

**NEWS & UPDATE**

# **AiSP New Corporate Partner**

AiSP would like to welcome Boston Consulting Group (BCG) and DBS Bank Ltd as our new Corporate Partners. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem in 2021.

The logo for Boston Consulting Group (BCG) consists of the letters 'BCG' in a bold, green, sans-serif font.The logo for DBS Bank Ltd features a red square icon with a white 'X' shape inside, followed by the letters 'DBS' in a bold, black, serif font.

## MOU SIGNING WITH DIVISION ZERO (DIV0)

AiSP signed a Memorandum of Understanding (MOU) with Division Zero (Div0) on 14 April 2021 to further deepen the engagement and collaboration for both parties. Div0 is an open, inclusive and completely volunteer-driven cybersecurity community which aims to promote a vibrant cybersecurity community and safer cyberspace.

Through this MOU, it aims to create a formal basis for co-operation and collaboration between AiSP and Div0 to create a vibrant and dynamic international information and cybersecurity ecosystem. This will help to expand on the various areas of cooperation and increase exposure for members from both sides.

As like-minded partners, AiSP and Div0 are committed to organize more exciting events and activities for our members.



## CYBER ATTACK 2021

Cyber Attack 2021 was held on 16 April 2021 at Parkroyal Hotel where AiSP President Mr Johnny Kho was invited to be one of the panelists to discuss on The Million Dollar Question: Are Your Assets Safe?

Interesting questions such as “What is an asset in your organisation”, “How do you define the criticality of the different assets in your organisation” were exchanged during the event. It was an engaging and insightful afternoon for the audience as they learned about the role and responsibility in managing the Security of these assets.



## JOB OPPORTUNITIES IN THE CYBERSECURITY SECTOR

On 20 April, Mr Johnny Kho (AiSP President), Ms Soffenny Yap (EXCO Committee Member) and Ms Sugar Chan (EXCO Co-Opted Member) gathered with representatives from CSA and NTUC to share on the various job opportunities in the cybersecurity sector. Audience took away valuable insights from our cybersecurity experts and were inspired by their passion in their area of expertise.



## Knowledge Series Events

AiSP Knowledge Series Webinar – Software Security on 14 Apr 21

On 14 April night, **Mr Donald Wee from Data Terminator** and **Mr Eugene Lim from Division Zero (Div0)** shared with our participants on the insights of Software Security as part of our BOK series. Many thanks to our sponsor, **Data Terminator** who have generously supported the event.



Our upcoming Knowledge Series Webinar Event – Business Continuity will be on 12 May 2021 by speakers from Cisco & Responsible Cyber.



# AiSP Knowledge Series – Business Continuity

**12 May 2021 | 3 PM – 5 PM (SGT)**

**3.00 PM**    **Opening Address**  
By AiSP

**3.15 PM**    **Business Continuity and Cyber Resilience**  
By Mr Joshua McCloud, National Cybersecurity Officer, CISCO



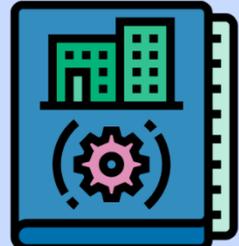
With board and executive-level recognition of cybersecurity as a key enterprise risk, cyber resilience has become an important aspect of business continuity planning. In this session we will discuss how Cisco operationalizes cyber resilience as part our business continuity activities, holding ourselves to account through board-led, cross functional governance and auditing processes.



**4.05 PM**    **Is your business continuity aligned with cybersecurity requirements?**  
By Mr Mikko Laaksonen, Technical Information Security Officer, Responsible Cyber



Convergence of cybersecurity and business continuity is a must. Ensuring an integration of appropriate technology aspects into the BCM plans and processes is not yet a common practice. This topic addresses main considerations when building a BCM. It also brings up good practices for integrating cyber security incidents into BCM.



**4.55 PM**    **Closing**  
By AiSP



Organised by:



Corporate Partners:



## 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 and Privacy SIG, 29 Jun
2. Cyber Defence – Ethical Hacking, 14 Jul (hybrid\*)
3. OT/IOT – IoT Security, 25 Aug (hybrid\*)
4. Operation and Infrastructure Security, 15 Sep
5. CTI SIG, 29 Sep (hybrid\*)
6. Security Operations – Incident Response Management, 13 Oct
7. Emerging Trends – Blockchain & AI for Cyber Security, 17 Nov

\*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 2021!**

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 [event@aisp.sg](mailto:event@aisp.sg) for assistance. Please refer to our scheduled 2021 webinars in our [event calendar](#).





# THE CYBERSECURITY Awards 2021

We have received new enquires from Singapore and overseas for award nomination after the 2020 call for nomination was closed on 30 Sep 2020. For our nominees to have more time to prepare their submission, we are pleased to commence **TCA 2021** marketing and the nomination period will be from **1 Feb 2021 to 15 May 2021**.

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

Professionals

1. Hall of Fame
2. Leader
3. Professional

Enterprises

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

Students

4. Students

The Cybersecurity Awards 2021 winners will be announced in October 2021 at the Award Ceremony. The nomination period will be from **1 Feb 2021 to 15 May 2021**.

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



Do you know any individuals or organizations who had made a great impact on the cybersecurity ecosystem in SG and internationally?

Don't miss this opportunity to give them that extra bit of recognition and appreciation for their contributions! Nominate your Cybersecurity Heroes for the categories listed below:

- PROFESSIONALS**
  - ★ Hall of Fame
  - ★ Leader
  - ★ Professional
- ENTERPRISES**
  - ★ MNC (Vendor)
  - ★ MNC (End-User)
  - ★ SME (Vendor)
  - ★ SME (End-User)
- STUDENTS**

**NOMINATIONS ARE OPEN NOW!**  
Send in your nominations by 15 May 2021!

Visit [www.thecybersecurityawards.sg](http://www.thecybersecurityawards.sg) or email [thecybersecurityawards@aisp.sg](mailto:thecybersecurityawards@aisp.sg) for more information.

ORGANIZED BY:  
**AISP**  
Advance Connect Excel

# TCA2021 Sponsors & Partners



Organised by



Supported by



Supporting Associations



Community Partner



Supporting Organisation



Platinum Sponsors



Gold Sponsors



Silver Sponsors



# Cybersecurity Awareness & Advisory Programme (CAAP)

AiSP hope to elevate CyberSecurity 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. Join our upcoming event on 2 June either physically or virtually to discover the importance of cybersecurity and cloud data protection.

## Cybersecurity Awareness Workshop

| 2 June 2021 | 1.30PM - 5.00PM |  
Lifelong Learning Institute

Organised by:



**SIGN UP NOW**

### KEY HIGHLIGHTS



#### Importance of Cybersecurity and Solutions

By Mr Tony Low, CAAP Co-Chair

With the disruption of the pandemic, many cyber threats such as phishing and data breaches has increased over the past 12 months. For 2021, many SMEs in Singapore are looking to increase their cybersecurity to protect against the increased cyber threats.



#### Beginning your journey on cloud data protection with Thales

By Mr Collin Chow, Managing Director, Root Security

With the rising number of data breaches, it has been proven that data is the new oil. Are you at lost on how to secure your critical data that your company holds? Join us to understand how you can easily protect your data anywhere, meet compliance mandates while focusing on your core business needs.

