

News & Update

- Knowledge Series
- CAAP
- AiSP SME Cyber Conference
- SVRP
- SCSIA
- Ladies in Cyber
- Special Interest Groups
- CREST Singapore
- The Cybersecurity Awards
- Upcoming Events

Contributed Contents

- Protection Against Ransomware to Comply with Data Protection Law
- Huawei Cloud Cybersecurity
- Cisco top 5 practices that organizations can use to up-level their cybersecurity programs
- Trend Micro 2022 Security Predictions
- Top Myths about Zero Trust
- Enhancing Operational Technology Security in Asia Pacific
- TCA 2020 Winner – Dr Steven Wong

Professional Development

Membership



NEWS & UPDATE

New Corporate Partners

AiSP would like to welcome Cyber Security Agency of Singapore (CSA), Centre for Strategic Infocomm Technologies (CSIT) and Recorded Future as our new Corporate Partners. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem.



Continued Collaboration

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



Knowledge Series Events

Cyber Threat Intelligence on 1 Dec 21

On 1 Dec 21, we had our first Hybrid event since the last time restrictions were imposed. We had Mr Andrew Ong, Ms Yvonne Wong, Mr YC Lian and Dr. Guy Almog as well as Mr Ray Koh sharing on issues with Cyber Threat Intelligence which was the key topic for the day.

We would like to thank Cyberint for supporting the event!



Data Security on 27 January 2022

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



AiSP Knowledge Series – Data Security



KNOWLEDGE SERIES
DATA SECURITY
3PM-5PM | Zoom

JAN 27

AARON ANG
APAC Project Manager & Trainer
ThriveDX SaaS

CHOW LAI LENG
Head of Enterprise - SEA
Kaspersky



Organised by:



Supported by:




As part of AiSP Knowledge Series, we have ThriveDX SaaS and Kaspersky with us to share about data security. The global COVID-19 pandemic has accelerated the pace of digital transformation. Businesses are creating, processing, and storing more data than ever before. Cybercriminals are also ramping up their campaigns targeting businesses. Building cybersecurity foundation is now a priority instead of an option. Join us as we learn about mitigating risk factor as well as integrating cybersecurity in your digital transformation journey.

Data Security – Patching the Human Firmware
By: Aaron Ang, APAC Project Manager & Trainer, ThriveDX SaaS

The global COVID-19 pandemic has accelerated the pace of digital transformation and have forced many of us to change the way we live, work and play. Businesses are also creating, processing and storing more data than ever before. In addition,

today's sophisticated computing environments spanning public and private clouds, on-premise infrastructure, remote endpoints, Operational Technology (OT) systems and Internet of Things (IoT) devices have made securing data an increasingly complex challenge. With the myriad of data protection technologies and solutions in our cybersecurity ecosystem today, the human factor remains the weakest link in the data protection strategies of many organizations.

Come join us at this session to learn how organizations can mitigate the human risk factor and secure their data by patching the human "firmware".

Building a cybersecure and sustainable future for SMBs in Singapore

By: Chow Lai Leng, Head of Enterprise – SEA, Kaspersky

Businesses have rapidly modernized to meet the needs of our digital age. The last two years also proved that technology is an essential tool to survive and even break through from this pandemic and beyond. Fast-tracked digitalization, however, comes with its fair share of cyber risks. As businesses shift major processes and billions of data online, cybercriminals are also ramping up their campaigns targeting businesses in every size and sector. As such, building cybersecurity foundation is now a priority instead of an option.

Join us in this session to know how to integrate cybersecurity in your digital transformation journey and to understand how you could better secure your business as you prepare for a post-pandemic recovery.

Date: 27th January 2022 (Thurs)

Time: 3PM to 5PM

Venue: Zoom

Registration: https://zoom.us/webinar/register/WN_LoYd6XryS0WNvxTG3jGcuQ

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. Data Security, 27 Jan 22
2. Red Team VS Blue Team, 17 Feb 22
3. Cryptography, 17 Mar 22
4. Cloud Security, 13 Apr 22

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

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

Cybersecurity Awareness & Advisory Programme (CAAP)

Upcoming CAAP Event

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

AiSP x ASPRI – Cybersecurity Best Practices & Data Privacy Risks



BACKGROUND

Following the launch of the Process Construction & Maintenance (PCM) Industry Digital Plan (IDP) last year, the Association continues to advocate for the adoption of digitalisation. With most digital tools available online, there is an increased dependency on the Internet to perform day-to-day operations. While the nation is advanced in Internet connectivity than ever, the industry's cybersecurity practices are still falling short.

WEBINAR OVERVIEW

To address the cybersecurity concerns and raise awareness of the industry, ASPRI has collaborated with the Association of Information Security Professionals (AiSP) to organise a webinar on 26 January 2022, 10:00am to 11:30am. The webinar aims to provide insights into the best cybersecurity practices and how to manage data privacy risks.

PROGRAM SCHEDULE

Time	Agenda
10:00am	Introduction by ASPRI
10:05am	Presentation 1: The best cybersecurity practices for companies to follow during the rise of cyber threats The PCM industry is in a digitisation period where traditional, legacy operates in modern times. While the industry is advanced in internet connectivity than ever, the cybersecurity practices are still falling short. This presentation will share with you a high level understanding cybersecurity awareness and best practices for you. Speaker: Faith Chng, EXCO Member, AiSP
10:40am	Presentation 2: Protecting Your Data - Managing Data Privacy Risks Cyber criminals are devising better ways to penetrate network defences to steal data for commercial gains. The government is stepping up Data Privacy and Data Protection regulations to get companies to do a better job in protecting their citizen's sensitive data. For example, Singapore's Personal Data Protection Act (PDPA) has raised the fines in its recent amendments. In this challenging environment, how can your company protect your data and manage your data privacy risks in a cost effective manner? Speaker: Phillip Ng, Co-founder and CEO, BitCyber
11:10am	Sharing of Cybersecurity Courses
11:15am	Q&A Session
11:30am	End of Webinar

Speakers' Profiles



Ms Faith Chng
EXCO Member
AiSP

Faith is a mathematics NUS graduate with about 20 years of experience in IT and telecommunications industry handling sales, marketing and product. She has been handling cybersecurity product since 2012 with primary role in vendor management, product marketing and product management.

