement the strategy to secure Singapore's critical information infrastructure and boost its cybersecurity capabilities."

Globally, it has never been a more important time for governments, regulators, professional bodies like AiSP and CREST, and their members and partners to collaborate and develop more resilient cybersecurity ecosystems. Changes in the way we live and work, combined with the growth and diversification of threat vectors, present challenges and opportunities in equal measure.

2022 promises to be a busy year for CREST, and we are delighted to begin it by renewing our close working relationship with AiSP. We warmly welcome the opportunity to reach out to AiSP members and partners. Please contact singapore@crest-approved.org for more information on CREST examination in Singapore or any matters related to CREST.



Mr Emil Tan
Chair, CREST Southeast Asia Council



Mr Rowland Johnson
President of CREST

The Cybersecurity Awards

THE CYBERSECURITY 2022 *Awards*

TCA 2021 Judges' Appreciation

On 25 February, Judges for TCA 2021 gathered together at Nanyang Institute of Management (NIM) for an appreciation session. We would like to thank Nanyang Institute of Management (NIM) for their kind sponsorship of the venue to make the Appreciation Ceremony possible and thank all the judges for their contributions.



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

Please email us (secretariat@aisp.sg) if your organisation would like to be our sponsors! Limited sponsorship packages are available.

Nominations details will be announced shortly.

THE CYBERSECURITY Awards 2022

Organised by



Supported by



Supporting Associations



Community Partner



Supporting Organisation



Platinum Sponsors



Gold Sponsors



Silver Sponsors



IOT Innovation Day

The AiSP IoT Innovation Day & Exhibition is the can't-miss event of the year as professionals come together for a day of sharing on Smart City, Driverless Transportation and Health Technology Ecosystem connect for the education, innovation, and collaboration they need to reimagine as part of innovation and smart nation for everyone, everywhere. This event which will be held in May 2022 is targeting at professionals from CIOs and senior executives to providers and payers to IT consultants and entrepreneurs to join in and attend this influential to get the information and solutions they need to reimagine on a Smart City for everyone, everywhere.

Sponsors:

CISCO, Elastic, ExtraHop, Recorded Future and SecureCraft

Scam Awareness Engagement Series

16 March (English)

Scam Awareness Engagement Series

16 March 2022 | 2:00 PM – 4:00 PM | Zoom Webinar

Out of the total reported crime cases in 2021, more than half involved scams, a sharp surge in scam cases from the year before. "Scammers have been constantly evolving their tactics and taking advantage of the COVID-19 situation to prey on the public's increase in online activities, and also their heightened sense of vulnerability and uncertainty," said the police.
[Source: CNA Article dated 16 Feb 2022]

AiSP and Acronis collaborate to bring you a series of webinars to raise awareness on how to mitigate scams, in support of the Digital for Life movement. Learn to identify fake news, online risks and harms, and protect yourself from these online threats.

Join the webinar and stand a chance to win Acronis Cyber Protect Home Office, the only personal cyber protection solution that delivers easy-to-use, integrated backup and anti-malware in one package.

Our Awesome Speakers :



Soffenny Yap
EXCO Member
AiSP



Amos Dong
Technology Evangelist
Acronis



Wendy Ng
EXCO Member
AiSP



Organised by:



Supported by:



Click [here](#) to register.

17 March (Mandarin)

[back to top](#)



Zoom Webinar

三月十七日

骗局意识参与系列

在 2021 年报告的犯罪案件总数中，超过一半涉及诈骗，诈骗案件比前一年急剧增加。警方说：“诈骗者一直在不断发展他们的策略，并利用 COVID-19 的情况来掠夺公众增加的在线活动，以及他们高度的脆弱感和不确定性。”

[来源: 2022 年 2 月 16 日 CNA 文章]



庄惠婷
执行委员会
资讯通信专才协会

资讯通信专才协会和安克诺斯合作为您带来一系列网络研讨会，以提高人们对如何减少诈骗的认识，以支持数码益终身全国运动。学习识别假新闻、在线风险和危害，并保护自己免受这些在线威胁。

加入网络研讨会，就有机会赢取安克诺斯网络保护的家庭解决方案，这是唯一一款在一个软件中提供易于使用的备份和反恶意软件的个人网络保护解决方案。



何鹏
网络安全销售顾问
安克诺斯

Organised by:



Supported by:







Click [here](#) to register.