#### Identity and Access Management 101 with Thales

By Mr Collin Chow, Managing Director, Root Security

With the changes that is happening in the threat landscape for information technology, the importance of cybersecurity has never been more important. Join us in this session to learn how you can implement an effective cloud identity and access management (IAM) strategy in your organization which will help to prevent a cybersecurity attack.



#### Sharing on Cybersecurity Courses

With the rising cyber threats, SMEs need to continuously enhance their knowledge in cybersecurity to protect themselves. Find out what are the cybersecurity courses available for SMEs to upskill themselves.

#### Supporting Partners:



## Student Volunteer Recognition Programme (SVRP)



The SVRP Awards Ceremony was held on 24 Mar 21 at Lifelong Learning Institute Event Hall with Senior Minister of State for Communications and Information and Health, Dr Janil Puthucheary as the Guest of Honour. He presented the awards to the Gold winners. The Award Ceremony was supported by:



A total of 64 winners from ITEs and Polytechnics received the award for the various categories. Our heartiest congratulations once again to all the winners! Please click [here](#) for the list of winners for 2020.



Our **SVRP 2021 nomination form** is available now for IHL students to apply! To encourage more students to volunteer, secondary school and pre-university students are welcome to participate! Please refer to [SVRP framework](#) and **SVRP 2021 nomination form for secondary school and pre-university students!** We are having a student volunteer drive from now till Dec 2021 for those who are interested to volunteer but not sure where to start. Please [click here](#) to apply today.

## STEER YOUR WAY INTO SINGAPORE'S CYBERSECURITY ECOSYSTEM TODAY!

Since 2018, the Association of Information Security Professionals (AiSP) has been recognising student volunteers in Singapore, through its **Student Volunteer Recognition Programme (SVRP)**.

SVRP has also expanded to cater to varied interests of our youths in Singapore by,

1. Volunteering in our activities as student volunteers, be it events, research or using your skills to help others to be more cybersafe.
2. Participating in our SVRP nominations (annual cycle commences on 1 Sep) for IHL students or secondary school and pre-university students, listing your voluntary activities that are cybersecurity-related.
3. Attending our events to raise knowledge, these events are free for student members from our Academic Partners.

Please visit <https://www.aisp.sg/svrp.html> for more details!

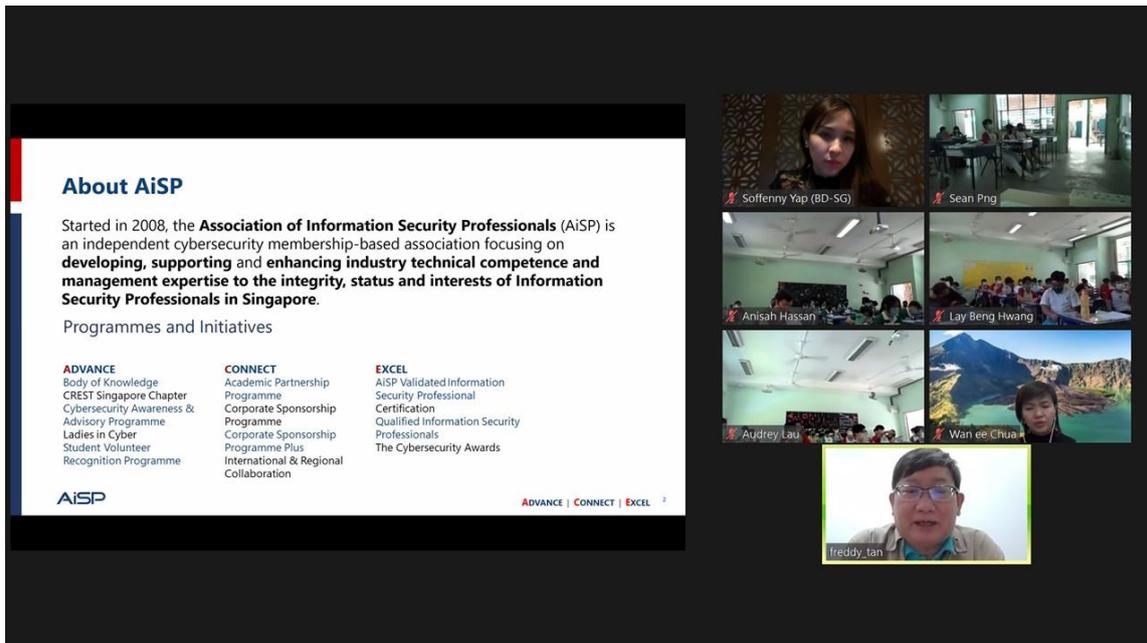


Connect with us on LinkedIn, Facebook, Instagram, YouTube and Telegram today.

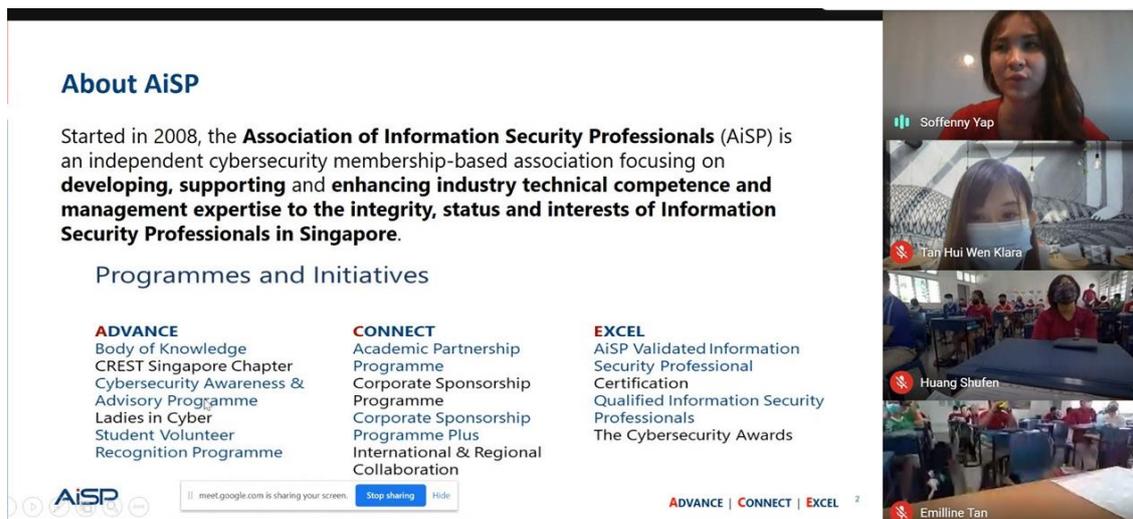
Under AiSP's [Academic Partnership Programme \(APP\)](#), the IHLs can include AiSP Student Chapter in their respective institutes. Please refer to our [Student Chapters](#) for the list of current committee members and we look forward to expanding the list in 2021!

# Career Talk & Sharing in Schools

On 7 April 2021, students from Tanjong Katong Secondary School had the opportunity to hear from Ms Soffenny Yap and Mr Freddy Tan who are our SVRP leads. It was an insightful session for the students as they learned about cybersecurity career, challenges faced in the industry and our very own SVRP program.



