AiSP

NEWSLETTER

February 2022

NEWS & UPDATE

New Partners

AiSP would like to welcome Savinyt as our new Corporate Partner and Singapore University of Social Sciences (SUSS)as our new Academic Partner. AiSP looked forward to working with our Partners to contribute to the Cybersecurity Ecosystem.

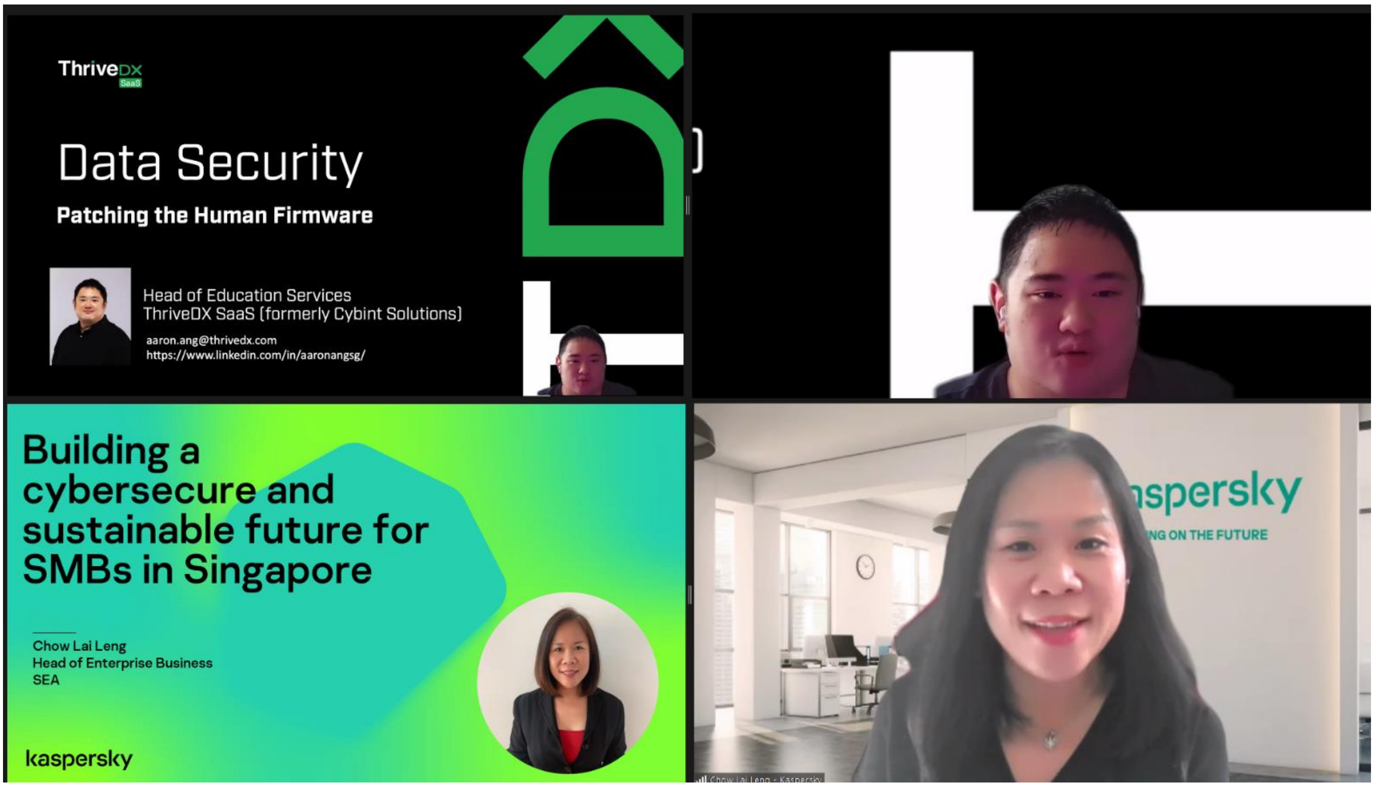
SAVIYNT

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

Knowledge Series Events

Data Security on 27 Jan 22

As part of Digital for Life movement, we hope to help people of all ages and walks of life to embrace digital learning as a lifelong pursuit. It was a pleasure to have Mr Aaron Ang from our CPP ThriveDX SaaS and Ms Chow Lai Leng from our CPP Kaspersky to share their knowledge on Data Security for our Knowledge Series for the month of January. We would like to thank all participants who have joined the webinar on 27 January and the support from our two partners, ThriveDX SaaS and Kaspersky.



ThriveDX SaaS

Data Security

Patching the Human Firmware

Head of Education Services
ThriveDX SaaS (formerly Cybint Solutions)
aaron.ang@thrivedx.com
https://www.linkedin.com/in/aaronangsg/

Building a cybersecure and sustainable future for SMBs in Singapore

Chow Lai Leng
Head of Enterprise Business
SEA

kaspersky

back to top

Red Team Blue Team on 17 Feb 22

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

AiSP Advance Connect Excel

AiSP Knowledge Series – Red Team Blue Team

AiSP Knowledge Series:
RED TEAM
BLUE TEAM
17 Feb | 7PM-9PM | Zoom
KOK KIAT HAN
Systems Engineer (Cyber Intelligence Analyst)
Cyber Security Agency of Singapore
GUO GEN
Consultant
Cyber Security Agency of Singapore
TEO KIA MENG
Systems Engineer
Cyber Security Agency of Singapore
Organised by:
AiSP Advance Connect Excel
Supported by:
CSA SINGAPORE
IMDA INFOCOMM MEDIA DEVELOPMENT AUTHORITY
In support of:
DIGITAL FOR LIFE

As part of Digital for Life movement, we hope to help people of all ages and walks of life to embrace digital learning as a lifelong pursuit. In the month of February Knowledge Series, we are excited to have Cyber Security Agency of Singapore (CSA) on board. CSA will be sharing with us exciting technical information and best practices across domains such as Red Teaming, Threat Intelligence, and Incident Response. More information can be found below.

A bag of red tricks
By: Guo Gen | Consultant, Cyber Security Agency of Singapore

This talk aims to demonstrate recent Tactics, Techniques, and Procedures (TTP) used by ransomware operators and nation state threat actors. The emphasis will be on Initial Access, Execution, Persistence, Defense Evasion and Command and Control.

back to top

A bag of blue tricks
By: Teo Kia Meng | Systems Engineer, Cyber Security Agency of Singapore

In this talk, we outline possible blue team actions that would lead to effective detection and response to the tactics, techniques, and procedures as outlined in the previous presentation - 'A Bag of (Red) Tricks'. Modern forensic techniques and artifacts will also be showcased.

Too many tricks! Which one to pick?
By: Kok Kiat Han | Systems Engineer (Cyber Intelligence Analyst), Cyber Security Agency of Singapore

In this talk, we will outline Cyber Threat Intelligence (CTI) best practices that strategise the application of various techniques during an investigation. With presentations - 'A Bag of (Red) Tricks' & 'A Bag of (Blue) Tricks' as the backdrop, this talk aims to demonstrate CTI as a force multiplier for offensive and defensive techniques covered.

Date: 17th February 2022 (Thurs)
Time: 7PM to 9PM
Venue: Zoom
Registration: https://zoom.us/webinar/register/2516389412390/WN_WC39-EKSQtakKS56GCVh7A

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 2022 are as follows (*may be subjected to changes*),

1. Red Team VS Blue Team, 17 Feb 22
2. Cryptography, 31 Mar 22
3. Cloud Security, 13 Apr 22

Please let us know if your organisation is keen to be our sponsoring speakers in 2022!
AiSP members who registered for the event, can playback the recorded event via their member profile in Glue Up. If you did not sign up for the event, please email secretariat@aisp.sg for assistance. Please refer to our scheduled 2022 webinars in our event calendar.

back to top

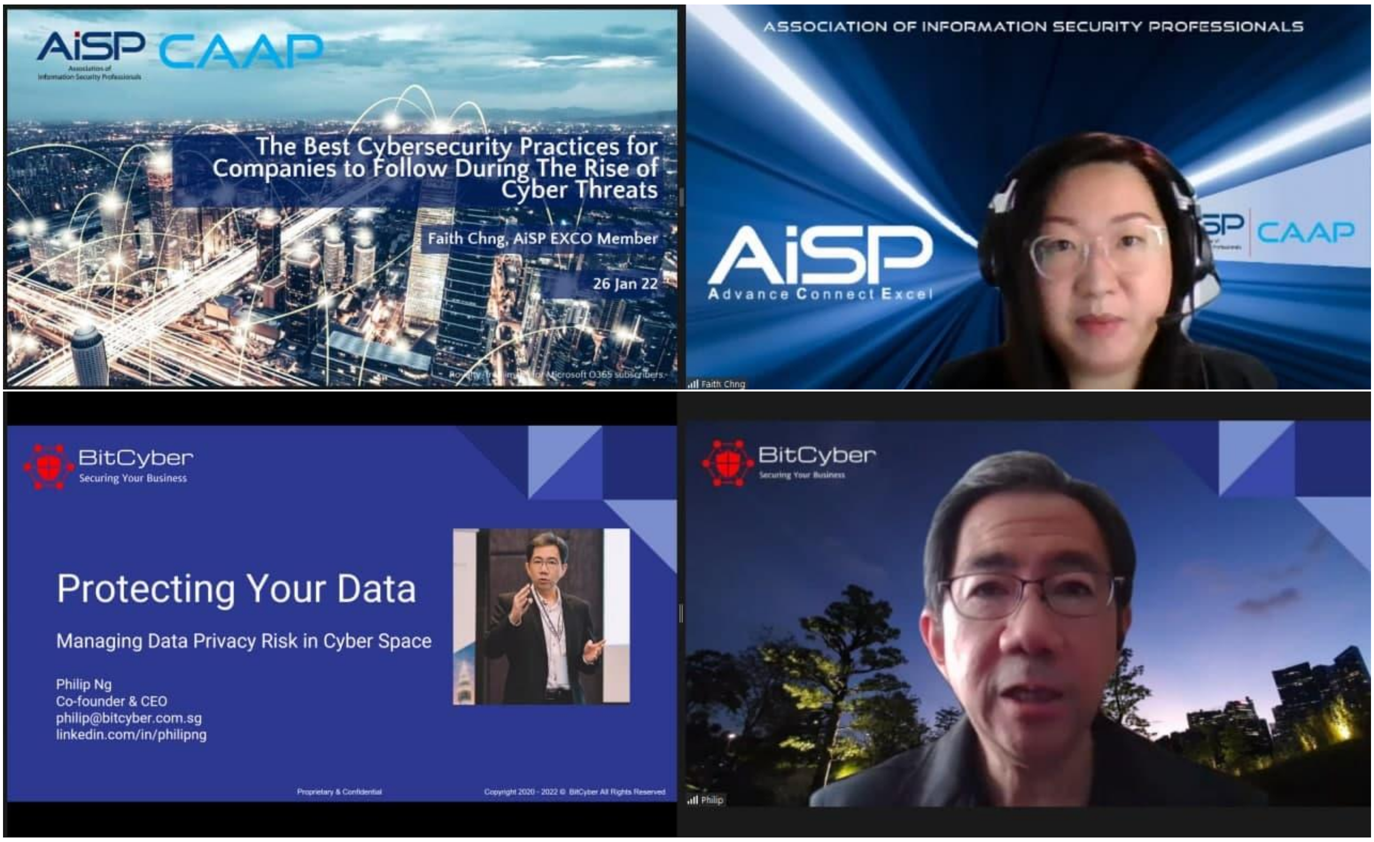
Cybersecurity Awareness & Advisory Programme (CAAP)