She has worked with managed security services provider and productised end to end services for enterprises. End to end cybersecurity services includes training, network and risk compliance assessments, managed security services, incident responses, holistic architecture design, consolidated IT Security solution, etc.



Mr Phillip Ng
Co-founder and CEO
BitCyber

Philip co-founded BitCyber with a vision to simplify cybersecurity in this age of digital transformation. An IT veteran who has built a successful career in cybersecurity and hybrid cloud technologies, Philip has held GM roles at public listed companies Achieva & Frontline, and senior sales leadership roles at MNCs Symantec, NetApp, British Telecom, Sun Microsystems, HP, and Unisys. He has also been an Angel investor since the Dot.Com period and is always on the lookout for promising young entrepreneurs.

Being a father of 3, Philip is naturally very concerned about the online dangers that children face in today's highly connected world of social media. Philip is making it his mission to make cyber defence accessible to every person and to promote cyber awareness to make the world a safer place.

Click [here](#) to register

[back to top](#)

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 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 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.

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.

The conference will be held in a hybrid format with the following details:

Date: 7 January 2022 (Friday)

Time: 10:00 am – 4:00 pm

Venue: Lifelong Learning Institute

Join us in the launch on the AiSP SME Cyber Safe portal to provide an online sitemap for Businesses & individuals in terms of Cyber Awareness Maturity Journey and AiSP CAAP E-Learning Modules. Join us to get a 1month free trial on the E-Learning materials and videos. 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.

Agenda:

Key Highlights

Welcome Address by AiSP

Mr Johnny Kho, President,
Association of Information Security
Professionals (AiSP)



Opening Address by GOH

Ms Gwenda Fong, Assistant Chief Executive
(Policy & Corporate Development),
Cyber Security Agency of Singapore



**Sharing by AiSP & Launch of CAAP
E-Learning & AiSP SMECyberSafe
website**

Mr Tony Low, CAAP Lead, Association of
Information Security Professionals (AiSP)



**Cybersecurity is key to a secure
and trusted business in the digital
environment**

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 both small and large organisations facing increased exposure to cyber risks. Join us in this sharing by the Cyber Security Agency of Singapore (CSA) to find out how organisations can strengthen cybersecurity to safeguard their businesses.



Lunch & Viewing of Booth

**Prepare Today for Tomorrow's
Challenges**

Alvin Teo, Technical Customer Success
Manager, ONESECURE Asia

The rapid switch to a distributed workforce expanded well beyond the traditional corporate perimeter and effectively ended the firewall era, making IT hygiene more important than ever. As you will discover, endpoint visibility and vulnerability management is critical to protecting all levels of the security stack.



Block Evolving Email Threats

Thomas Wee, Senior Technical Consultant,
Green Radar

Overall email threats are on the rise, as attacks initiated via email continue to be inexpensive and effective method for fraudsters. Phishing emails are increasingly well designed, elaborate and using sophisticated techniques. Email security technologies struggle to identify social engineering, making Business Email Compromise (BEC) attacks a key threat in the near term. Malware Among email attacks that used malicious document attachments, Exploit.MSOffice family is the most frequent malware spread by spammers. Green Radar, a Next generation Managed Security, Security-As-A-Service, with local Security Operations Centre (SOC) and local threat hunting team, provide gsmail™ monitoring services powered by aids™ (AI-Detection, Analytics and Response) allow business to focus on their core business, ensuring any clean emails are delivered to their organisation.



**Managing Identity and Access with a
Dynamic Workforce**

Charles Lim, APJ Commercial Director for
SecurID, an RSA Business

The session will cover the current market trends and how identity and access management (IAM) is at the front and centre of these market trends. Organisations are going through digital transformation and tackling critical business initiatives like moving to the cloud, adopting a zero trust security model, implementing an identity assurance solution and many more. The session will also discuss how identities and accesses are being addressed given the diverse workforce that organisations are embracing.



**Simplify Business Security, Without
Sacrifice**

Andrew Moey, Business Development,
Fortinet SEAHK

As businesses continue to consume more technology to be more effective and productive, businesses also undertake higher risks from advance security threats.

Simplifying security does not mean having to live with mediocre protection. Having a sound security strategy will take your Business a long way.



**Strengthening Cybersecurity Awareness to
Defend Against The Increased Cyber Threats**


Alvin Teo
ONESECURE Asia


Thomas Wee
Green Radar


Tony Low
AiSP
Moderator


Charles Lim
SecurID


Andrew Moey
Fortinet

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

Organised by Supported by



Sponsors



Supporting Partners



[back to top](#)

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:



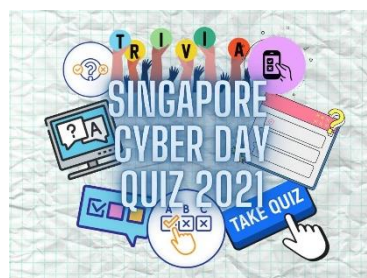
Singapore Cyber Security Inter Association (SCSIA)