Second career talk for April was held on 9 April which our AiSP EXCO Co-opted Member & Co-Lead for Student Volunteer Recognition Programme (SVRP), Ms Soffenny Yap shared with students from Greenridge Secondary on the insights for career prospects in Cybersecurity industry.



# SINGAPORE CYBER SECURITY INTER ASSOCIATION (SCSIA) CYBER DAY QUIZ



As part of **AiSP's CyberFest 2021** and in conjunction with **Singapore Cyber Day 2021** (11 November 2021), the **Singapore Cyber Security Inter Association (SCSIA)** is organizing an online quiz competition for primary, secondary and tertiary students (aged 25 years and below) in Singapore. This competition aims to pique interest in students and equip with knowledge on Cyber Security.

From 25 March onwards, 3 questions will be posted on Facebook and LinkedIn every Thursday. **Answers will be revealed after 30 September** (when the competition ends). Please note that you must complete all **29 weeks of questions** to qualify for the total scoring.

E-Certificate of Participation will be given to all participants. **Attractive Prizes will be given to the top scorers.** You may find the link access below to the past quiz questions. Stay tuned to our [Facebook](#) and [LinkedIn](#) for the upcoming quiz questions!

Week	Link Address
Week 1 Quiz	<a href="https://forms.office.com/r/XGHBUPQJJe">https://forms.office.com/r/XGHBUPQJJe</a> or Scan the QR Code below 
Week 2 Quiz	<a href="https://forms.office.com/r/gWsmr1ZfLs">https://forms.office.com/r/gWsmr1ZfLs</a> or Scan the QR Code below

	
Week 3 Quiz	<a href="https://forms.office.com/r/ikiwzBiSnV">https://forms.office.com/r/ikiwzBiSnV</a> Scan the QR Code below 
Week 4 Quiz	<a href="https://forms.office.com/r/C0XdFvtqcs">https://forms.office.com/r/C0XdFvtqcs</a> Scan the QR Code below 
Week 5 Quiz	<a href="https://forms.office.com/r/bPYdNn3Ytm">https://forms.office.com/r/bPYdNn3Ytm</a> Scan the QR Code below 
Week 6 Quiz	<a href="https://forms.office.com/r/gmgSSn2syS">https://forms.office.com/r/gmgSSn2syS</a> 

# Sharing of Cybersecurity with NTUC Members

Sign up for NTUC Union Membership today and have access to a wide array of benefits from workplace protection to lifestyle benefits (attached below for merchants deals)!



**NTUC Membership**  
**Here supporting your needs at work & in life**  
#hereforyou

**Not a member? Receive a FREE OTO Spinal Support worth \$238**  
when you pay 6 months membership fees and arrange Credit/Debit Card Recurring (CCR) payment

**Apply now**

In collaboration:



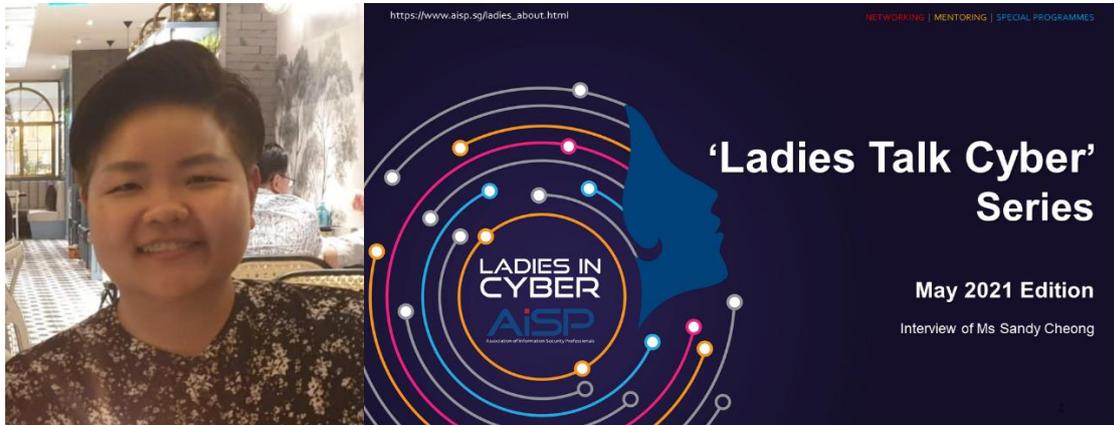

	Union members can sign up for NTUC FairPrice Membership to <b>earn up to \$240 cash rebate*</b> on your groceries, health & wellness products and services as well as purchase shares to earn dividend^		Available on BetterHealth mobile app: • <b>\$10*</b> GP Teleconsultation • <b>\$12*</b> GP Consultation
	Up to <b>15% OFF*</b> NTUC Value Meals		One-year <b>FREE*</b> subscription to access GetDocPlus mobile app
	<b>\$0.50 Hot Kopi/Teh*</b> on Wednesdays at NTUC Foodfare as well as Kopitiam Food courts and coffee shops.		Get up to <b>\$60*</b> electricity bill rebates
	<b>\$1.80 Breakfast Set*</b>		<b>20% OFF*</b> monthly mobile subscription
	Flash NTUC Plus! Card for members' rates		<b>\$8 OFF*</b> with min. spend of \$15 at foodpanda or pandamart (for new users only)
	Enjoy premium rates for as low as <b>\$0.70/day*</b> with LUV Term Life Insurance		• <b>\$6 OFF*</b> first order (for new users only, capped at the first 2,000 redemptions) • <b>\$8 OFF*</b> with min. spend of \$15 (for existing users, capped at 3 redemptions per user)
	Get <b>\$102 worth of LinkPoints*</b> per year when you enrol your child	<b>Flash your NTUC Plus! Card for members' rates*</b>	
	Earn and redeem LinkPoints at over 1,200 merchant outlets!	  	
	NTUC Club – the club for union members! Enjoy <b>special privileges</b> at Wild Wild Wet, Marina Bay Golf Course, Orchid Bowl and more!	  	

And many more!

Visit [ntucmembership.sg](http://ntucmembership.sg) to discover more savings!

Sign up [now](#) and receive an OTO Spinal Support worth \$238!

## Ladies in Cybersecurity



## Ladies Talk Cyber Series

For the Second edition of AiSP's 'Ladies Talk Cyber' series, we interviewed Sandy Cheong, who works with Cyber Risk Management team in her role at OCBC Bank Group Operational Risk Management (ORM) about her experiences in the industry 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

Sandy focused on cybersecurity governance and technology risk management throughout her career, covering both public and private sector organisations such as the Monetary Authority of Singapore, the Cyber Security Agency of Singapore and KPMG. She joined OCBC Bank's Group Operational Risk Management (ORM) function in 2019, where she works with the Cyber Risk Management team to continuously enhance cyber risk management and governance for the Bank.

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

## Join us in our next Ladies in Cyber Cross Border Webinar on 31 May 21 (Mon)

AiSP & Cyber Together from Israel will be organising the Ladies in Cyber Cross Border Webinar on **31 May 21 (Mon) at Singapore time 8pm / Israel time 3pm**. Please click [here](#) to register for the event. Please feel free to invite all your female colleagues and female friends to join in the session too.