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
3 Mar	IBM CISO Club Briefing - How CISOs can secure a strategic partnership	Partner
4 Mar	Your Mind Matters (Y2M) with AiSP	AiSP & Partner
8 Mar	AiSP International Women Day Celebrations at Trend Micro	AiSP & Partner
10 Mar	AiSP x CISCO x SCCCCI CAAP Event	AiSP & Partner
11 Mar	CSC Sharing - Countering Emerging Technology's Potential for Malicious Abuse	Partner
16 to 17 Mar	IoT Asia+ 2022	Partner
16 Mar	Digital for Life – Scam Awareness Sharing (English)	AiSP & Partner
17 Mar	Digital for Life – Scam Awareness Sharing (Chinese)	AiSP & Partner
18 Mar	SBF TACs Budget 2022 Discussion	Partner

back to top

19 Mar	AiSP Scam Awareness & Cyber Sharing at Ang Mo Kio Community Centre	AiSP & Partner
19 Mar	AiSP Scam Awareness & Cyber Sharing at Tampines East Community Centre	AiSP & Partner
22 Mar	Ladies in Cyber Symposium	AiSP
23 Mar	AiSP x Microsoft CAAP Roundtable	AiSP & Partner
23 to 25 Mar	Fintech India expo 2022	Partner
25 Mar	CTI SIG Event with Recorded Future	AiSP & Partner
28 to 30 Mar	Protect 2022	Partner
29 Mar	AiSP Scam Awareness & Cyber Sharing at Braddell Heights Community Centre	AiSP & Partner
30 Mar	ITE East Cybersecurity Lab opening	Partner
30 Mar	Annual General Meeting 2022	AiSP
31 Mar	Knowledge Series – Cryptography	AiSP & Partner
31 Mar	EnGarde TTX Primer: Assess your organisation's readiness in the event of a cyber attack	Partner
1 Apr	AiSP x Huawei CAAP Roundtable	AiSP & Partner
13 Apr	Knowledge Series – Cloud Security	AiSP & Partner
19 to 20 Apr	Cloud Security Summit APAC 2022	Partner
26 to 27 Apr	Cyber Security for Critical Assets APAC Summit	Partner
28 Apr	Knowledge Series- IS Governance	AiSP & Partner
29 Apr	CTI SIG Event	AiSP

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

CONTRIBUTED CONTENTS

Article from Cyber Threat Intelligence SIG

CTI Perspective – Mitigating Data Breaches and Protecting Personal Data

Data breaches are increasingly more common and, in some cases, evolved into a viable income revenue for perpetrators during the Covid 19 pandemic. Given the proliferation of high-profile breaches in Singapore, organisations should review their cybersecurity posture thoroughly and identify how cyber threat intelligence (CTI) could enhance their security of personal and business data.

The [Association of Information Security Professionals \(AiSP\)](#) organised a knowledge-sharing event on 1 December 2021 for its [Cyber Threat Intelligence Special Interest Group \(CTI SIG\)](#), to discuss the trends in data breaches in Singapore and how we can safeguard sensitive data as part of organisations' compliance to the Personal Data Protection Act (PDPA). Some highlights of the event's panel discussion are covered here.

Perpetrators' motivation for causing data breaches

[back to top](#)

Personal data or personal identifiable information (PII) is valuable, not just to the data subjects who own their personal data, but to others who want to commit identify fraud. In reality, identify fraud is not as insidious as in movies; it is fairly common when one wants to exploit what others have through impersonation, such as social network, credentials and credit standing. Our speaker and panellist [Dr. Guy Almog](#) from Cyberint, also shared about ways individuals can mitigate their exposure of personal data.