Singapore Cyber Day Quiz 2021

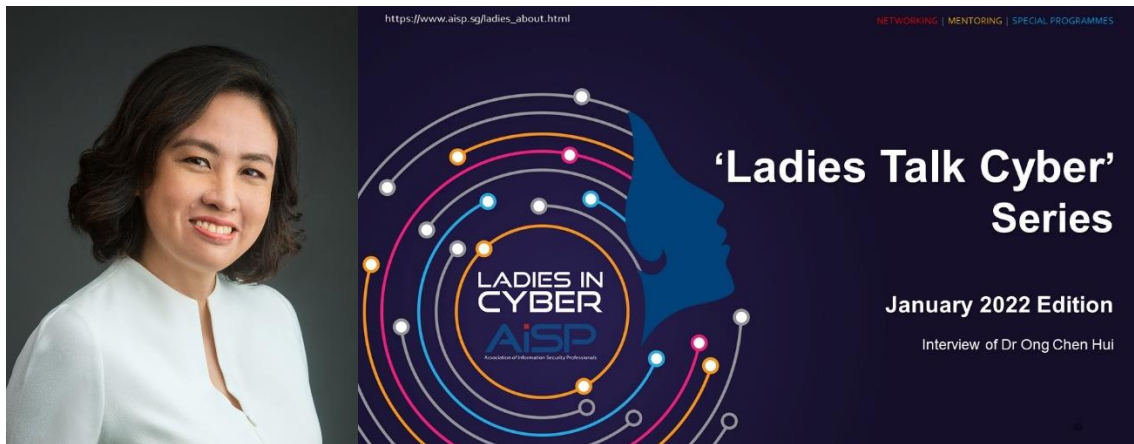
Singapore Cyber Day Quiz was held throughout the month of December for the students (Singaporean or PR) to take part in during the December school holidays. The online quiz competition was opened to primary, secondary and tertiary students (aged 25 years and below) in Singapore with the support from Cyber Security Agency of Singapore & Fortinet. This competition aims to pique interest in students and equip them with knowledge on Cyber Security.

The quiz has officially ended on 29 December 2021 and the results will be released soon. Prize presentation will be held in January 2022 at Fortinet. Winners will be contacted during the 1st week of January.

Thank you for your support and participation!



Ladies in Cybersecurity



Ladies Talk Cyber Series

For the Eighth edition of AiSP's 'Ladies Talk Cyber' series, we interviewed Dr Ong Chen Hui, AiSP EXCO Nominated Member representing IMDA & Cluster Director of Business Technology Group in IMDA where she oversees IMDA's efforts in developing the industry and research ecosystem around emerging technologies such as AI, Future Communications including 5G, and Trust Technologies.

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

I am Chen Hui, the Cluster Director of Business Technology Group in IMDA, where I oversee IMDA's efforts in developing the industry and research ecosystem around emerging technologies such as AI, Future Communications including 5G, and Trust Technologies. I am also the chair of Singapore Women-in-Tech and in the Exco of Association of Infocomm Security Professionals.

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



AiSP Ladies in Cyber Learning Journey & Fireside Chat 21 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.

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.

Date: 21 January 2022

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

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

An event poster with a dark blue background and a subtle globe graphic. At the top, it lists 'JOINTLY ORGANISED BY:' with logos for AiSP and Ladies in Cyber, 'SUPPORTED BY:' with the Cisco logo, and 'AS PART OF' with the CSR Singapore logo and 'SG CYBER WOMEN X SERIES'. Below this are four portrait photos of the speakers: Ms Sim Ann, Ms Wendy Ng, Ms Catherine Lee, and Ms Sherin Y Lee. Under each photo is their name and title in white text.

JOINTLY ORGANISED BY: AiSP | LADIES IN CYBER

SUPPORTED BY: CISCO

AS PART OF: CSR 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

AiSP Ladies in Cyber Inaugural Symposium - 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 in March 2022 at Life-Long Learning Institute with Minister Mrs Josephine Teo as the Guest of Honour as part of International Women Day 2022 Celebrations. 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



Special Interest Groups

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

- Cloud Security
- 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. If you are keen to be part of a SIG, please contact secretariat@aisp.sg



CREST Singapore

From 1 January 2022 onward, CREST International will manage Singapore's exam directly. Please contact singapore@crest-approved.org for more information on CREST examination in Singapore.

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 on 14 January 2022.

Please email us (secretariat@aisp.sg) if your organisation would like to be our sponsors for The Cybersecurity Awards 2022! Limited sponsorship packages are available.

TCA2021 Sponsors & Partners

THE CYBERSECURITY Awards 2021

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

Supported by: **CSA SINGAPORE**

Platinum Sponsors: BeyondTrust, CISCO, ENSIGN INFOSECURITY, HUAWEI, ST Engineering, TREND MICRO

Gold Sponsors: CyberProof, CSTI (Centre for Strategic Information Technologies), DBS, kaspersky, Singtel, wizlynx group

Silver Sponsors: PCS SECURITY, RSA, SIT (SINGAPORE INSTITUTE OF TECHNOLOGY), THALES, wsg (Workforce Singapore)

Supporting Associations: CSCIS, CSA cloud security alliance, HTCIA, ISACA (Singapore Chapter), OFFICIAL CHAPTER (ISC) SINGAPORE, SINGAPORE COMPUTER SOCIETY, SGTECH, SINGAPORE SOCIETY OF INFORMATION SECURITY

Community Partner: image engine

Supporting Organisation: SFA (SINGAPORE FEDERATION OF RESEARCH)

Upcoming Activities/Events

Ongoing Activities

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

Upcoming Events

Date	Event	Organiser
7 Jan	SME Cybersecurity Conference	AiSP & Partner
14 Jan	TCA Awards Ceremony 2021	AiSP
19 Jan	SVRP Awards Ceremony 2021	AiSP
20 Jan	ICT Supply Chain Resilience Kaspersky Asia-Pacific Online Policy Forum IV	Partner
21 Jan	LIC Learning Journey to CISCO	AiSP & Partner
26 Jan	AiSP x ASPRI CAAP Workshop	AiSP & Partner
27 Jan	Knowledge Series – Data Security	AiSP & Partner
28 Jan	Cyber Day 2021 Quiz Prize Presentation	AiSP & Partner
17 Feb	Knowledge Series – Red Team, Blue Team	AiSP & Partner
23 Feb	CISCO x SCCCCI CAAP Event	AiSP & Partner
25 Feb	The Cybersecurity Awards 2021 Judges Appreciation	AiSP
3 Mar	AiSP CTI SIG Event	AiSP
4 Mar	Your Mind Matters (Y2M) with AiSP	AiSP & Partner
8 Mar	International Women Day 2022 Celebrations	AiSP
16 Mar	Knowledge Series – Cryptography	AiSP & Partner
Mar	Ladies in Cyber Symposium	AiSP & Partner

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

CONTRIBUTED CONTENTS

Article from Data & Privacy SIG

Protection Against Ransomware to Comply with Data Protection Law

In 2021, Singapore's Personal Data Protection Act (PDPA) was amended to include mandatory data breach notification requirements. It is now an offence not to notify the affected individuals, if certain conditions are met, and the Personal Data Protection Commission (PDPC) (refer to Section 26A to 26E of PDPA for more information on these requirements).

