

News & Update

- SG Cybersafe Programme
- GOVWARE Week
- Knowledge Series
- CAAP
- AiSP SME Cyber Conference
- SVRP
- SCSIA
- Ladies in Cyber
- Special Interest Groups
- CREST Singapore
- Regionalisation
- The Cybersecurity Awards
- Upcoming Events

Contributed Contents

- What cybersecurity practitioners need to take note of GDPR
- Cybersecurity in the Protection of Personal Data
- Enabling Self-Healing SD-WAN from the WAN Edge to the Cloud Edge
- The First Steps in Securing Hybrid Work
- **Owning your own Access Security**
- **CloudSec**
- FireEye Advances XDR Platform to Arm Security Operations Teams

Professional Development

Membership

NEWS & UPDATE

New Corporate Partners

AiSP would like to welcome **Kaspersky and ThriveDX** (formerly Cybint), as our new Corporate Partners. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem in 2021.



Continued Collaboration

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

APP: Singapore Institute of Technology (SIT) and Singapore Management University (SMU)

CPP: ITSEC Services Asia Pte Ltd and ST Engineering Info-Security Pte Ltd

We look forward to the exciting collaborations with these partners.



SG Cybersafe Programme

AiSP is excited to work with CSA to be one of the partners for the new SG Cyber Safe Programme that was launched on 7 October at the SICW.

AiSP President, Mr Johnny Kho received the Token of Appreciation from Minister of State Tan Kiat How for AiSP support towards CSA's initiatives.

Visit <https://www.csa.gov.sg/Programmes/sgcybersafe/about> to find out more on the SG Cyber Safe Programme.



GOVWARE Week

Day 1

Day 1 of GOVWARE had speakers sharing on Cyber Resiliency and our AiSP President, Mr Johnny Kho as the moderator for the Q&A sessions.

Our CPP Partner, Privasec was represented by Ms Shamane Tan as she highlighted key cyber risks success criteria for board and executives. It was an enriching Day 1 for all participants!



Day 2

An insightful day has been for Day 2 with GovWare SG speakers and Chair of AiSP CAAP, Mr Tony Low was the facilitator for the Q&A sessions.





Mr Chng Tien San, from Mastercard (our CPP Partner), gave an energetic sharing on the recommended actions for organizations to assess their cybersecurity posture and secure the broader digital ecosystem.



Knowledge Series Events

Internet of Things on 27 October


In this Knowledge Series - IoT, we are joined with Mr Jonathan Chin (AiSP Corporate Partner - Fortinet) and Mr Andrew Ong (AiSP-CSCIS IoT SIG). We discussed about securing OT Environment amidst Digital Transformation, as well as the Rise in IoT and Cybersecurity Threats. We would like to give a big thank you to everyone who attended today's webinar and we hope everyone has gained more knowledge with regards to Internet of Things.

 <p>Andrew Ong</p> <div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <p>Background</p> <p>Andrew Ong is currently the Regional Sales Manager for ExtraHop Network Inc. He is managing the rapid adoption of Network, Detect and Response (NDR) technology in customers' mission critical environment.</p> <p>Andrew has more than 16 years of experience in Cybersecurity, ranging from Firewalls, NG-IPS, APT, EDR, CTI to NDR.</p> <p>He has been in various roles in the cybersecurity industry from leading a team of 20 - delivering US\$596M, to VP of Sales (APAC) of a Israel Threat Intelligence vendor.</p> </div> <div style="width: 45%;"> <p>Selected Experience</p> <ul style="list-style-type: none"> Chairperson, Cyber Threat Intelligence (CTI) SIG CSCIS AiSP <p>VP of Sales (APAC) – Cyber Threat Intelligence</p> <ul style="list-style-type: none"> Lead the growth and adoption of CTI in APAC 1st Homeland security project adoption outside of Israel 1st Defence project adoption outside of Israel 1st Banking regulator adoption outside of Israel </div> </div> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div style="width: 45%;"> <p>Industry Experience</p> <ul style="list-style-type: none"> Govt & Telco Banking & Financial Services Manufacturing IRL & Healthcare </div> <div style="width: 45%;"> <p>Functional Experience</p> <ul style="list-style-type: none"> Network Security APT & EDR Cloud Security Cyber Threat Intelligence </div> </div> <p style="font-size: small; text-align: center;">CSCIS CENTRE FOR STRATEGIC CYBERSPACE & INTERNATIONAL STUDIES © 2021 Copyright © All Rights Reserved 2021</p>	
<p>Agenda</p> <ul style="list-style-type: none"> Introduction Evolution of Industrial Networks <ul style="list-style-type: none"> Old World, New World, Future World Security Challenges The Answer: Fortinet Security Fabric Cybersecurity Maturity Model Customer Case Studies Summary <p style="font-size: x-small; text-align: right;">© Fortinet, All Rights Reserved</p>	
<p>AiSP Knowledge Sharing Series (IS-BOK) Knowledge sharing Networking Events Webinars</p> <p>Based off Information Security Body of Knowledge (IS-BOK) 2.0 content topics</p> <p>AiSP completed the update of its Information Security Body of Knowledge (IS-BOK) on 8 Nov 2019.</p> <p>To enable our members with a better understanding of how IS-BOK can be implemented at workplaces, AiSP has been organising a series of knowledge-sharing & networking events since 2020, based on the following topics:</p> <div style="display: grid; grid-template-columns: repeat(4, 1fr); gap: 10px;"> <div style="text-align: center;"> Governance & Management</div> <div style="text-align: center;"> Physical Security: Business Continuity & ADR</div> <div style="text-align: center;"> Security Architecture & Engineering</div> <div style="text-align: center;"> Operations and Infrastructure Security</div> <div style="text-align: center;"> Software Security</div> <div style="text-align: center;"> Cyber Defence</div> <div style="text-align: center;"> Cyber Threat Intelligence</div> <div style="text-align: center;"> OT/IT</div> <div style="text-align: center;"> Emerging Trends</div> </div> <p style="font-size: x-small; text-align: center;">© 2020 - 2021 Association of Information Security Professionals. All Rights Reserved. Royalty-free image for Microsoft Office subscribers.</p>	



Emerging Trends – Blockchain & AI for Cyber Security on 17 Nov


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
Advance Connect Excel

AiSP Knowledge Series – Emerging Trends – Blockchain & AI for cybersecurity


**AiSP Knowledge Series -
Emerging Trends - Blockchain &
AI for cybersecurity**




Anthony Lee
Vice President
Senior Cyber Advisory
Manager
Marsh




Jeremie Deschamps
Vice President
Senior Cyber Advisory
Manager
Marsh





Dr Xue Tengfei
Blockchain Service
Architect
HUAWEI CLOUD




Organised by:



Supported by:

Via:



17 November | 3-5PM | WebEx

Blockchain technology and digital assets create an increasingly complex environment. Cryptocurrencies use cryptography to secure and verify transactions in a network. They are often perceived as safe, but are still vulnerable to cyber-attacks, fraud, and social engineering scams. In this knowledge series, we discuss the cyber risks of cryptocurrency, as well as Industrial blockchain practices.

Cryptocurrency cyber risks: Are you prepared?

By: Anthony Lee, Vice President, Senior Cyber Advisory Manager, Marsh & Jeremie Deschamps, Vice President, Senior Cyber Advisory Manager, Marsh

Novel technology, a dynamic and borderless market, and an uncertain regulatory environment create an increasingly complex environment for companies operating with Block chain technology and digital assets. Digital assets might include cryptocurrencies and digital currencies. Digital currencies, though, refer to the electronic form of fiat money issued by governments, whereas cryptocurrencies use cryptography to secure and verify transactions in a network.

Cryptocurrencies' rapid growth is bringing increased scrutiny from policymakers, investors, critics, and traditional industry, and has led many to lose millions of dollars. Similarly, to other technologies, cryptocurrencies are based on a human-developed technology that is exposed to specific cyber risks. While often perceived as "un-hackable", it certainly remains vulnerable to specific cyber-attacks. Those cyber-attacks might include exploiting vulnerabilities in the code itself developed by random coders, or social engineering scams where cryptocurrency holders get manipulated into disclosing the key that protects their assets.

Join me in this webinar, where I discuss the different good practices to store cryptocurrencies and share safeguards and standards related to their protection and integrity.

Industrial blockchain practice for security and data privacy protection and computing

By: Dr Xue Tengfei, Blockchain Service Architect, HUAWEI CLOUD

HUAWEI CLOUD is a leading cloud service provider, which brings Huawei's 30-plus years of expertise together in ICT infrastructure products and solutions. Huawei launched Blockchain Service (BCS), which is a highly available and secure blockchain platform allowing enterprises and developers to conveniently create, deploy, and manage applications with the superb performance and cost-effectiveness of HUAWEI CLOUD. This presentation will introduce the overall architecture of HUAWEI CLOUD BCS and some security features built on it to ensure data security and privacy protection for users. Including decentralized identity service, trusted data exchange, and trusted computing.

Date: 17 November 2021 (Wed)

Time: 3PM to 5PM

Venue: WebEx

Registration:

<https://aisp.webex.com/aisp/j.php?RGID=r6eab4d8b0647b53d3666167d4ea6607f>

Cyber Threat Intelligence on 1 Dec



AiSP Knowledge Series – Cyber Threat Intelligence

AiSP Knowledge Series - Cyber Threat Intelligence



RAY KOH
Sales Director - APJ
Cyberint



DR. GUY ALMOG
Cyber Threat Intelligence
Team Leader
Cyberint



Based off 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. In today's session, we will be discussing the issues with Target Intelligence.

A peek into the Dark Side with Target Intelligence: What the threat actors know about you?

By: Ray Koh, Sales Director – APJ, Cyberint & Dr. Guy Almog, Cyber Threat Intelligence Team Leader, Cyberint

The COVID-19 global pandemic has created a new normal - the hybrid work model - a combination of office-based and remote work which businesses today are adapting and figuring out how to secure the expanding attack surface.

Just like businesses, threat actors have also adapted to the new normal, with a rise in attacks targeting the personal devices and home networks of remote workers. According to a Gartner article in July 2021, the human element (85%) continued to be a primary catalyst for data breaches over the last 12 months, with phishing accounting for 36% of breaches.

In this session, CYBERINT will highlight the importance of security best practices by

the organization's workforce, share real-world credential/data compromise use cases, provide a live peek into the deep and dark web, show you the information that the threat actors can get about you / your organization, and how the threat actor can use this information against you/your organization. Also, CYBERINT will share with you how Target Intelligence is an emerging security function that security teams rely on to address and/or remediate such cyber threats proactively.

Date: 1st December 2021 (Wed)

Time: 7pm – 9pm

Venue: Hybrid

Physical Registration:

<https://www.eventbrite.sg/e/aisp-knowledge-series-cyber-threat-intelligence-tickets-175231551287>

Virtual Registration:

<https://aisp.webex.com/aisp/j.php?RGID=r0a50cb6916b3d5be14d84620516449c2>

About our Knowledge Series

As part of knowledge sharing, AiSP is organising regular knowledge series webinars based on its [Information Security Body of Knowledge 2.0](#) topics. Our scheduled topics for webinars in 2021 are as follows (*may be subjected to changes*),

1. Emerging Trends – Blockchain & AI for Cyber Security, 17 Nov
2. CTI, 1 Dec, Hybrid*
3. Data Security, 27 Jan
4. Red Team VS Blue Team, 17 Feb
5. Cryptography, 17 Mar

*Subjected to Singapore Government's directives for physical events during COVID-19 pandemic.