There are also a wide range of phishing attempts and data breach related activities monitored in the dark web involving corporate and personal data, as presented by one of our speakers Ray Koh from Cyberint,

Phishing / Brand abuse	Dark Web monitoring
Executive impersonation in social media	Employee credentials
Brand impersonation in social media	Private access token
Brand abuse websites detection	Customer credentials exposed
Mobile applications impersonation	Customer payment cards exposed
Domain squatting	Credential stuffing tool targeting company
Phishing websites detection	Brute force tool targeting company
Phishing beacon	Data scraping tool for company application
Advanced phishing detection	Vulnerability scanner targeting company
	Advanced attacks detection
	Source code disclosed
	Leaked documents
	Advanced sensitive information disclosure
	Refund fraud services and tutorials
	Carding services and tutorials
	Advanced fraudulent activities

During Covid pandemic, many people are working remotely and are not able to have in-person identification for verification. This has attracted more perpetrators to steal personal data from less tech-savvy individuals, through data breaches.

Gaps in Protecting Personal Data in Organisations

In the context of the November 2021 data breaches involving individuals' personal data that warrants a higher level of protection, the panel moderator [Mr Andrew Ong](#) facilitated a discussion involving three panellists, on the state of PDPA compliance pertaining to [NUS Society breach](#) and [RedDoorz's 5.9 million affected customers](#). Given the trend of heavier fines imposed by the Personal Data Protection Commission (PDPC) (see [source](#)), I shared on the impact and implications to such a breach from the capacity from [AiSP Data & Privacy Special Interest Group](#).

Besides the PDPA fine arising from the data breaches, the reputation and credibility of being a trusted and properly managed organisation have been affected. Notably for the start-up RedDoorz (company: [Commeasure Pte Ltd](#)) which has a number of investors, its business model is highly dependent on processing customers' bookings and personal data via digital platform. It was reported that the company has been losing money during the Covid pandemic, and this event may worsen its financial situation further.

For NUS Society (NUSS), the data was taken from its website, which was hosted by a third-party Web hosting provider - the database was hacked. It is evident that NUSS may not have assessed why it has to retain full NRIC numbers of its graduates (from local and foreign universities). Since it has generated membership number, it should minimise its data collected, given that it is a lucrative market in selling and re-selling personal data for nefarious means (see [source](#)). PDPC has reiterated the proper use of NRIC numbers since [August 2018](#).

Our panellist [Mr YC Lian](#), who is also a member of the CTI SIG, shared his views at the event and post-event, on guidelines for organisations to handle personal data. Data security is often an afterthought to developers, there is a need to left-shift for threat modelling. In addition, agile and lean startups have changed the way software is built. The need for speed and MVP has robbed many developers from giving deep thoughts on adapting incrementally.

The ease of implementing controls is not a substitute for understanding JTBD¹. CIA² is better as CIAPS³ where P refers to privacy, and S would be safety. Under privacy, there are rights to withdraw consent, update and destroy. Safety would be the freedom from risks. Migrating to clouds creates a model of shared responsibility between the organisations and the cloud service providers. Organisations do not outsource the management of customer data without proper consideration on its fit-for-performance, performance, and continuity, etc.

When asked about the current observation or misconception of handling such sensitive data, YC elaborated that one does not need fancy tools and technical jargons (SIEM, SOAR, CWPP, CSPM, etc) to build good culture, hygiene and processes. Organisations' understanding of their competence and constraints would help them to make better decisions, such as choosing between an IaaS and PaaS or DBaaS.

Besides explaining how CTI service can assist organisations from addressing a potential data breach, Dr. Guy also elaborated on the accuracy and usefulness of the information extracted from CTI, from his experience. More details are available in AiSP's member-only playback of the webinar recording⁴.

On best practices or current guidance for organisations handling personal data, I feel it is important to consider organisation's risk appetite, level of staff awareness, effectiveness of training, and how to use CTI strategically. Organisations are often challenged by limited resources and bandwidth, and it would be helpful to prioritise mitigation controls by referencing CTI and data breach trends. Not all risks are equal in terms of impact for two organisations in the same industry; it depends on your risk appetite and culture. In the course of my data protection work, I often have to dig deep into people's behaviours as it can make or break operational compliance.

