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 Partner

AiSP would like to welcome Responsible Cyber as our new Corporate Partner from 21 February 2021 onwards. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem in 2021.

Responsible Cyber

Knowledge Series Events

AiSP Knowledge Series Webinar - Cyber Threat Intelligence on 24 Feb 21

We had our second knowledge series webinar of the year, **Cyber Threat Intelligence** with insights from our speakers, **Mr John Lee, Managing Director (Asia Pacific) from GRF Asia-Pacific Pte Ltd and Mr Lim Yihao, Principal Threat Intelligence Enablement Consultant at FireEye**.

Our upcoming Knowledge Series Hybrid Webinar Event - Cloud Security will be on 30 Mar 2021 by AiSP Cloud Security Special Interest Group & (ISC)².

Dear AiSP Member,

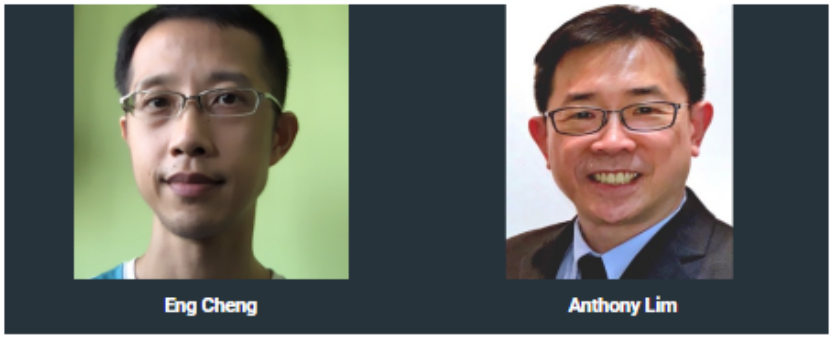
AiSP has completed the update of its Information Security Body of Knowledge (IS-BOK) 2.0 on 8 Nov 2019. To enable our members can better understanding how the IS-BOK topics can be implemented at workplaces, the Association is organising a series of knowledge-sharing & networking events in 2021 based on nine topics.

This webinar will be on **Cloud Security**, including user's and vendor's perspectives.

This event is by registration only and is complimentary to active AiSP members including students who are Affiliate members from our APP organisations.
For AiSP Partners, please indicate your membership number upon registration and proceed to purchase your tickets at a discounted rate.
For members of public, please proceed to register and purchase your tickets.

Session would be recorded for active AiSP members to access post-event.

SPEAKERS



I Will Attend | No

ORGANISER

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 (hybrid*)
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. The Award Ceremony was held on 26 Feb 2021 at Marina Bay Sands. Minister for Communications and Information and Minister In-Charge for Cybersecurity, Mr S Iswaran graced the event and presented the awards to 7 winners in the Professional, Student and Enterprise category.

List of Winners:

Leader	Dr Steven Wong Kai Juan Singapore Institute of Technology
Professional	Tan Nian Qi Alina Land Transport Authority
Student	Hugo Chia Yong Zhi Nanyang Polytechnic
MNC (Vendor)	Singapore Telecommunications Limited
MNC (End-User)	Acronis Asia Pte Ltd
	DBS Bank Ltd
SME (Vendor)	Data Terminator Pte Ltd

AiSP would like to thank all the Sponsors, Supporting Agency, Cybersecurity Agency of Singapore, Supporting Associations from the SCSIA and our Community Partners for their support to make The Cybersecurity Awards 2020 a great success.

TCA2020 Sponsors & Partners

Organised by

Supported by

Supporting Associations

Community Partners

Platinum Sponsors

Gold Sponsors

Silver Sponsors

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

Students
4. Students

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

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) 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

TCA2021 Sponsors & Partners

Organised by

Supported by

Supporting Associations

Community Partner

Supporting Organisation

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 year 2020. 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, specifically

- 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 24 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**!

