NEWSLETTER

February 2021

NEWS & UPDATE

In line with Government's directives on COVID-19 pandemic and AiSP's business continuity plan, AiSP Secretariat has commenced partial telecommuting during Phase 3. Please **email us** or **WhatsApp** to our office number (+65 6247 9552), for assistance before you drop by our office.

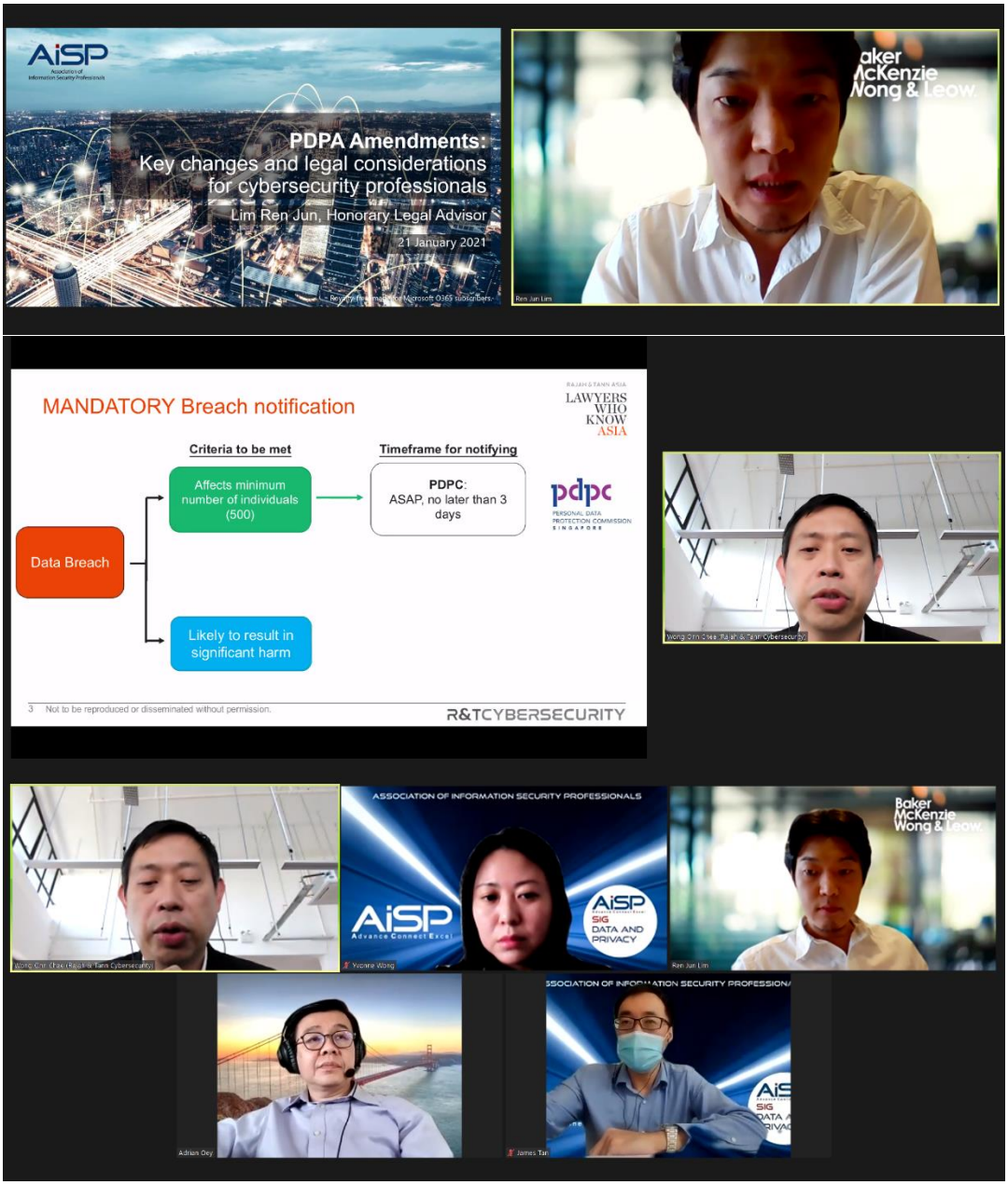
Do check out our **community calendar of events** or follow us on social media for events and updates!

AiSP New Corporate Partners

AiSP would like to welcome CISCO and FireEye as our new Corporate Partners from 10 January 2021 onwards. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem in 2021.