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

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

Cybersecurity Awareness & Advisory Programme (CAAP)

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.

Cybersecurity Awareness and Cybersecurity Courses on 10 Nov

	
AiSP CAAP Focus Group Discussion – Cybersecurity Awareness and Cybersecurity Courses	
<div style="display: flex; justify-content: space-between; align-items: center;"> <div style="text-align: center;">  <h1 style="margin: 0;">Cybersecurity Awareness & Cybersecurity Courses</h1> </div> <div style="text-align: center;">  </div> </div> <div style="display: flex; justify-content: space-between; align-items: center; margin-top: 20px;"> <div style="text-align: center;">  <div style="background-color: #c00000; color: white; padding: 5px; font-size: 0.8em;"> Catherine Lee CAAP Facilitator AiSP </div> </div> <div style="text-align: center;"> <p> 10 November 2021 </p> <p> 10.30AM – 12.30PM </p> <p> MS Teams </p> </div> </div> <div style="text-align: center; margin-top: 20px;"> <p>Organised by:</p>  <p style="font-size: 0.7em;">Association of Information Security Professionals</p> </div>	
<p>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.</p> <p>With you taking the first step into the Cybersecurity Industry, this focus group discussion aims at raising awareness of cyber risks and adoption of cyber practices. It caters to professionals across industries, particularly those not in the IT fields to better protect your businesses in the cyber space.</p>	

Find out more about some of the cybersecurity courses that are available and how AiSP members can benefit from the courses to advance in the Cybersecurity Industry.

Join us in this focus group discussion as we discuss together about the immediate concerns arising from rising cyber threats, concerns about cybersecurity incidents in companies and cybersecurity courses.

Date: 10 November 2021 (Wed)

Time: 10.30AM to 12.30PM

Venue: MS Teams

Registration: <https://forms.office.com/r/cf0FQ2g6iA>

Singapore SMEs' Digital Adoption and Concerns on 24 Nov



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

Singapore SMEs' Digital Adoption and Concerns



Faith Chng
CAAP Facilitator,
EXCO Member
AiSP

| 24 Nov 2021 |
| 10AM – 11.30AM |
| MS Teams |



Organised by:
AiSP 
Association of Information Security Professionals People's Association

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

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

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

Date: 24 November 2021 (Wednesday)

Time: 10.00am to 11.30am

Venue: MS Teams

Registration: <https://forms.office.com/r/AbuE6bS1Yb>

AiSP x Mastercard: Cybersecurity for SMEs on 24 Nov



AiSP x Mastercard: Cybersecurity for SMEs

AiSP x Mastercard: Cybersecurity for SMEs



3-4.30PM | WEBEX



Organised by :



Supported by :



Via:





Michael Lew
CEO
Rajah & Tann Technologies



Veronica Tan
Director
Safer Cyberspace
Cyber Security Agency of Singapore



Tony Low
CAAP Lead
AiSP



Urooj Burney
Global Products Leader
Cyber & Data
Mastercard

AiSP is collaborating with Mastercard® to organise a cybersecurity awareness session for leaders in the SME space to understand new cyber risks as well as help SMEs manage their cybersecurity.

Joining us for our panel discussion will be Mr. Michael Lew, a veteran in the cybersecurity space. Michael is the CEO at Rajah & Tann Technologies, a leading Legaltech advisory service provider in the region. He has over 20 years of consulting experience in e-discovery, cyber forensics, data analytics, financial crime and more recently, blockchain and cryptocurrencies investigations.

The 1.5hour session will start with experts from CSA, AiSP and Mastercard sharing their knowledge and useful tips on cybersecurity for SMEs.

Practical guidance for small businesses to strengthen their cybersecurity

By: Veronica Tan, Director, Safer Cyberspace, Cyber Security Agency of Singapore

As organisations continue to digitalise rapidly amidst a global shift to operate online, we have correspondingly observed organisations – small businesses in particular – facing increased exposure to cyber risks. The Cyber Security Agency of Singapore (CSA) will share practical guidance on how small businesses can strengthen their cybersecurity to safeguard their businesses.

Understanding Your Responsibility on Data & Privacy

By: Tony Low, CAAP Lead, AiSP

Roles and responsibilities for data protection are specified as part of the data governance framework. Join us as we share about the people process for Data & Privacy and what are the responsibilities for Data Protection Officer.

Demystifying Cybersecurity for Small Businesses

By: Urooj Burney, Global Products Leader, Cyber & Data, Mastercard

The use of digital technology – further accelerated by COVID-19 – is fast becoming a business imperative to streamline operations, achieve efficiencies, dissolve borders and reach consumers. However, the risk of cyber threat rises in tandem with connectivity. Each connection, both internal and with third-parties, are a potential point of vulnerability, and an opportunity for fraudsters to exploit.

The 2020 Allianz Risk Barometer Survey results show that for the first time, cybersecurity is the leading risk for businesses in AP. Supply chain risk management is essential as Small-Medium Enterprises (SME) face potential vulnerabilities through third-party relationships, including multi-party cyber incidents that affect numerous organizations with both direct and indirect connections to the initial victim. We will share how we can help SMEs manage cyber vulnerabilities and fortify their supply chains.

We hope you will be able to join us for the exciting session.

Date: 24 November 2021 (Wed)

Time: 3PM to 4.30PM

Venue: WebEx

Registration:

<https://aisp.webex.com/aisp/j.php?RGID=raf2eab7e1d123177ae912987c757514d>

AiSP SME Cybersecurity Conference



Business owners of small and medium enterprises (SMEs) and Enterprise are only focused on business needs and are not aware of the digital risks and cybersecurity resources available for them. The purpose of the AiSP SME Conference is to help Enterprises, SMEs and individuals to be more cyber aware and the different solutions out in the market that can help them in it.

Organised by the Association of Information Security Professionals (AiSP), the AiSP SME Conference is a unique event that brings together organisations to discuss the importance of being cyber aware and stay protected. The event will provide our speakers with the opportunity to share their experience, skills and knowledge to show how cybersecurity can help companies to stay protected. AiSP aims to elevate cybersecurity awareness among companies and establish a self-sustaining ecosystem with active participation from government agencies, business associations, cybersecurity communities, and solutions provider.

As part of AiSP Cybersecurity Awareness and Advisory Programme (CAAP), this event is for Singapore Enterprise and SMEs to know more about cybersecurity as a business requirement and how they can implement solutions and measures for cyber-resilience. CAAP hopes to elevate cybersecurity awareness as integral part of business owner's fundamentals and establish a self-sustainable support ecosystem programme with active participation from agencies, business associations, security communities and solutions provider.

Under CAAP, AiSP aims to launch the Cybersecurity Awareness e-learning which is based on the Cybersecurity Awareness and Advisory Programme (CAAP) Body of Knowledge to enhance digital and cyber awareness levels targeted at SME's and Individuals. AiSP also

aims to launch the SME Cyber Safe portal to provide an online sitemap for Businesses & individuals in terms of Cyber Awareness Maturity Journey.

The conference will be held physically subjected to the COVID restrictions and government guidelines with the following details:

Date: 7 January 2022 (Friday)

Time: 10:00 am – 4:00 pm

Venue: Lifelong Learning Institute

Join us to hear what our speakers have to say and provide on the solutions to help in your business and tour the Solution Booths and Cybersecurity Courses to find out more on Cybersecurity.

Secure your seat here: <https://www.eventbrite.sg/e/168509655917>

Visit <https://www.aisp.sg/cyberfest/smeconf2021.html> for more details.

Organised by

Supported by



Sponsors



Supporting Partners



Student Volunteer Recognition Programme (SVRP)

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. The third SVRP Awards Ceremony will be held on 19 January 2022 at Lifelong Learning Institute Event Hall.

The Awards Ceremony is sponsored by:



Singapore Cyber Security Inter Association (SCSIA)

Singapore Cyber Day 2021



The second inaugural Singapore Cyber Day will be held on 8 November 2021. The Singapore Cyber Day aims to reach out to students in Singapore who are keen to find out

[back to top](#)

more about cyber security and how they can be part of our community.

The Singapore Cyber Security Inter Association (SCSIA) consists of professional and industry associations: AiSP, Centre for Strategic Cyberspace + International Studies (CSCIS), Cloud Security Alliance Singapore Charter, HTCIA Singapore Chapter, ISACA Singapore Chapter, (ISC)2 Singapore Chapter, SCS, SGTech and The Law Society of Singapore will be organising the second Singapore Cyber Day.

SCSIA aims to inspire future generation of youths on opportunities in Cybersecurity. They are reaching out to primary and secondary schools and pre-universities to talk about the cybersecurity profession and how everyone can take part in Singapore's cybersecurity ecosystem and contribute towards our cyber resilience.

SCSIA volunteers are involved in a series of school talks for primary and secondary school students. There are two parts to the virtual talks:

Part 1: Virtual Event with the launch of cyber hygiene and career advice videos from the professional bodies and associations.

Part 2: Singapore Cyber Day Quiz for the students to take part in during the December school holidays. The online quiz competition is opened to primary, secondary and tertiary students (aged 25 years and below) in Singapore with the support from Fortinet. This competition aims to pique interest in students and equip them with knowledge on Cyber Security.

Video Link available on 8 Nov: <https://www.youtube.com/watch?v=R9k67bOod54>

Organised by



Supporting Agency



Supported by



Supporting Associations



Ladies in Cybersecurity



Ladies Talk Cyber Series

For the Seventh edition of AiSP's 'Ladies Talk Cyber' series, we interviewed Sugar Chan, Cybersecurity Project Leader in Boston Consulting Group (BCG) where she works closely with her clients to solve complex topics. She shared on her experiences with BCG and how we can encourage more women to enter the field.

How to be successful in cybersecurity field

In celebration of [SG Women year](#), AiSP's secretariat decided it was timely to launch a series of interviews of female leaders across industries who fulfil high impact roles, and learn about their journeys, experiences and insights. The initiative aims to shed some light on what it takes to make it in this field. The interviews can be source of invaluable career insights as well as opportunities for those in the field to get a deeper understanding of the industry, and how its leaders are innovating to disrupt the cyber landscape.

Introducing women with a deep interest in cybersecurity

Sugar is a Cybersecurity Project Leader in Boston Consulting Group (BCG) where she works closely with her clients to solve complex topics. She has over 8 years of working experience in the consulting industry and has received multiple awards from local and global Industrial Control Systems (ICS) and Internet-of-Things (IoT) Capture-the-Flag competitions, to include back-to-back 1st runner-up placements at DEFCON in 2018 and 2019.

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

International Cyber Women Day 2021



As part of International Cyber Women Day 2021, AiSP will be featuring some of our Female Leaders on AiSP LinkedIn Page. Visit <https://www.linkedin.com/company/aisp-sg/> to hear our female leaders experience Cybersecurity.

AiSP will also be organising a few ladies in cyber events in September to commemorate International Cyber Women Day 2021. We looked forward to having you in our AiSP Ladies in Cyber events. To find out how you can sponsor, volunteer, or play a part in our programmes, please contact us at secretariat@aisp.sg today.



(Photo taken in 2019 during the AiSP Ladies Night)

AiSP Ladies in Cyber Learning Journey & Fireside Chat In January 2022 at CISCO Office (Hybrid Format)

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

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

This September, **AiSP Ladies in Cyber** is organizing a hybrid fireside chat together with our Corporate Partner Cisco Systems. Join **SMS Sim Ann, Wendy, Catherine and Sherin** - our female leaders from Cybersecurity industry as they share their experience, advice and provide guidance on career in IT industry for females. Please email to secretariat@aisp.sg to find out more details on the event.