AiSP x ASPRI – Cybersecurity Best Practices & Data Privacy Risks

It was an insightful morning on 26 January with AiSP EXCO Member, Ms Faith Chng sharing on the best cybersecurity practices for companies to follow during the rise of cyber threats and Mr Philip Ng, CEO of our CPP Bitcyber who shared on Protecting your data - Managing Data Privacy Risks.

Thank you all who joined us in the event on the best practices and data privacy risks to help your business. We hope that everyone had benefit the session.

Do visit https://www.aisp.sg/smecybersafe/ on the list of solutions and toolkits that can help in your business.



The Best Cybersecurity Practices for Companies to Follow During The Rise of Cyber Threats
Faith Chng, AiSP EXCO Member
26 Jan 22

Protecting Your Data
Managing Data Privacy Risk in Cyber Space
Philip Ng
Co-founder & CEO
philip@bitcyber.com.sg
linkedin.com/in/philipng

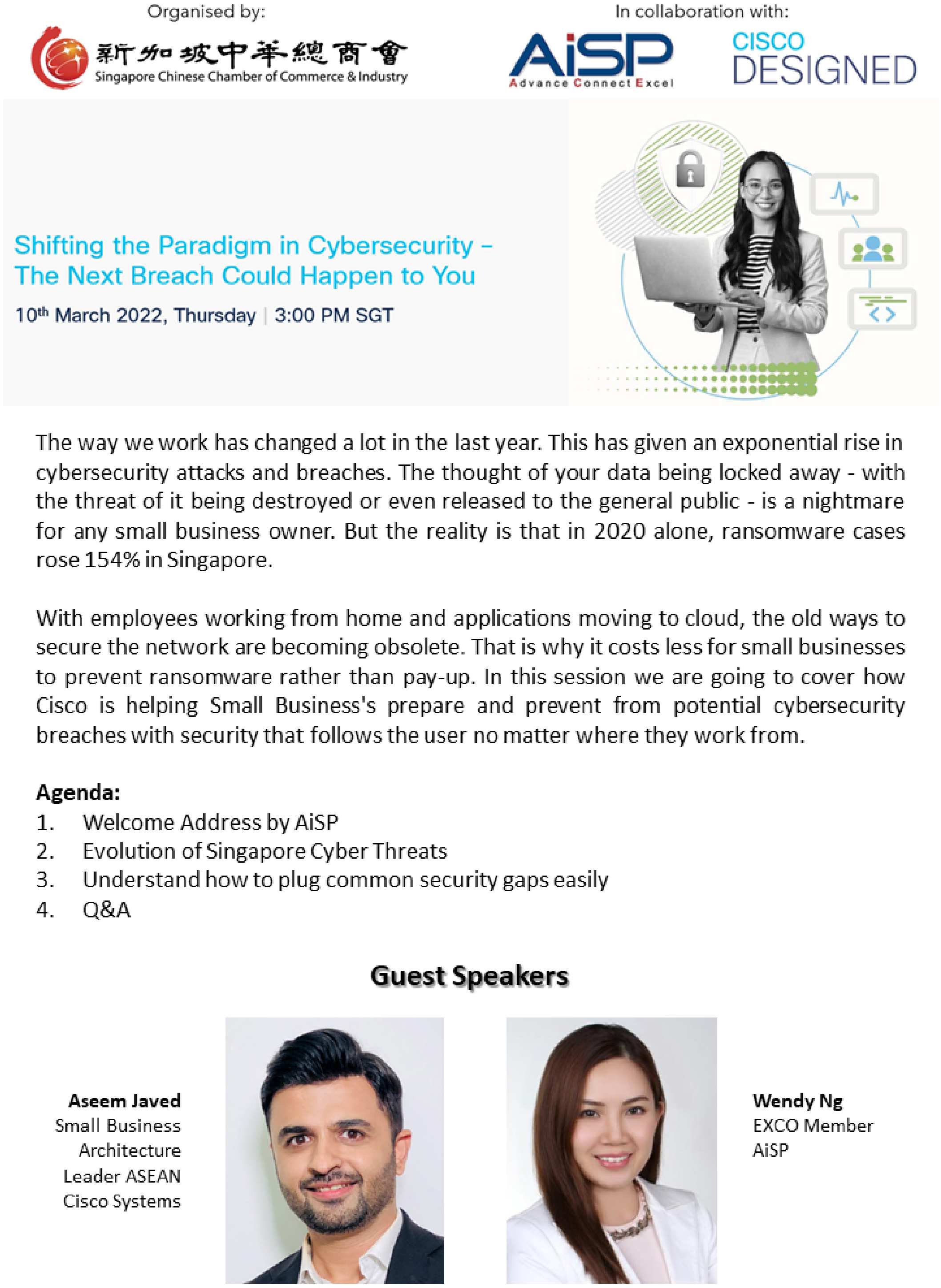
AiSP CAAP
ASSOCIATION OF INFORMATION SECURITY PROFESSIONALS
AiSP Advance Connect Excel
Faith Chng
BitCyber Securing Your Business
Philip

back to top

Upcoming CAAP Event

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

CISCO& SCCCI CAAP Event on 10 March



Organised by:

新加坡中華總商會 Singapore Chinese Chamber of Commerce & Industry

In collaboration with:

AiSP Advance Connect Excel

CISCO DESIGNED

Shifting the Paradigm in Cybersecurity – The Next Breach Could Happen to You

10th March 2022, Thursday | 3:00 PM SGT

The way we work has changed a lot in the last year. This has given an exponential rise in cybersecurity attacks and breaches. The thought of your data being locked away - with the threat of it being destroyed or even released to the general public - is a nightmare for any small business owner. But the reality is that in 2020 alone, ransomware cases rose 154% in Singapore.

With employees working from home and applications moving to cloud, the old ways to secure the network are becoming obsolete. That is why it costs less for small businesses to prevent ransomware rather than pay-up. In this session we are going to cover how Cisco is helping Small Business's prepare and prevent from potential cybersecurity breaches with security that follows the user no matter where they work from.

Agenda:

1. Welcome Address by AiSP
2. Evolution of Singapore Cyber Threats
3. Understand how to plug common security gaps easily
4. Q&A

Guest Speakers

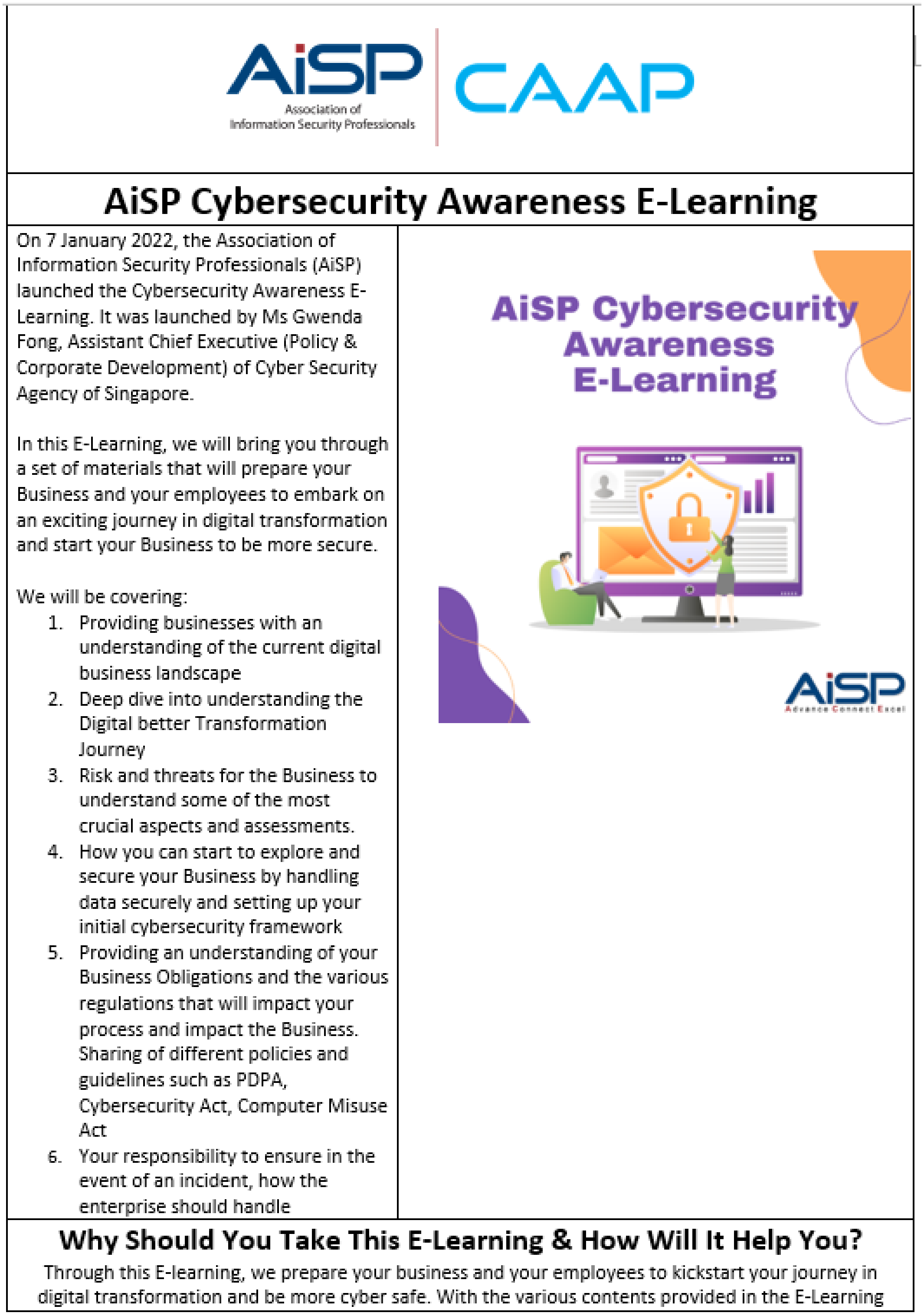
Aseem Javed
Small Business Architecture Leader ASEAN
Cisco Systems