Successful ransomware attacks will result in unauthorised modification or disposal of sensitive data, such as personal data, and possible unauthorised exfiltration of such data. Hence, ransomware attacks on personal data is a notifiable data breach.

A common misinterpretation is that as long as there is no detected exfiltration of personal data, one does not need to report successful ransomware attacks on personal data to PDPC. This attitude is akin to playing Russian roulette, as one is trying to avoid the long arm of the law by hiding the fact of successful ransomware attacks. If ever such attacks are made known to the authorities, your organisation will be facing additional charges of breaching the mandatory data breach notification requirements on top of breaching the protection requirements. In other words, your organisation could effectively be held ransom, in a different form, by disgruntled personnel who are aware of such non-compliance with the law.

In summary, to protect your organisations against ransomware attacks, the following security controls are recommended:

1. Business Continuity Planning

- a) Develop Business Continuity Plan(s) (BCP) with measures to minimise impact to their operations in the event of an ransomware attack.
- b) Conduct regular BCP exercises should be performed with operational departments and key decision-makers to ensure every stakeholder is familiar.
- c) Update the BCPs when there are important changes in assets or stakeholders.

2. Incident Response Planning

- a) Develop Incident Response Plan(s) (IRP) and playbooks, with explicit coverage of ransomware attacks.
- b) Regular IRP exercises should be performed with operational departments and key decision-makers to test the plans and playbooks before a ransomware attack.
- c) Update the IRPs when there are important changes in assets or stakeholders.

[back to top](#)

3. Backups

- a) Identify critical data and prioritise their protection.
- b) Develop comprehensive backup and recovery plans for critical data.
- c) Maintain clean “golden images” of your critical systems allows you to rebuild or recover the critical system in a timely manner.
- d) Have offline or disconnected backups also ensure the viability of the backups of critical data during a ransomware attack since ransomware is known to transmit over networked storage devices.

4. Access Controls

- a) Control and limit privileged access to only authorised individuals who require full access to carry out their work.
- b) Implement multi-factor authentication for such administrative privileges.
- c) Give users, other than the administrator, the lowest user privileges necessary for work.
- d) Review and manage the use of all user accounts and disable inactive accounts when they are no longer in use.

5. Data Encryption

- a) Encrypt critical data to protect their confidentiality in the event they are stolen in a ransomware attack.

6. Patch Management

- a) Update systems, applications and software to the latest version and ensure that security patches are applied in a timely manner, especially for business-critical functions.

7. Network Security

- a) Implement network segmentation to reduce contagion effect across the different segments in the network in the event of a ransomware attack.
- b) Monitor their networks and systems closely for suspicious activities, for e.g. monitor and block any suspicious inbound/outbound connections with known malicious IP addresses and URLs, suspicious scanning activities and unauthorised login attempts.

8. Anti-Malware Protection

- a) Install anti-virus/anti-malware software and keep the software (and its definition files) updated.
- b) Perform regular anti-malware scans of your systems and networks, at least once a week.
- c) Removable storage devices should be scanned upon connection.
- d) Scan all received files for presence of malware, for e.g. received via email or downloaded from the Internet.
- e) Explore the use of signature-less endpoint protection solutions, such as Endpoint Detection and Response (EDR) or User Entity and Behaviour Analytics (UEBA), to defend against zero-day ransomware attacks.

9. Application Control

- a) Implement application controls to allow only whitelisted applications to run.
- b) Enable Microsoft Office macros only when required and disable macros by default.
- c) Do not allow the use of ActiveX controls.

10. User Awareness Training

- a) Conduct regular training to raise employees' awareness of cyber threats such as phishing emails and malicious websites.

11. Secure Configuration Audit

- a) Review configuration settings for any exposed services and open network ports to ensure there are no exposed or vulnerable remote administration services such as SSH, RDP, SMB and WMI ports.

With the above recommended controls, your organisation will be in a better position to prevent and to mitigate against potential ransomware attacks.

Have a cyber-safe 2022!

About the Author



Wong Onn Chee
Data & Privacy SIG Lead
Association of Information Security Professionals, Singapore

Onn Chee is currently working as the Chief Executive Officer of Rajah & Tann Cybersecurity and the Technical Director of 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 (<http://www.wipo.int>), 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.

Article from our CPP Partner, Huawei



HUAWEI CLOUD Cybersecurity

Trust Center

HUAWEI CLOUD makes trustworthiness the most important aspect of product quality. We are building a globally credible public cloud featuring security, compliance, privacy, transparency, and resilience.

*"Stands out with robust security and ALM capabilities. Huawei provides broad security coverage, such as escape prevention and traffic control over different layers."
(The Forrester New Wave™: Public Cloud Enterprise Container Platforms, Q3 2019)*

<p>Trust White Paper HUAWEI CLOUD Releases the Industry's First White Paper on Trustworthiness</p> <p>Learn More</p>	<p>Privacy White Paper Safeguard strict service boundaries, helping customers protect privacy.</p>	<p>Security White Paper Learn from our extensive experience with cloud security. Make the security industry more open and develop better.</p>	<p>Data Security White Paper Learn about our best practices, and experiences in the data security field and throughout the industry.</p>
<p>Containers Enter the Strong Performer Quadrant "Huawei provides broad security coverage, such as escape prevention and traffic control over different layers." (Forrester, Public Cloud Enterprise Container Platforms, Q3 2019)</p>		<p>First Provider Qualified for Information Security HUAWEI CLOUD was one of the first companies to obtain information security service qualifications (cloud computing security, level 1) from CNITSEC.</p>	