Mitigating Data Breaches in Organisations

Data breaches have become the norm; thus, it would be productive to reduce the impact of breach e.g., segregation of types of personal data - e.g., sensitive data. A useful way is to have 2FA or multiple factor authentication depending on the criticality of the access. Take a holistic approach and map out the infosec measures available to your organisation in terms of resources and budget, sustainability, corporate culture and people behaviour, as part of your 2022 planning.

There are various best practices for organisations' operational compliance (as we are dealing with people behaviour, organisational culture and resources available for information security measures). For these two incidents, NUSS needs to reconcile its business purpose for the types of personal data collected and if it is proportionate to its business needs. Is it over-collecting from members and does it have the resources to ensure adequate protection?

Another important point is vendor management, if NUSS has assessed the risks involved for vendor to process the personal data. For organisations intend to process a significant amount of personal data or sensitive data, they should conduct a data protection impact assessment (DPIA) to review its security

¹ Jobs to be done.

² Confidentiality, Integrity and Availability.

³ Izar Tarandach's Core Principles as stated in his book.

⁴ AiSP members are welcome to playback the recorded webinar and the full panel discussion, by [contacting the Secretariat](#).

measures and vendor management. This applies to the case of RedDoorz where it cited high staff turnover as the reason for security oversight. The DPIA helps the management team to identify potential blind spots. If your security measures are highly dependent on human intervention, you should consider if these measures or tasks can be automated and potential impact of identity theft (email address, password). Can an unauthorised user make transaction once he can access the account?

The PDPC has listed out a detailed investigation report for its decision to impose the fine of \$74,000 on RedDoorz. Besides maintaining currency of its security measures and having regular and comprehensive audit, companies should be aware of the competencies of their information security team including their vendors, as data breaches and technological advancements are evolving. This aspect is covered under cyber threat intelligence, where companies can ensure their cybersecurity posture remains relevant to breaches and attacks. Also, data protection impact assessment can cover high-level risk identified by threat intelligence on sale of personal data as a business model by hackers during covid pandemic. As we are coming to an end of first quarter of 2022, we can all start to do away data that does not sparkle. Housekeeping is a simple yet important way to reduce the scale of personal data retained for most small medium enterprises in Singapore. If organisations can remember the PDPC's two criteria on assessing data breach impact – scale (meaning number of affected individuals) and sensitivity (meaning if it is going to cause significant harm to the individuals once it is exposed), they can think about reducing “scale” and “sensitivity” gradually as part of proper data management.

About the Author



Yvonne Wong
EXCO Member, AiSP

Yvonne is currently a Co-opted Committee Member, EXCO, in AiSP. She is volunteering in the Cyber Threat Intelligence Special Interest Group (SIG), and Data and Privacy SIG. Yvonne has been a practitioner, consultant and trainer for Governance, Risk and Compliance (GRC) since 2015. Prior to GRC, she has been involved in branding, communications, intellectual property management and strategic planning work in private and public sectors. She is presently the Senior Manager in the Yishun Health Data Protection Office.

Article from our CPP Partner, Huawei

[back to top](#)



Huawei Cyber Security Transparency Centre

Committed to Securing our Shared Digital Future



Experience & Communication

The establishment of the Brussels Cyber Security Transparency Centre demonstrates Huawei's commitment to all stakeholders across Europe, public and private, and intent to facilitate cyber security collaboration.



Showcase Huawei's end-to-end cyber security practices, from strategies and supply chain to R&D and products and solutions through presentations, videos, demos, etc.



Experience cyber security with Huawei's products and solutions, in areas including 5G, IoT, cloud, etc.



Collaboration & Innovation

Communicate with key stakeholders on cyber security practices, to explore and promote the development of security standards, verification mechanisms, and technological innovation in cyber security across the industry.



Collaborate with industry organizations (i.e. GSMA, C4C WEF) and standard organizations (3GPP, IETF, ITU-T), to promote and develop security standards and verification mechanisms.



Collaborate and innovate jointly with the EU cyber security verification organizations (ENISA, BEREC, etc.).



Collaborate with industry and EU regulators to establish verification partnerships and promote industry innovation.