Date: 21 January 2022 (Date to be confirm again)

Time: 7.30pm to 8.45pm (Please join in 5 mins before the session)

JOINTLY ORGANISED BY: **AiSP** | **LADIES IN CYBER**

SUPPORTED BY: **CISCO**

AS PART OF **CSA SINGAPORE**
SG CYBER WOMEN X SERIES

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

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

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

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

Sign up at <https://tinyurl.com/lic24092021>

AiSP Ladies in Cyber Inaugural Symposium on March 2022

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. The theme for this year Symposium is **“How can Women in Tech define the future of Cyber & Tech”**.

AiSP's Vice-President and Founder for AiSP Ladies in Cyber Initiative, Ms Sherin Y Lee shared, “What we're trying to do here is not to highlight women because they are women. Rather, we're trying to amplify the message that women can and have been doing great work in cybersecurity – and by providing tangible examples. From any roles such as building companies, products & services, to technology security design and operations, all the way to incident response and recovery for organisations. The other message we're trying to get out there is that cybersecurity is more than programming. There are diverse roles available – come join us to learn more about what you can do by interfacing with industry professionals from diverse roles in this sector.”

The event will be held on 18 March 2022 at Life-Long Learning Institute with Minister Josephine Teo as the Guest of Honour as part of International Women Day 2022. She will be having a dialogue session with the attendees during the event.

Visit https://www.aisp.sg/cyberfest/ladies_symposium.html for more details on the event. Contact AiSP Secretariat at secretariat@aisp.sg for more information of the event and if you sponsor and be part of it.

Supported by




Sponsors



[back to top](#)


Special Interest Groups




SIG Day

SIG Day


9 Nov 2021 | 7PM - 9PM | WebEx





Thomas Pan
EXCO Member of
IoT SIG, CSCIS



Niel Pandya
Cybersecurity
Lead, APJ
Micro Focus





Organised by  Via 


Supported by











The Association of Information Security Professionals (AiSP) has set up Special Interest Group (SIG) to:

1. Engage AiSP Members to advance their knowledge in this area;
2. Connect with fellow volunteers through discussion, events and activities; and
3. Excel together while contributing volunteers' expertise and application to the evolving Information Security Body of Knowledge (IS BOK) and Cybersecurity Awareness and Advisory Programme (CAAP) Body of Knowledge (BOK).

To mark the start of our SIG, we will be organising the inaugural AiSP Special Interest Group Day on 9 November 2021 during our CyberFest®. Join us as we share about our 4 SIGs, Cloud Security, Cyber Threat Intelligence, Data & Privacy and Internet of Things and find out more on the different aspects on Cybersecurity.

Introduction of Special Interest Group

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

Cyber Threat Intelligence SIG

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

Data & Privacy SIG

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

Internet of Things SIG

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

Why IoT and Security Matters?

By Thomas Pan, EXCO Member of IoT SIG, CSCIS

With IOT becoming more important in our daily lives, Enterprises and The Federal have also incorporated IOT elements into their business operations. IOT is heavily anticipated as the Next Industrial Revolution. Therefore, enterprise security methodology has to change and evolve in tandem. For this particular presentation, we aim to provide a platform for IOT security knowledge sharing and share the best practices for the industry.

Protecting Against Ransomware – An Enterprise Resiliency Guide

By Niel Pandya, Cybersecurity Lead, APJ, Micro Focus

Everyday, news breaks out of yet another ransomware attack, impacting enterprises across the globe. The ransomware attack on the Colonial Pipeline, an American oil pipeline system that originates in Houston, Texas, and carries gasoline and jet fuel mainly to the Southeastern United States, suffered a ransomware cyberattack that impacted computerized equipment managing the pipeline – is there a need to revisit our strategy to be more resilient against ransomware?

This is just the latest to make the news, and the trends are daunting:

- Ransomware attacks increased 41% in 2019 with 205,000 businesses who lost access to their files.
- 21% of ransomware involved social actions, such as phishing.
- 68,000 new ransomware Trojans for mobile were detected in 2019.
- Once ransomware is deployed, IBM X-Force estimates 70% of victims are paying ransoms.

In this session, we will look at a detailed approach from Board Members, CISO to Cyber and IT operations that will help enterprise be more resilient to ransomware threats.

Date: 9 November 2021 (Tuesday)

Time: 7PM to 9PM

Venue: WebEx

Registration: <https://aisp.webex.com/aisp/j.php?RGID=r5aee9edc0ffdfcc0e41df54722803c80>

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
- Cyber Threat Intelligence
- Data and Privacy
- 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. Please contact us if you are keen to be part of our SIGs as we are actively recruiting members!



Special Interest Group (SIG) Events

Date	Event
9 November 2021	Combined SIG Event

CREST Singapore

The CREST Singapore Chapter was formed by CREST International in partnership with CSA and AiSP to introduce CREST penetration testing certifications and accreditations to Singapore in 2016. Our CREST practical exam had resume on 26 August 2021. Please click [here](#) for the exam schedule for 2021.



CREST Webinar

23 November | 3PM - 4.30PM | Webex



CREST Webinar



Arthur Bagiryan
Security Consultant
Member of AiSP



Sergey Belov
Application Security Lead
Acronis

Organised By:



Supported By:



Via:



AiSP has been organising a series of CREST webinar for 2021.

You have secured your AD. How about your Azure AD ?
By Arthur Bagiryan, Security Consultant, Member of AiSP

Businesses and IT leaders are replacing on-premise technology with flexible, scalable, and cost-effective computing power in the cloud. However, making this transition or integration is not without its risks as it could create additional attack surface that your systems are exposed to. Microsoft's Azure platform is one of the heavy hitters operating in the Cloud market. This growth is largely powered by the Active Directory component at the heart of Azure. Azure Active Directory (Azure AD) is a cloud-based identity and access management service, which helps users sign in and access resources. Despite increasing users, there are some

misconceptions around Azure AD which results in increased numbers of incidents due to lack of awareness and security misconfigurations around Azure AD. In this presentation, we will discuss Azure AD from an offensive security perspective to raise awareness of its weaknesses. We will show how the matrix of the MITRE ATT&CK could be used to create a threat matrix and will cover some of common attacks ranging from enumeration to lateral movement. Last but not least, we will also look at the defending features in Azure AD.

Releasing secure features: Top mistakes of huge web-portals

By Sergey Belov, Application Security Lead, Acronis

Sending emails, generating temporary tokens and downloading files by links are some of the typical functions which are usually implemented insecurely, possibly resulting in resource or users getting hacked. This talk will cover many different features and discuss how to implement them for it to be both safe and convenient for end-users. We will talk about how to store temporary tokens, converting images and videos, how to download a file from a link, stateless VS stateful authentication and more - everything is in this talk.

Date: 23 November 2021 (Tues)

Time: 3.00PM – 4.30PM

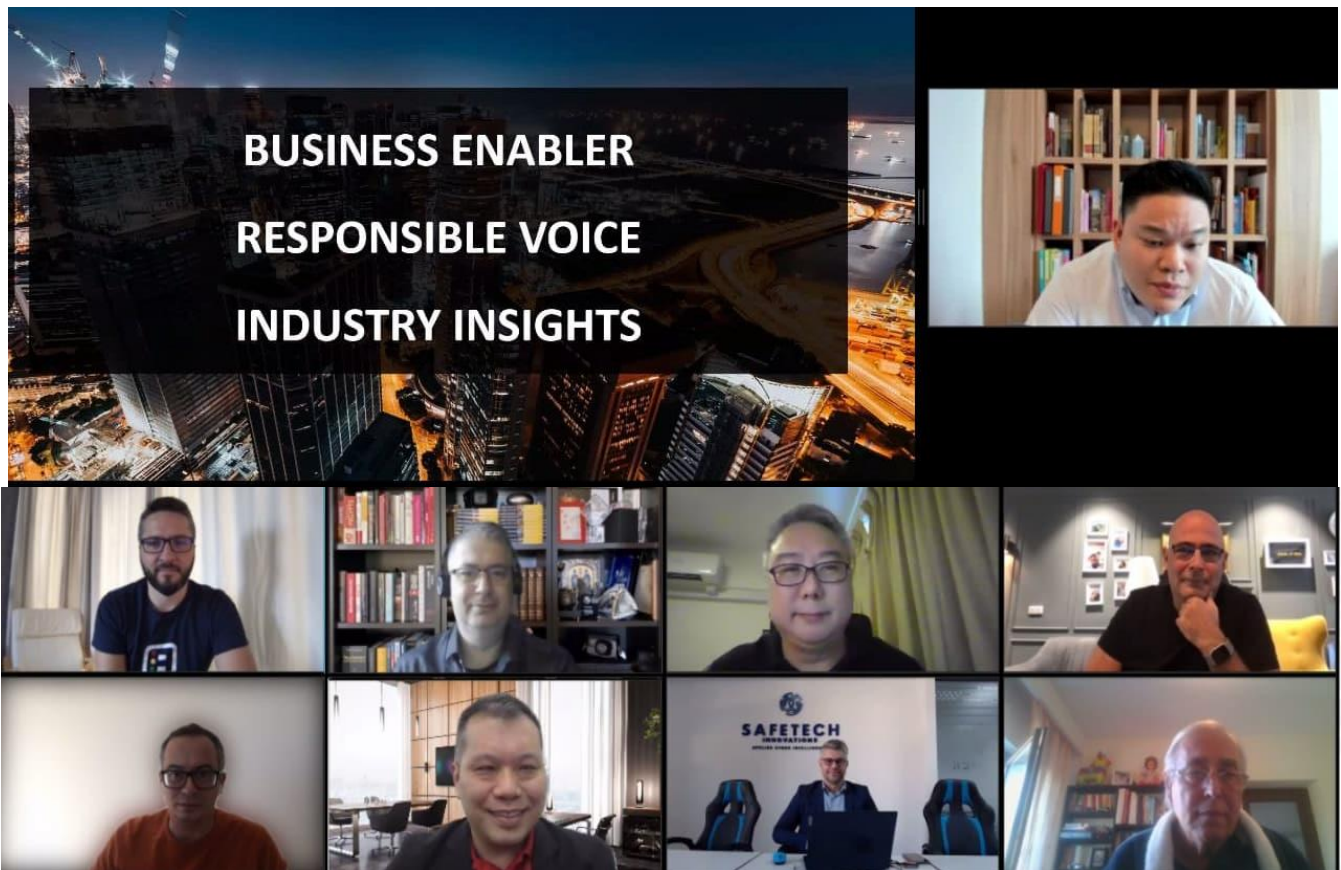
Venue: Webex

Registration: <https://aisp.webex.com/aisp/j.php?RGID=r83f8628697c694fd6038b7464db62e6e>

Regionalisation

Singapore – Romania: Webinar on Cybersecurity

Singapore – Romania: Webinar on Cybersecurity concluded successfully on 26 October afternoon and we would like to thank The Ambassador of Romania in Singapore, our speakers, SGTech and Enterprise Singapore as well as all the participants who have joined the webinar. The event began with opening addresses by key personnel from ATIC and our AiSP President, Mr Johnny Kho as well as Mr Eugene Lam from SGTech. An enriching afternoon it has been as the webinar shared interesting insights on the cybersecurity sector for Romania vs Singapore.