Scan QR to Download
Key Information White Paper

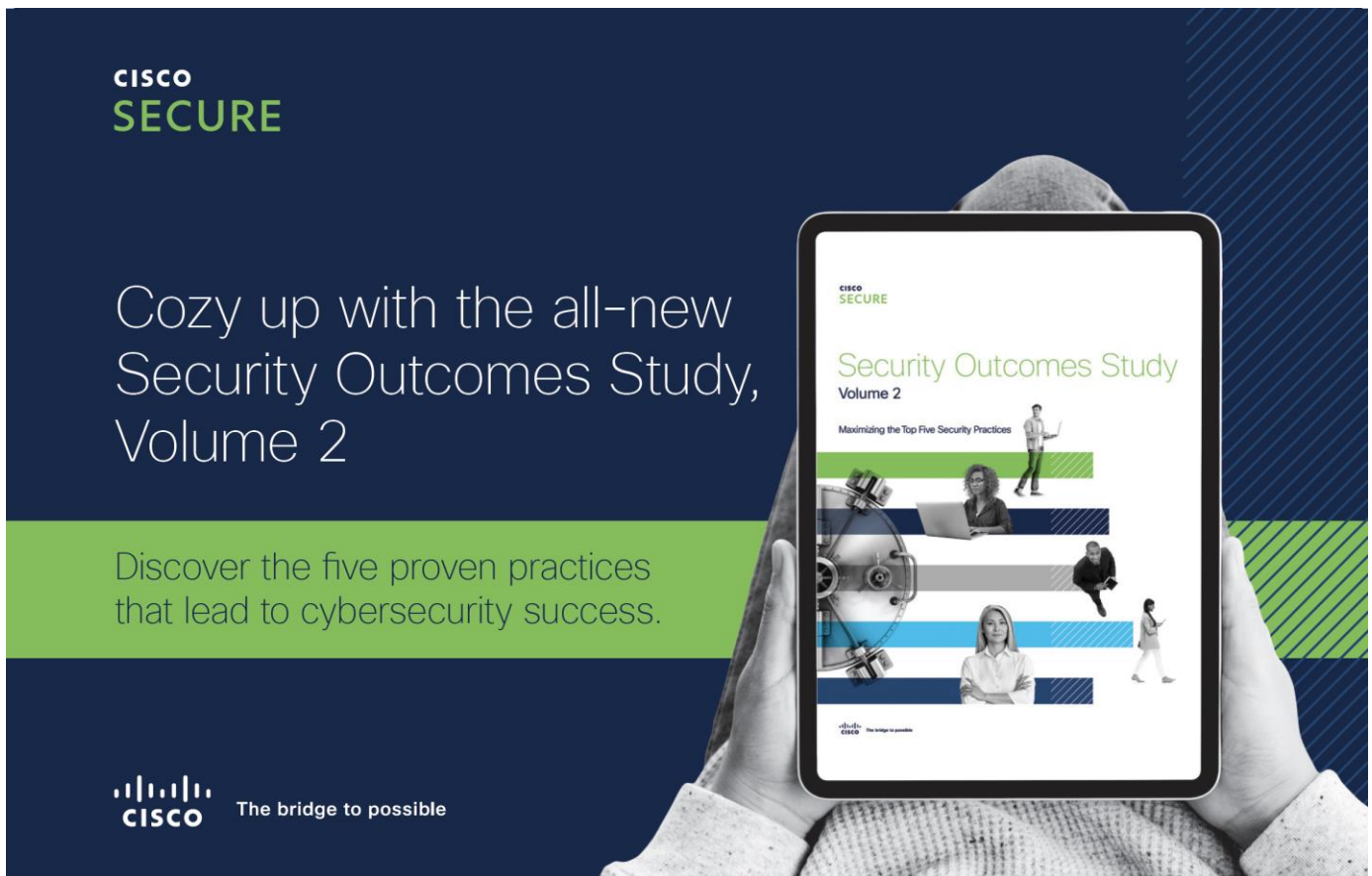
We place trustworthiness above all else, over functions, features, or the product schedule.

— Ren Zhengfei



Article from our CPP Partner, Cisco

Cisco's latest cybersecurity research explores the top 5 practices that organizations can use to up-level their cybersecurity programs

A promotional graphic for the Cisco Secure Security Outcomes Study, Volume 2. The background is dark blue with a green and white striped pattern on the right. A person's hands are holding a tablet displaying the study's cover. The cover features the Cisco Secure logo, the title 'Security Outcomes Study Volume 2', and the subtitle 'Maximizing the Top Five Security Practices'. The cover art includes icons of a person at a laptop, a person sitting on a step, and a person walking, set against a background of horizontal bars in green, white, and blue. The Cisco logo and tagline 'The bridge to possible' are at the bottom left of the graphic.

**CISCO
SECURE**

Cozy up with the all-new
Security Outcomes Study,
Volume 2

Discover the five proven practices
that lead to cybersecurity success.

CISCO The bridge to possible

What if you could build a successful, world-class security program with just five practices?

And what if shifting focus to these areas could put your security program ahead of 79% of other organizations? Our latest cybersecurity research study suggests that this is not only true but is also a tangible reality for organizations that choose to follow some practical steps.