Knowledge Series Events

[BOK] Knowledge Series Webinar — Data Security – PDPA Amendments on 21 Jan 21



We had our first knowledge series webinar of the year, **Data Security – PDPA Amendments**, with insights from our speakers, **Lim Ren Jun** and **Wong Onn Chee**. We ended the session with a panel discussion with Lim Ren Jun, James Tan, Adrian Oey & Yvonne Wong on application of new PDPA amendments to the COI SingHealth case moderate by Wong Onn Chee.

Our upcoming webinar Cyber Threat Intelligence will be on 24 Feb 2021 by FireEye on Evolving Cyber Threats in 2021 and GRF on Why Intelligence Matters.

Our Speakers:
Speaker 1:
Yihao Lim, Principal Threat Intelligence Enablement Consultant at FireEye Singapore Pte Ltd will be sharing on Evolving Cyber Threats in 2021.

Speaker 2:
John Lim, Managing Director of GRF Asia-Pacific Pte Ltd will be sharing on From Strategy to Operations: Why Intelligence Matters.

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. Cloud Security SIG, 30 Mar 2021 (hybrid*)
2. Software Security, 14 Apr
3. Physical Security, Business Continuity and Audit, 12 May
4. Security Architecture and Engineering, 16 Jun
5. Data and Privacy SIG, 29 Jun (hybrid*)
6. Operation and Infrastructure Security, 14 Jul
7. OT/IOT – IoT Security, 18 Aug
8. Cyber Defence – Ethnical Hacking, 15 Sep
9. CTI SIG, 29 Sep (physical event* with recording)
10. Security Operations – Incident Response Management, 13 Oct
11. Emerging Trends – Blockchain & AI for Cyber Security, 17 Nov
12. IoT SIG, 8 Dec (physical event* with recording)

*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 for assistance. Please refer to our scheduled 2021 webinars in our **event calendar**.

The Cybersecurity Awards (TCA) 2020 seeks to honour outstanding contributions by individuals and organisations, to local and regional cybersecurity ecosystems. In view of COVID-19 pandemic and well-being of our guests at the award ceremony, AiSP has moved the physical event to **26 Feb 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

Students
4. Students

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

The winners will be announced at The Cybersecurity Awards ceremony

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

For more information,
please visit www.thecybersecurityawards.sg
or contact us at thecybersecurityawards@aisp.sg

Organised by:
AiSP
Association of Information Security Professionals

TCA2020 Sponsors & Partners

Organised by

Supported by

Supporting Associations

Community Partners

Platinum Sponsors

Gold Sponsors

Silver Sponsors

Student Volunteer Recognition Programme (SVRP)

The SVRP working committee has interviewed our potential Gold Awardees and has confirmed our list of Gold, Silver and Bronze Award recipients. We want to congratulate all students for their contributions and dedication during the challenging 2020 year. Against all odds, each nominee contributed an average of 99.9 hours.

Over **9,792** hours were contributed from 1 Sep 2019 to 31 Aug 2020, where

- 1,250 hours were for Leadership pillar,
- 4,411 hours were for Skills pillar
- 4,176 hours were for Event pillar

Please click **here** for the list of winners for 2020. The SVRP Award Ceremony will be held on 15 Mar 21 at 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 will be presenting the awards to the Gold winners. The Award Ceremony is supported by:

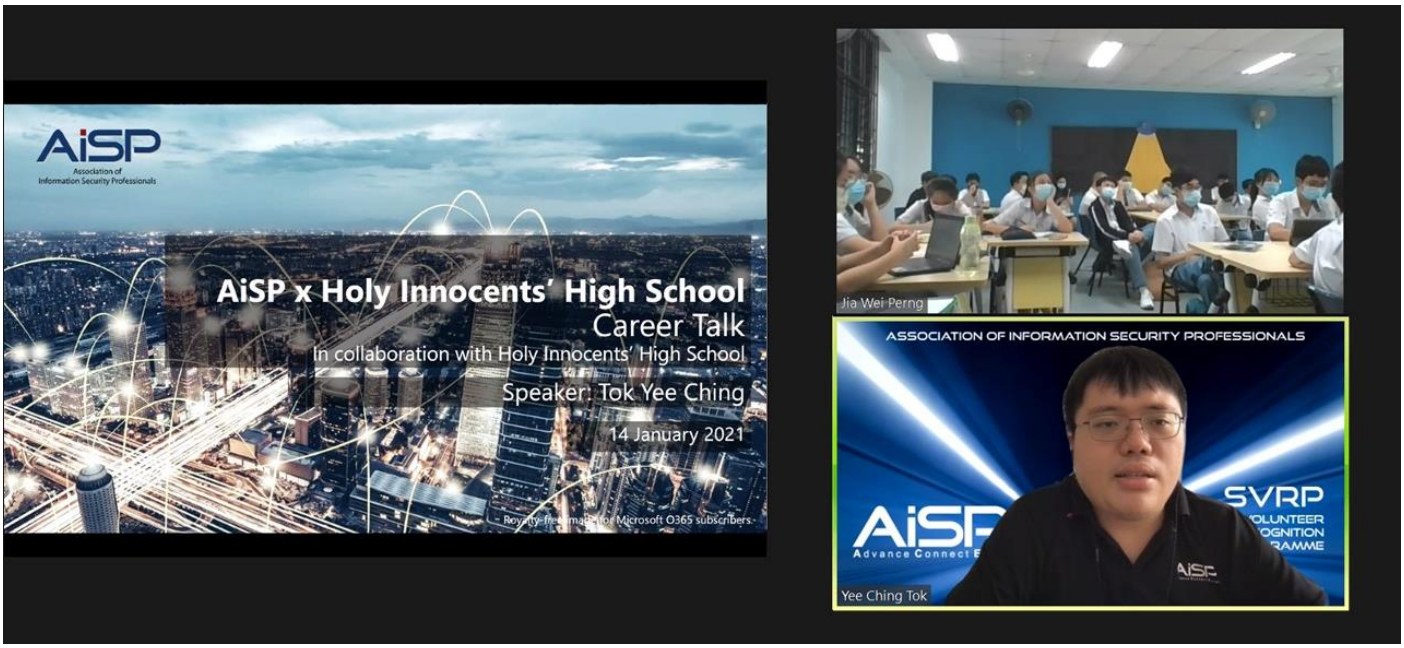
Our **SVRP 2021 nomination form** is available now for IHL students to apply! To encourage more students to volunteer, secondary school and pre-university students are welcome to participate! Please refer to **SVRP framework** and **SVRP 2021 nomination form for secondary school and pre-university students**!

We are having a student volunteer drive from now till Dec 2021 for those are interested to volunteer but not sure where to start. Please **click here** to apply today!

Under AiSP's **Academic Partnership Programme (APP)**, the IHLs would 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

Our AiSP EXCO Committee Member Mr Tok Yee Ching shared on the profession in Cybersecurity and Student Volunteer Recognition Programme (SVRP) with 40 secondary school students from Holy Innocents' High School on 14 Jan 21.



Interested to have us in your school to share on the Professional in Cybersecurity or on the Student Volunteer Recognition Programme (SVRP). Please **email us** for more details!

Ladies in Cybersecurity

AiSP would like to thank our team of dedicated female mentors for been part of the AiSP Ladies in Cyber 2020 mentorship programme for their advice and guidance to the female students in 2020.

Abha Sood	Alexandra Mercz	Alina Tan
Catherine Lee	Chan Meow Shiang	Chin Yee Ping
Claudean Zheng	Daisy Radford	Debbie Chia
Eileen Yeo	Elizabeth Tan	Emilie Philippe
Emilie Wolff	Esther Soh	Faith Chng
Gwenda Fong	Ivy Young	Katherine Tan
Lee Zhe Mein	Lim Ee Lin	Lim Leh Hoon
Monica Nathalia	Ong Chen Hui	Priyanka Gupta
Sandy Cheong	Sherin Lee	Soffenny Yap
Su Mon Kywe	Sugar Chan	Tan Mei Hui
Yuna Yeh	Yvonne Wong	

Under our **Ladies in Cybersecurity Charter**, AiSP's volunteer team of female cybersecurity professionals have been mentors to female students through our Ladies in Cyber Mentorship Programme. We welcome female volunteers and students to join our programme as **mentors** and **mentees** (please refer to the online forms).

AiSP hopes to work closer with our industry partners to attract more female cyber professionals in Singapore. Please **contact us** if your organisation would like to take this conversation further.

Our next Ladies in Cyber event will be on 18 Mar 21 at Trend Micro office.

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) if you need any assistance.

We wish to remind our members to renew their 2021 membership before Chinese New Year!