NETWORKING | MENTORING | SPECIAL PROGRAMMES

### Ladies in Cyber Cross Border Webinar on 31 May 21 (Mon)

15:00PM to 17:00PM (Israel Time) / 8PM to 10PM (Singapore Time)

**A community empowering female cybersecurity professionals**

**United Ladies in Cyber**  
Ms Faith Chng  
Associate Director at Trustwave  
Co-Lead for AiSP Ladies in Cyber  
AiSP EXCO Committee Member

Sharing on how a non-technical person in Cyber Security can contribute to the local Eco System



**Cybersecurity: Overcoming Challenges by Diversity**  
Ms Gily Netzer  
CMO at Cymulate, Advisory Board and Member of Forbes Communication Council

Sharing her personal story, her thoughts on cybersecurity today, the "Start-up Nation" and how diversity is key to success moving forward.



**Notable Cyber Incidents & Threats in an Unprecedented Year**  
Ms Sandy Cheong  
Vice-President, Cyber Risk Management at OCBC  
AiSP Ladies in Cyber Mentor

Sharing on how a non-technical person in Cyber Security can contribute to the local Eco System



**Incident Response**  
Ms Reut Menashe  
Founder of Tetrispona  
Leading Cyber Ladies

Sharing on the world of incident responder and incidents that I investigated on a daily basis, especially on the rare ones and guide you through this adramatized world.



**CYB TOGETHER**  
Israeli Cyber Security Association

**AiSP**  
Association of Information Security Professionals

**LADIES IN CYBER**

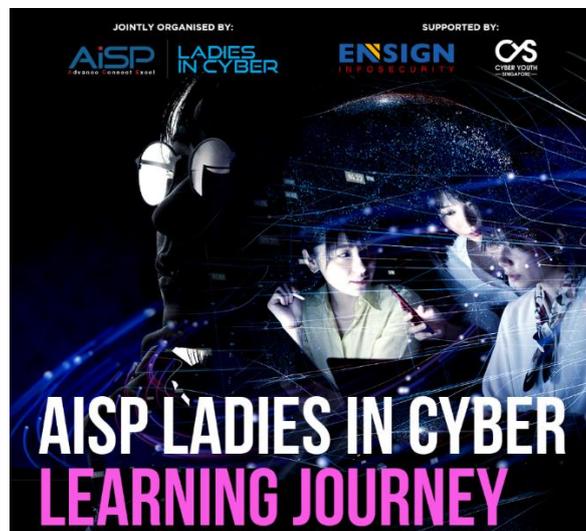
Hosted & Moderated By:  
Ms Sherin Y Lee  
AiSP Vice-President & Founder for AiSP Ladies in Cyber Programme



The Association of Information Security Professionals (AiSP) Ladies in Cyber Team in Singapore together with Cyber Together, Israeli Cyber Security Association is coming together to organise a cross border webinar for any ladies that are interested to find out more on Cyber Security in Singapore and in Israel. Join our speakers (Technical & Non-Technical) to hear more about what they do daily in their job in cyber security, their personal experience, advice and motivation in Cyber Security. During the session, we can also share and discuss on how Israel and Singapore had made tremendous progress over the decades and how our needs and aspirations will continue to grow and become more diverse and how we can all strive to continue to do better in Cyber Security where we all can fulfill our dreams to be leaders in business and society.

## Join us in our next Ladies in Cyber Dialogue Session on 14 Jun 21 (Mon)

AiSP will be organising a Virtual Dialogue Session on 14 Jun 21 for female students. Join Ms Sun Xueling, Minister of State for Ministry of Education and Ministry of Social and Family Development and Dr Tan Mei Hui, Vice-President of Singapore Computer Society Cybersecurity Chapter moderate by Ms Sherin Y Lee, AiSP Vice-President in a closed-door dialogue session on the issues of Supporting women in the workplace and in their career aspirations. Please click [here](#) to register for the event. Please feel free to invite all your female colleagues and friends to join in the session too.



# Regional Cyber meets Physical Security 2021

(PRE - RECORDED VIDEOS)

**Date**  
11 May, Tuesday

This session features pre-recorded videos by our speakers. Targeted at security professionals from both the Cyber and Physical security domains, the two-part **Regional Cyber Security meets Physical Security digital event** brings together a panel of high-profile speakers to share their expertise that will help you keep abreast of the latest development in the security industry and upgrade your skillsets.

### Welcome Address



**Johnson Ng**  
Head  
Security Industry Institute



**Peter J. O'Neil**  
FISMA CAC  
Chief Executive Officer  
AIS International



**Clar Rosso**  
Chief Executive Officer  
eS&P

### Guest of Honour



**Raj Jeshua Thomas**  
SIS President & National Member of Parliament  
Security Association Singapore

### Our Speakers



**Danny Chan**  
Regional Security Officer  
Asia Pacific  
Mandiant Inc.  
Topic: The Impact of Convergence on Cyber and Physical Security



**Dex Yuan**  
Assistant Regional Vice President  
Shanghai CISR  
AIS's INTRUST Ltd.  
Topic: Converging Cyber and Physical Security Through Interdiction



**Anthony Lim**  
Advisor  
ISC2 Singapore Chapter  
Topic: Industry 4.0 and Cyber-Physical Security Considerations



**Zhou Zhiliao**  
Vice Secretary  
ISC2 Singapore Chapter  
Topic: Identity Access Management in a Cyber-Physical converged World



**Peter Gwee**  
ISAC Singapore Chapter Young Leaders in ISAC Chapter and Director Academic Outreach  
Topic: Explorations in Cyber to protect your industrial control systems from Cyber attack



**Hank Parot**  
Program Director  
Certified Cyber Incident Response Specialist  
CCTP  
Topic: How Can People of Workship Safeguard Themselves from Terrorist Attacks?



**David Chow**  
Managing Director  
KnowledgePoint Training Centre  
Topic: The importance of Cyber security training for security officers



**Jeffrey Lam**  
Senior Project Manager  
APAC Asia Pacific  
Asia Consumer Solutions  
Topic: Enhancing Defence in Depth using automated systems



**Kelvin Goh**  
Managing Director at  
Sovaris Pte Ltd  
Topic: Transformation towards Cyber Guarding



**Lee Jing Yi**  
JaiChye  
Debaritator, Scientists  
Research Analyst  
From Terms  
Methodical: Science Centre  
Topic: The Threat of Cyber Espionage: Motivations Behind It And How Organisations Can Manage Such A Risk



**Pawan Desai**  
Chief Executive Officer  
KBC Advisory Services Pvt. Ltd  
Topic: A Time to Change: Merging Physical and Cyber Security



**Shawn Chua**  
Communications Manager  
Protequi Singapore Pte. Ltd.  
Topic: Revelation of Modern Physical Security

For registration, please click on [bit.ly/3g58F2V](https://bit.ly/3g58F2V) or scan QR Code



Co-Organised by  
**Temasek** Security Industry Institute



Proudly supported by



## 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 in 2021. Please contact us if you are keen to be part of our SIGs as we are actively recruiting members for 2021!