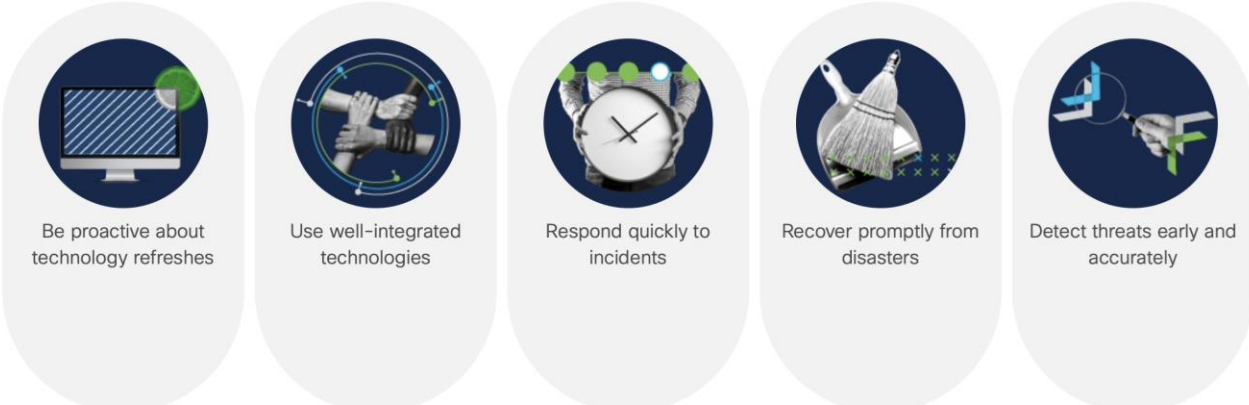
The Security Outcomes Study, Volume 2. This vendor-agnostic cybersecurity research report offers a data-driven understanding of how you can achieve success in your own security programs. Plus, get some insight into how cybersecurity professionals are performing across industries.

[back to top](#)

The data doesn't lie. Through this rigorous cybersecurity research, we can specifically point to how these five data-backed practices can bolster your cybersecurity programs and help you achieve better outcomes. This report should be a trusted friend of any IT and security professional that will answer some of their most critical questions.

Top 5 cybersecurity practices

According to our research, the five key drivers of cybersecurity program success are:



- Be proactive about technology refreshes
- Use well-integrated technologies
- Respond quickly to incidents
- Recover promptly from disasters
- Detect threats early and accurately

Cisco Secure wants to partner with organizations in building the strongest cybersecurity practices on the planet. And our hope is that, through this report, organizations can determine which next steps must be taken to get from point A to point B.

Start your journey today by reading the full

[Cisco Security Outcomes Study, Volume 2](#)

Article from our LIC Symposium Partner, TrendMicro



[Trend Micro 2022 Security Predictions](#) outlines the security issues that they predict will shape the threat landscape of 2022, and provide recommendations to keep organizations protected.

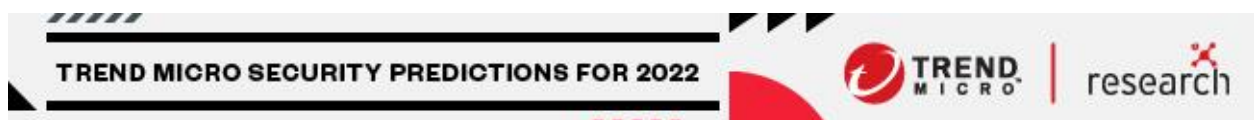
[Download Report](#)

The global pandemic has pushed organizations to swiftly modify their processes and operations to adapt to a landscape that has undergone drastic changes. In 2022, the landscape will still be in flux. But organizations will attempt to further drive progress with the trends and technologies that they have embraced since the pandemic began.

Here are several developments that enterprises can anticipate in the year ahead:

- **Malicious actors will continue to think of SMBs as easy prey, but cloud-heavy SMBs will come prepared with security measures that can fend off commodity attacks.**
- **As they focus on making their supply chains more robust via diversification and regionalization, enterprises will implement zero trust principles to stay secure**
- **To remain protected against evolving ransomware threats, enterprises will set their sights on protecting their servers with stringent server-hardening and application control policies.**

Trend Micro's report, [Toward A New Momentum: Trend Micro Security Predictions for 2022](#), offers valuable insights and security recommendations to help organizations make informed decisions that can shore up their defenses and mitigate threats in the coming year.



Article from our SME Sponsor, SecurID



BLOG

Top Myths About Zero Trust

 SecurID

Zero Trust is more than just a catchphrase or flavour of the month. It is a legitimate cybersecurity response to methods of attack that have evolved to circumvent perimeter-based network controls. The Zero Trust methodology is accurately described as exactly that – a methodology or philosophy that starts with a simple concept: never trust, always verify.

In the real world this is a lot harder to do than say. Legacy systems, remote access, cloud-based applications and a myriad of unmanaged devices all intersect to increase the difficulty for many organisations to begin adopting Zero Trust architecture and its supporting methodologies.

Notice what I said there: methodologies, architecture. I didn't actually mention a product. Don't let anyone tell you differently: the first myth about Zero Trust is that if your business buys this product or installs that software, then you'll have everything you need. The truth, as always, is caveat emptor: Zero Trust is not a product. It's more accurate to say Zero Trust is a philosophy that is bolstered by certain products together with their deployment characteristics, their architecture, and tied together by an overarching philosophy. Zero Trust is actually not a product at all, although there are many products out there that will legitimately help your organisation adopt a Zero Trust approach that makes sense for you.

Secondly: I've heard many times from organisations that they are adopting "a Zero Trust product" and therefore no longer require strong authentication or multifactor authentication (MFA). This is also a misinterpretation on many levels of what a Zero Trust modality can offer the organisation. "Never trust, always verify" extends not only to the endpoints, the unmanaged devices, the downstream applications and network access.

[back to top](#)

It includes users too. Always verify your users during access decisions and especially when their (sometimes unique) privilege is part of that access! In my opinion, MFA and zero trust go hand-in-hand.

Finally, another cornerstone of Zero Trust (among many) includes the notion of context for users and devices that are being validated. And this is where the question of entitlement comes in. Does the user **require** access to this service, endpoint or application? How would you know? Entitlements management is a tricky problem for the majority of organisations out there, not simply because of the number of users or applications. One tenet of Zero Trust implies that entitlements are not static – they'll be checked **every time** for access and permissions. Identity Management platforms like the [SecurID Governance and Lifecycle](#) (SecurID G&L) provides exactly this in full alignment with the tenets of Zero Trust, either as a managed service hosted in the cloud, or as an on-prem self-managed deployment to help organisations with this very difficult aspiration.

In conclusion, adopting Zero Trust is critical in the face of an eroded modern perimeter. SecurID, an RSA business, fully applauds and supports any organisations that are embarking on this journey.