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.

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 will resume from February 2021 onwards with the first exam on 18 February 2021 and 19 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!

AiSP Association of Information Security Professionals | CYBER FEST

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
4 Feb	[SVRP] ITE West Industry Sharing	Partner
18-19 Feb	CREST Practical Exam	**AiSP CREST SG**
22 Feb	[CAAP] AiSP x NTUC Career Talk for PMETs	**AiSP & Partner**
23 Feb	[SVRP] Bukit Panjang Government High School Sharing	Partner
24 Feb	Knowledge Series Webinar: Cyber Threat Intelligence	**AiSP**
26 Feb	The Cybersecurity Awards 2020 Ceremony	**AiSP**
2 Mar	Cyber World Congress 24r Virtual Cyber Security Event	Partner
8 Mar	[SVRP] Regent Secondary School Career Sharing	Partner
15 Mar	SVRP Award 2020 ceremony	**AiSP**
17 Mar	ASEAN Cybersecurity Summit	**AiSP**
18 Mar	Ladies in Cyber Fireside Talk	**AiSP**
24-26 Mar	Fintech India 2020/2021 Expo	Partner
25 Mar	CREST Practical Exam	**AiSP CREST SG**
26 Mar	AiSP Annual General Meeting	**AiSP**
26-28 Mar	Inter-poly CTF: Lag and Crash	**AiSP**
30 Mar	Knowledge Series - Cloud Security	**AiSP**
31 Mar	[CAAP] Post Budget Discussion on Cybersecurity	**AiSP & Partner**
31 Mar	The Cybersecurity Awards 2020 Judges Appreciation	**AiSP**

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.

Thinking about joining the cybersecurity industry?
Hear from our speakers as they share about working in the non-technical field of cybersecurity and what it takes to join the industry.
Join us at this lunch time webinar to find out more!

22 Feb 2021, Monday | 12pm - 1pm | zoom

Speakers:

David Siah
Vice President,
Channels (APAC, Middle East and Africa) for Trend Micro,
EXCO member of AiSP and SGTECH

Sherin Y Lee
APAC Head of Marketing,
Brand & Communications for Ensign InfoSecurity ,
Vice President of AISP

Register now

Organised with:

AiSP Association of Information Security Professionals
TTAB Tech Talent AssemBly

Supported by NTUC ICM Cluster

#everyworkermatters

pme@ntuc.org.sg @UPMECentre NTUC U PME @ntucUPME

CONTRIBUTED CONTENTS

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

Protecting your hybrid workforce from cyber threats

The current pandemic forced companies worldwide to quickly make the transition to a remote workforce in order to maintain business continuity. However, with only 53% of respondents from our recent survey stating they were only "somewhat prepared" for this change, cybersecurity policies need to adapt quickly as well.

What are some of the cybersecurity challenges companies are facing as they embrace a hybrid workforce?

- 61% experienced a jump of 25% or more in cyber threats and alerts since the start of COVID-19.
- 56% stated that office laptops/desktops are a challenge to protect in a remote environment.
- 59% said the lack of employee awareness and education was the top challenge faced in reinforcing remote working cybersecurity protocols.
- 66% indicated they will likely increase their cybersecurity investments due to the COVID-19 situation.

Download our exclusive report, Future of Secure Remote Work, to get the insights you need to help your business remain flexible, secure, and resilient.

Link: https://www.cisco.com/c/en/us/products/security/future-secure-remote-work-report.html?oid=rptsc023542&ecid=27070&ccid=cc000157

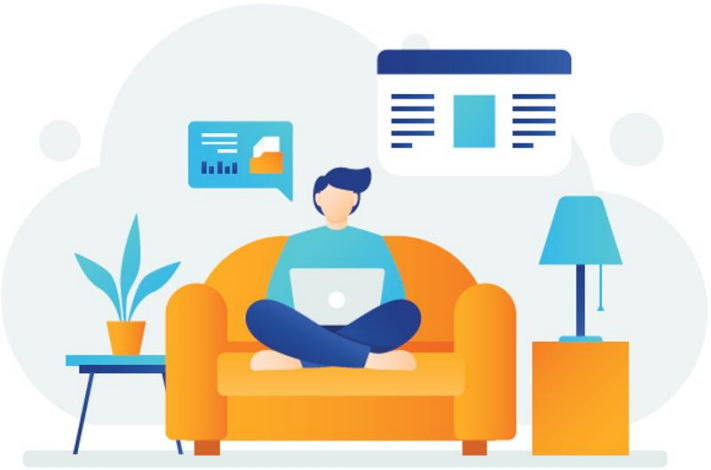
CONTRIBUTED CONTENTS

Insights from our new Corporate Partner Programme (CPP) – ST Engineering

With more people working from home due to the COVID-19 situation, organisations and IT teams need to ensure employees are cyber safe. That means providing them with cybersecurity best practices, tools and resources to protect their data and devices.