We place trustworthiness above all else, over functions, features, or the product schedule.

— Ren Zhengfei



Article from our CPP Partner, Saviynt



A Real-World Guide to Modernizing Your IGA Platform

[Author: Dan Mountstephen, Senior Vice President, APAC, Saviynt]

IT modernization has grabbed the spotlight throughout the Covid-19 pandemic. Enterprises rushed to update infrastructures, secure data, and improve compliance over the past year. However, the fallout from remote work, ballooning cloud app estates, and new, varied identities now stretch legacy Identity Governance and Administration (IGA) solutions to the limit.

This technical debt keeps enterprises from adopting new digital business models for customer engagement and operational efficiency. So what's the key to kickstarting IGA initiatives? It's transitioning to a cloud-based identity platform.

No matter the size of your organization, this is no small undertaking. The benefits of the cloud (scalability, flexibility, rapid deployment, easier maintenance, upgrades, and solid support for cloud applications and infrastructure) are attractive. Still, companies struggling with legacy solutions may be overwhelmed with the prospect of migration.

Expert Advice for IGA Modernization

The following excerpts from Saviynt's recent eBook, *Making the Move to Modern IGA*, features expert guidance on preparing for, executing, and measuring an IGA modernization campaign's success. Topics covered in the ebook include:

- Building consensus
- Evaluating platforms
- Managing migration
- Measuring success

Importantly, we also feature real-world examples from practitioners on the other side of successful transitions – leaders just like you.

Read on for an abridged overview, or [explore the complete guide](#). It's packed with advice and anecdotes from leaders at Simeio, MassMutual, Campbell's Soup Co., Cerner, and Saviynt.

Build Executive Buy-In

Modernizing legacy IGA requires buy-in from a variety of stakeholders. Be clear about the benefits – not just how the approach will be different, but *more accessible*. Reach out to those in areas where modern IGA intersects – areas like cloud infrastructure and security, data privacy, and enterprise SaaS management.

Measure What Matters

Target improvements that matter to senior leaders early on. At a minimum, identify an executive champion who is a single point of contact for issue resolution and decision making.

Create a Data-Driven Roadmap

Businesses operate at the speed of the cloud, which requires flexibility and scalability across IGA processes. Every roadmap is different, so let business needs dictate your starting place. This demands a data-informed evaluation.

Consider Costs

Modern IGA solutions deliver agility in a variety of ways. Cloud-native solutions in particular support business changes – from managing cloud identities to securing SaaS applications. Companies must consider total cost-of-ownership (TCO) factors.

According to a recent [Forrester](#) study, benefits with cloud-based IGA platforms include many quantifiable and unquantifiable factors, including:

- A 90% time reduction in employee and contractor onboarding
- Coding talent cost avoidance
- Flexibility to support the work-from-anywhere IT model

Leverage Systems Integrators and Partners

Partnering with a systems integrator (SI) offers meaningful returns regarding reduced drain on internal resources, stakeholder morale, and overall deployment speed/time-to-value. Lean on leading SIs' orchestrator tools to help automate platform configurations.

Assess Migration Success

Plan toward a few key metrics that typify real improvement so that your migration, implementation, and deployment efforts lead to your target outcomes. Ask questions that help quantify your progress like:

- How quickly were you able to onboard?
- How many new services or capabilities were you able to introduce?
- Did audit findings decline and compliance posture improve? By how much?

The digital norm is a reckoning for laggard enterprises. Embracing strong IGA processes and technologies – and grappling with compliance, security, and trust are must-dos to stay competitive.

Our world leaped into the work-from-anywhere age overnight, and it's time for IGA platforms to follow. To learn more about modernizing your IGA, read the complete guide [*Making the Move to Modern IGA*](#).

For any enquiries, please contact Christoph Spitz, Identity Governance Associate at chris.spitz@saviynt.com

Article from our CPP, Recorded Future



Please scan the QR Code below for the full report.



For any enquiries, please contact Ms Karen Lee at karen.lee@recordedfuture.com

Article from our LIC Symposium Sponsor, Cybersecurity Association of Singapore

Let's Grow Singapore's Cybersecurity Talent Pipeline Together!