Cyber Leader Series on 23 Nov



Cyber Leader Series

CYBER LEADER SERIES

23 November 2021 | 7-9 PM (SG) 2-4PM (IL) | WebEx

				 Organised by: 
Johnny Kho President AiSP	Alon Refaelli Founder, Partner CyberTogether	Guy Segal VP Cyber Security Services, APAC Sygnia	David Warshavski VP Enterprise Security Sygnia	
				Supported by:  Via: 
Shiran Kleiderman CSO, Head of IT Celsius Networks	Joshua McCloud CISO, ASEAN Cisco System (USA)	Andre Shori Regional CISO Schneider Electric	Ron Moritz Chairman, CyberTogether	

In this Cyber Leader Series hosted by AiSP and CyberTogether, we have with us industry experts from Celsius Networks, Cisco, Schneider Electric, and Sygnia. We will be discussing several issues including ransomware defense strategies, SaaS collaboration and increased security risks to enterprise. This session is also moderated by Ron Moritz, Chairman, CyberTogether.

From the Front Lines: The Ransomware Defense Strategies that Worked

By David Warshavski, VP Enterprise Security, Sygnia & Guy Segal, VP Cyber Security Services, APAC, Sygnia

Over the past year, we partnered with more than 100 organizations around the world and in APAC to defeat ransomware attacks. Join our session to find out what strategies worked for these CISOs, and how you can build on their experience to secure your network. Ransomware attacks have evolved, but if you identify the threat early-on, technologies already in place can be used to eliminate it with no need for additional spend.

Join us for insights from 100+ ransomware cases and get defense recommendations you can implement right away.

You will discover:

- The new, increasingly malicious techniques used by threat actors in real-world attacks throughout APAC

- Key vulnerabilities commonly overlooked by security teams
- What CISOs can do to prevent these attacks, focusing on highly effective quick wins
- How to become ransomware ready without investing in additional, often redundant products

Deciphering the Decentralized Crypto Ecosystem.

By Shiran Kleiderman, CSO & Head of IT, Celsius Networks.

A Crypto CSO's cyber security threat landscape, framework, and toolkit. Decentralized Finance requires a unique mindset.

How the Covid pandemic accelerated SaaS collaboration and increased security risks to enterprises

By Joshua McCloud, CISO, ASEAN, Cisco System (USA)

As the CoViD pandemic took hold, almost overnight work-from-home became the default for millions of individuals around the globe. SaaS-based collaboration tools such as video conferencing, team messaging, and workflow management once used largely to extend traditional modes of work, suddenly became the only means of running the business. And while the enterprise IT perimeter has been steadily eroding for years, employee home routers and WiFi devices suddenly became the enterprise edge. This session will explore how the pandemic forced information security teams to rethink enterprise risk, change old assumptions, and adopt new frameworks, processes, and controls to better secure our new world of hybrid work

Owning cybersecurity strategy and driving security operations - practical tales from the trenches

By Andre Shori, Regional CISO, Schneider Electric

- Managing risks that can affect our customers, operations, and critical infrastructure in a "bifurcated world."
- Moving the cybersecurity maturity needle in both OT and IT.
- Partnering with our ecosystem across the value chain to raise the defence level of the industry at large.
- Establishing a company-wide cybersecurity culture.

Date: 23 November 2021 (Tues)

Time: 7 PM to 9 PM (SGT) | 2PM to 4PM (IDT)

Venue: WebEx

Registration: <https://aisp.webex.com/aisp/j.php?RGID=r5e0c532fc88a4bc08b1806dbd626cfed>

The Cybersecurity Awards



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

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

The Cybersecurity Awards 2021 winners will be announced at The Award Ceremony 2021 in Q1 of 2022.

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

TCA2021 Sponsors & Partners

THE CYBERSECURITY Awards 2021

Organised by: **AISP** (Advance Connect Excel)

Supported by: **CSA SINGAPORE**

Supporting Associations:

- CSCIS**, **CSA cloud security alliance**, **HTCIA**, **ISACA Singapore Chapter**
- OFFICIAL CHAPTER (ISC) SINGAPORE**, **SINGAPORE COMPUTER SOCIETY**, **SGTECH**, **TELECOM SOCIETY SINGAPORE**

Community Partner: **image engine**

Supporting Organisation: **SFA SINGAPORE FINTECH ASSOCIATION**

Platinum Sponsors



Gold Sponsors



Silver Sponsors



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
15 Sep – 30 Nov	SMEICC Conference Series 2021	Partner

Upcoming Events

Date	Event	Organiser
2 to 3 Nov	CISO ASEAN	Partner
2 to 3 Nov	Cyber Security for Financial Services Asia Part II	Partner
3 Nov	Zero Trust Future: Why Endpoint Security is Critical in Modern-Day Threat Landscape	Partner
6 Nov	Secure Singapore Conference 2021	Partner
8 to 12 Nov	Singapore FinTech Festival 2021	AiSP & Partner
8-Nov	Singapore Cyber Day	AiSP
9-Nov	SIG Day	AiSP
10-Nov	CAAP Focus Group Discussion & Sharing of AiSP Courses	AiSP & Partner
16 to 18 Nov	CLOUDSEC 2021	Partner
17-Nov	Knowledge Series – Emerging Trends – Blockchain & AI for Cybersecurity	AiSP & Partner
17-Nov	AiSP x Privasec Event – ISO 27001 Certification Journeys	AiSP & Partner
23-Nov	Cyber Leaders Series	AiSP & Partner
23-Nov	CREST Webinar	AiSP & Partner
24-Nov	CAAP Focus Group Discussion with PA	AiSP & Partner
24-Nov	AiSP x Mastercard CAAP Workshop	AiSP & Partner
24 to 26 Nov	DigiTech ASEAN Thailand 2021	Partner
1 Dec	Knowledge Series - CTI	AiSP & Partner
3 Dec	CyberCrimeCon2021	Partner
9 Dec	Micro Focus x SCW - Secure Code Tournament	Partner

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

CONTRIBUTED CONTENTS

Article from Data & Privacy SIG

What cybersecurity practitioners need to take note of GDPR

European Union's General Data Protection Regulation (GDPR) is known to be more stringent than Singapore's Personal Data Protection Act (PDPA). With the latest amendments to the PDPA, Singapore's data protection regime has incorporated certain aspects of the GDPR, such as the mandatory data breach notification and higher penalty.

As Asia deepens stronger economic links with the European Union (EU), it is viable for cybersecurity practitioners to know more about GDPR, to benefit the organisations they serve in. This can also help our information security professionals to prepare ahead for forward-looking data protection practices as Singapore's PDPA progresses.

PDPA versus GDPR

Here is a quick comparison between Singapore's PDPA and EU GDPR,

Legislation	SG PDPA	EU GDPR
Applicable to	Private sector (including sole proprietorship)	Comprehensive (including public sector)
Record keeping	An organisation must keep records on the ways it has used or disclosed personal data for at least 12 months as part of its obligation to provide individuals with access to their personal data. No mention of employment size.	Derogation for organisations with fewer than 250 employees with regard to record-keeping.
Data Protection Officer	Mandatory, including sole proprietorship	If fulfil these conditions, <ul style="list-style-type: none"> • Processing is carried out by a public authority or body, except for courts acting in their judicial capacity; • Core activities of the controller or the processor* require regular and systematic monitoring of data subjects on a large scale; or • Core activities of the controller or the processor consist of processing on a large scale of special categories of data (refer to <u>sensitive personal data</u> below) or personal data relating to criminal convictions and offences.

[back to top](#)

Sensitive personal data	Though the PDPA does not have a special or separate category of "sensitive" personal data, the PDPC does take a stricter view when considering a case where the personal data compromised is of a sensitive nature. Disclosure of such data may expose the client to the risk of fraud and identity theft.	Data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.
Individuals	<p>Data protection for a deceased individual for 10 years from the date of death.</p> <p>Individuals affected by a data breach can only bring an action against organisations (and not data intermediaries) for losses and damages suffered as a result of the breach.</p> <p>Both do not apply to the processing of personal data by a natural person in the course of a purely personal or household activity.</p>	<p>Living individuals only.</p> <p>Data subjects affected by a data breach can take action against both controllers and processors.</p>
Extraterritorial effect	Physical presence of the organisations does not matter.	
	GDPR: It applies to entities located outside the EU, and it imposes a number of direct obligations on data processors.	
Basis of processing	Consent is the only basis of processing. Arising from the Amendments, deemed consent framework is expanded and there are new exceptions to the express consent requirement.	High standard for consent, and it is not the only basis.
Data breach notification	Arising from the Amendments ¹ , organisations need to abide with the mandatory data breach notification obligation (3 calendar days), including financial information, sensitive health information.	Controller must report such a breach to the supervisory authority within 72 hours, and possibly to affected data subjects.
Penalty	<p>Arising from the Amendments, increased financial penalty which would <i>take effect at a later date</i>:</p> <ul style="list-style-type: none"> Maximum financial penalty for organisation's annual turnover in Singapore that exceeds S\$10 million is organisation's 10% of the annual turnover in Singapore. 	The EU's data protection authorities can impose fines of up to up to €20 million, or 4% of worldwide turnover for the preceding financial year—whichever is higher.

*Controller and processor refer to organisation and data intermediary in Singapore's context.

Observations on our cybersecurity practitioners' application of GDPR in Singapore

¹ Amendments to the PDPA, with effect on 1 February 2021: <https://www.pdpc.gov.sg/news-and-events/announcements/2021/01/amendments-to-the-personal-data-protection-act-take-effect-from-1-february-2021>

I have the opportunity to moderate a panel session: [GDPR for Cybersecurity Practitioners webinar](#) on 29 June 2021, organised by the [Association of Information Security Professionals \(AiSP\)](#). The panellists - [Joyce Chua](#), UOB; [Bryan Tan](#), Pinsent Masons LLP; and [Ivan Lai](#), Crypto.com, shared their observations on our practitioners' application of GDPR in Singapore. Here are some highlights of our virtual session,

What are the common misconceptions of GDPR in our local cybersecurity community?

They think their organisation is not offering services in EU and they may not understand what cannot be done. Practitioners are handling personally identifiable information, but they are not adhering to the GDPR. As the businesses are focusing on increasing customer base, there is not much development in the procedures involved. Also, some Singapore companies perceive that it is not necessary for them to understand GDPR as PDPA would suffice.

Has GDPR changed the dynamics how MNCs conduct their businesses in the region outside of the European Union?

GDPR is recognised as the golden standard among data protection laws. If you look at the sweeping changes in how we work in the non-EU countries, since GDPR comes into effect on 25 May 2018. Companies have to review and update their data protection measures, paying more attention on how to implement their measures. There was chaotic change among the vendors due to the US's Privacy Shield², which EU does not deem as an adequate GDPR compliance mechanism. Data subjects' Right to delete is not easy to be implemented when you have different systems in different regions. More efforts are in place to manage data inventory and the regulatory requirements for data breaches.

There is a stronger emphasis to use Privacy Impact Assessments (PIAs, or in Singapore's case, Data Protection Impact Assessment) for specific purposes that leverages processing of personal data. This risk-based assessment enables senior management to prioritise controls and resources for risky activities that are important for business processes and innovation. There is also greater demand to ensure the business processes have controls in place on daily basis, which gives rise to the mobile applications for companies to track and monitor the controls and compliance efforts.