## For AiSP Members only

As we are always looking for new ways to engage our members, AiSP has categorised the various ways for [member-only access](#) as part of our digital engagement during COVID-19 pandemic,

1. Members-only access for [webinar playback](#)
2. [LinkedIn closed group](#)
3. Participate in [member-only events](#) and closed-door dialogues by invitation
4. [Volunteer](#) in our initiatives and interest groups, as part of career and personal development

If you have missed our virtual events, some of them are made available for members' access via [Glue Up](#) platform. Please email ([event@aisp.sg](mailto:event@aisp.sg)) if you need any assistance.

**We wish to remind our members to renew their 2021 membership if they have not done so.**

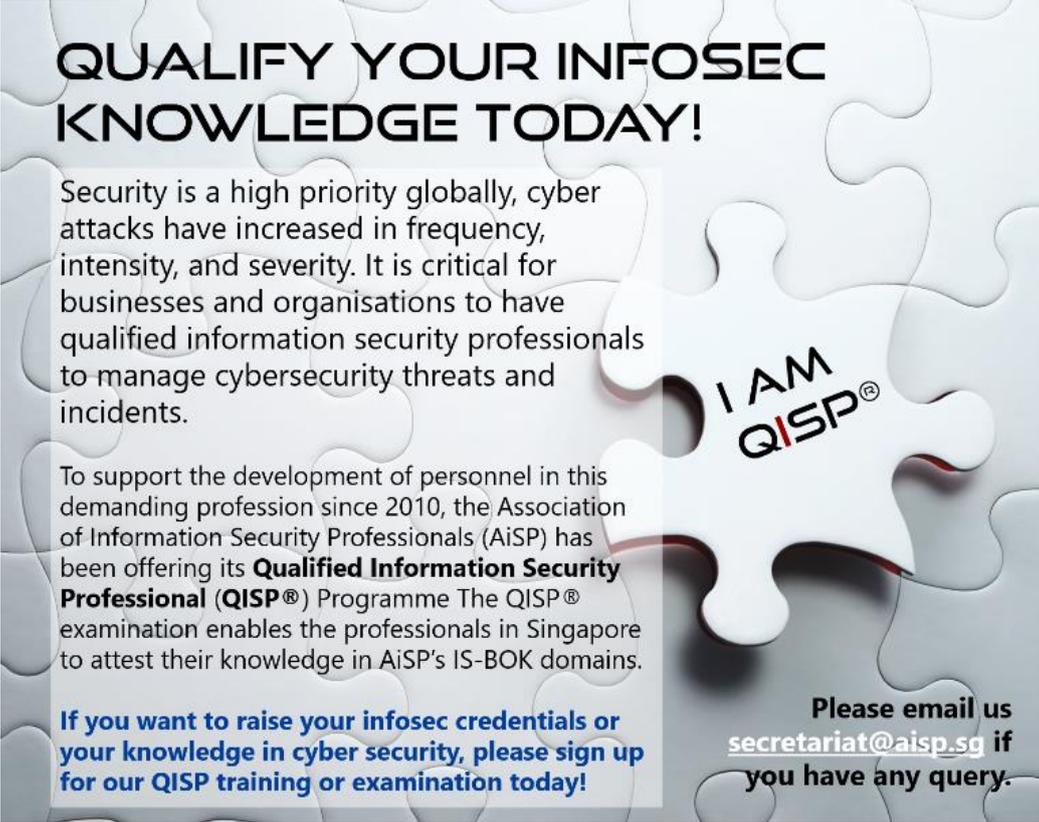
## Call for Volunteers

As AiSP focuses in raising the professional standing of information security personnel and professions in Singapore since 2008, we have been running various initiatives to address diverse needs and developments. Please [email us](#) for more details!

## PROFESSIONAL DEVELOPMENT

Qualified Information Security Professional (QISP®) Course

**QISP®** is designed for entry to mid-level Information Security Professionals, and any IT Professionals who are keen to develop their knowledge in this field. It will be enhanced to complement AiSP's Information Security Body of Knowledge (IS-BOK) 2.0. Our online examination via Pearson VUE platform would be deployed worldwide in 2021.



**QUALIFY YOUR INFOSEC KNOWLEDGE TODAY!**

Security is a high priority globally, cyber attacks have increased in frequency, intensity, and severity. It is critical for businesses and organisations to have qualified information security professionals to manage cybersecurity threats and incidents.

To support the development of personnel in this demanding profession since 2010, the Association of Information Security Professionals (AiSP) has been offering its **Qualified Information Security Professional (QISP®)** Programme. The QISP® examination enables the professionals in Singapore to attest their knowledge in AiSP's IS-BOK domains.

**If you want to raise your infosec credentials or your knowledge in cyber security, please sign up for our QISP training or examination today!**

**Please email us [secretariat@aisp.sg](mailto:secretariat@aisp.sg) if you have any query.**



Connect with us on LinkedIn, Facebook, Instagram, YouTube and Telegram today.

Please **contact AiSP** if you are keen to leverage the enhanced QISP® for your learning and development needs, or you would like to develop courseware based on AiSP's IS-BOK 2.0 overseas.

## BOK 2.0 Knowledge Series

As information security developments are accelerating during COVID-19 pandemic and the trend is expected to be the same for 2021, we have covered the application and implementation of our BOK 2.0 topics at workplaces in our past webinars. This series is useful for working professionals who are preparing for our **QISP®** examination so that their knowledge remains current.

## CREST SINGAPORE CHAPTER

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 since February 2021. Please click [here](#) for the exam schedule for 2021.

## CRESTCon Singapore 2020/2021

The CREST Singapore Chapter is organising the **first CRESTCon Singapore 2020/2021** in November 2021 and is now calling for paper submission till 30 Jun 2021. Please [email secretariat](#) if your organisation is keen to sponsor the event!

 **20/21** Call for Paper starts now.  
**Are You Ready?**

For 2021 we are organising the **first CRESTCon Singapore** in November and are inviting presenters to submit their topics from now till 30 Jun 2021.

- Security Testing • Data Security in Asia • Ethical hacking • Cyber Threat Intelligence
- Incident Response Management • IOT/OT vulnerabilities

The technical presentations (30 to 45-min with Q&A) must relate to penetration testing and assurance, incident response or threat intelligence. We are looking out for presentations that showcase new or ongoing security research, new threats and vulnerabilities or demonstrating the advances and innovation. Please email your synopsis along with speaker's biography. We look forward to welcome presenters and delegates from all over the world to Singapore.

If you and your organisation are keen to be part of this technical conference as speakers and sponsors, please email [secretariat@aisp.sg](mailto:secretariat@aisp.sg) for more details.



The AiSP **CyberFest™** is a series of cybersecurity events and initiatives that take place from 8 to 12 November 2021 in Singapore.

Connect with us on [LinkedIn](#), [Facebook](#) and [Instagram](#) today.