The global shortage of cybersecurity talent has long been acknowledged as a perennial challenge within the field. Even as we see statistics of a growing cybersecurity talent pool – with Singapore's own pool of cybersecurity professionals growing from 6,000 in 2018 to 10,700 in 2020⁵ – the breadth and depth of cybersecurity roles and responsibilities have also grown. Cyber threats continue to evolve and grow in sophistication. In particular, ransomware has evolved into a massive and systemic threat which can pose concerns to national security and disrupt critical services. Online scams remain a concern, for example, cybercrime grew to account from 18.6% in 2018 to 43% in 2020⁶ of overall crime in Singapore, with 16,117 cases reported. With the introduction and mainstream adoption of new and emerging technologies such as Internet-of-Thing (IoT) devices, cloud and 5G networks, this has also exposed us to new attack surfaces and vectors.

Cybersecurity is no longer an abstract concept or merely a technical issue. It has become essential, and even existential, to Singapore's continued prosperity. As such, beyond ensuring an adequate and well-trained cybersecurity workforce, growing a robust cyber talent pipeline to meet Singapore's cybersecurity and digital economic needs was included as one of the foundational enablers in the recently updated Singapore Cybersecurity Strategy 2021.



Figure 1: Strategic Pillars and Foundational Enablers in the updated Singapore Cybersecurity Strategy 2021

SG Cyber Talent – a national initiative to nurture talented cybersecurity enthusiasts from a young age, and to help cybersecurity professionals deepen their skills – aims to support this foundational enabler. Under SG Cyber Talent, CSA works with industry partners, academia and

⁵ As reported in the Singapore's Cybersecurity Strategy 2021

⁶ Singapore Cyber Landscape 2019 and 2021/22

the community to develop a range of programmes targeting diverse groups, as we progress towards the next bound of the strategy where we will move upstream to engage talent, whilst strengthening the cybersecurity workforce, through three strategic thrusts.

Strategic Thrust 1: Positioning Cybersecurity as an Attractive Profession



Figure 2: Past SG Cyber Talent initiatives

To nurture young Singaporeans' interests in cybersecurity, CSA has launched SG Cyber Youth – a national programme aimed at guiding youths in their cybersecurity journey, with support from academia, community, industry, and other government agencies. Since 2018, we have reached out to more than 10,000 youths through training bootcamps, Capture-the-Flag competitions, student volunteer activities and career mentoring sessions. The initiatives under SG Cyber Youth are guided by the newly launched SG Cyber Youth Odyssey – a learning roadmap which provides clear milestones to guide students in their cybersecurity journey. One key initiative is the Youth Cyber Exploration Programme (YCEP) targeted to teach pre-tertiary students the fundamentals of cybersecurity and excite them about prospects in the cybersecurity industry.

Beyond that, CSA also co-organises and co-develops initiatives with the community, such as the Student Volunteer & Recognition Programme (SVRP) with AiSP and the Cybersecurity Career Mentoring Programme (CCMP) with the Singapore Computer Society (SCS). Through the various programmes, we aim to grow a pool of local youths to take up cybersecurity as a future career. We also want to identify exceptional cybersecurity talent from young, who can then be groomed under our newly launched SG Cyber Olympians programme. This programme aims to nurture these talented youths through cyber sparring sessions, deeper training and international competitions.

We also aim to grow a more diverse cybersecurity workforce, by attracting under-represented demographics – such as women, neuro-diverse individuals and mid-career professionals – to join the profession. For example, we work closely with industry and international partners to encourage girls to take up cybersecurity education. We will also continue to roll out professional conversion programmes and scholarships to attract talents into the field.

Strategic Thrust 2: Developing and sustaining a world-class workforce



Figure 3: CSA’s upcoming Cybersecurity Strategic and Leadership Programme and the Operational Technology Cybersecurity Competency Framework

A highly skilled workforce is key to driving a dynamic sector such as cybersecurity. The Government will thus continue to support the professional development and upskilling of existing cybersecurity talent – by facilitating the development of deep skills and enhancing career pathways.