Companies in general, not just the MNCs, are relying more on their legal counsels to navigate GDPR-related contractual terms. Overseas insurers are more well-versed in managing breaches while some legal counsels are not aware of what is ransomware. Data subjects are asked to file class suit for damages by lawyers and this would become more common as more cybersecurity incidents occur.

During your engagement with companies on their cybersecurity posture and strategies, what are the common questions they have on data protection compliance in Singapore? Is there a difference when they are evaluating their data protection strategies in Singapore and Asia?

There is no magic bullet in the terms and conditions for Singapore companies when working with clients and partners that have to be GDPR-compliant in Asia; it is a lot of hard work, depending on how the organisation is set up. No organisation is identical in its compliance measures, and business owners should be aware that the legislation is evolving and there are new developments in overseas markets. For instance, Hong Kong, Japan, South Korea are ahead of us, while there is no much enforcement in Malaysia. Singapore takes enforcement seriously while some countries have not put in their data protection legislation.

For cybersecurity practitioners have to work with different external partners in the cross-border supply chain in MNC environment, what are the common challenges or areas they face for data protection?

The most common areas would be partnership and outsourcing. The practitioners may not be using PIAs to identify their risks, especially when it comes to vendor due diligence. There could be better understanding of data minimisation while balancing business objectives. On the data breach aspect, incident response management and reasonable security measures can be improved as well. On managing data risks, it is important to review the data lifecycle and assess the criticality of vendors.

The panel also addressed participants' questions on qualifications for data protection officer, cybersecurity insurance, employee data, vendor due diligence, privacy concerns over virtual and digital platforms during Covid period. AiSP members are welcome to playback the recorded webinar, by [contacting the Secretariat](#).

How our cybersecurity professionals can benefit from understanding the GDPR?

² Privacy Shield is mechanism that enables participating companies to meet the EU requirements for transferring personal data to third countries. (Source: <https://www.privacyshield.gov/>)

Knowing the GDPR and implications to Singapore-based organisations enable our information security professionals to prepare ahead for forward-looking data protection practices. GDPR emphasises on areas where our professionals can advance and value add, e.g.,

- Provide technical and development teams with training on data protection by design, and keep the relevant training records.
- Organisations must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.
- Benchmark against ISO 27001 and other international standards, as well as setting business KPIs for the cybersecurity team.

More Asian countries are embracing GDPR such as Japan and South Korea. If companies want to stay ahead to capitalise on the EU market, our cybersecurity practitioners should consider taking proactive steps ensure their knowledge is relevant in the fast-developing borderless world, especially during the Covid times.

About the Author



Yvonne Wong | AiSP Committee Member

Yvonne is a Committee Member of 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 Data & Privacy SIG

Cybersecurity in the Protection of Personal Data

- If the use of portable storage devices to store or transfer personal data cannot be avoided, more stringent physical controls for such devices should be considered.
- To identify if there is malice in the unauthorised disclosure of personal data, it is critical to retain logs related to the access of personal data.
- On top of technical controls, awareness training for office staff is also necessary to reduce the probability of human errors.



A cybersecurity breach can jeopardise credibility and be incredibly costly for small businesses in terms of damages. Photo: Canva Pro

Since the second half of 2020, there have been numerous reported cases of personal data breaches of Singapore-based entities, with the latest being from [Singtel](#).

Coincidentally, from 1 February 2021, new amendments to the Personal Data Protection Act (PDPA) have come into force. With the new amendments, there is an increased emphasis for organisations to better protect personal data that is under their care.

This article seeks to share some salient points for cybersecurity protection in relation to the newly amended PDPA.

1. Mandatory requirement of reasonable security arrangements to prevent the loss of any storage medium or device on which personal data is present

Section 24(b) is a newly added protection sub-clause in the PDPA. This clause applies to storage media, such as storage drives, that contain personal data.

There are typically two types of storage media – immovable or portable storage media. For immovable storage media, such as those found in your stationary servers or personal computers (PCs), the risk of loss is minuscule, hence they will not be the focus of this article. Proper storage media disposal procedures can address the risks of loss of storage media from immovable devices. Instead, let us focus our attention on portable storage media or devices, such as laptops, external USB drives and USB thumb drives.

Laptops

For laptops, it is important that organisations issue laptop cable locks to all laptop users and remind them to use the issued cable locks if their laptops are left unattended in any public areas. Even for staff that are working from home, it is also recommended that they use the cable locks at home so as to avoid accidental displacement or removal of their corporate laptops.

External USB drives and USB thumb drives

The best option is to avoid the use of such storage devices for storage or transfer of personal data. Possible alternatives include internal file transfer services, such as internal network shared folders, or cloud-based file sharing services. Do note that for cloud-based file sharing services, it is important that the service provider provides a level of protection that satisfies the requirements of the PDPA. It is also preferable that the location of the service be physically located in Singapore for data sovereignty purposes and to avoid additional cross-border data transfer requirements. Password protection of files containing personal data is highly recommended when such documents are stored in cloud-based file sharing services.

If the use of portable storage devices to store or transfer personal data cannot be avoided, more stringent physical controls for such devices should be considered.

Possible measures include restricting to a permitted list of USB storage devices and restricting such permitted devices from leaving the office premises. The latter could be enforced by requiring daily end-of-day return of every permitted USB storage media to a designated custodian.

Awareness Training



Controls placed on storage devices alone are insufficient in preventing data breaches. Photo: Canva Pro

Notwithstanding the above technical controls, adequate awareness training for office staff is required to reduce the likelihood of human errors negating the benefits of the above-mentioned technical controls.

2. More explicit personal liability for malicious and reckless behaviour resulting in unauthorised disclosure of personal data

In the newly added Section 48D, it is an offence for an individual to disclose or cause the disclosure of personal data where the disclosure is not authorised, and the

individual either knows the disclosure is not authorised, or is reckless as to whether the disclosure is authorised or not. The penalty is a fine not exceeding \$5,000 and/or imprisonment for a term, not exceeding two years or both.

To identify if there is malice in the unauthorised disclosure of personal data, it is critical to retain logs related to the access of personal data. Information such as source IP addresses, time of access, type and amount of personal data access etc. can help to gauge whether the access is with or without malice. To achieve this, it is important to monitor and log all access to personal data, such as from websites, databases and shared folders.

Another type of unauthorised disclosure is related to recklessness. In simple layman terms, recklessness is defined as “gross negligence”, which sets a higher bar when compared to “negligence” in the earlier version of the PDPA. Hence, the new amendments actually raise the bar for an individual to be found guilty of breaching the PDPA, specifically Section 48D.

Just as we are personally responsible for getting our cars inspected every eighteen months to ensure that they are fit for our local roads, it is also imperative that IT environments be inspected on a regular basis to ensure that they are adequate in protecting personal data. If you have been ignoring reports of critical vulnerabilities from your IT or IT Security colleagues, you could also be deemed reckless for operating in an environment that is “unfit” for protecting personal data.

Another example of recklessness is the continual use of IT products in which support has expired, such as the use of Windows XP. This is akin to driving a car that has reached its lifespan here in Singapore (more than 10 years) without any official extension of its Certificate of Entitlement (COE).



3. Mandatory data breach notification to regulators and/or customers.



Companies have to be held accountable if their customer data becomes compromised. Photo: Canva Pro

The new Part VIA of the PDPA contains new clauses related to new mandatory data breach notification requirements.

In this part, Section 26B specifies the conditions for notifiable data breaches:

- (a) result or likely to result in significant harm to an individual; or
- (b) result or likely to result in insignificant harm to individuals exceeding 500 individuals.

For the former, both the affected individuals and the Personal Data Protection Committee (PDPC) must be notified. For the latter, the PDPC must be notified but it is not mandatory to notify the affected individuals. Nevertheless, notification to affected individuals in the latter case may be viewed favourably by the PDPC.

Do note that a data breach that relates to the unauthorised access, collection, use, disclosure, copying or modification of personal data within an organisation is deemed not to be a notifiable data breach.

Subsequent sub-sections under Section 26 covers the following areas:

- i. The need to assess whether a breach is notifiable in a reasonable and expeditious manner;
- ii. Duty of a data intermediary to notify their customers immediately; and
- iii. Notification period of 3 calendar days or 72 hours after you have ascertained it is a notifiable breach.

In order to comply with the new requirements in Part VIA, it is important for an organisation to have the following controls in place before a data breach occurs:

A. Establish a pre-approved panel of forensic investigators to help you assess whether a breach is notifiable in a reasonable and expeditious manner.

As most SMEs are not suited to build and maintain an internal team of forensic investigators, it is preferable for SMEs to engage a panel of pre-approved forensic investigators. By doing so, SMEs can be assured of a faster response time from the forensic experts and better clarity on the expected costs of assessment.

B. Establish a data breach management plan/incident response plan and playbooks, and communicate them.

Formulating a plan for what should be done during a data breach is important as you do not want to be clueless when faced with one. More detailed incident response playbooks can also be valuable references for staff when responding to data breaches. In addition, such plans and playbooks provide assurance that the company can assess any breach in a reasonable and expeditious manner, as well as notify the PDPC and relevant stakeholders in a timely manner.

C. Conduct regular data breach simulation exercises based on your plans and playbooks.

The plans and playbooks mentioned in the previous paragraph will be futile if staff are not aware of, or are not familiar with them. Hence, regular communication of such plans and playbooks is important. An excellent way to ensure that these plans and playbooks are comprehended by staff is to conduct regular data breach simulation exercises. Such exercises also provide excellent opportunities for the fine-tuning and refinement of relevant plans and playbooks. In addition, these exercises

can provide assurance that the processes, procedures and, most importantly, staff, are ready to handle any potential data breaches in the future.

As we enter into 2021, let us look forward to a safer year, both in health and cybersecurity.

About the Author



Wong Onn Chee | Data & Privacy SIG Lead, MAISP | Association of Information Security Professionals (AiSP)

Wong Onn Chee is currently the Chief Executive Officer at Rajah & Tann Cybersecurity and Technical Director at Rajah & Tann Technologies. His areas of expertise include information leakage protection, web/cloud security and security strategy. Onn Chee is also one of the co-inventors for at least six international PCT patent rights, besides several US, EU and Singapore patents. He volunteers at the Association of Information Security Professionals (AiSP) and is involved in a wide range of AiSP initiatives such as the Data & Privacy Special Interest Group.