Wendy Ng
EXCO Member
AiSP

Click here to register.

back to top

AiSP Cybersecurity Awareness E-Learning



AiSP Cybersecurity Awareness E-Learning

On 7 January 2022, the Association of Information Security Professionals (AiSP) launched the Cybersecurity Awareness E-Learning. It was launched by Ms Gwenda Fong, Assistant Chief Executive (Policy & Corporate Development) of Cyber Security Agency of Singapore.

In this E-Learning, we will bring you through a set of materials that will prepare your Business and your employees to embark on an exciting journey in digital transformation and start your Business to be more secure.

We will be covering:

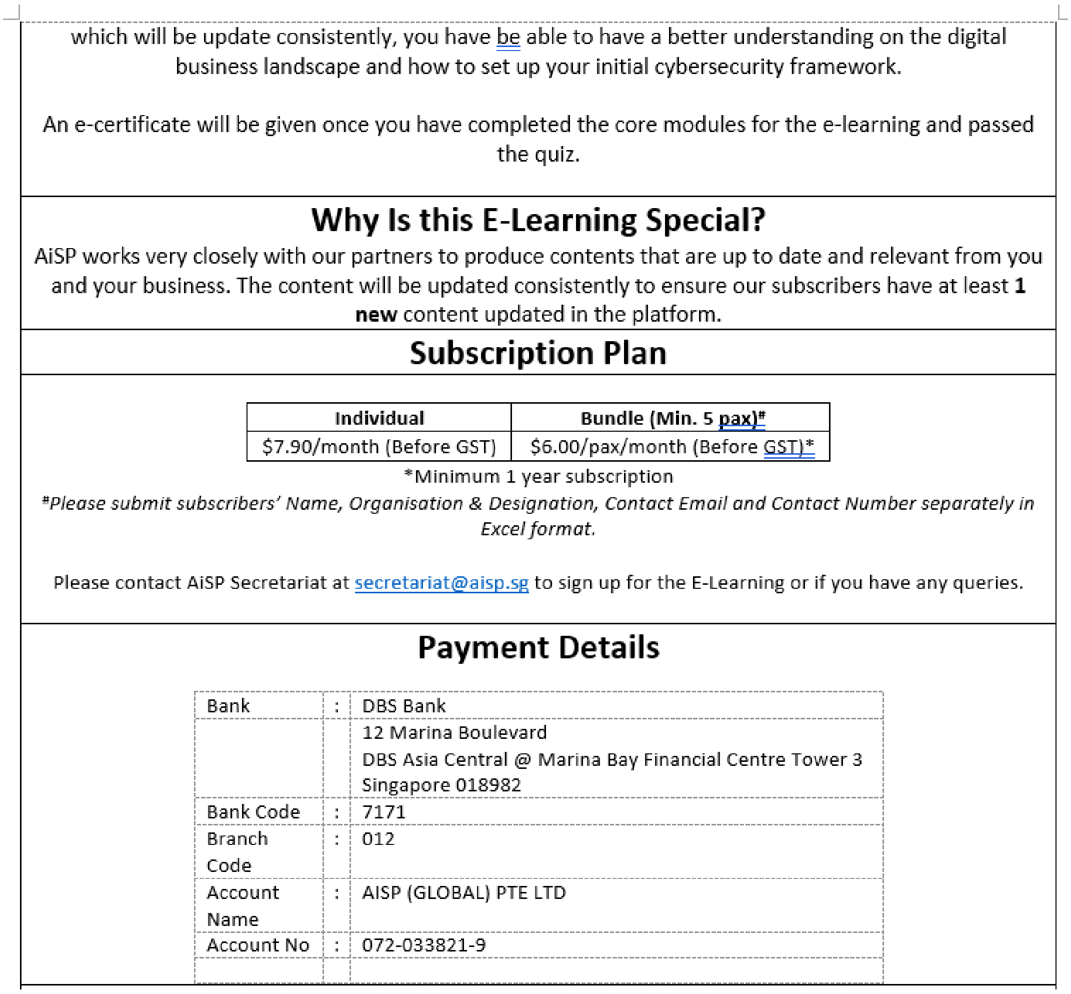
1. Providing businesses with an understanding of the current digital business landscape
2. Deep dive into understanding the Digital better Transformation Journey
3. Risk and threats for the Business to understand some of the most crucial aspects and assessments.
4. How you can start to explore and secure your Business by handling data securely and setting up your initial cybersecurity framework
5. Providing an understanding of your Business Obligations and the various regulations that will impact your process and impact the Business. Sharing of different policies and guidelines such as PDPA, Cybersecurity Act, Computer Misuse Act
6. Your responsibility to ensure in the event of an incident, how the enterprise should handle

AiSP CAAP
Association of Information Security Professionals
AiSP Cybersecurity Awareness E-Learning
AiSP Advance Connect Excel

Why Should You Take This E-Learning & How Will It Help You?

Through this E-learning, we prepare your business and your employees to kickstart your journey in digital transformation and be more cyber safe. With the various contents provided in the E-Learning

back to top



which will be update consistently, you have be able to have a better understanding on the digital business landscape and how to set up your initial cybersecurity framework.

An e-certificate will be given once you have completed the core modules for the e-learning and passed the quiz.

Why Is this E-Learning Special?

AiSP works very closely with our partners to produce contents that are up to date and relevant from you and your business. The content will be updated consistently to ensure our subscribers have at least **1 new** content updated in the platform.

Subscription Plan

Individual	Bundle (Min. 5 pax)#
$7.90/month (Before GST)	$6.00/pax/month (Before GST)*

*Minimum 1 year subscription

#Please submit subscribers' Name, Organisation & Designation, Contact Email and Contact Number separately in Excel format.

Please contact AiSP Secretariat at secretariat@aisp.sg to sign up for the E-Learning or if you have any queries.

Payment Details

Bank	:	DBS Bank
		12 Marina Boulevard DBS Asia Central @ Marina Bay Financial Centre Tower 3 Singapore 018982
Bank Code	:	7171
Branch Code	:	012
Account Name	:	AISP (GLOBAL) PTE LTD
Account No	:	072-033821-9

SME Cybersafe provides

Enhanced Security Awareness & Training

Cohesive Security Knowledge Resources

Security Solutions & Services Support

Click here to find out more about the E-Learning.

back to top

AiSP SME Cybersecurity Conference

AiSP SME Cybersecurity Conference was held in hybrid format on 7 January at the Lifelong Learning Institute with the support from Cybersecurity Agency of Singapore (CSA). The welcome address was shared by Mr Johnny Kho, AiSP President and opening address by Ms Gwenda Fong, Assistant Chief Executive (Policy & Corporate Development) of Cyber Security Agency of Singapore - CSA followed by a sharing from Mr Tony Low, AiSP CAAP Lead.

Both virtual and physical participants benefitted from Mr Andrew Moey's sharing on "Simplify Business Security, Without Sacrifice",Mr Thomas Wee's sharing on "Block Evolving Email Threats", Mr Alvin Teo's sharing on "Prepare Today for Tomorrow's Challenges" and Mr Charles Lim, for sharing on "Managing Identity and Access with a Dynamic Workforce". The conference ended with a panel discussion moderated by Mr Tony Low, AiSP CAAP Lead on "Strengthening Cybersecurity Awareness to Defend Against the increase cyber threat".

AiSP would like to thank Fortinet, Green Radar, Onesecure Asia Pte Ltd, SecurID and Thales for sponsoring SME Cybersecurity Conference. If you want to revisit the conference, you can view it here.

Welcome A[...]s By AiSP
AiSP
Advance Connect Excel
SecurID
The Trusted Identity Platform
GREEN RADAR
PANEL DISCUSSION
"Strengthening Cybersecurity Awareness to Defend Against The Increased Cyber Threats"
HALES

back to top

Student Volunteer Recognition Programme (SVRP)

SVRP Awards Ceremony 2021

The third SVRP Awards Ceremony was held on 19 January 2022 at Lifelong Learning Institute Event Hall. Congratulations to all our award winners for SVRP 2021. The Student Volunteer Recognition Programme is co-developed by AiSP and the Cyber Security Agency of Singapore - CSA. Thank you Minister of State Tan Kiat How for gracing the event.