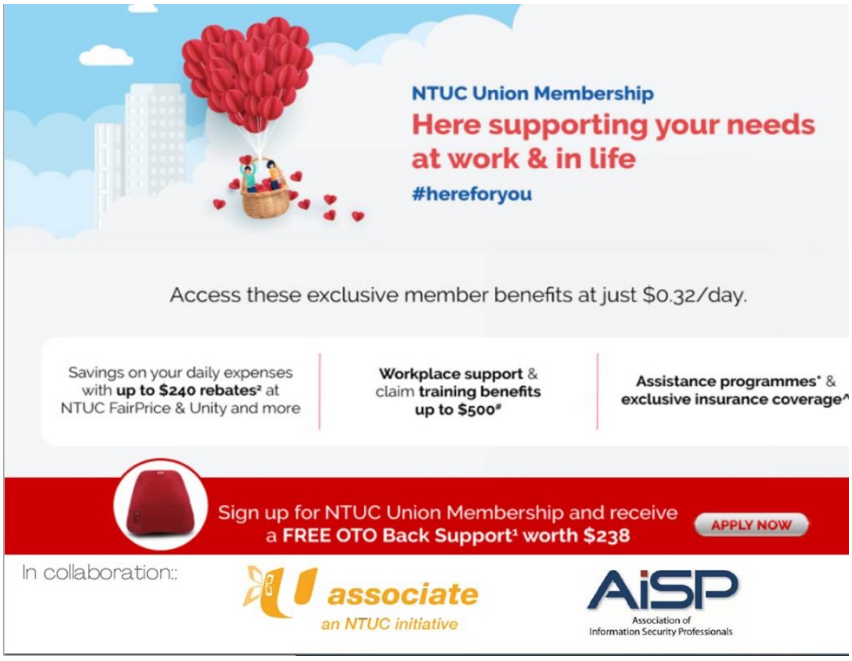
We are having a student volunteer drive from now till Dec 2021 for those who are interested to volunteer but not sure where to start. Please **click here** to apply today!

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!

Sharing of Cybersecurity with NTUC Members

Our AiSP Vice-President Ms Sherin Y Lee and AiSP EXCO Co-Opted Member Mr David Siah shared on the different profession in Cybersecurity and the different activities, programme and QiSP course that AiSP had with 200 NTUC members on 22 Feb 21 over the lunch talk.

Interested to have us to share on the Professional in Cybersecurity or on the activities, programmes and courses that AiSP provided. Please **email us** for more details!



We would like to invite you to sign up as NTUC Union Member as a support to the Labour Movement. You can sign-up via the below QR Code to show your support – by doing so, you will also be receiving a sign-up gift (OTO Back Support Massager) worth **$238**.

Career Talk & Sharing in Schools

Our AiSP EXCO Committee Member & EXCO lead for Student Volunteer Recognition Programme (SVRP), Mr Freddy Tan shared on the profession in Cybersecurity and Student Volunteer Recognition Programme with 400 students from ITE Central, ITE East and ITE West on 4 Feb 21.

Our AiSP Student Volunteer Recognition Programme (SVRP) Committee Member, Mr Sam Goh shared on the profession in Cybersecurity and Student Volunteer Recognition Programme with 350 students from Bukit Panjang Government High School on 23 Feb 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 being 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.

Please click here to register for the session. Only for female students only.
If you have any queries, please email to secretariat@aisp.sg

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 had resume since February 2021. The next practical exam will be on 25 March 2021 and 26 March 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