One of the key initiatives is the SG Cyber Leaders’ Strategic Leadership Programme, which aims to nurture and develop our management talents by strengthening the knowledge, leadership and networks of current and upcoming cybersecurity leaders. If you are an aspiring or current cybersecurity leader within your organisation, we look forward to having you join this programme and receive strategic leadership training, and join the study trips and communities of practice to become a more effective cyber leader.

To better guide existing professionals in their career pathways and skills training, there are also existing frameworks the Government has developed, e.g. the Skills Framework for ICT and Operational Technology Competency Framework (OTCCF). Beyond that, CSA and IMDA are also leading efforts to leverage the in-house cybersecurity training programmes of larger companies to train participants from the wider industry through the Cyber Security Associates and Technologists (CSAT) programme.

Strategic Thrust 3: Creating Vibrant Communities in Cybersecurity



Figure 4: The Cybersecurity Awards 2021

The Government also works closely with industry associations, such as AiSP, to introduce and build strong communities of practice and foster trust within the profession. We will continue to

support ground-up community events, workshops, conferences and programmes that help strengthen the talent pipeline and develop our professionals. The Cybersecurity Awards, is a good example of an inter-association collaboration which aims to recognise the contributions of individuals and organisations to the cybersecurity ecosystem.

Existing cybersecurity professionals, such as yourselves, play a key role in attracting and shaping our future cybersecurity practitioners. You know the field best – understanding the realities and ground experience of cybersecurity operations, the struggles, and gaps within the profession and, most importantly, the skills and expertise required to thrive and grow in the field. It is, through your insights, that we are better able to develop relevant initiatives that support your career growth and advancement within the field.

Keen to play a role in strengthening our talent pipeline? You can start by participating in some of the existing SG Cyber Talent initiatives! Mentor and share your expertise with new entrants to the field, or deepen and enhance your management skills through our Strategic Leadership Programme. If you have ideas on community projects or skills development and recognition initiatives, you may also apply for our SG Cyber Talent Development Fund, which aims to support ground-up initiatives by individuals and communities.

Cybersecurity is a team sport, and everyone has a part to play. Join in our efforts to grow a robust cyber talent pipeline that allows us to unleash our full digital potential! Scan the QR code to our SG Cyber Talent website below and find out more about how you can contribute!



For further enquiries, please contact CSA at CSA_SGCyberTalent@csa.gov.sg

Article from The Cybersecurity Awards 2021 Winner – Mr Eugene Lim



Mr Eugene Lim
TCA 2021 Winner of Professional Category

I am honoured to be the recipient of The Cybersecurity Awards 2021 (Professional Category). As a relative newcomer to infosec, I hope to highlight two things:

First, I learned the ropes from the white hat hacking community which continues to contribute to the cybersecurity posture of companies and organisations via responsible disclosure. Thanks to the abundance of free learning resources and opportunities shared by the community, beginners have been able to get a foot in the door in the industry regardless of their background. I hope that this spirit of sharing continues to grow. I also hope that companies and organisations support the responsible disclosure process by working with white hat hackers and researchers. I have had the good fortune of experiencing both sides of this process – as a bug bounty hunter and a contributor to GovTech’s vulnerability disclosure efforts. To this end, I am grateful to my colleagues and managers such as Rong Hwa, Terence, Heng Shi, Hui Yi and Max for supporting my work. In 2021, we coordinated responsible disclosure with numerous third-party organisations for critical products, such as code execution bugs in Microsoft Office and several internet-connected devices.

Secondly, I benefited greatly from the local infosec community. I am particularly grateful to my nominator Emil Tan, a previous recipient of The Cybersecurity Awards and founder of Division Zero (Div0). Through events such as the HackSmith cybersecurity hackathon and the Government Bug Bounty Programme, I gained my first exposure to infosec which eventually led to my current career. Additionally, after presenting at Black Hat Asia Arsenal, Emil encouraged me to apply for Black Hat USA. At that time, presenting at Black Hat USA appeared to be a far-off dream for me, but his words made it seem concrete and achievable. I was proud to present at DEF CON and Black Hat USA with my GovTech colleagues on AI-powered phishing research last year. Emil’s impact on me has highlighted the importance of good mentors and I hope to live up to his example in the future.