This article is first published on ASME Website:

<https://asme.org.sg/article/newsroom/96/Cybersecurity%20in%20the%20protection%20of%20personal%20data>

Article from our CPP Partner, Fortinet

Enabling Self-Healing SD-WAN from the WAN Edge to the Cloud Edge

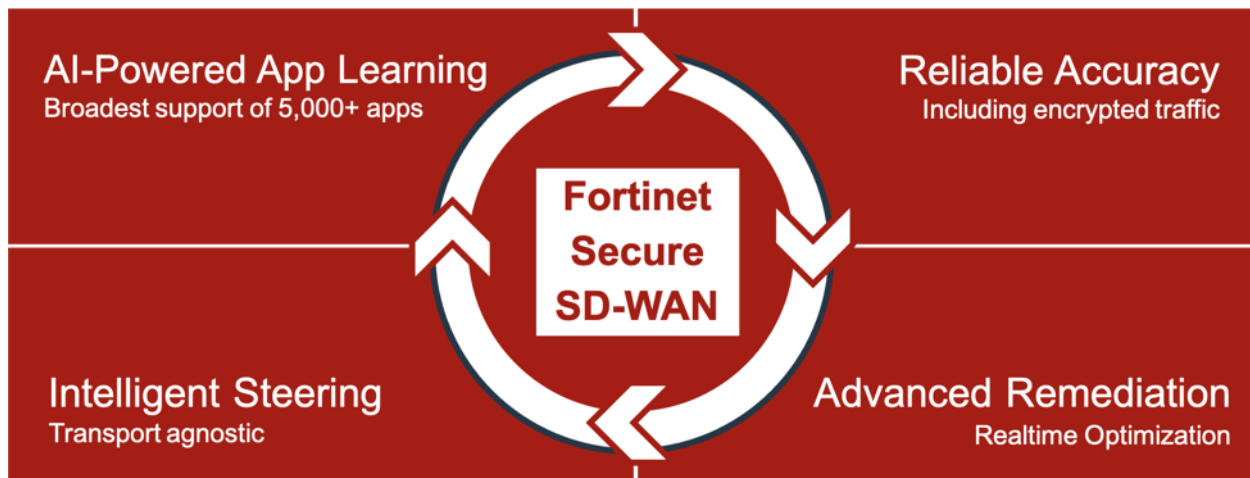
By Nirav Shah | June 22, 2021

By [Nirav Shah](#) | June 22, 2021

The Internet is at times unpredictable and unreliable, and no matter how robust your [WAN](#) infrastructure is, brownout and blackout outages are sometimes unavoidable. Unreliable connectivity is especially a challenge for large and distributed enterprises that span multiple countries and regions that grapple with regular internet impairment.

As networks shift from traditional IP-based to application-driven, reactive to predictive, and manual to automated, as well as change to support work-from-anywhere, the business outcomes and expectations to deliver enhanced user experience and instant ROI benefits remain the same. Organizations that have deployed basic SD-WAN solutions are realizing that the time and hassle of a wide-area network that needs to be reconfigured or manually intervened-upon every time there's a wider internet connectivity issue has completely negated many benefits they sought to realize by implementing [SD-WAN](#) in the first place. As a result, the need for SD-WAN to enable a self-healing network – one that automatically fixes issues before they are widely realized – from the WAN edge to the [cloud](#) edge has now become a key requirement for organizations. So what does it take to enable [Self-Healing SD-WAN](#)?

Four Key Features of Self-Healing SD-WAN:



Four Key Features of Self-Healing SD-WAN

AI-Powered Application Learning:

One of the key use cases of SD-WAN solutions has been to deliver the best application experience regardless of where the application resides, whether it be from the datacenter to the cloud. In order, to deliver a great application experience for end users, the number of applications a solution can recognize needs to be considered.

Fortinet Secure SD-WAN provides broad support of 5,000+ applications and, more importantly, this is not a static list, rather one that Fortinet continuously adapts and evolves to meet business needs. In today's world where applications are more dynamic than ever, Fortinet's [AI](#)-powered application learning helps not only with the scale of applications supported, but also with faster application learning.

Reliable Accuracy:

Accurate application detection becomes essential to ensuring the proper prioritization of business-critical applications over those that are non-critical. However, the challenge is that over 80% of the traffic in today's world is encrypted, and most SD-WAN solutions are unable to handle this type of traffic.

Fortinet Secure SD-WAN enables reliable accuracy even for encrypted traffic, including TLS 1.3. What makes this even more compelling for our customers is the ability to do this at scale without compromising on performance.

Advanced WAN Remediation:

One of the big promises of SD-WAN solutions has been the remediation of WAN traffic during brownout and blackout conditions, leveraging capabilities like Forward Error Correction (FEC) and Packet Duplication. FEC and Packet Duplication have been key to enabling seamless unified communications like voice and video streaming based on critical parameters such as latency, jitter and packet loss.

In today's world where we rely on voice and video streaming more than ever, whether it be applications like Zoom, Webex, or Skype, the standard approach of Forward Error Correction needs a significant boost. With the latest [FortiOS 7.0](#) release, Fortinet has advanced its WAN remediation capabilities with adaptive FEC, designed to dynamically enable FEC based on bandwidth conditions without manual assistance.

Intelligent Application Steering with passive WAN monitoring:

Beyond the number of applications supported, the accuracy and speed in which those applications can be detected must also be considered, and most importantly, the ability to steer the application in the right direction without reactively changing configurations – something many organizations struggle with.

Fortinet Secure SD-WAN provides a transport-agnostic solution to deliver the best experience over multiple paths – whether it is [MPLS](#), broadband or LTE. Fortinet Secure SD-WAN is powered by a purpose-built SD-WAN processor that allows for faster application recognition and steering between multiple paths. The solution leverages passive WAN monitoring without adding more overhead to already burdened WAN situations. It also enables dynamic application switchover between multiple links without having to send active synthetic probes to measure WAN characteristics like latency, jitter and packet loss.

Integrating all of that functionality into a single, easy to deploy solution combined with AIOps to ensure consistent performance and reliability, enables networks to be more proactive than reactive. Fortinet Secure SD-WAN with its centralized management console can not only orchestrate connectivity, but also manage advanced routing and security functions, all through the same pane of glass. When you combine this with advanced analytics for a granular view of network and application performance, Fortinet Secure SD-WAN enables organizations to detect and respond to network anomalies and threats across the entire distributed deployment to enable a consistent, self-healing WAN experience across all edges.

Take a security-driven networking approach to improve user experience and simplify operations at the WAN edge with [Fortinet Secure SD-WAN](#).

For more enquiries, please reach out at seahkhdr@fortinet.com

Article from our CPP Partner, SecurID

The First Steps in Securing Hybrid Work

By Kelly Sarber
CISO, SecurID

The following first appeared on the [SecurID blog](#) on October 4, 2021 as part of an ongoing series highlighting best practices and insights during Cybersecurity Awareness Month. It is reprinted here with permission.

Like most business processes, cybersecurity tends to exist on a pretty broad spectrum. For every organization that's deploying more mature techniques like [zero trust security](#) or [risk-based authentication](#), there are plenty that leverage traditional defense in depth approaches for their network security postures.

Providing secure remote network access by creating a virtual private network (VPN) is one of the quickest methods to provide business users with access as if they are in the office. As such, it should come as no great surprise that VPN use surged as a result of the pandemic. For many businesses just starting off on their cybersecurity journeys, VPNs represented a quick, effective and immediate way to secure hybrid work and continue operations:

- A January [survey](#) found that roughly 70% of cybersecurity professionals reported increasing their VPN capacity during the pandemic—and that roughly 35% had more than doubled their VPN capacity because of the pandemic.
- *TechBullion* called 2020 a "[breakout year for business VPNs](#)," noting one study which reported that "global demand for VPNs [had jumped 41%](#) in the second half of March, and continued at 22% above pre-pandemic levels.
- In India, VPN use grew seven times over the first half of 2021. India recorded more than [348 million VPN installs in the first half of the year](#), representing 671% in growth compared with 2020.

That's remarkable growth and an important first step for many businesses trying to secure hybrid work—but it's only a first step. Because VPNs are only as good as the authentication used to access them. And in far too many cases, businesses are asking their users to access VPN using only a password to sign-in.

Given that they provide access into a business' corporate network, VPNs can create a major vulnerability. Simply put, the risk exposure of this one entry point can be far too high—and that exposure becomes even more pronounced when an organization only relies on passwords to manage access. That risk can also be exacerbated by third-parties requesting intermittent access.

Another way of putting it: using a password to secure a VPN is like building a steel bank vault and setting the combination lock to 0-0-0. The walls might be strong, but just about anyone can stroll right in. And in far too many cases, that's exactly what happens.

Don't use passwords to secure VPN

Passwords are expensive and insecure. The National Cybersecurity and Infrastructure Agency recently added single-form authentication to its list of "[Bad Practices](#)," calling the use of passwords and usernames an "exceptionally risky cybersecurity practice."

As a result, it's no surprise that there have been several high-profile instances when password-protected VPNs failed to keep out cybercriminals.

[back to top](#)

One of the most memorable failures is [Colonial Pipeline](#). According to [Bloomberg](#), hackers breached the company's networks through a VPN account that was a) no longer actively in use and b) not protected by MFA.

But as other [recent stories](#) have revealed, many organizations are still using passwords to 'secure' their VPNs.

That practice—combined with the [FG-IR-18-384 / CVE-2018-13379](#) glitch—would allow attackers to “perform data exfiltration, install malware and launch ransomware attacks.”

The high costs of passwords

It's not that passwords are particularly bad at securing VPNs—it's that they're bad at securing *everything*. Passwords are hard for legitimate users to manage and easy for hackers to guess. They're the #1 attack vector for bad guys—the 2020 [Verizon Data Breach Investigations Report](#) found that more than 80% of hacking-related breaches involved either brute force or the use of lost or stolen credentials.

Passwords are also expensive: for bigger enterprises, nearly 50 percent of IT help desk costs go to password resets. That can add up to more than [\\$1 million](#) in staffing.

Passwords have tremendous costs—both as security liabilities and to a business's bottom line.

Take the next step in securing your hybrid workforce

If you've invested in a VPN to provide secure network access for your hybrid workforce, you've taken an important first step in protecting your team, assets and IP.

But there are other important steps that organizations must take to protect themselves, including using [multi-factor authentication \(MFA\)](#). MFA is a fundamental part of any organization's cybersecurity stance—recently, President Biden signed an [executive order](#) directing public agencies to implement MFA. That advice was borne out by Fortinet's recent advisory regarding an [SSL-VPN](#) vulnerability, in which the company cautioned organizations to “treat all credentials as potentially compromised” and “implement multi-factor authentication, which will help mitigate the abuse of any compromised credentials, both now and in the future.”

Other steps businesses can take to secure remote workers include minimizing hackers' favorite vulnerability by deploying [passwordless authentication](#) and using [risk-based authentication](#) to create step-up authentication for critical assets.

Each of these steps builds on the next. And as businesses continue maturing their security practices, they can build toward [zero trust](#) principles by enforcing least privilege and always verifying access requests.

Regardless of where you are on your journey, identity is key. Knowing who your users are, what they should have access to and how you're going to authenticate them is essential to any successful cybersecurity program.

Additional Resources

Want to take the *next* step in securing hybrid work? Contact Douglas Lim at: Douglas.Lim@rsa.com or see these links for additional resources:

- **White paper:** [Identity and Access Management in the Cloud: Make it Easy on Yourself](#)
- **E-Book:** [Step by Step by Step: Managing Risk in the Hybrid Workforce](#)
- **Free trial:** [SecurID multi-factor authentication](#)
- **E-Book:** [Five ways To Transform Access and Secure the Digital Enterprise](#)

Article from our Partner, Trend Micro

CLOUDSEC 2021
REIMAGINE YOUR CLOUD

AISP
Advance Connect Excel

**REGISTRATIONS
NOW OPEN**

3 Days of You
Your Imagination
Your Cloud

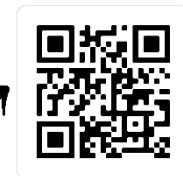
16-18 November

REGISTER NOW

CLOUDSEC 2021 is here. Gear up for 3 days of the best in cloud & cybersecurity. Immerse in an unparalleled experience. Insights and engagement that are purpose-built and tailored to your role's unique demands.

PURPOSE BUILT EXPERIENCE AWAITS!

- Reimagine Enterprise Cybersecurity: CISO Exclusive**
Interact and engage with industry leaders like AWS, Synk & more. Enrich your enterprise cybersecurity.
- Reimagine Cloud: Cloud Leaders & DevOps Exclusive**
Discover how cloud-native security platforms protect cloud infrastructure end-to-end. Dive into dedicated session tracks for Cloud Native DevOps & Infrastructure-as-code
- Reimagine Treat & Detection: SOC & Infrastructure Security Exclusive**
Protect the borderless enterprise. Enable your team with threat intelligence.