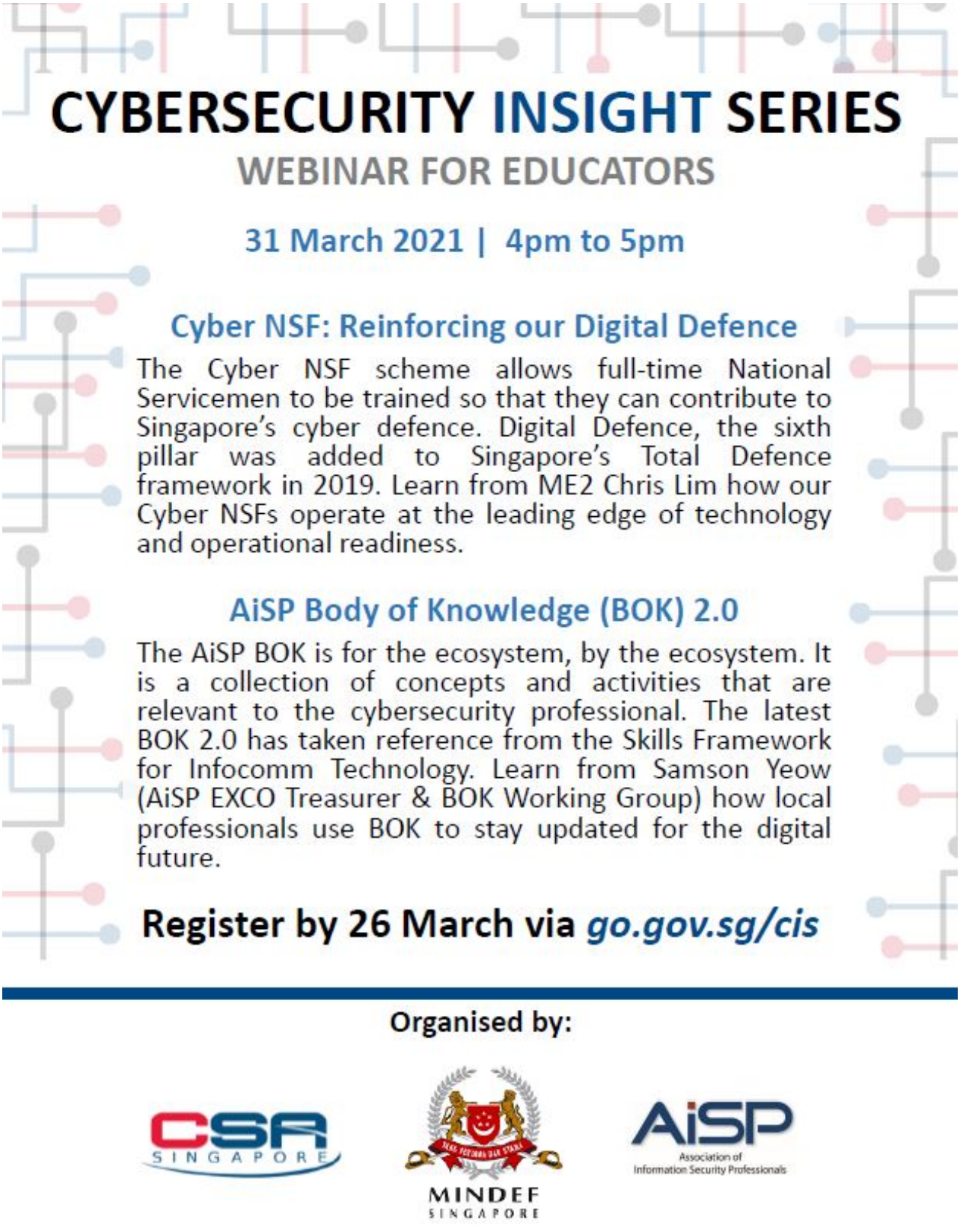
Date	Event	By
Jan-Dec	Call for Female Mentors (Ladies in Cyber)	**AiSP**
Jan-Dec	Call for Volunteers (AiSP Members, Student Volunteers)	**AiSP**
Feb-May	Call for Nomination for The Cybersecurity Awards 2021	**AiSP**
Feb-Jun	Call for Paper Submission for CRESTCon Singapore 20/21	**AiSP CREST SG**

Upcoming Events

Date	Event	By
2 Mar	Cyber World Congress 24r Virtual Cyber Security Event	Partner
3 Mar	Securing the Cloud – An Integrated Approach	Partner
8 Mar	[SVRP] Fairfield Methodist Secondary School Career Sharing	Partner
8 Mar	[SVRP] Regent Secondary School Career Sharing	Partner
10 Mar	[SVRP] Bedok Green Secondary School Career Sharing	Partner
10-12 Mar	Inter-poly CTF: Lag and Crash	**AiSP**
18 Mar	Ladies in Cyber Fireside Talk	**AiSP**
19 Mar	Inter-poly CTF: Lag and Crash Award Ceremony	**AiSP & Partner**
24 Mar	SVRP Award 2020 ceremony	**AiSP**
24-26 Mar	Fintech India 2020/2021 Expo	Partner
25-26 Mar	CREST Practical Exam	**AiSP CREST SG**
26 Mar	AiSP Annual General Meeting	**AiSP**
30 Mar	AiSP Hybrid Knowledge Series Sharing on Cloud Security and MOU Signing with ISC(2)	**AiSP & Partner**
31 Mar	[CAAP] Cybersecurity Outlook 2021 with SCCCI	**AiSP & Partner**
31 Mar	The Cybersecurity Awards 2020 Judges Appreciation	**AiSP**
31 Mar	Cyber Insight Series (CIS) for SG Cyber Educators	**AiSP & Partner**
7 Apr	[CAAP] SBF Focus Group Discussion	**AiSP & Partner**
7 Apr	[SVRP] Tanjong Katong Secondary School Career Sharing	Partner
14 Apr	AiSP Hybrid Knowledge Series Sharing on Software Security and MOU Signing with Div0	**AiSP & Partner**
15-16 Apr	Cyber Attack Singapore 2021	Partner