## UPCOMING ACTIVITIES/ EVENTS

### Ongoing Activities

Date	Event	By
Jan-Dec	Call for Female Mentors (Ladies in Cyber)	AiSP
Jan-Dec	Call for Volunteers (AiSP Members, Student Volunteers)	AiSP
Feb-May	Call for Nomination for The Cybersecurity Awards 2021	AiSP
Feb-Jun	Call for Paper Submission for CRESTCon Singapore 20/21	AiSP CREST SG

### Upcoming Events

Date	Event	By
1-31 May	SGUnited Career & Skills Discovery Fair by SCCC	Partner
4 - 7 May	Black Hat Asia Virtual	Partner
11-May	Regional Cyber Meet Physical Security 2021	Partner
12-May	<b>AiSP Knowledge Series – Physical Security, Business Continuity and Audit</b>	<b>AiSP &amp; Partner</b>
18-May	<b>AiSP CREST Webinar</b>	<b>AiSP &amp; Partner</b>
21-May	<b>AiSP CAAP Focus Group with SBF</b>	<b>AiSP &amp; Partner</b>
21-May	<b>AiSP &amp; Trend Micro Zero Trust Webinar</b>	<b>AiSP &amp; Partner</b>
21-May	MFA-SCP Smart Nation: Strategies, Opportunities and Cybersecurity Management by Civil Service College	Partner
25-May	Punggol Digital District Industry Event	Partner
28-May	<b>AiSP CAAP Focus Group with People Association</b>	<b>AiSP &amp; Partner</b>
31-May	<b>AiSP Ladies in Cyber Session with Cyber Together</b>	<b>AiSP &amp; Partner</b>
2-June	<b>AiSP CAAP Workshop</b>	<b>AiSP &amp; Partner</b>
10-June	<b>AiSP SIG Combined Event</b>	<b>AiSP &amp; Partner</b>
11-June	<b>AiSP CAAP Focus Group with NTUC</b>	<b>AiSP &amp; Partner</b>
14-June	<b>AiSP Ladies in Cyber Learning Journey to Ensign</b>	<b>AiSP &amp; Partner</b>
16-June	<b>AiSP Knowledge Series – Security Architecture &amp; Engineering</b>	<b>AiSP &amp; Partner</b>
21-June	CAAP Awareness with People Association at Harmony Camp	Partner
21 – 25 Jun	CYS Summit	Partner
22-Jun	<b>AiSP &amp; Cyber Together Webinar – Cybersecurity Leaders Series</b>	<b>AiSP &amp; Partner</b>
25-Jun	<b>AiSP x SFA CAAP Awareness Workshop: Singapore SMEs' Digital Adoption and Concerns</b>	<b>AiSP &amp; Partner</b>
29-Jun	<b>AiSP Knowledge Series - Data &amp; Privacy</b>	<b>AiSP &amp; Partner</b>

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



**CyberFest®** is a community-led initiative that would take place from 08 to 12 Nov 2021 in Singapore.

# CONTRIBUTED CONTENTS

Insights from The Cybersecurity Awards 2020 Winner – Data Terminator

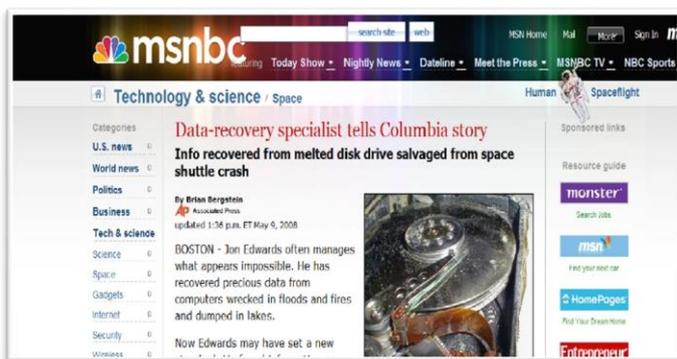


## Why Data Destruction is Absolutely Vital for Cybersecurity

In this current highly digitised world, we appreciate the usage of electronic devices that enable us to store and process huge amounts of information. However, when such storage devices (viz. flash and hard drives) reach the end of their useful lives, many are unaware of the consequences of not disposing of data appropriately.

In fact, besides Government agencies having the need to protect official secrets, enterprises are also required to comply with regulatory requirements like PDPA (Personal Data Protection Act) or GDPR (General Data Protection Regulation) to ensure the protection of personal data.

With the advancement of technology, data stored can easily be recovered if it is not destroyed correctly. A good case would be the US Space Shuttle Columbia that crashed on 1 February 2003. Data recovery specialists retrieved 99% of the information stored in the charred hard drives in over just two days.\*



There are many other forms of data storage within servers, photocopiers, printers, CCTV recorders and some IoT devices. The need for proper destruction of the data stored within these items was mostly forgotten when they reached their end-of-life or due for a technical refresh.

At Data Terminator, we provide One-Stop Data Destruction Products and Services to ensure that our customers' data are securely destroyed, either on-site or in our secured facility.

With our 3P (Products, Peoples and Process) approach, customers can have complete peace of mind, trusting us to destroy their end-of-life data with confidence and in compliance with the necessary regulatory requirements.

**Our Business Approach**  
To Deliver Security with Confidence to Our Customer

<p><b>1 Products &amp; Technology</b> <small>Niche and Best in Class Solution</small></p> <div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> <p><small>Degaussers for Magnetic Media</small></p> </div> <div style="text-align: center;"> <p><small>Disintegrators for Optical and Flash Media</small></p> </div> <div style="text-align: center;"> <p><small>Secure Erasure for Hard Disks and Solid State Disk</small></p> </div> </div>	<p><b>2 People</b> <small>Experiences and Well Trained Hands-On Specialist</small></p>	<p><b>3 Process</b> <small>ISO 9001:2015, ISO 14001:2015, ISO 18001:2015, ISO 2001:2015, Cert No: CN/15499, Cert No: CN/15498</small></p> <p style="text-align: center;"><b>certified for "Provision of Electronic Data Erasure and Destruction Services"</b></p>
---	--	---

Data Terminator was founded and managed by experienced and trained specialists with over 30 years of IT and security experience; with a proven track record serving Data Centres, key Government Ministries and Agencies. It is also the recipient of The Cybersecurity Award 2020 (TCA 2020) \*\* – SME (Vendor) category.

Our services are in tandem with enterprises' strategies of meeting stringent security guidelines and standards required for the appropriate sanitisation and destruction of their electronic storage media.

To find out how your data can be securely disposed of, please speak with our specialist on 6463 9212 or visit [www.data-terminator.com](http://www.data-terminator.com)



enquiry@data-terminator.com  
Tel: +65 8482 4550



www.data-terminator.com  
Tel: +65 6463 9212



\*<https://www.computerworld.com/article/2535754/shuttle-columbia-s-hard-drive-data-recovered-from-crash-site>

\*\*The Cybersecurity Awards 2020 honours outstanding contributions by individuals and organisations, to local and regional cybersecurity ecosystems.

The Awards are organised by the Association of Information Security Professionals (AISP), and supported by Cyber Security Agency of Singapore (CSA) and the following professional and industry associations that are part of the Singapore Cyber Security Inter Association - Centre for Strategic Cyberspace + International Studies (CSCIS), Cloud Security Alliance Singapore Chapter, HTCIA Singapore Chapter, ISACA Singapore Chapter, (ISC)2 Singapore Chapter, The Law Society of Singapore, Singapore Computer Society and SGTech.