Register here

CLOUDSEC 2021
REIMAGINE YOUR CLOUD

Hosted by
**TREND
MICRO**

Article from our CPP Partner, FireEye

FireEye Advances XDR Platform to Arm Security Operations Teams

MILPITAS, Calif., Aug. 16, 2021 – [FireEye, Inc.](#) (NASDAQ: FEYE), the intelligence-led security company, today introduced [FireEye XDR](#), a unified platform designed to help security operations teams strengthen threat detection, accelerate response capabilities, and simplify investigations.

The FireEye XDR platform provides native security protections for Endpoint, Network, Email, and Cloud with a focus on improving organizations' capabilities for controlling incidents from detection to response. FireEye Helix unifies the security operations platform by providing next-generation security incident and event management (SIEM), security orchestration, automation and response (SOAR), and correlation capabilities along with threat intelligence powered by Mandiant.

"Our superior knowledge of threats and the adversary is unmatched. Hands down, I believe we manage the best XDR platform in business by integrating threat intelligence into an advanced detection engine which is delivered centrally and extensibly via the cloud," said Bryan Palma, EVP of FireEye Products. "Our XDR platform translates insight to action across more than 600 security technologies. FireEye XDR furthers our mission to relentlessly protect our customers."

FireEye's Helix native cloud design provides an improved analyst experience allowing for the seamless integration of disparate security tools regardless of vendor or data source. FireEye's XDR platform is best suited for enterprise and mid-market security operations teams that are increasingly at risk from cyber-attacks due to an array of factors including sophistication of threats, suboptimal security tool management, and personnel shortages.

Over the next few quarters, the FireEye Products business plans to introduce new features to the FireEye XDR platform including enhanced Endpoint cloud capabilities, FireEye Helix upgraded dashboards and threat graphing capabilities, additional support for leading third-party security tools, and continued integration with the Mandiant Advantage platform which includes Automated Defense.

"Forward-thinking security and risk leaders are looking to defend their enterprises in ways that can reduce complexity and upfront investment, while at the same time speeding the time it takes to detect and respond to pervasive threats," said Jon Oltsik, Senior Principal Analyst and ESG Fellow. "Leveraging an approach to XDR built on threat intelligence can help security leaders improve efficacy and avoid becoming the next headline."

Learn more in the blog post, "Introducing FireEye Extended Detection and Response (XDR): A Flexible XDR Solution Born from the Front Lines of Threat Detection and Response": <https://www.fireeye.com/blog/products-and-services/2021/08/introducing-fireeye-extended-detection-and-response-xdr.html>.

FireEye XDR Available Today

The FireEye XDR Platform is available today and includes FireEye Helix and any combination of FireEye products including Endpoint, Network, Email, and Cloud delivered via cloud subscription licenses with per user or by data consumption options.

FireEye XDR Resources

- Watch the launch of XDR:
https://www.brighttalk.com/webcast/10469/502749?utm_source=assoc&utm_medium=newsletter&utm_campaign=aisp
- Request a demo: <https://tinyurl.com/XDRdemo>
- Download the report from Gartner, Innovation Insights for Extended Detection and Response: <https://content.fireeye.com/fireeye-xdr/rpt-gartner-innovation-insight-for-xdr>

To find out more, please contact:

Stephanie Lim – stephanie.lim@fireeye.com

© 2021 FireEye, Inc. All rights reserved. FireEye and Mandiant are registered trademarks or trademarks of FireEye, Inc. in the United States and other countries. All other brands, products, or service names are or may be trademarks or service marks of their respective owners.

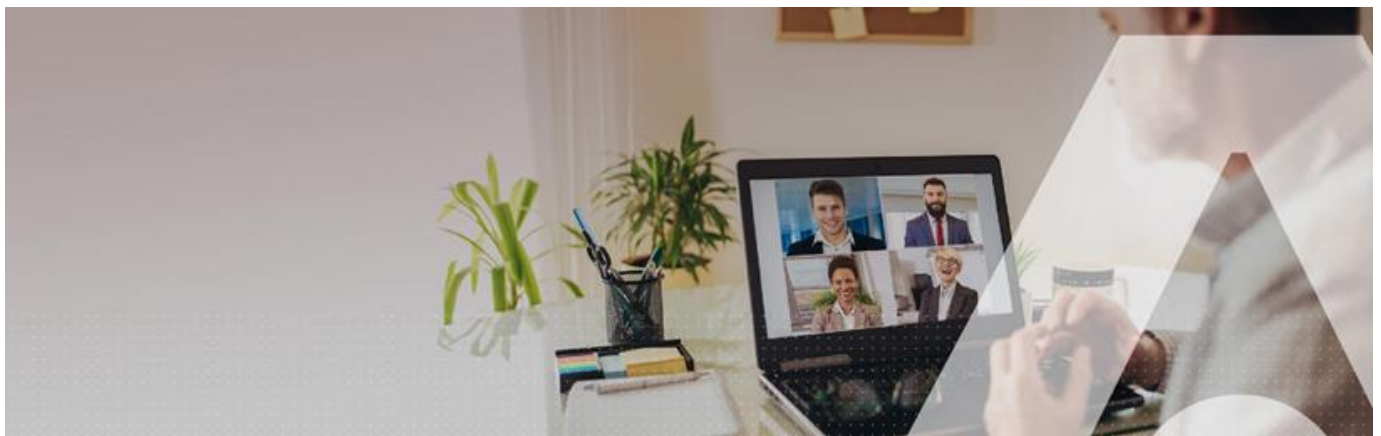
Article from our SME Cybersecurity Conference Sponsor, Thales

cpl.thalesgroup.com

THALES
Building a future we can all trust

Owning your own Access Security

The key to building strong cloud security and avoiding the risk of vendor lock-in



Contents

- 3** **Executive Summary**

- 3** **What a Shared Security Model is**

- 5** **Risks and limitations of having everything with a single service provider.**
 - 5 1. Human error
 - 5 2. External attacker
 - 5 3. Insider threat

- 6** **Regulatory motivations for a neutral cloud security solution**

- 7** **Tangible benefits of shared security model**

[back to top](#)

8 The benefits of Thales agnostic security**8 About Thales**

Executive Summary

The latest cybersecurity incidents affecting government agencies and organizations as well as large enterprises around the world, who have invested heavily in digital and cloud initiatives, have demonstrated the urgent need for a different approach to security. Based on cloud security's shared responsibility model, businesses should segregate their security duties from those of cloud service providers, bring their own security tools to avoid cyber threats and from criminals moving laterally into their corporate networks.

Security duties segregation can also help organizations in meeting and sustaining compliance with an evolving regulatory and jurisdictional landscape, as the "Schrems II" rule proved. The purpose of this white paper is to showcase the tangible benefits of selecting a vendor-neutral cloud security solution to address the evolving security risks and privacy requirements.

What a Shared Security Model is

In a traditional, on-premises data center model, you are responsible for security across your entire operating and computing environment, including your applications, physical servers, user controls, and even physical security.

When you migrate your services, applications, workloads, and data to the cloud, you need to be aware that cloud service providers adhere to a shared security responsibility model, which means that your security team maintains some responsibilities for security, while the provider takes some responsibility, but not all. The key to a successful cloud security implementation is understanding where your provider's responsibility ends, and where yours begins.

- In the AWS Shared Security model¹, AWS claims responsibility for "protecting the hardware, software, networking, and facilities that run AWS Cloud services."
- Microsoft Azure² claims security ownership of "physical hosts, networks, and data centers."
- Both AWS and Azure state that your retained security responsibilities depend upon which services you select.

1 Amazon Web Services, Shared Responsibility Model, <https://aws.amazon.com/compliance/shared-responsibility-model/>

2 Microsoft Azure, Shared responsibility in the cloud, <https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>

The following diagram provides a high-level, vendor-agnostic, conceptual view of a shared responsibility model:

		On-prem	IaaS	PaaS
Application elements are specific to the customer's business, so they are the customer's responsibility	Application user access management			
	Application-specific data assets	●	●	●
	Application-specific logic and code			
Workload responsibility depends on IAAS Vs PAAS model (PAAS often referred to as "serverless")	Application / platform software			
	Operating system and local networking	●	●	●
	Virtual machine / server instance			
Lower-level infrastructure is more generic and commoditized, and the provider assumes responsibility	Virtualization platform			
	Physical hosts / servers / computers			
	Physical and perimeter network	●	●	●
	Physical datacenter environment			

Customer Provider

Figure 1: A vendor-agnostic view of responsibilities in the shared responsibility model. Source: Cloud Security Alliance¹.

No matter what your computing environment, whether on-premises, public cloud, private cloud, or just hybrid, you are always responsible for securing what's under your direct control, including:

- **Data:** By retaining control over your data, you control how and when your data is used. The cloud provider has zero visibility into your data, and you maintain all access to your data.
- **Applications:** Your proprietary applications are yours to secure and control throughout the entire application lifecycle –from development to testing and deployment.
- **Identity and Access:** You are responsible for all facets of your identity and access management (IAM) program, including authentication and authorization mechanisms, single sign-on (SSO), multi-factor authentication (MFA), access keys, and credentials.
- **Platform Configuration:** When you deploy cloud computing environments, you control the configuration of the underlying operating environment. Platform configuration varies based on whether your instances are server based or serverless.

¹ Cloud Security Alliance, Shared Responsibility Model Explained, <https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/>

Risks and limitations of having everything with a single service provider

Cloud service providers have launched their own security tools to help businesses protect their cloud-based instances and assets. Opting for a vendor-native cloud security solution means trusting the security of your data, applications, encryption keys and credentials to the cloud service provider. Although this seems enticing, can you place such a level of trust to a single provider?

Security and privacy regulations and laws contribute to building trust in your cloud computing environment. However, it is easier to trust if you can trust less¹. Although you can certainly trust the technologies behind cloud computing, you should decrease the amount of trust you place into the security solutions offered by the cloud service providers.

This is of huge importance, because risks, vulnerabilities, and threats to the service provider are traversing the customers, allowing adversaries to move laterally across corporate networks. Here are three threat vectors you need to consider before selecting a cloud security solution.

1. Human error

Human error and negligence account for a large percentage of cloud security incidents. In fact, according to the 2020 Cloud Security Report², misconfiguration of the cloud platform (68%) is ranked as the biggest security threat to cloud deployments.

Configuration errors, as well as developers' mistakes, poor source of entropy and accidental loss of keys, create cloud security challenges such as unauthorized data disclosure, loss of data privacy, and accidental exposure of credentials.

2. External attacker

External attackers tend to find the above-mentioned human errors and turn these weaknesses into compromises as a result. Advanced threat actors have been known to attack key management systems (KMS) and weak authentication schemes to gain wider access to data. For example, during the recent SolarWinds supply chain compromise, attackers exploited "systemic weaknesses³" in the native authentication mechanism of a cloud service provider to move laterally within the networks of many cloud customers. It became apparent that the model of deploying a vendor native security solution not only did not prevent attackers from launching their attack, but it became the driver for escalating their malicious actions.

3. Insider threat

A rogue or disgruntled service provider employee, having access to keys and/or credentials, may leverage their privileges to access and disclose sensitive data or disrupt cloud-based functions of customers.