We would also like to thank Ensign InfoSecurity for supporting the ceremony. Our nomination for SVRP 2022 is ongoing from 1 Aug 21 to 31 July 22. Please **click here** to apply today.

back to top

Singapore Cyber Security Inter Association (SCSIA)

Singapore Cyber Day Quiz 2021

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

The quiz has officially ended on 29 December 2021 and the prize presentation was held on 28 January 2022 at Fortinet's office. Congratulations to the top 10 winners listed below

1) Gadiel Lau Rongzheng
2) Sabrina Kor Jia En
3) Er Song Kai
4) Yuen Si Hao
5) Chai Pin Zheng
6) Wong Qi Jun Hazel
7) Kishor Kumar Haribaskar
8) Gary Tan Jin Xian
9) Wong Xin Yi Dawn
10) Ju Zihao

Thank you for your participation and support for our Singapore Cyber Day Quiz 2021. We would also like to thank all the below supporting associations who contributed to the quiz content to make Singapore Cyber 2021 a success.

back to top

Ladies in Cybersecurity

https://www.aisp.sg/ladies_about.html
NETWORKING | MENTORING | SPECIAL PROGRAMMES
LADIES IN CYBER
AiSP
'Ladies Talk Cyber' Series
February 2022 Edition
Interview of Ms Wendy Ng

Ladies Talk Cyber Series

For the Nineth edition of AiSP's 'Ladies Talk Cyber' series, we interviewed Ms Wendy Ng, AiSP EXCO Member, country head of cyber security sales for one of the largest global technology MNCs, with Singapore as its Asia Pacific headquarters. As a leader in cyber security, Wendy is passionate about helping companies to overcome security challenges, elevate security posture and meet business goals. She believes that security should not only by its design, but also its simplicity to implement, operate and complement business objectives.

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

Wendy is the country head of cyber security sales for one of the largest global technology MNCs, with Singapore as its Asia Pacific headquarters.
As a leader in cyber security, Wendy is passionate about helping companies to overcome security challenges, elevate security posture and meet business goals. She believes that security should not only by its design, but also its simplicity to implement, operate and complement business objectives.

Please click here to view the full details of the interview.

back to top

AiSP Advance Connect Excel | LADIES IN CYBER

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

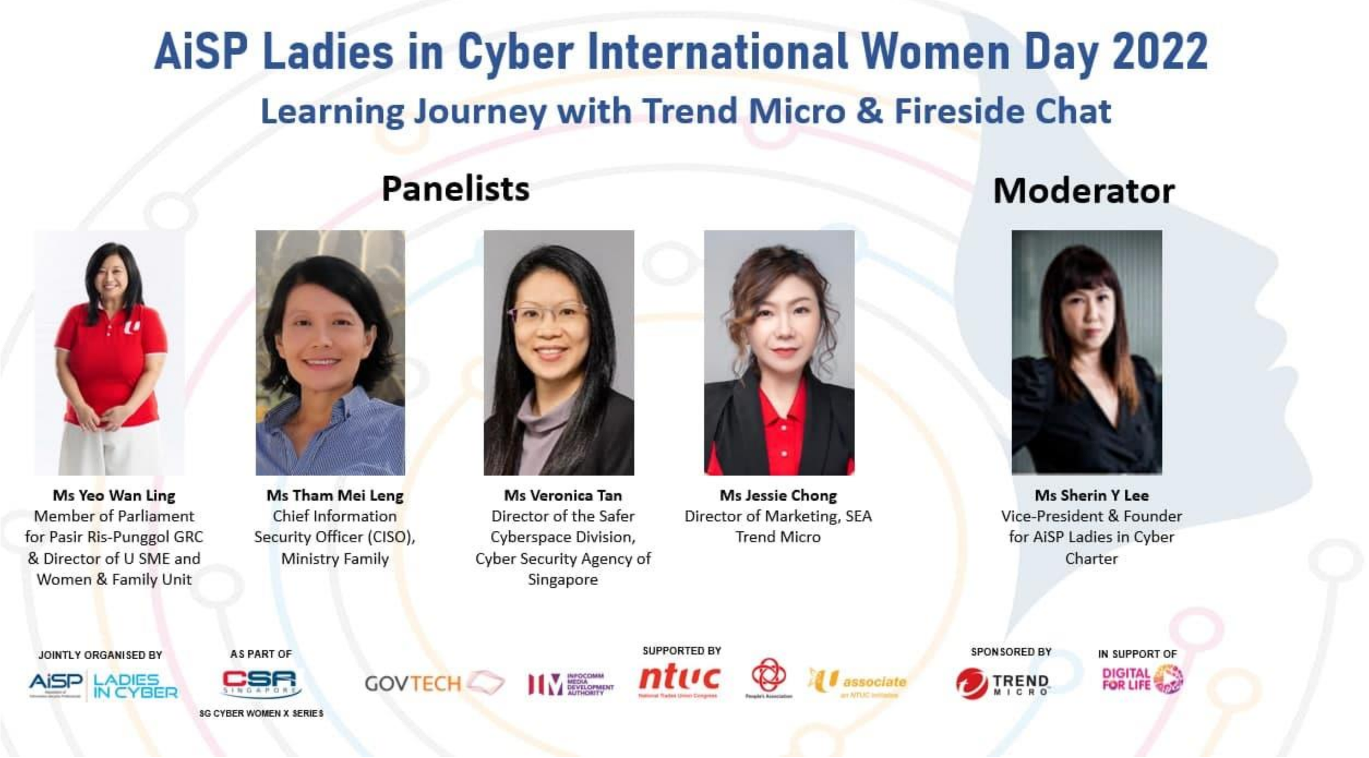
AiSP organised the Learning Journey to Cisco ASEAN on 21 Jan 22 and we have the honour of having Senior Minister of State in the Ministry of Foreign Affairs and the Ministry of National Development Ms Sim Ann, Ms Catherine Lee, Ms Wendy Ng & Ms Sherin Y Lee to join more than 80 female students & 40 female professionals in a hybrid fireside after the learning journey. Many questions were raised during the session such as what can Singapore do differently to dispel the misconception that cybersecurity is not a suitable career choice for women and why is it important for Singapore to have more women join the cybersecurity sector?

We would like to thank SMS Sim Ann for joining us in the session and Cisco for their kind sponsorship for the event and for hosting all the students in their beautiful office and supporting the event.

Join us in our next AiSP Ladies in Cyber Learning Journey & Fireside Chat as part of AiSP International Women Day 2022 Celebrations on 8 Mar 22 in a Hybrid Fireside Chat. Sign up virtually at https://lnkd.in/exvt8Zwb. Physical registration is open to students only and please email to secretariat@aisp.sg to sign up or sign up through their lecturers.

back to top

AiSP International Women Day Celebrations – 08 March 2022



AiSP Ladies in Cyber International Women Day 2022

Learning Journey with Trend Micro & Fireside Chat

Panelists

Moderator

Ms Yeo Wan Ling
Member of Parliament for Pasir Ris-Punggol GRC & Director of U SME and Women & Family Unit

Ms Tham Mei Leng
Chief Information Security Officer (CISO), Ministry Family

Ms Veronica Tan
Director of the Safer Cyberspace Division, Cyber Security Agency of Singapore

Ms Jessie Chong
Director of Marketing, SEA Trend Micro

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

JOINTLY ORGANISED BY

AS PART OF

SG CYBER WOMEN X SERIES

SUPPORTED BY

SPONSORED BY

IN SUPPORT OF

With men in tech outnumbering women by 3 to 1, Cybersecurity industry has always had an undeserved reputation of being a man's world. And there are quite a few reasons for the disproportionate number but arguably the main reason for it, is the lack of understanding of what women can do in an industry that's perceived to be tough and unforgiving. Yet, recent studies show that women are more likely to hold high-level roles in cybersecurity industry. It has also been proven that organizations advocating gender diversity tends to be more profitable.

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

This coming International Women Day 2022 on 8 Mar 22 (7.30pm to 8.30pm), **AiSP Ladies in Cyber** is organizing a hybrid fireside chat together with our Corporate Partner Trend Micro. Join **Ms Yeo Wan Ling, Ms Tham Mei Leng, Ms Veronica Tan, Ms Jessie Chong and Ms Sherin Y Lee** - our female leaders from Cybersecurity industry as they share their experience, advice and provide guidance on career in IT industry for females.

Sign up virtually at:
https://zoom.us/webinar/register/3016429005761/WN_EDPpwcSGRViZ55PwJjt4nw.
Physical registration is open to students only and they can email to secretariat@aisp.sg to sign up or sign up through their lecturers.

back to top

AiSP Ladies in Cyber Inaugural Symposium – 22 March 2022

AiSP Ladies in Cyber Symposium

"How Can Women In Tech Define The Future Of Cyber & Tech?"

Dialogue Session

Minister Josephine Teo
Minister for Communications and Information and Minister-in-Charge of Smart Nation and Cybersecurity

Ms Tammie Tham
Chief Executive Officer of Ensign InfoSecurity
Co-Chair of the AiSP Advisory Council

Ms Teo Yi Ling
Senior Fellow, Centre of Excellence for National Security , S Rajaratnam School of International Studies

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

Attend Breakout Sessions By Female Cybersecurity Experts

Dr Tan Mei Hui
AiSP Mentor
Director at Tencent
Speaker for AI in Cybersecurity / Threat Modelling

Ms Soffenny Yap
AiSP IoT SIG Lead
Security Services Sales Leader of IBM
Speaker for IoT

Ms Sugar Chan
AiSP EXCO Member
Manager at Boston Consulting Group (BCG)
Speaker for Risk

Ms Daisy Radford
AiSP Mentor
Head of Operations & Delivery APAC at BAE Systems
Speaker for Security Operations

JOINTLY ORGANISED BY

AS PART OF

SG CYBER WOMEN X SERIES

SUPPORTED BY

IN SUPPORT OF

SPONSORS

AiSP will be organising the inaugural Ladies in Cyber Symposium for the female Youths that highlights 4 different topics on cybersecurity, including the importance of cybersecurity, and how women can play a role in it. We are expecting 150 Youths and professionals (Subject to COVID-19 restrictions) at the event on 22 March 2022 at Life-Long Learning Institute. The theme for this year Symposium is "**How can Women in Tech define the future of Cyber & Tech".**

Visit https://www.aisp.sg/cyberfest/ladies_symposium.html for more details on the event.

back to top

Special Interest Groups

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

- Cloud Security
- Cyber Threat Intelligence
- Data and Privacy
- IoT

We would like to invite AiSP members to join our **Special Interest Groups** as there are exciting activities and projects where our members can deepen their knowledge together. If you are keen to be part of a SIG, please contact secretariat@aisp.sg

CREST Singapore

CREST is an international not-for-profit accreditation and certification body representing and supporting the technical cybersecurity market.