Here's sharing 5 essential cybersecurity tips to keep yourself cyber safe in the current work-from-home environment.

Tip 1: Separate Personal Matters from Work



For those staying and working at home, it can be tempting to handle both personal matters - such as e-learning and online purchases and work duties on the same computer. However, this can introduce potential vulnerabilities and compromise the security of your work accounts.

One solution is to use Secure Browser with BIOS-SHIELD™ Computer. You can safely work on your confidential data on the trusted workspace and use the Secure Browser to browse the web and perform internet-based activities like conference calls, banking transaction, etc. As the Secure Browser is isolated from the trusted workspace, any malware infection on the Secure Browser will not affect the trusted workspace.

If that sounds like a solution for you, check out our BIOS-SHIELD™ series.

Tip 2: Connect to Corporate Gateways Securely

With more people working from home, the number of devices accessing corporate gateways will increase dramatically. This poses a significant security risk as it introduces potential vulnerabilities into the corporate network and infrastructure.

The answer to this is a portable Virtual Private Network (VPN) Client that provides safe and secure way to access the corporate network. Our NetCrypt series is a hardware-based VPN solution, which allows users to establish remote connection to their corporate gateways securely.

Tip 3: Ensure Secure Communication Channels

More people than ever are turning to platforms such as messaging services (WhatsApp, WeChat) and video conferencing (Zoom, Skype) to communicate while working from home. This poses security risks, as many of these channels are prone to security breaches and threats such as eavesdropping and leaking of sensitive information in non-secured channels.

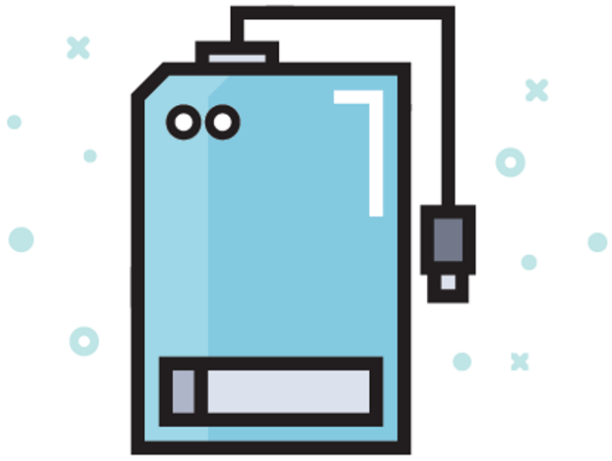
Organisations, especially those in sensitive sectors, should strengthen the security of their communication channels. Our Secure Phone series is able to provide end-to-end protection for your voice calls, Instant Messaging, and attachments.

Tip 4: Watch out for COVID-19 Email and SMS Scams

While the world is coming to terms with the COVID-19 situation, hackers have seized the opportunity to send out emails and SMS messages, masquerading as health organisations and enterprises. Unsuspecting victims have opened or clicked through these messages and found their systems infected by malware or ransomware.

Beyond educating team members on the importance of email cyber hygiene, organisations can look at enhancing their endpoint security against phishing and malware attacks, the same way corporate firewalls do in the office. Check out how our BIOS-SHIELD™ series and Secure Phone series can help to prevent cyber-attacks.

Tip 5: Use Storage Devices with Hardware Encryption



Team members working from home often need access to files and data storage. However, conventional storage drives and USB flash drives pose a huge security risk if they are lost or stolen. Each year, organisations lose vast amounts of unsecured data this way – resulting in heavy losses, both financial and reputational.

The solution to this comes in the form of encrypted data storage drives, such as our Secure Storage DiskCrypt M10, which comes with hardware encryption (AES-XTS 256bits), shielding your critical data from cyber-attacks and data theft. Meanwhile, it's 2-Factor Authentication using PIN and smartcard means only you are able to access the data within.

Let us strengthen our cyber-resilience in this challenging time and protect our sensitive data from cyber-attacks.