# CONTRIBUTED CONTENTS

Insights from our new Corporate Partner Programme (CPP) – Acronis

## Cybersecurity trends to look out for: extortion among the top threats in 2021

With the massive Solarwinds-based attack shockingly exposed in December 2020, having hit major corporations, like the US Government and Microsoft, it's become clear that the targets for cyber criminals in 2021 will be everyone – including corporations, remote workers and MSPs.

Cybercrime is evolving, driven by emerging trends – 2021 may be the first year when data extortion officially becomes the main threat to businesses worldwide. With more criminals exposing private data, even after they've successfully extorted a ransom, we've already seen ransomware destroy businesses and lives this year.

Attacks on healthcare operators continue as hackers seek to cause maximum chaos - hospitals worldwide have reportedly experienced a 45% increase in cyber-attacks in the last 2 months. Even vaccine researchers are not safe from state actors and other groups wishing to steal secrets for profit.

The big attacks of 2020 set the tone for 2021, and it's worth analysing the recent key trends. History tends to repeat itself, and those who have learned the lesson are better prepared to meet the challenges and defy attackers when it counts.

The below findings are reflected and analysed in the [Acronis Cyberthreats Report 2020](#), prepared by our global network of Cyber Protection Operation Centers (CPOC) – and available for free.

### In 2020, the world saw:

- 31% of global companies were attacked by cybercriminals at least once a day – a dramatic ramping up of attacks. Microsoft patching close to 1,000 flaws in its products in just 9 months - as high as 15-20% more than in 2019 - with Windows and Office still the biggest malware magnets.
- More than 1000 companies had their data leaked due to ransomware attacks, at least 20% more than last year – with ransomware still No.1 among cyberthreats. Maze ransomware, in particular, accounted for almost 50% of all known cases.
- COVID-19 scams offering fake financial support and fake free testing, both of which were phishing scams to harvest data. Also, fake remote education apps and medical leave documents installing malware.
- New variations on sextortion scams that threaten the leaking of supposedly recorded video from a victim's webcam, as well as threats to infect a victim's family with COVID-19.
- Remote workers under massive attack, with 92% of global organizations adopting new technologies to facilitate remote workers, IT departments struggling to cope.

### Staggering malware stats of 2020

With independent malware testing lab AV-Test recording 400,000 new malware samples per day in Q3 2020, cybercriminals are taking automation to a whole new level. The top-10 malware families included Emotet, Agent Tesla, XMRig, Formbook, Trickbot, LokiBot, Remcos, Qbot, Nanocore and Azorult.

With ransomware still the No.1 threat to businesses worldwide, the top-10 ransomware families are Maze, REvil/Sodinokibi, SNAKE (EKANS), Nemty, NetWalker (aka Mailto), Ragnar Locker, MegaCortex, CLOP, DopplerPayer and Thanos – with some groups trying to infect as many users as possible, while others focus on high value targets only.

The Maze ransomware family proved most troublesome, not just encrypting data but stealing terabytes of private data in targeted attacks – with both small businesses and massive global brands falling victim to it virtually every week throughout much of 2020, it's clear that no-one is safe.

And while some strains pretend to pride themselves on not attacking hospitals, schools or governments, there is zero honour among thieves, especially when ransom payments can now be anywhere from \$200,000 to tens of millions, depending on the size of company hooked or data's sensitivity.

Malicious websites have also grown in numbers, with the US seeing the largest number of blocked URLs in Q3 2020 at 16.4%, followed by Germany, the Czech Republic, Spain, the UK, China, South Africa, Hong Kong, Italy and Australia rounding out the top-10 countries. While showing significantly less blocked URLs last year, both Japan and Singapore made it to the top-20 countries.

## Key research findings for Acronis Cyber Protection Week Global Report 2021

### Investing in more solutions doesn't mean more protection

To protect business data, applications, and systems – particularly during the pandemic's shift to remote work environments – organizations added new solutions to their IT environments. It's not working.

- ~75% of IT professionals report that their organizations have all recommended cybersecurity technologies in place
- 80% of organizations have up to 10 different protection and security tools running simultaneously
- Despite this, securing remote environments, ensuring availability, and maintaining employee productivity are still top challenges for IT pros
- More than half of organizations saw downtime due to data loss last year

### A lack of awareness is creating a lack of protection

Significant gaps in awareness regarding cybersecurity and technology capabilities are costing individuals and organizations time, money, and security.

- Just 13% of IT users and IT professionals follow backup best practices
- 68% of IT users and 20% of IT professionals wouldn't know if their data had been unexpectedly modified because tools don't make it easy to find out
- 43% of IT users don't know if their anti-malware stops zero-day threats because it's not easy to find out
- ~25% of IT users don't know what ransomware, cryptojacking, Dos/DDoS, and IoT attacks are
- 10% of IT pros don't know if they're subject to data privacy regulations, risking major fines for potential compliance violations

### IT users don't feel accountable for the protection and security of their data and devices

Personal reliance on technology continues to grow but efforts to protect that technology isn't keeping pace, likely due to false assumptions and a reliance on automatic solutions.

- 85% of IT users spent more time on their devices last year. Only half of them took extra steps to protect those devices.
- 1/3 of IT users don't update their devices for a week after being notified
- While 90% of IT users perform backups, 75% have irretrievably lost data at least once, suggesting that they don't know how to back up or recover properly
- Patch management and vulnerability assessment tools that would simplify cybersecurity see low adoption

## Top cyberthreats for the Asia-Pacific region

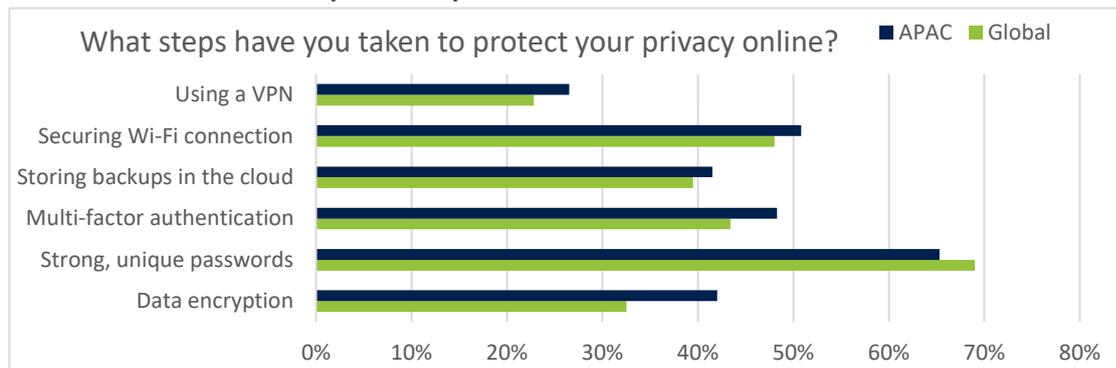
- Personal IT users in the Asia-Pacific (APAC) region are taking a broader approach to defending their data, applications, and systems from the same challenges and issues as the rest of the world.
- The cyberthreats that concern personal and professional IT users in the APAC region are consistent with our [Global Report findings](#) – indicating that the potential damage of these cyberthreats is universally understood.