CREST has a network of approaching 300 accredited member companies operating in many countries worldwide. In addition, thousands of cybersecurity professionals globally hold one or more CREST certifications. CREST also has links to governments, regulators and partner organisations in numerous countries.

CREST has a proud history of working with organisations in Southeast Asia, including AiSP. Indeed, AiSP ran a project in partnership with CREST between 2016 and 2021 to help establish the CREST Singapore Chapter. The project concluded successfully in March 2021 and CREST began a process of transition to a fully autonomous chapter.

Thanks to the work of AiSP, and others around the world, CREST now has a truly international structure covering Southeast Asia, Australasia, the Americas, the EU and the UK. Members in each of these regions are represented on elected CREST Regional Councils.

The CREST Southeast Asia Council was elected in December 2021 and comprises of 11 members. It is chaired by Emil Tan, Chief Operating Officer of cybersecurity talent development company Red Alpha. Emil founded Singapore’s largest cybersecurity community group, Division Zero (Div0), and he previously worked for the Infocomm Media Development Authority (IMDA).

back to top

Emil, and the Chairs of the other Regional Councils, sit on the CREST International Council, ensuring our governance structure is representative and reflects CREST's global reach.

The broad objectives of CREST in Southeast Asia are to support members to grow their businesses, grow the CREST membership, and support governments and regulators as they seek to enhance and elevate cybersecurity for their infrastructures and businesses.

CREST recently contributed to the Consultation on the Licensing Framework for Cybersecurity Service Providers, issued by the Cyber Security Agency of Singapore (CSA), at the end of 2021. CREST is committed to working in partnership to support the development of the cybersecurity industry in Singapore and the wider region.

CREST President Rowland Johnson also welcomed the CSA's updated Cybersecurity Strategy, launched in October 2021, saying: "CREST welcomes the strategy's focus on supporting organisations to adopt appropriate and high-quality cybersecurity solutions, underpinned by a skilled cybersecurity workforce linked to strong professional communities.

"CREST and its members look forward to working with the CSA to help to implement the strategy to secure Singapore's critical information infrastructure and boost its cybersecurity capabilities."

Globally, it has never been a more important time for governments, regulators, professional bodies like AiSP and CREST, and their members and partners to collaborate and develop more resilient cybersecurity ecosystems. Changes in the way we live and work, combined with the growth and diversification of threat vectors, present challenges and opportunities in equal measure.

2022 promises to be a busy year for CREST, and we are delighted to begin it by renewing our close working relationship with AiSP. We warmly welcome the opportunity to reach out to AiSP members and partners. Please contact singapore@crest-approved.org for more information on CREST examination in Singapore or any matters related to CREST.

Mr Emil Tan Chair, CREST Southeast Asia Council	Mr Rowland Johnson President of CREST

back to top

The Cybersecurity Awards

THE CYBERSECURITY Awards 2021

TCA 2021 Winners with Minister for Communications and Information and Minister-in-charge of Smart Nation and Cybersecurity, Mrs Josephine Teo

Congratulations to the winners of the 4th Cybersecurity Awards! Organised by the AiSP (Association of Information Security Professionals) and supported by Cyber Security Agency of Singapore - CSA and the Singapore Cyber Security Inter Association (SCSIA), the Awards ceremony honoured the outstanding contributions of individuals and organisations to the cybersecurity ecosystem. Mrs Josephine Teo, Minister for Communications and Information and Minister-in-charge of Smart Nation and Cybersecurity, graced the event as the Guest of Honour and thanked the winners for their contributions.

We hope that the winners and nominees will serve as an inspiration for others to contribute actively in the cybersecurity ecosystem towards securing our digital future!

Our heartiest congratulations to the Winners for The Cybersecurity Awards 2021:
Hall of Fame: Ng Hoo Ming
Leader: Huang Shao Fei
Professional: Eugene Lim & Shamane Tan
Student: Yu Pengfei
MNC (Vendor): Acronis Asia Pte Ltd
MNC (End User): DBS Pte Ltd
SME (Vendor): Responsible Cyber Pte Ltd

back to top

AiSP would like to thank all sponsors and partners who have supported and made the event successful!

back to top

Introduction to Cybersecurity in Public Healthcare - NHG's Perspective

On 27 January 2022, in collaboration with the National Healthcare Group (NHG) Group Information Security Office (GISO), AiSP organised a webinar for our Youths to gain more awareness and knowledge of cybersecurity in public healthcare for students. The students have a great time at the event and gain insights through the session.

back to top

Upcoming Activities/Events

Ongoing Activities

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

Upcoming Events

Date	Event	Organiser
01 Feb	Launch Ceremony of Hill Street Virtual Heritage Trail	Partner
03 to 04 Feb	School Talk at Millenia Institute	AiSP
07 Feb	School Talk at Horizon Primary School	AiSP
09 Feb	TAC Roundtable on Digitalisation	Partner
17 Feb	Knowledge Series – Red Team, Blue Team	AiSP & Partner
22 Feb	Data Privacy Panel Discussion	AiSP & Partner
22 to 23 Feb	IT Security Frontiers 2022	Partner
25 Feb	TCA2021 Appreciation	AiSP
3 Mar	CTI SIG Event	AiSP
4 Mar	Your Mind Matters (Y2M) with AiSP	AiSP & Partner
8 Mar	AiSP International Women Day Celebrations at Trend Micro	AiSP & Partner
10 Mar	AiSP x CISCO x SCCCI CAAP Event	AiSP & Partner
16 to 17 Mar	IoT Asia+ 2022	Partner
22 Mar	Ladies in Cyber Symposium	AiSP
23 Mar	AiSP x Microsoft CAAP Roundtable	AiSP & Partner
23 to 25 Mar	Fintech India expo 2022	Partner
28 to 30 Mar	Protect 2022	Partner
30 Mar	Annual General Meeting 2022	AiSP
31 Mar	Knowledge Series – Cryptography	AiSP & Partner

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

back to top

CONTRIBUTED CONTENTS

Article from Internet of Things SIG

Internet of Thing (IoT) Security Whitepaper

1. Introduction

Internet of Things (IoT) technology has grown rapidly around the world in the past years. The growth will continue, and it is expected to have billions of IoT devices installed and operate by 2025.

IoT enables anything that is embedded with electronics, software, sensors, actuators, and connectivity to interact with each other. Devices within the IoT network are able to communicate and interact over the internet, and can be remotely monitored and controlled. For example, we can monitor our pets at home from office via an IoT enabled webcam. Although IoT devices make life easier and simpler, the convenience also has brought along new security challenges. The lack of trust on the IoT security becomes a huge barrier for IoT adoption.

IoT vulnerabilities were introduced by uncertainty and negligence on IoT devices during the design, deployment, maintenance and usage of the devices. A well-defined IoT security framework is required to educate both the IoT device developers and users, as well as providing necessary recommendations and best practices for the development and application of IoT.

1.1. Purpose and Scope

The Centre for Strategic Cyber Space and Security Science (CSCSS) Internet of Things (IoT) Security Framework described in this whitepaper aims to define processes and standards for secure IoT infrastructure usage and development. This whitepaper will help to strengthen the security of IoT by making technical and policy recommendations and developing best practices for the design, deployment, maintenance and usage of IoT devices.

Due to the complexity of the IoT architecture, it is not ideal to include all security issues related to each architecture in the world in the framework. Instead, this framework focus on the most common core components of the IoT architecture, which are: Edge Clients, Gateway and Cloud.

back to top

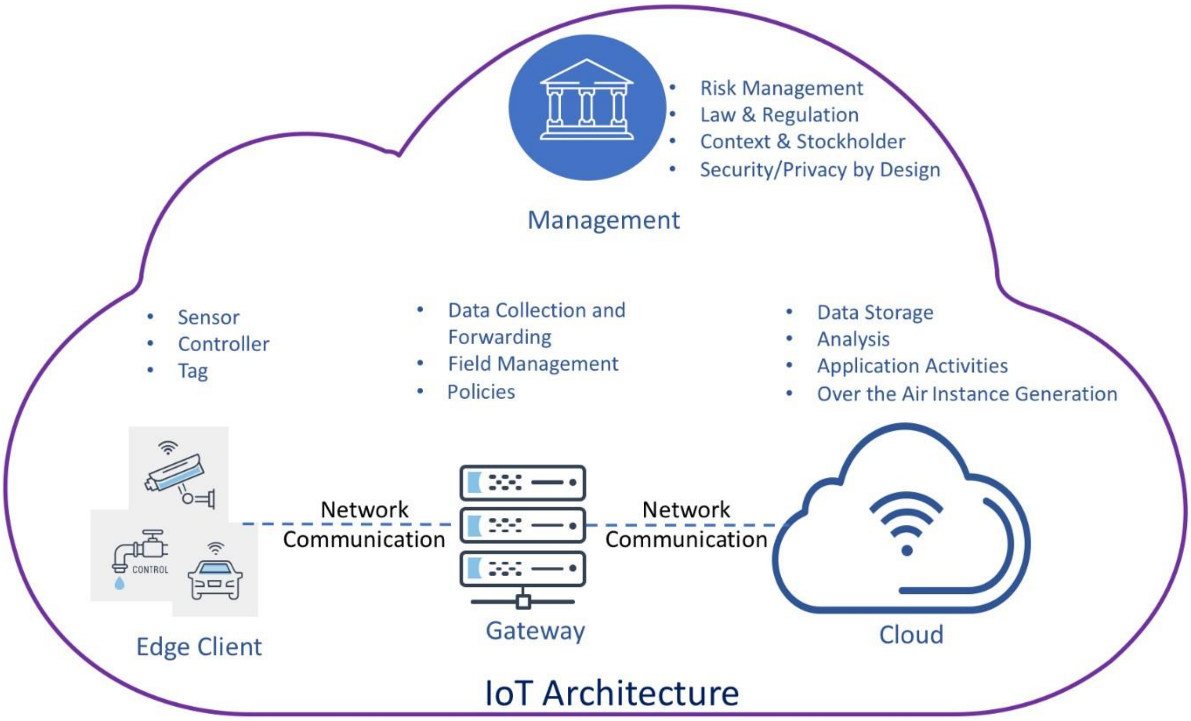


Figure 1 IoT Architecture

Common use cases of the core IoT components:

- **Edge Clients**[1] senses and collects data, then send the collected data to the **Gateway**.
- **Gateway** acknowledges and confirms the reception of the data with **Edge Client**, then perform identification on the data before sending it to the **Cloud**.
- **Cloud** receives the data from **Gateway**, then saves the data into its storage. After analyzing the data, output will be broadcasted to the **Edge Clients** through **Gateway**.