At the end of the day, our community can only continue to grow by welcoming and nurturing new members. I look forward to contributing to these efforts and building up infosec in Singapore.

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

PROFESSIONAL DEVELOPMENT

Listing of Courses by Wissen International

New course by
EC-Council
www.eccouncil.org

A First of its kind
**Vendor Neutral and
Vendor Specific Certification**

The **Next Dimension**
in Cloud Computing

CCSE
Certified Cloud Security Engineer

Become a **Certified Cloud
Security Engineer (CCSE)**

The CCSE Program Advantage

- 50+ Hands-on Intensive Labs
- Mapped to 20 Cloud Job Roles
- Mapped with Real-Time Industry Job Roles

AWS AWS Cloud **Azure** Azure Cloud **Google Cloud** Google Cloud Platform

REGISTER NOW

Brought to you by Wissen – EC-Council Exclusive Distributor APAC

WISSEN
Cyber Security Competency Development

Email us for more info
aisp@wissen-intl.com

Introducing new course by EC-Council
Certified Cloud Security Engineer (CCSE)

Organizations need cloud security engineers to help them build a secure cloud infrastructure, monitor vulnerabilities, and implement incidence response plans to mitigate cloud-based threats. CCSE, with its unique blend of vendor-neutral and vendor-specific concepts, trains candidates in the fundamentals while equipping them with job-ready practical skills.

Email us to find out more aisp@wissen-intl.com

[back to top](#)

Listing of Courses by ALC Council



“The global standard for Cyber Security Architecture”

SABSA Foundation 23-27 May 2022
Live Virtual training 9:00 am – 5:00 pm SGT
Special **10% discount for AiSP members**

Getting your architecture right is the critical success factor for robust and effective cyber security in business and government.

SABSA represents the world standard for cyber security architecture. When you get your SABSA accreditation you become a member of an exclusive group positioned strategically between two domains – that of top management and that of the technical subject matter expert.

SABSA mandates the most highly-qualified instructors

Fully-accredited SABSA training is conducted only by instructors who hold the SABSA Master certification - the most demanding certification in the industry. Accredited SABSA trainers have to pass three exams – SABSA Foundation and two Advanced courses - with a minimum mark of 75%. They then have to attain the SABSA Master certification by preparing a university-style thesis demonstrating experience and understanding, subject to review by two assessors.

[SABSA Certification >>](#)

[back to top](#)

ALC is the only accredited SABSA provider in Singapore

ALC Training Pte Ltd is the only accredited provider of SABSA cyber security architecture training in Singapore.

Start your SABSA journey with the globally recognised **SABSA Foundation Certificate**. Next course to be held in the Singapore time zone on 23-27 May 2022.

[Full course details and registration >>](#)

ALC Training Pte Ltd is proud to be an AiSP Partner.

Take a look at our full [Singapore training program](#).

You can claim your AiSP 10% member discount against any course. All you have to do is copy-paste **ALCAiSP10** on the Promotion Code field on the registration form.

Any questions, don't hesitate to contact us at customerservice@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

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

2022 Course dates can be found on https://www.aisp.sg/qisp_training.html

Time: 9am-6pm

Fees: \$2,500 (before GST)*

*10% off for AiSP Members @ \$2,250 (before GST)

*Utap funding is available for NTUC Member

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





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*

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 \(Path 1\)](#) to apply for AVIP.

Your AiSP Membership Account

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

The platform allows our members to sign up for events and voluntary activities and check membership validity.

Membership Renewal

Members will receive an auto-generated email from Glue Up and it will send the reminder 1 month before the expiry date of your membership. Members can renew and pay directly with Glue Up or one of the options listed [here](#). We will be adding GIRO (auto-deduction) this year. 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





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.

[back to top](#)

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

 116 Changi Road, #04-03 WIS@Changi, S419718

Please [email](mailto:secretariat@aisp.sg) us for any enquiries.