***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.



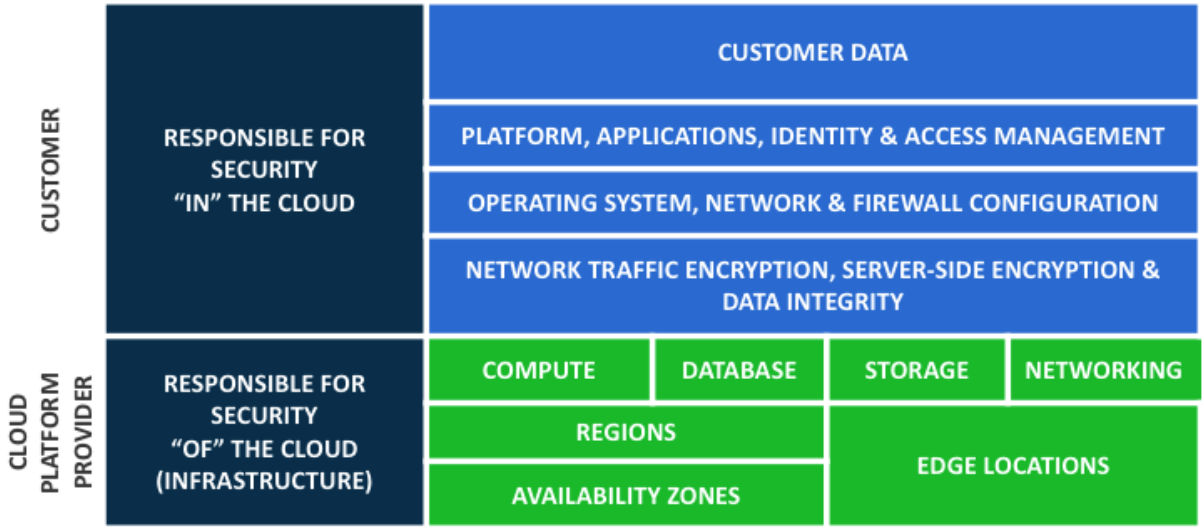
CONTRIBUTED CONTENTS

Insights from our new Corporate Partner Programme (CPP) – Responsible Cyber

Cloud technologies adoption continues to grow. Gartner forecasts that by 2022, **90% of companies** in the market will be using cloud services, generating a total value of **278.3 billion dollars**.

Cloud is one of the *buzz* words that we have heard the most these past years. Small and Medium Enterprises "SMEs" perceive it as a magical solution to all problems. Truth to be told, it is an exceptional technology, cost-effectively providing essential benefits. With the Cloud, you can upgrade to the latest equipment in a few clicks with no more old technology. There are no more scalability problems: it takes a few clicks to add or remove servers from your cloud infrastructure. Cloud also means that you only pay for what you need, which is essential when you are just starting your business. And these are only a few over many more advantages.

However, if it looks too good to be true, it probably is. The associated problems and complications concerning cloud security have come to the forefront. Cloud Providers such as Amazon Web Services, aka AWS, Microsoft Azure, or Google Cloud Platform, aka GCP, rely on a shared responsibility model. In other words, the customer still has **many** responsibilities to ensure security and privacy.



Since they own and manage the hardware, cloud providers are responsible for the security **"in" the Cloud**, meaning they are responsible for protecting their infrastructure, including the facilities, the hardware, the software, and the networking components they use to run their services. However, it does not mean that these cloud providers are responsible for everything. The customer is responsible for the security **"of" the Cloud**.

Let's take a straightforward example. If your company is hosting a website on a web server using an AWS EC2 instance, AWS will ensure that no one messes with the actual physical server where your EC2 instance is hosted. However, making sure that the services are not vulnerable on your web server remains your responsibility. In other words, you are responsible for what you do with the provided services. And there is a lot to manage: applications, access management, operating systems, firewall, encryption, etc.

Social media accounts are an excellent example to understand the shared responsibility model. You are provided with the privacy and security settings for your accounts, and you need to take steps to enable those. They are not enabled for you by default.

Without the right considerations of the shared responsibility model, businesses find themselves exposed to high business risks, such as possible data breaches and business operation paralysis.

In conclusion, even though Cloud technology enables you to "jump-start" your business, it often fails you because the security requirements are complex and various. Most SME owners don't know where to start, what to do and how to cost-effectively choose their cybersecurity budget in association with their cyber risks. Antivirus, firewall, network-based *intrusion detection system* (*NIDS*), host-based *intrusion detection system* (*HIDS*) , host-based *intrusion prevention system* (HIPS), security information and event management (SIEM), data loss protection (DLP), the list is very long and full of acronyms that look all the same to the non-cyber security specialists.