¹ Anton Chuvakin, Il-Sung Lee, The cloud trust paradox: To trust cloud computing more, you need the ability to trust it less, <https://cloud.google.com/blog/products/identity-security/trust-a-cloud-provider-that-enables-you-to-trust-them-less>

² Cybersecurity Insiders, 2020 Cloud Security Report, <https://www.cybersecurity-insiders.com/portfolio/2019-cloud-security-report-isc2/>
<https://www.infosecurity-magazine.com/news/crowdstrike-slams-microsoft-over/>

Regulatory motivations for a neutralcloud security solution

Besides the above threat considerations, you should pay attention to various developments surrounding data privacy regulations, and especially the concept of data portability and sovereignty. Regional requirements are playing a large role in how organizations migrate to the cloud and operate workloads in public cloud. Regulators in Europe, Japan, India, Brazil and other countries are considering or strengthening mandates for keeping unencrypted data and/or encryption keys within their boundaries.

In addition, the Court of Justice of the European Union issued its decision in “Schrems II” on 16 July 2020. This is a landmark decision that invalidates the EU-U.S. Privacy Shield arrangement. Until July 16, Privacy Shield had served as an approved “adequacy” mechanism to protect cross-border transfers of personal data from the European Union to the United States under the EU General Data Protection Regulation. More than 5,000 organizations participate in Privacy Shield. Many thousands more EU companies rely on Privacy Shield when transferring data to these organizations. With the “Schrems II” rule, the conditions for the lawful transfer of this data have been removed¹.

Considering the major cloud service providers – namely Amazon, Microsoft and Google – are not based in the European Economic Area (EEA) region, raises certain concerns regarding the access of EU personal data. The European Data Protection Board (EDPB) has identified two Unlawful Use Cases:

- Unlawful Use Case 6: Transfer to cloud services providers or other processors which require access to data in the clear.
- Unlawful Use Case 7: Remote access to data for business purposes.

The existence of Unlawful Use Cases 6 and 7 mean that common cloud vendor practices leave corporate officers and boards of directors open to liability risks from the potential for unlawful data access².

To meet the new data sovereignty requirements, cloud service providers have modified their Standard Contractual Clauses (SCC)³ to add guarantees that their services occur entirely within the EU. However, organizations can mitigate the risks for unlawful data access by deploying their own vendor-neutral security solution data pseudonymization and managing access credentials to satisfy the EDPB requirements for lawful transfer of EU pseudonymized data.

A final motivation for opting for a vendor neutral security solution is to address the scenario when cloud providers are obliged by law enforcement agencies to permit access to customer data. If you are the owner of your own security, the provider does not have access to any keys or credentials that would permit any requesting entity to gain access to your data.

The concept of Bringing-Your-Own-Security (BYOS) in the cloud is essential considering both the initiatives by certain countries to introduce “backdoors” into end-to-end encryption, protecting the privacy and confidentiality of personal data, and the terms and conditions for using cloud services and platforms.

For example, the AWS contractual clauses mention the following⁴ :

“Disclosing the minimum amount necessary: We also commit that if, despite our challenges, we are ever compelled by a valid and binding legal request to disclose customer data, we will disclose only the minimum amount of customer data necessary to satisfy the request.”

1 Brian Hengesbaugh, CIPP/US, What Privacy Shield organizations should do in the wake of ‘Schrems II’, <https://iapp.org/news/a/what-privacy-shield-organizations-should-do-in-the-wake-of-schrems-ii/>

2 Gary LaFever, Magali Feys, ‘Schrems II’: How to protect against liability when using non-EEA vendors, <https://iapp.org/news/a/schrems-ii-how-to-protect-against-liability-when-using-non-eea-equivalency-country-vendors/>

3 Amazon’s Standard Contractual Clauses (SCC): <https://aws.amazon.com/blogs/security/aws-and-eu-data-transfers-strengthened-commitments-to-protect-customer-data/>, Google Cloud: https://services.google.com/fh/files/misc/gsuite_foredu_whitepaper_gdpr_schremsii.pdf, Microsoft Azure: <https://blogs.microsoft.com/eupolicy/2020/07/16/assuring-customers-about-cross-border-data-flows/>

4 Stephen Schmidt, AWS and EU data transfers: strengthened commitments to protect customer data, <https://aws.amazon.com/blogs/security/aws-and-eu-data-transfers-strengthened-commitments-to-protect-customer-data/>

4 Tangible benefits of shared security model

The shared cloud security model is a concept that helps businesses and organizations adopt industry best practices for separating the protection of their data in the cloud from the other services offered by the cloud provider. In fact, the greater the segmentation of duties, the better the security you can offer your data.

Segmentation of duties by adopting a vendor-neutral solution covers both the protection of encryption keys and the authentication and access mechanisms to access corporate data. There are some tangible benefits that stem from separating security in the cloud from the service provider.

Better to be independent from service providers for breach mitigation

During the Congressional hearings for the SolarWinds attack, many participants elaborated that the use of different methodologies or technologies, independent from the cloud service provider, can eliminate a considerable threat vector and introduce greater obstacles for adversaries. Considering that adversaries seek to exploit vulnerabilities to let them into networks and move laterally undetected, increasing the level of difficulty in doing so acts as a deterrent. Cloud service providers provide great infrastructure, services, resources and apps but wrapping BYOS around these is considered to be best security practice in this scary new world.

Tip 1

Use a specialist identity and access management (IAM) solution supporting a wide range of authentication techniques to create a barrier to your networks and data, should your cloud service provider get compromised.

Select the solution that allows you to maintain regulatory compliance now and tomorrow.

The patchwork of privacy and data protection requirements requires businesses to adopt solutions to provide the required flexibility to operate under various jurisdictions. Segregating duties and opting for authentication and key management solutions that meet the specific operating and compliance requirements of your organization is the best practice for mitigating unlawful processing of personal data.

Tip 2

Select a neutral IAM solution and a Hardware Security Module (HSM) platform that meet your business needs and your regulatory framework. Pay special attention to data sovereignty and protection contractual clauses.

Control your own security.

Deploying your own, neutral solution allows you to maintain a centralized, flexible control of your access security, keys, and data. Reducing the reliance, and placing less trust on your cloud service provider, results in a reduced threat surface, and decreased potential of lateral damage because of attacks on the provider.

Tip 3

Opt-in for a security solution for authentication and key management that allows you to manage your corporate security centrally and flexibly.

Avoid the dangers of vendor lock in.

Opting for a native security solution entails the danger of vendor lock in. Vendor lock in presents risks from a commercial, regulatory and threat perspective, which may increase the overall risk environment. As businesses are looking to reduce their exposure to business risks and increase resilience, segregation of duties is the best practice for strengthening their security and privacy posture.

Tip 4

Segregate your security duties from your cloud service provider and opt-in for specialist IAM and HSM solutions to increase your overall business resilience.

The benefits of Thales agnostic security

Thales is a world leader in providing vendor agnostic security solutions to help you protect your assets and data wherever they are – on-premises or in the cloud. Thales SafeNet Trusted Access lets you keep control of your access security and averts the risks of vendor lock-in.

- Maintain flexibility: IT managers can maintain flexibility by using any user directory, while strengthening business continuity by ensuring interoperability throughout multi-cloud deployments.
- Reduce your threat surface: The CISO can reduce the attack surface and strengthen corporate security posture by separating access security from apps and data, limiting the scope of lateral attacks within corporate networks.
- Future proof against emerging regulations: Regulations are emerging and changing rapidly. By controlling your access security you will be able to future-proof against emerging regulations on data privacy and data sovereignty and reduce the risk of third parties accessing sensitive corporate data.
- Ensure commercial leverage: CFOs gain flexibility and can achieve a strong negotiating position when it comes to renewals and licenses by adopting a multi-vendor strategy.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

THALES

Building a future we can all trust

Contact us

For all office locations and contact
information, please visit
cpl.thalesgroup.com/contact-us

> cpl.thalesgroup.com <




PROFESSIONAL DEVELOPMENT

Listing of Courses by Wissen International




EC-Council Training and Certifications For AiSP Members

Besides attending EC-Council training and certification courses at local authorised training partners, AiSP members can now enjoy alternative learning options with members-only discounts!

C EH CERTIFIED ETHICAL HACKER	C ND CERTIFIED NETWORK DEFENDER	C CISO CERTIFIED CHIEF INFORMATION SECURITY OFFICER	C HFI COMPUTER HACKING FORENSIC INVESTIGATOR	C PENT CERTIFIED PENETRATION TESTING PROFESSIONAL	E CES CERTIFIED ENCRYPTION SPECIALIST
DARK WEB	MALWARE & MEMORY	MOBILE FORENSICS	ICS/SCADA CYBER SECURITY	R M RISK MANAGEMENT	Web Application Hacking and Security
C TIA CERTIFIED THREAT INTELLIGENCE ANALYST	C ASE Certified Application Security Engineer (Net)	C BP CERTIFIED BLOCKCHAIN PROFESSIONAL	E DRP DISASTER RECOVERY PROFESSIONAL	E CIH CERTIFIED INCIDENT HANDLER	C SA Certified SOC Analyst

 <p>Members enjoy 20% discount</p> <p>Self-Paced Learning with Videos</p> <p>Asynchronous, self-study platform with pre-recorded training videos, official e-courseware, virtual lab for hands-on practice and remote proctored exams. Please visit https://iclass.eccouncil.org/our-courses/ for more course details.</p>	 <p>Students enjoy academic price</p> <p>Self-Paced Learning without Videos</p> <p>Applicable for current students enrolled with AiSP Academic Partner institutions who are studying relevant courses.</p>	 <p>Contact us for member's rate</p> <p>Masterclass Training Workshop</p> <p>Attend a face-to-face or online LIVE instructor-led training course specially conducted for Certified CISO, CEH Practical, ECSA Practical, etc.</p>
--	--	--

More EC-Council Products for AiSP Partners!

 <p>CyberQ</p> <p>Cyber range Platform-as-a-Solution TRAIN PRACTICE ASSESS COMPETE</p>	 <p>EC-Council aware</p> <p>When Everyone Protects</p> <p>Phishing simulation, cyber awareness e-learning platform and mobile app</p>	 <p>codered FROM EC-COUNCIL</p> <p>Learn on-the-go subscription platform for Premium Cybersecurity courses</p>
---	--	--

Brought to you by Wissen International, EC-Council's exclusive distributor. Email us for more info aisp@wissen-intl.com

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

Date 13-17 December 2021

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

Register your interest here: <https://forms.office.com/r/Ab0MKfgQXg>

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

Date 22-24 November 2021

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

Register your interest here: <https://forms.office.com/r/SQuHCcifKS>

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: 2020\1 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.

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

BCG

 BitCyber
Securing Your Business

 BD

 Checkmarx

 CISCO

 DBS

 ENSIGN
INFOSECURITY
CONQUER
THE UNKNOWN

 ExtraHop

 FIRE EYE™

 FORTINET®

GOVTECH
SINGAPORE 

 HUAWEI CLOUD
Grow with Intelligence

 ITSEC
ASIA

 IBM®

 INSIGHTZ
TECHNOLOGY

kaspersky

 Marsh



 MICRO
FOCUS®

 MINDEF
SINGAPORE

Privasec

 Responsible
Cyber

 SecurID™
An RSA Business

 ST Engineering

 TANIUM®

 ThriveDX
Formerly Cybint

 TREND
MICRO™

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

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

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

Our office is closed. We are currently telecommuting.
Please [email](mailto:secretariat@aisp.sg) us during office hours.