As IoT ecosystem consists of various IoT devices and cloud services from different vendors to collect data, preprocess data or filter data. Security issues might not be produced by only one type of IoT component but in fact, might cause by the poor design of the an entire IoT or through the technical incompatibility of two or more IoT components. As such, the design of IoT architecture should also be taken into account while evaluating the security of an IoT ecosystem. On the other hand, IoT ecosystem management issues such as risk management, law & regulation and security/privacy by design should also be considered throughout the whole IoT development lifecycle as well as during the adoption of IoT.

[1] Edge clients are IoT devices that are commonly installed or used in the client environment. For example, sensor or IP camera.

back to top

1.2. Market Need

The overarching purpose of this whitepaper is to make it possible for new IoT-enabled products and services to enter the market and meet the needs of both industrial and consumer users with the minimum possible risk. This obviously requires high levels of security at every level in order to create trust and reduce possible harm; but these high levels of security must be anchored in security standards that are definable, practicable and compatible with each other across entire supply and value chains, and where it is possible to measure and enforce compliance. Specifically, these security standards must answer the following market needs:

1. Governments and other large users and providers of IoT systems need to be able to rely on clear minimal standards of IoT security when sourcing and purchasing technology. There is currently a proposed law in the US Congress, the 'Internet of Things Cybersecurity Improvement Act,' that requires all IoT devices to be free of known security vulnerabilities and to be patchable in order to protect them from future attacks.
2. Clear standards will make it easier for both providers and users to deal with product liability issues that will inevitably arise as IoT become increasingly ubiquitous.
3. Clear standards will also make it easier for the insurance industry to provide suitable and unambiguous cover against both malicious attack on IoT-based systems and failures caused by negligence.

1.3. Normative References

ENISA Baseline Security Recommendations for IoT [1]
NIST Federal Information Processing Standards Publication 140-2: Security Requirements for Cryptographic Modules [2]
OWASP Internet of Things Top Ten [3]

1.4. Structure of this Paper

This whitepaper covers four major chapters.
Chapter 1 introduces purpose and scope; normative references; and outlines the structure of this whitepaper.
Chapter 2 examines the key security challenges that are associated with IoT technology.

Chapter 3 discusses the CSCSS IoT security requirements and provides recommendations to the development and adoption of IoT.
Chapter 4 provides mapping for the use of CSCSS IoT security requirements on edge clients, gateway and cloud. It also lists out the IoT security controls related to each of the IoT security requirements.

2. Internet of Things Security Challenges

With the rapid growth of IoT, new IoT vertical domains such as Industrial Internet of Things (IIoT), Internet of Medical (IoM) and Internet of Agriculture (IoA) emerge as a part of integration of IoT ecosystem. As the subcategories of IoT, each of these

back to top

verticals utilize similar Edge clients – Gateway – Cloud architecture. Although IoT brings opportunities to innovation such as connectivity and data collection for big data analytics to the industries, but at the same time, introduces new security threats to the environment as well. Such integrations might not be able to fulfil the regulations or standards of the security compliance, and thus slow down the adoption of IoT throughout the industries.

CSCSS has identified 8 common IoT security challenges that has emerged during the adoption and integration of IoT, which includes the following:

1. Privacy: IoT devices are instrumental in collection and analysis of sensitive data. These devices might not be secured enough to protect the users against security incidents such as data leakage.
2. Vulnerability: Due to the massive network connectivity generated by IoT devices, if one of the nodes is vulnerable to malicious attack, attackers might take advantage over the weakest link and attack the IoT network through the vulnerable node.
3. Mobile Devices: Mobile devices are becoming an indivisible part of our life and is often connected to the IoT network. These mobile devices are often used in checking or verifying the operation of the IoT network through it's own application and connectivity to the cloud infrastructure. Others could participate as part of the sensor network in the data collection process. These mobile devices, if not properly secured, could become a new attack vectors to the IoT network.
4. IoT Architecture: An IoT network consists of numerous IoT nodes which can be sensors, gateways or mobile devices. With the increasing number of nodes being connected to the IoT network, the chance of having a vulnerable node or malicious node within the network also increases.
5. Hardware Security: Hardware security is often neglected during the development of IoT devices. The IoT devices becomes vulnerable if security mechanisms against hardware attacks such as physical intrusion or physical tapping of these devices are not in place.
6. IoT Networking: Being remote controllable is often a key feature of IoT products. If network security mechanisms such as authentication is absent on the IoT device, malicious attacks can simply perform a remote attack toward the IoT network and gain access to multiple IoT devices or eventually other segments of the network.
7. System Upgrade/Update: System upgrade or update are common features for IoT devices. Without a strong authentication and verification mechanism, malicious users can leverage the system update/upgrade interface to control the software, hardware or firmware of the IoT devices.
8. Data Transmission: Distances between the IoT nodes varies. They can be next to each other, or they can be installed in different continents. As data transmissions between IoT nodes usually rely on wireless connections, without

back to top

sound authentication and identification mechanism, or even a secured network infrastructure for the data transmission, security incidents such as data leakage may occur.

The above eight IoT security challenges are the most common and critical security challenges associated with IoT. If they have not been considered during the development IoT, the IoT ecosystem will become vulnerable if more and more vulnerable IoT devices start to kick in. As such, CSCSS develops this whitepaper to provide recommendations and best practices for IoT developers.

The next section talks about the security requirements that are necessary to create a more secure IoT ecosystem.

3. CSCSS Internet of Things Security Requirements

Considering the security challenges associated with the IoT devices, such as unauthorized access and signal jamming, security recommendations and best practices on IoT are necessary to help secure the IoT ecosystem, as well as building trust on IoT utilization. As mentioned in the previous section, this whitepaper not only focuses security issues related to the development of IoT devices but also the application of IoT devices. IoT security incidents are not only caused by poorly designed IoT devices, but often, by the negligence on overall IoT infrastructure security from the IoT users.

Through outlining security requirements associated with IoT, CSCSS aims to provide recommendations and best practices for IoT development. It is also important to educate the IoT users on the security requirements of their IoT devices and how they can utilize the security mechanisms to have a more secured IoT experience.

CSCSS has identified 21 IoT security requirements and they can be categorized into 6 different categories, which are: general security, physical security, system security, communication security, authentication and authorization security, and privacy protection. Below is a list of the requirements:

3.1. General Security Requirements

3.1.1. Security by design

Consider the security of the whole IoT system from a consistent and holistic approach during its whole lifecycle across all levels of device/application design and development, integrating different security policies and techniques and design architecture by compartments to encapsulate elements in case of attacks throughout the development, manufacture, and deployment.

For IoT hardware manufacturers and IoT software developers it is necessary to implement test plans to verify whether the product performs as it is expected. Penetration tests help to identify malformed input handling, authentication bypass attempts and overall security posture.

Furthermore, human safety should be considered together with cyber security in mentioned lifecycle and designing for power conservation so as to ensure security will not be compromised.

back to top

3.1.2. Risk and Threat Identification and Assessment

A defense in depth approach to identify significant risk among the IoT ecosystem needs to be adopted. This include identifying the key network/information systems and the intended use/environment of a given IoT device within the IoT ecosystem.

3.1.3. Management of Security Vulnerabilities and Incidents

Establish procedures for analyzing and handling security incidents and participate in information sharing platforms to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners.

Based on the mentioned information-sharing platforms, create and coordinate and a publicly disclosed mechanism for vulnerability reports.

3.1.4 Third-Party relationships

It is necessary for IoT hardware manufacturers and IoT software developers to adopt cybersecurity supply chain risk management policies and communicate the cyber security requirements to their suppliers and partners.

All data processed by a third-party must be protected by a data processing agreement, especially when personal data of consumer sharing is involved.

Developer should only share personal data of consumer with third parties with express consent of the consumers, unless otherwise required and limited for the use of product features or service operations.

3.1.5. Cryptographic Management

Proper and scalable management mechanism and requirements should be implemented and enforced for cryptographic key generation, exchange, storage, usage, replace and discard.

Adopt well known cryptographic algorithms that are well recognized by the scientific community instead of proprietary or custom cryptographic algorithms for data process and communication.

3.1.6. Assessment of Impacts on Sensitive Information

Privacy impact assessments should be conducted before launching of any new developments and sensitive information should be identified and classified according to local laws during the development of IoT.

3.2. Physical Security Requirements

3.2.1. Physical Interface

IoT devices are not usually equipped with physical user interface as the requirement of user interaction is very limited. The physical ports on the devices are generally designed for debugging, providing connection to power source and network, entering engineering mode. Protection mechanism should be implemented against unauthorized access to firmware and operating system. If protection mechanism implementation is not possible, intrusion detection mechanism should be implemented.

back to top

A physical ‘reset’ button on the device or another physical buttons on the device should be implemented to trigger to ‘reset’ function which will be discussed in 3.1.2. Security mechanisms should be in place to prevent users from accidently pressing or unauthorized personnel on pressing the reset button. Such mechanisms can be having the ‘reset’ button ‘inside’ the device where it can only be reached after the device is dissembled or its cover is taken off. More secure mechanisms such as triggering the function only after the button is pressed for a period of time, or when a combination of different physical buttons is pressed at the same time should also be considered for restoring the devices to factory default settings.