Responsible Cyber understands this problem and has been relentlessly working to develop a tool that would provide SME owners with a straightforward way of dealing with their cybersecurity. This innovative tool, called IMMUNE, is designed specifically for professionals with no in-depth security knowledge or professionals who need further assistance. Thanks to its cutting-edge algorithm, it manages to get an overall picture of your organization's cybersecurity posture with its associated business risks with only a few questions and an automated assessment. It defines your company's digital footprint. It will then recommend the most relevant measures and controls to enhance your posture following a risk-based approach, generating an automated risk register and focusing on "quick wins" to get the best results at the lowest cost.

Tom Philippe
Junior Cybersecurity Consultant at Responsible Cyber

For further information, please contact Mikko Laaksonen at mlaaksonen@responsible-cyber.com or visit our website: www.responsible-cyber.com

CONTRIBUTED CONTENTS

Insights from our Corporate Partner Programme (CPP) – Bitcyber

Bitcyber.com.sg is a dynamic and sharp Value- added Distributor for Singapore and the region. As Country Partner of bitdefender.com.sg and regional Distributor for Falainacloud.com and emailauth.io, BitCyber resolves painful breaches like ransomware, email spoofing and phishing, and Insider threats (Identity Access, database protection, and log integrity). For responsive protection, BitCyber offers Managed Detection and Response and Threat modelling tools. Here is a critical area to act on:

Misconfigurations: An Open Door to Compromise and Data Breaches

- Endpoint misconfiguration accounts for 27 percent of entry points exploited by attackers today
- As enterprises increasingly move workloads to the cloud, overburdened IT administrators frequently misconfigure accounts, applications and components
- Organizations typically lack formal, systematic hardening processes and policies to close security gaps
- IT reps require integrated endpoint configuration risk analysis at the heart of their security operations

While sophisticated cyber-incidents like the Equifax breach in 2019 and the recent SolarWinds hack dominate news headlines and keep CISOs up at night, simple misconfigurations by IT managers are actually among the most lucrative attack avenues for cybercriminals. Misconfiguration-borne attacks are regarded as the low-hanging fruit of cybercrime, as organizations often neglect to apply systematic hardening processes and policies to properly close entry points. Research by ESG shows that endpoint misconfiguration accounts for 27 percent of entry points exploited to gain access into environments by attackers.

Malicious actors thrive by capitalizing on unsecured hardware, employees with unnecessary access to critical company resources, unpatched vulnerabilities, false alert storms, and others. As organizations move their workloads to the cloud, the chance for misconfigurations increases while visibility of threats diminishes, further compounding the issue.

Top misconfigurations used to breach organizations

To do their job well, security teams must assess risk and rapidly remediate configuration errors without disrupting IT systems. However, that's easier said than done.

Overburdened, under-resourced and typically understaffed, IT administrators frequently misconfigure OS-related applications and components. Common IT errors crop up in Microsoft Office, SharePoint, ACTIVE_X, and Windows Remote Management (WinRM). The COVID-19 pandemic has pushed remote access vulnerabilities and misconfigurations to the

forefront of cybersecurity as a favored attack vector. Unsurprisingly, configuration errors related to WinRM now rank highest among misconfigurations in Microsoft software.
WinRM allows a user to interact with a remote system, run an executable (such as deploy malware), modify the registry, or modify services, making it an area of great concern. Improper configuration of WinRM can often lead to a devastating cyber incident.

Bitdefender data shows that misconfigurations related to accounts, password storage and password management on endpoint are the most commonly misconfigured with a 12.5 percent share.

A misconfigured account opens the door to account takeover, spear phishing/BEC compromise, lateral movement, malware infection and data leaks. Most ransomware incidents occur because of a misconfigured component, an unpatched vulnerability or a successful social engineering scheme. Since ransomware attacks today are synonymous with data breaches, organizations risk multiple levels of extortion – because of a single misconfiguration or IT-related oversight.

Reducing the attack surface
To address the challenges of ensuring configurations are accurate and up-to-date, enterprises need integrated endpoint configuration risk analysis at the heart of their security operations. This provides key visibility and automated remediation.
Most endpoint protection platforms fail to assess risks associated with misconfiguration, forcing security teams to constantly react to trivial alerts and conduct repetitive, manual vulnerability management, incident triage, and patching.

To help organizations navigate through the dangerous waters of misconfigurations, Bitdefender offers solid support through advanced endpoint risk analytics, network analytics, cloud security and human risk assessment at the heart of its GravityZone security suite. The powerful platform enables security teams and administrators to minimize the attack surface, stop potential compromise and gain full visibility into risks associated with misconfigurations.

For further information, please contact Mike Ang at mike@bitcyber.com.sg or visit our website: BitCyber.com.sg

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.