Learn more: https://www.stengg.com/cybersecurity

CONTRIBUTED CONTENTS

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

The Covid-19 pandemic forced many enterprises and employees into a new way of working. Organizations had to implement new systems and policies to facilitate remote work, while office workers had to shift to work-from-home setups. In the struggle to adjust and ensure smooth operations, many long-simmering cybersecurity risks and security issues have come to the forefront.

Our 2021 Security Predictions report discusses the security challenges brought about by the new workplace environments and plausible threats that should be anticipated. It aims to empower enterprises to create an effective and comprehensive security response strategy that can withstand change and disruption.

What will the landscape look like in 2021?

Home offices will be the new criminal hub

Work is now done through home internet service providers over possibly unpatched routers and machines. We predict that cybercriminals will be selling access to hacked routers, giving threat actors an avenue into home networks. Threat actors will then use home networks as launch points to gain a foothold into corporate networks.

The Covid-19 pandemic will be fertile ground for malicious campaigns

In 2021, the use of fraudulent emails, spam, and phishing attempts will continue, but the social engineering lures will shift to vaccine-related issues and other health response efforts.

Hybrid environments will be a risk for organizations

Given that work and personal data are co-mingling on devices, some organizations might find it challenging to manage compliance with data processing rules and data storage guidelines.

Maintaining privacy standards will be a challenge

Health organizations and pandemic-response teams may need to access and store personal data to manage the spread of the virus — these databases are ripe targets for malicious actors.

The patching window will narrow

Attackers will quickly weaponize newly disclosed flaws and vulnerabilities. Trading or selling exploitable known bugs will increase — sellers will also package exploits specific to the threat actor's needs.

Exposed APIs will be the next attack vector

APIs are already integral for most businesses' operations, but security for them is still nascent. We predict that threat actors will use them as entry points into organizations.

Enterprise software and cloud applications will be at risk

Cybercriminals will quickly integrate weaknesses in popular software into their campaigns. Also, cloud environments will contain larger amounts of sensitive data, making them more valuable targets for criminals.

What can enterprises do?

- Educate and train employees
- Deploy patch management programs
- Maintain strict access control
- Threat detection + security expertise

Learn more about these security predictions and mitigation tactics in our full report: https://bit.ly/TurningTheTide2021

TREND MICRO | research

Click here for the full report.

MEMBERSHIP

Type	Benefits
Individual Membership	▪ Recognition as a Trusted Infocomm Security Professional. You can use the designation of AVIP (AiSP Validated Information Security Professionals) or MAISP (Ordinary Member) as your credentials. ▪ Regular updates on membership activities. ▪ Free and discounted rates for events organised by AiSP and partners. ▪ One-time discount for QISP® examination fee for Affiliate members who are working professionals. ▪ Priority for activities, talks and networking events. ▪ AVIP members enjoy Professional Indemnity coverage in Singapore and overseas.
Corporate Partner Programme (CPP)	▪ Listing on AiSP website as a Corporate Partner ▪ Free and discounted rates for events organised by AiSP and partners. ▪ Complimentary AiSP Affiliate membership for organisation's personnel. ▪ Special invite as speakers for AiSP events. ▪ One complimentary job advertisement or knowledge-sharing article on AiSP platform per month (i.e. a total of 12 ads or articles in a year).
Academic Partnership Programme (APP)	▪ Inclusion of an AiSP Student Chapter for the Institute. ▪ Ten (10) complimentary AiSP Affiliate membership for personnel from the Institute. ▪ Complimentary AiSP Affiliate membership for all existing full-time students in the Institute, not limiting to cyber/infosec domains. ▪ Listing on AiSP website as an Academic Partner. ▪ One annual review of Institute's cybersecurity course curriculum. ▪ AiSP speakers to speak at Student Chapter events, including briefings and career talks. ▪ Free and discounted rates for events organised by AiSP and partners. ▪ One complimentary info/cybersecurity or internship post in AiSP website per month.

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 **WhatsApp** (+65 6247 9552).

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**), the 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 Eventbank, 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.

Be part of the Cybersecurity Ecosystem, JOIN AiSP!

AiSP CORPORATE PARTNERS

AiSP ACADEMIC PARTNERS

OUR STORY...

www.AiSP.sg
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 WhatsApp at +65 6247 9552.

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** on events, membership, partnership, sponsorship, volunteerism or collaboration.