3.2.2. Physical Layer

In most cases, IoT devices are installed in an unattended environment to function as sensors, monitors or data collectors. IoT devices should be protected against attacks such as physical damaging, signal jamming and signal interferences.

An IoT device should be setup by authorized personnel. The authorized personnel should input the basic parameters to the device and store them in the device’s built-in memory.

A ‘reset’ function should also be implemented for debugging, recycling and redeployment purposes. The function can either be triggered with a physical ‘reset’ button on the device or with another physical buttons on the device.

3.3. System Security Requirements

3.3.1. Operating System

Operating System is the core of IoT devices. Basic tasks such as memory management and configuration, system resource supply and demand prioritization, input and output control, network operation and file system management are all handled by the operating system. A user interface for the users to interact with the IoT devices can also be found in the operating system. Operating system is mostly embedded in the firmware stored in the flash memory, EEPROM, or PROM, within the application integrated circuit or programmable logic device. Functional or security updates can be performed through either internet or physical connection port.

Similar to operating systems on the other platforms (i.e. personal computers or networking devices), IoT operating systems may have flaws in design and are vulnerable to attacks such as privilege escalation attack and injection attack.

To manually update IoT device firmware, users are required to obtain the firmware themselves. Usually this can be done by downloading the firmware from the manufacturer official website. However malicious parties might modify the firmware to include malicious backdoor. They could advertise the firmware as a better version of the original firmware and lure the IoT users to download it.

Malicious application is also a security threat to IoT operation systems. Since most IoT devices run with single-chip computing architecture, anti-virus software that is designed for various platforms such as personal computer cannot be installed onto the devices. As such, malicious applications can easily be installed onto the devices and disrupt the operation of IoT services. Security mechanism against malicious code

back to top

execution should be in place to protect IoT devices from malicious application. Such mechanisms can be whitelisting and verification using encrypted chips.

3.3.2. Sensitive Data Storage

IoT edge clients such as sensors are often being used to collect information such as images, sounds, motions and geographical information. More sensitive information such as heart rate, blood pressure, and blood glucose measures are often being collected via edge clients for medical purposes. These data are temporary stored in a specific data storage within the edge client for preprocessing purposes or act as a backup to prevent data loss if transmission of such data is being interrupted. Due to the sensitive nature of the data, security mechanisms such as encryption or privilege control should be implemented.

3.3.3. Web-Based Management Interface

IoT devices are often appear as a micro device or installed at a location that is not easy to be reached. Device management can be done through a web-based management interface provided by the devices. It is known that web has the most security issues since the invention of internet, including injection, cross-site scripting (XSS) and man-in-the-middle attack. Malicious users can utilize these attacks to obtain the highest level of authorization through the web-based management interface. Thus, gain control over the IoT device or leak the information collected by the IoT device.

Security of web-based management interface should be considered during the IoT development life cycle. It is important to make sure security mechanism is in place during the design of the IoT and penetration testing against the interface is performed.

3.3.4. Application Programming Interface

An Application Programming Interface (API) is the convention for connecting different components of a software system. Using the API to quickly integrate without system applications can simplify and accelerate the formation of IoT ecosystem. Third-party API or library (LIB) are often used in IoT development. These API and LIB are "black boxes" to the developers as they cannot verify the security of the API and LIB through their source code. Developers should use API or LIB that are verified and code signed by the IoT manufacturers.

3.3.5. System Logging

The system log is used to record device system changes, such as settings changes, system errors, data file changes, and security incident auditing. It can also be used for system debugging, data recovery, or security incident investigation.

As security incident investigators use system log to understand the nature of security incidents, the completeness and accuracy must not be tampered. This can be achieved by enforcing security mechanism such as cryptography and privilege control on the system log.

back to top

Another consideration is that the built-in storage of IoT devices is very limited. Developers can consider using compression, backup and uploading the log to another location, depending of the regulation, security risk, storage life span and cost.

3.4. Communication Security Requirements

3.4.1. Network Port

A network port is a logical construct that identifies a type of network service. Edge clients can establish connection with the server (i.e. IoT gateway) for specific services with corresponding IP address and port number. Typically, there are two types of communications in IoT: communication between edge clients and gateway, and communication between gateway and cloud. IoT developers should choose a suitable network port for the IoT connections, such as ports that are not commonly used by network services (i.e. TCP 80/443). On the other hand, only enable ports that are required for the functionalities of IoT to prevent malicious attacks such as guessing, eavesdropping and service interruption.

3.4.2. Sensitive Data Transmission

Sensitive data might be collected or transmitted in the IoT ecosystem. To protect the security and privacy of the data owner, security mechanism should be implemented with reference to applicable regulations and guidelines. Also, transmission channel that is not known by unauthorized parties should be used for transmission of personally identifiable information (PII) or confidential information. Encryption should also be used to further protect the security of such information.

3.4.3. Communication Interface

IoT user should have the ability to enable/disable the connectivity of their devices. For example, if the user only uses Wi-Fi for IoT connection, he/she should be able to disable other functions such as Bluetooth and near-field communication. By disabling unused connection channel, it reduces the attack vectors for the malicious users to take advantage on. Encrypted communication and user authentication should also be considered to further protect the security of user-edge clients communication.

3.4.4. Communication Protocol

Various communication protocols are used between the IoT devices, services and users for different purposes. IoT developers should consider the maintainability and security of the protocols before adopting them into the design. For example, the developers can check rather the protocols have known vulnerabilities and their capabilities on mitigating attacks.

3.5. Authentication and Authorization Requirements

3.5.1. Authentication

Authentication is the function of verifying the identity of a user. To prevent unauthorized access, authentication should be used during the communication

back to top

between IoT edge clients, gateway and cloud. Multifactor authentication should also be considered to further improve the strength of the authentication mechanism.

3.5.2. Password

The use of password is the most common method for user authentication to prove identity. Mechanism such as complex composition rules, forcing password changes after certain period of time and limiting number of password guesses should be implemented to increase the security of the passcode.

Mirai malware was one noticeable attack that utilized IoT devices with default username and password pairs to create a botnet for distributed denial of service (DDoS) attacks. During the incident, Dyn, a DNS service provider was the target of the botnet created by IoT devices with Mirai malware installed. As the result, several high-profile websites from various fortune 500 companies were inaccessible for more than 6 hours in the 3-waves DDoS attack.

3.5.3. Authorization

Authorization is the function of specifying access right/privileges to resources. IoT users and devices should be given access to resources or IoT devices following the principle of least privilege. When designing the IoT, developers should consider the interaction between devices and devices, and users and devices to assign proper authorization to the user or devices.

3.6. Privacy Protection Requirements

3.6.1. Assessment of Sensitive Information

Privacy should be taken into account throughout the entire development process.

The following are design strategies that are related to sensitive data access and protection from "Privacy and Data Protection by Design – from policy to engineering" by European Union Agency for Network and Information Security (ENISA) [1]:

Minimize: The amount of personal data that is processed should be restricted to the minimal amount possible.

Hide: Personal data, and their interrelationships, should be hidden from plain view.

Separate: Personal data should be processed in a distributed fashion, in separate compartments whenever possible.

Authentication and authorization recommendation mentioned in the previous subsections should also be used to protect the privacy of IoT users.

The above 21 security requirements are commonly found in the IoT ecosystem. General security, physical security, system security, communication security, authentication and authorization, and privacy protection should be considered in the development and usage of IoT. Any negligence on such requirements may result in security incidents such as data leakage, or even causing a systemwide crash. In the next chapter, it includes the CSCSS IoT security requirements mapping on the 3 core IoT components: edge client, gateway and cloud.

4. CSCSS Internet of Things Security Requirements Mapping

Due to the nature of each core IoT components, security requirements that are mentioned in chapter 4 might not be applicable for each of them. In this chapter, it

back to top

includes the mapping of each security requirements against the core IoT components which are edge client, gateway and cloud. Below is a table (Table 1) of applicability for the security requirements with the core IoT components.

Table 1 Applicability of security requirements

Component Category	Security Requirement	Management	Architecture	IoT Components		
				Edge Client	Gateway	Cloud
General Security	Security by Design	○	○	○	○	○
	Risk and Threat Identification and Assessment	○	○	○	○	○
	Management of Security Vulnerabilities and Incidents	○	○	N/A	N/A	N/A
	Third-Party Relationships	○	N/A	N/A	N/A	N/A
	Assessment of Impacts on Sensitive Information	○	N/A	N/A	N/A	N/A
	Cryptographic Management	N/A	○	○	○	○
Physical Security	Physical Interface	N/A	N/A	○	○	N/A
	Physical Layer	N/A	N/A	○	○	N/A
System Security	Operating System	N/A	N/A	○	○	N/A
	Sensitive Data Storage	N/A	N/A	○	○	○
	Web-Based Management Interface	N/A	N/A	○	○	○

back to top

	Application Programming Interface	N/A	N/A	○	○	○
	System Logging	N/A	N/A	○	○	N/A
Communication Security	Network Port	N/A	N/A	○	○	N/A
	Sensitive Data Transmission	N/A	N/A	○	○	○
	Communication Interface	N/A	N/A	○	○	N/A
	Communication Protocol	N/A	N/A	○	○	○
Authentication and Authorization	Authentication	N/A	N/A	○	○	○
	Password	N/A	N/A	○	○	○
	Authorization	N/A	N/A	○	○	○
Privacy Protection	Assessment of Sensitive Information	○	○	○	○	○

Applicable：○ Non-applicable：N/A

The next six sections list out the CSCSS IoT security controls which are categorized under the 6 requirements.

4.1. General Security

4.1.1. Security by Design

MP-A01 Security by design

Manufacturer should have a stringent security by design procedure for firmware, driver and operating system components development. Security tests should be performed before the release of each update patches. Manufacturer should also have proper notification procedure to notify the users on updating their IoT devices.