Personal IT users	IT professionals
1. Data theft	1. Data theft
2. Malware	2. Malware
3. Phishing Attacks	3. (Tie) DoS / DDoS and Phishing attacks
4. Ransomware	4. IoT attacks
5. DoS / DDoS attacks	5. Ransomware

## Committed to protecting privacy online

IT users in the APAC region reported higher rates of adoption for all online privacy services and processes compared to the global response. This suggests that individuals in the region are more willing to dedicate time and money to their privacy and protection.

### What does Acronis recommend to stay safe today – and tomorrow?



- Patch your OS and apps – software exists to handle this automatically
- Always be prepared for phishing attempts, don't click on any suspicious files
- Use a VPN while working with business data – no exceptions
- Make sure your cyber protection solution is running properly
- Use an encrypted password manager – and never reuse work passwords for personal needs, not to put your corporate network at risk
- Ensure your IT staff are expertly trained in all of these areas so all staff have work and home computers that are properly secured and updated
- Run security training in your organization, so the staff are exposed to insecure situations and can recognize them

We live in the world where digital space became the 5<sup>th</sup> basic human need, in addition to air, water, food and shelter. We rely on digital space to make our life more comfortable, but with that, we're exposing ourselves to a whole new dimension – with its own rules and risks. Nowadays, most businesses consume the benefits of the digital world on a daily basis – and simple cyber hygiene rules, like the ones above, can help lower the risks. There are simple but advanced defence tools – like [Acronis Cyber Protect](#), that helps businesses safely exist in the digital world.

Each business is to decide for themselves – but if you want to continue operating in the digital world in 2021, you won't be able to remain dependant on weak elements, like outdated complex solutions and unsuspecting employees. Otherwise, you won't do business long enough to know better.

Learn more at [www.acronis.com](http://www.acronis.com) or contact Seok Cheng at [SeokCheng.Chia@acronis.com](mailto:SeokCheng.Chia@acronis.com).

## CONTRIBUTED CONTENTS

Insights from our Corporate Partner Programme (CPP) – Trend Micro



### Providing Higher Confidence Detections

In this year's simulations, MITRE Engenuity focused on techniques associated with notorious threat groups Carbanak and FIN7. The test included two simulated breaches, one at a hotel and one at a bank, using typical advanced persistent threat (APT) tactics such as elevation of privileges, credential theft, lateral movement, and data exfiltration.

Register for Trend Micro's **live webinar 5 May** as they unwrap the results for SOC & Security Teams: <https://bit.ly/3eqULWo>



*Register for webinar*

### Highlights of Trend Micro's Results from the MITRE Engenuity ATT&CK Evaluations

**96%**

of attack coverage delivered to provide visibility of 167 out of 174 simulated steps across the evaluations, allowing customers to build a clear picture of the attack and respond faster.

**100%**

of attacks against the Linux host were detected, capturing all 12 attacker steps, which is especially important considering the huge increase of use by many organizations.

**139**

pieces of telemetry were enriched by the Trend Micro Vision One™ platform, providing extremely effective threat visibility to better understand and investigate attacks—a critical piece for security operations center (SOC) analysts.

**90%**

of attack simulations were prevented very early in each test thanks to automated detection and response. Deflecting risk early on frees up investigation resources so teams can focus on solving harder security problems.

**Access Report and Resources: <https://bit.ly/3dAMeAN>**



Cloud based applications is one of the areas in which threats will increase in 2021. It is more critical than ever to understand the risk posed by potentially compromised user identities. How do you determine malicious behaviour and the infiltration of your organization by a rogue actor?

On **21 May 11am**, join **Trend Micro & AiSP** to learn more about the Zero Trust Model, get clarity on misconceptions and how organisations can use this security framework to help secure their networks, applications, and data in this cloud-native era. The webinar will discuss what this model means for SOC, Security and Network teams and get an early look at how Trend Micro can help your journey.



### Featured Speakers:



Johnny Kho,  
President,  
AiSP



Biswajit De,  
Snr Technical Consultant,  
Trend Micro

### What you'll learn in 60 minutes:

- What the Zero Trust Model really means and understanding the mindset
- Various approaches and steps towards Zero Trust Transformation including use cases
- Importance of Zero Trust Risk insights and how to get continuous assessment and visibility
- How to provide ability to dynamically control user access to authorized corporate resources only based on the user's risk posture
- Threat detection to protect emails, endpoints, cloud workloads, and network

[Register Now](#)

# 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 to 2021) from 1 Jul 2020 to 30 Jun 2021. 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](http://www.aisp.sg/membership.html)

## Be part of the Cybersecurity Ecosystem, JOIN AiSP!

# AVIP MEMBERSHIP

Limited to 1st  
100 sign-ups  
For 2021

## BENEFITS OF MEMBERSHIP

- Recognition as a **Trusted Infocomm Security Professional**. You can use the designation of **AVIP (AiSP Validated Information Security Professionals Member)** as your credentials.
- Special Invite to **Exclusive Activities & Events**.
- AVIP members enjoy the **Professional Indemnity Coverage in Singapore and Overseas (FIRST in Asia)!**
- AVIP members will be invited for **key dialogue sessions with national & industry leaders** for their opinions on cyber security.
- AVIP members will be **invited to represent AiSP for media interviews** on their opinions on cyber security.



### CORPORATE PARTNER PROGRAMME

Registration Fee  
(One Time): \$321\*  
Annual Membership Fee: \$267.50\*



### ORDINARY MEMBER (PATH 1)

Registration Fee  
(One Time): \$481.50\*  
Annual Membership Fee: \$267.50\*

*\*Price includes GST*

Email [membership@aisp.sg](mailto:membership@aisp.sg) to sign up and for enquiries.

## AiSP CORPORATE PARTNERS

Acronis

BCG

 BitCyber  
Securing Your Business

 CISCO

 DBS

 ENSIGN  
INFOSECURITY  
CONQUER  
THE UNKNOWN

 FIREEYE™

GOVTECH   
SINGAPORE

 ITSEC  
ASIA

  
MINDEF  
SINGAPORE

 Responsible  
Cyber

 ST Engineering

 TREND  
MICRO™

## AiSP ACADEMIC PARTNERS

  
Institute of Technical Education

 NANYANG  
THE INNOVATIVE POLYTECHNIC

 Ngee ANN  
POLYTECHNIC

 REPUBLIC  
POLYTECHNIC  
DISCOVER. TRANSFORM. ACHIEVE

 SIT  
SINGAPORE  
INSTITUTE OF  
TECHNOLOGY

SINGAPORE  
POLYTECHNIC | SP

 SMU  
SINGAPORE MANAGEMENT  
UNIVERSITY

 Temasek  
POLYTECHNIC

## OUR STORY...



 [www.AiSP.sg](http://www.AiSP.sg)  
 [secretariat@aisp.sg](mailto:secretariat@aisp.sg)  
 +65 6247 9552  
 116 Changi Road  
#04-03 WIS@Changi  
Singapore 419718

*Our office is closed during Phase 3. We are currently telecommuting.*

*Please email us or message us via Telegram at [+65 8878 5686](https://t.me/aisp_sg).*



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.

Please contact [secretariat@aisp.sg](mailto:secretariat@aisp.sg) on events, membership, partnership, sponsorship, volunteerism or collaboration.