If you would like to learn more about how we are helping organisations enable their zero trust strategies and more, please contact us at Douglas.Lim@rsa.com

Article from our SME Sponsor, Fortinet

Author: Peerapong Jongvibool, Regional Director, Southeast Asia and Hong Kong at [Fortinet](#)

Enhancing Operational Technology Security in Asia Pacific

The cyber physical world around us is becoming more digitised, which forces organisations to adopt new operational processes to stay afloat. This leads to an increased need for meaningful automated awareness that can address the scale of potential threats associated with the rise in connected cloud security environments within Operational Technology (OT) with Industrial Control Systems (ICS).

With diverse economies and societies, the Asia Pacific region is facing significant challenges when it comes to protecting OT with ICS that powers critical services such as water, power, oil and gas, telecommunications and transportation services. To address the growing complexity and risks, governments within the region are pushing for initiatives that will boost the resilience of critical infrastructures against increasing cyberthreats. In Singapore for instance, the government established the [OT Cybersecurity Masterplan](#) and [Operational Technology Cybersecurity Expert Panel](#) to enhance the security and resilience of the country's critical sector, by tapping on the expertise of stakeholders such as the Government, operators of Critical Information Infrastructure (CII) facilities, and the academic sector to mitigate cyber threats in the OT environment.

The speed of technology-driven innovation is arguably faster than ever, which makes it difficult to enforce security controls continuously. When executing solution strategy to secure OT cloud environments, security teams must be able to address the following challenges:

- **Broad attack surface:** Amid the convergence of information technology (IT) and OT networks, as well as increased cloud adoption, the attack surface continues to broaden exponentially.
- **Cloud misconfigurations:** Building on the broadened attack surface, misconfigured cloud-based resources leave critical OT environments at risk. Malicious actors targeting a misconfiguration when moving laterally within the OT infrastructure can wreak havoc.

[back to top](#)

- **Legacy IT:** Moving legacy hardware and software, which are often decades old, to the cloud means potentially introducing a range of vulnerabilities to the infrastructure. This presents cyber criminals with an opportunity to leverage historical tradecraft to gain access and perform reconnaissance before employing more sophisticated techniques once they have achieved their target.

Establishing a Robust Cloud Security Plan

Proactively protecting ICS is a crucial aspect of successfully mitigating risks in the Fourth Industrial Revolution era. Amid the digitisation of operations, organisations must be able to protect data as it moves back and forth between OT and IT infrastructures. They should weave cybersecurity into their initial plans as new hybrid infrastructures are built and implement centralised network security across the IT and OT environments with a network operations centre (NOC), as well as all applications and platforms within the network.

Moreover, securing the business edge requires an adaptive approach to cloud security that spans across on-premise, multi-cloud, and hybrid infrastructures. As part of the plan, organisations can take a four-pillar approach to their adaptive cloud security strategy to yield continuous earned trust:

- **Zero Trust:** Using intent-based segmentation that interprets business and security requirements, then automatically converts them into a segmentation policy, can help isolate workflows and applications.
- **Security-driven networking:** Integrating network infrastructure with security architecture using an integrated security platform to enable access control and segmentation.
- **Adaptive cloud security:** Connecting resources to protect from multiple threat vectors while leveraging consistent models and integrating with third-party applications.
- **Artificial Intelligence-driven security operations:** Deploying technologies like artificial intelligence (AI) and machine learning (ML) coupled with automated processes can detect and neutralise threats at the speed of business.

Securing Converged IT/OT Environments

Like any infrastructure expansion, the benefits of moving OT to the cloud can outweigh the risks. However, organisations must concurrently implement a robust security strategy to mitigate these potential risks. This requires leveraging automation to improve processes, enhance analytic

accuracy and reduce errors. To secure these IT/OT interconnected layers, organisations must view them as systems within systems and understand the complexity of the infrastructure it supports. Vigilance across the OT architecture must extend from the plant floor all the way up through to the cloud. Foundationally, visibility remains a primary problem to address as firms move toward a digitally transformed IT/OT environment.

These transformational challenges associated with migrating to the cloud can be addressed with the adoption of a platform built around a common operating system and management framework. By doing so, the system can continuously assess risks and automatically adjust to provide comprehensive real-time protection.

Having an integrated cybersecurity platform enables consistent security across the network, provides seamless interoperability and complete visibility, as well as granular control for hybrid deployments.

It enables organisations to build security by design with the broadest set of offerings to maintain the same level of security across their IT and OT network environments. The centralised management system enables OT businesses to configure, manage, and monitor all components, to eliminate silos and provide greater visibility.

Moreover, an integrated security architecture minimises threat detection and response times while also enabling automated incident response for enhanced threat remediation across the extended network.

All of these security solution components work together to ensure safe, sustained operations – a concept that is top of mind across OT and embodies the ICS infrastructure upon which they are built. By identifying and adopting services that provide sustained situational awareness, OT leaders can achieve a sense of omnipresence to protect the transactions of their new cloud businesses.

Article from The Cybersecurity Awards 2020 Winner - Dr Steven Wong



I am extremely honoured to be the recipient of The Cybersecurity Awards 2020 (Leader Category). With the work I have done as well as the impact that it has created being recognised by so many of my peers in the cybersecurity ecosystem really warms the cockles of my heart. However, these achievements would not be possible if not for the great collaborations between everyone in the cybersecurity community, therefore I would also like to take this opportunity to thank everyone for your relentless support.

Quoting one of my fellow AiSP EXCO member who commented, “When Steven inspires, we perspire”. Thus, I really appreciate all the hard work that the AiSP EXCO, secretariat and volunteers put in over the years to eventually bringing some of our ideas to fruition. Together, we have managed to launch some significant initiatives and programmes such as the revamp of the Information Security Body-of-knowledge (IS-BoK), the AiSP Validated Information Security Professionals (AVIP) scheme, the Student Volunteer Recognition Programme (SVRP), the Cybersecurity Awareness and Advisory Programme (CAAP), the Ladies-in-Cyber initiative, etc. I am sure these activities will continue to grow with the continual support from everyone.

Looking back, one of my most memorable achievements will be in the creation of Singapore’s first locally conferred undergraduate information security degree programme. This was made possible only because of the giant leap of faith from the former President of the Singapore Institute of Technology (SIT), Prof Tan Thiam Soon, for me to start one of SIT’s first set of degree programmes. I benefitted greatly from his guidance, wisdom and leadership. Just like how Prof Tan was a role model to myself, I hope many of my students will also take me as their role model and follow my lead to volunteer and contribute to the cybersecurity ecosystem in the future.

Lastly, this award reaffirms that I am going down the right path as I continue to contribute to the cybersecurity academia, industry and community in Singapore. Moving forward, I will also be working with our regional partners to build a more vibrant cybersecurity ecosystem in the region. As the saying goes, “Our house is only as safe as our neighbourhood”. Thus, I hope we will all continue to work together to build a safer cyberspace for everyone.

PROFESSIONAL DEVELOPMENT

Listing of Courses by Wissen International



Dear AiSP Members,
Are You Ready to Challenge the Toughest Penetration Testing Exam on the Planet?

CPENT
Certified Penetration Testing Professional
EC-Council

First 3 sign-ups will enjoy **50%** discount from CPENT iLearn Kit!

CERTIFIED PENETRATION TESTING PROFESSIONAL
GO BEYOND | KALI | AUTOMATED TOOLS
FLAT CYBER RANGES
Special pricing for AiSP Members!

Purchase CPENT Training Course via iLearn at a special price of **SGD 1809** (usual price SGD 2261)!

Each iLearn kit includes:
12 months access to CPENT e-book
12 months access to CPENT training videos by EC-Council Instructor
6 months access to CPENT iLab + guide
30 days access to CPENT cyber range + guide
12 months validity for CPENT exam with remote proctoring service by EC-Council

FIRST 3 SIGNUPS WILL ENJOY 50% DISCOUNT!
Email aisp@wissen-intl.com to register!

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

Qualified Information Security Professional (QISP®) Course



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

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

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

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

COURSE DETAILS

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

Time: 9am-6pm

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

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

*Utap funding is available for NTUC Member

TARGET AUDIENCE

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

COURSE CRITERIA

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

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

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

Program Partner

Delivery Partners



Cybersecurity Essentials Course


Essential Course Briefing on 15 Dec 21

Our Training Partner, Mr Allen Chua from Ai Network did a comprehensive sharing on our Essential Course for cybersecurity. He provided a brief introduction on the importance of cybersecurity knowledge and also the modules which will be covered for the course. He also shared that the course is available for UTAP funding for NTUC members and AiSP members will have 10% discount as well before GST.

Recent Cyber Threats from Around the World:

<p>US food importer Atalanta admits ransomware attack 09 December 2021</p>	<p>Transport cybersecurity TSA issues mandatory requirements for high-risk rail infrastructure 08 December 2021</p>	<p>"Mass-scale impact" Flaws in Tonga's top-level domain left Google, Amazon, Tether web services vulnerable to takeover 07 December 2021</p>
<p>Crypto-exchange BitMart reports \$150 million theft 06 December 2021</p>	<p>Insider threat Tech firm was hacked and extorted by its own employee, says FBI 02 December 2021</p>	<p>Florida school district data breach impacts 50,000 02 December 2021</p>
		<p>Panasonic admits data breach after attackers gain access to server 30 November 2021</p>

AiSP 2



Union Training Assistance Programme (UTAP)

What is UTAP?


- UTAP is a training benefit for NTUC members to defray their cost of training. This benefit is to encourage more NTUC members to go for skills upgrading.
- NTUC members enjoy 50% *unfunded course fee support for up to \$250 each year when you sign up for courses supported under UTAP. NTUC members aged 40 and above can enjoy higher funding support up to \$500 per individual each year, capped at 50% of unfunded course fees, for courses attended between 1 July 2020 to 31 December 2022.
- *Unfunded course fee refers to the balance course fee payable after applicable government subsidy. This excludes material fees, registration fees, miscellaneous fees, etc.

Who can apply?

All NTUC members can apply for UTAP. However, the following criteria must be met to be eligible for UTAP:

- Paid-up NTUC membership before course commenced**, throughout whole course duration and at the point of claim
- Course by training provider must be supported under UTAP and training must commence within the supported period
- Course must not be **fully funded through company sponsorship or other types of funding**
- You must achieve a **minimum of 75% attendance** for each application and sat for all prescribed examination(s), if any
- UTAP application must be **submitted within 6 months** after course completion

AiSP 14





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

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

Course Objectives

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

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

COURSE DETAILS

Training dates for year 2022 can be found on https://www.aisp.sg/cyberessentials_training.html

Time: 9am-6pm

Fees: \$ \$1,600 (before GST)*

*10% off for AiSP Members @ \$1,440 (before GST)

*Utap funding is available for NTUC Member

TARGET AUDIENCE

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

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

Program Partner



Delivery Partners



MEMBERSHIP

AiSP Membership

Complimentary Affiliate Membership for Full-time Students in APP Organisations

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

Complimentary Affiliate Membership for NTUC Members

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

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

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

AVIP Membership

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

Your AiSP Membership Account

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

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

Membership Renewal

Members will receive an auto-generated email from Glue Up and it will send the reminder 1 month before the expiry date of your membership. Members can renew and pay

[back to top](#)

directly with Glue Up or one of the options listed [here](#). We will be adding GIRO (auto - deduction) this year. Please email secretariat@aisp.sg if you would like to enrol for GIRO payment.

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

Please check out our website on [Job Advertisements](#) by our partners.

For more updates or details about the memberships, please visit www.aisp.sg/membership.html

AiSP Corporate Partners





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

AiSP Academic Partners



Our Story...

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

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

Our Vision

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

Our Mission

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


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



 www.AiSP.sg

 secretariat@aisp.sg

 +65 8878 5686

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

Please [email](#) us for any enquiries.