4.1.2. Risk and Threat Identification and Assessment

MP-A02 Conducting risk and threat assessments

Risk assessments which include the following specific tasks should be conducted:

I. Identify threat sources that are relevant to IoT ecosystem/environment or components within; II. Identify threat events that could be produced by those sources;

back to top

III. Identify vulnerabilities within organizations that could be exploited by threat sources through specific threat events and the predisposing conditions that could affect successful exploitation;

IV. Determine the likelihood that the identified threat sources would initiate specific threat events and the likelihood that the threat events would be successful;

V. Determine the adverse impacts to organizational operations and assets, individuals, other organizations, and the Nation resulting from the exploitation of vulnerabilities by threat sources (through specific threat events); and

VI. Determine information security risks as a combination of likelihood of threat exploitation of vulnerabilities and the impact of such exploitation, including any uncertainties associated with the risk determinations.

MP-A03 Development of action plan

Based on the risk and threat assessed/identified, organization should develop a risk treatment strategy and action plan including: (i) proposed actions, priorities or time plans (ii) resource requirements (iii) roles and responsibilities of all parties involved in the proposed actions (iv) performance measures (v) reporting and monitoring requirements

4.1.3. Management of Security Vulnerabilities and Incidents

MP-A04 Establish procedures for responding security incidents

Procedures should be established for (i) Detection and analysis incident (ii) Containment, eradication, and recovery from an incident (iii) Post-Incident Activity of an incident.

MP-A05 Vulnerability Report and Disclosure via information-sharing platforms

Developers should participate in information-sharing platforms to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners.

MP-A06 Create and maintain public vulnerability report channels

Create a publicly disclosed mechanism for vulnerability reports, such as Security escalation channels or Bug Bounty programs.

4.1.4. Third-Party relationships

MP-A07 Data process outsourcing

Data processed by a third-party must be protected by a data processing agreement.

MP-A08 Supply chain cybersecurity management strategy.

Security requirements and supply chain security management strategy should be implemented and communicated to suppliers and partners. The strategy should include (i) Security governance (ii)
Security in manufacturing and operations (iii) Asset management (iv) Security incident management.

back to top

MP-A09 Share personal data of consumers with third parties

Only share personal data of consumers with third parties with express consent of the consumers, unless otherwise required and limited for the use of product features or service operations.

4.1.5. Assessment of Impacts on Sensitive Information

MP-A10 Identify sensitive data

Identify sensitive data according to the operating environment.

MP-A11 Identify local regulations

Identify regulations of countries that are involved in the sensitive data transmission.

MP-A12 Privacy by design

Privacy by design should be implemented. Privacy should be taken into account throughout the entire development process.

4.1.6. Cryptographic Management

AP-B01 Key management

Proper management mechanism and requirements should be implemented for cryptographic key generation, exchange, storage, usage, replace and discard.

4.2. Physical Security

4.2.1. Physical Interface

TC-C01 Physical port safety control

To prevent unauthorized access via physical port to operating system.

TC-C02 Plug and unplug alert

To help detecting and alerting unauthorized access, during the event of plugging or unplugging physical port, alert should be issued or the event should be logged for audit purpose.

TC-C03 Reset Button Protection

There should be physical protection mechanism to prevent reset button from unauthorized access.

4.2.2. Physical Layer

TC-C04 Anomaly detection

Device should have the capability to create event log or alert when anomaly events such as sensing components, accessory component, ethernet port, wireless network antennas and power cable disconnection, or bad signaling occur.

TC-C05 Device destruction and disassembly

Physical security mechanism should be implemented to protect the device from easily destroyed or disassembled. The mechanism should also protect the data storage medium from easily removed.

TC-C06 Environmental factors

back to top

Natural disasters or accidental factors in the installation location, such as earthquakes, fires, floods, winds, abnormal temperature and humidity should be considered. Appropriate material and design should be used to protect device from failure or reduced performance caused by environmental factors.

4.3. System Security

4.3.1. Operating System

TC-D01 Firmware version

The firmware, driver and operating system components version should be verified during system boot.

TC-D02 Secure boot

Completeness of firmware, driver and operating system components version should be checked during system boot. Secure boot can be implemented with encryption module to ensure that the system is not tampered.

TC-D03 Trustable runtime environment

Secure boot on firmware, drivers and components should be confirmed before any trust is claimed in any other software or executable program.

TC-D04 Tamper protection and detection

Security mechanism should be implemented to detect and react to firmware tampering. Notification should be sent to the operator and the mechanism should interrupt system operation or restore the firmware to a secure version.

TC-D05 Security and patch support

A product lifecycle should be defined and disclosed. The lifecycle should include the duration and end-of-life security and patch support. During the period of a product lifecycle, the device should be monitored and patched against known vulnerabilities until the “end-of-support’ period.

TC-D06 Secure offline update

Authorization certificate or encrypted channel should be used if IoT operating system utilize intranet or offline for updates. Security mechanism should be designed and implemented to ensure the completeness and correctness of the firmware, drivers and operating system components.

TC-D07 Secure online update

Authorization certificate or encrypted channel should be used if IoT operating system utilize internet (remote) for updates. Security mechanism should be designed and implemented to ensure the completeness and correctness of the firmware, drivers and operating system components.

TC-D08 Updates backward compatibility

Firmware updates should not modify user-configured preferences, security, and/or privacy settings without user notification.

TC-D09 Change Log

Firmware, driver and operating system components update should be logged in the change log. The device should have the capability to record at least 10 records.

back to top

TC-D10 Secure system restoration

The operating system should have mechanism to restore the firmware, drivers, operating system to a stable version during system update.

TC-D11 Prevent access to debug mode

The operating system should have mechanism to prevent user from entering operating system debug mode via direct connection ports or internet.

TC-D12 Secure whitelisting

The operating system should use whitelisting mechanism on applications and core components to prevent unauthorized application operating in the system.

TC-D13 Code signed system components

Code signing and whitelisting mechanism should be implemented to ensure system components and code execution will not be tampered or overwritten after they are loaded.

TC-D14 Secure configuration

Any applicable security features should be enabled by default, and any unused or insecure functionalities should be disabled by default.

TC-D15 System resilience

Physical impact of the system, such as external force, power surge or low voltage, instantaneous power failure and other abnormal conditions should be considered during the design. Mechanism should be implemented to maintain the system integrity and functionality after recovering to normal operating environment.

TC-D16 Auto recovery

Self-diagnosis and self-repair/healing mechanism should be implemented to recover the system from failure, malfunction or a compromised state.

TC-D17 Standalone operation

The device should maintain operational and temporary store of undelivered data even with connection lost or chronicle negative impacts from compromised devices.

4.3.2. Sensitive Data Storage

TC-D18 Secure storage

A secure storage that complies with The Federal Information Processing Standard (FIPS) Publication 140-2 cryptographic modules should be designed and implemented for the storage of sensitive data.

TC-D19 Privilege control

Privilege control mechanism should be implemented for the secure storage.

TC-D20 Data encryption

Advanced Encryption Standard (AES) 256 bits or other cryptographic algorithms that have same level of encryption strength should be used to protect the sensitive before it is stored in the secure storage. Lightweight encryption and security techniques can be used to lower the power consumption or if the device has limited computational resources.

TC-D21 Data segmentation

Different storage segmentations should be implemented for the storage of common data and sensitive data.

back to top

4.3.3. Web-Based Management Interface

TC-D22 Web vulnerability mitigation

Web-based management interface should not be vulnerable to injection and cross site scripting attacks.

TC-D23 Transmission encryption

Security mechanism should be implemented for remote web-based management interface setting with reference to requirements in TC-E03 – TC-E12.

TC-D24 Identity authentication

Identity authentication mechanism should be implemented for access to web-based management interface with reference to TC-F01 – TC-F12. Multifactor authentication should be implemented for critical infrastructure.

4.3.4. Application Programming Interface

TC-D25 Secure source

Code signature should be used to verify the reliability and security of application interface and thirdparty API.

TC-D26 Application Security

Security should be considered during the entire development cycle of API and any third-party API should be subjected to security accreditation.

TC-D27 Connection authorization

Authorization management mechanism should be implemented on the integrated application interface and third-party API.

TC-D28 Error message

Integrated application interface and third-party API should not reveal or leak any sensitive information through error message issued by authentication or authorization management mechanisms.

4.3.5. System Logging

TC-D29 Basic log information

System log should have the capability to log and display all access from users logging in via console or remote access. The system log should at least include full timestamp, user identity and action.

TC-D30 Secure log access

Access control should be implemented for the system log.

TC-D31 System log storage

There should be sufficient storage reserved for system log.

TC-D32 System log exportation

Device should have the capability to export system log to external system log server.

back to top

4.4. Communication Security

4.4.1. Network Port

TC-E01 Use appropriate network ports

For the communication between edge clients and gateway, and communication between gateway and cloud, IoT developers should choose suitable network ports for the IoT connections. These ports can be ports that are not commonly used by network services (i.e. TCP 80/443).

TC-E02 Identify service port requirement

Only enable ports that are required for the functionalities of IoT to prevent malicious attacks such as password guessing, eavesdropping and service interruption.

4.4.2. Sensitive Data Transmission

TC-E03 Identify sensitive data

Carry out data classification within operating environment.

TC-E04 Identify local regulations

Identify regulations of countries that are involved in the sensitive data transmission.

TC-E05 Secure sensitive data transmission

Personally identifiable information (PII) or confidential information should not be transmitted over channel that could be accessed by unauthorized parties. Encryption should also be used to further protect the security of such information. Ensure that communication security is provided using stateof-the-art, standardized security protocols, such as TLS for encryption.

TC-E06 Secure credential transmission

Both internal and external credential transmission should be encrypted.

4.4.3. Communication Interface

TC-E07 Communication interface management

Manufacturer should consider enabling IoT user the ability to manage the connectivity of their devices, such as enabling and disabling wireless communication.

TC-E08 Necessity of communication interface

Manufacturer should implement communication interface according to the operating environment of the IoT device. Keeping only communication interfaces that are necessary for delivering the device functions can reduce the attack vectors.

TC-E09 Security mechanism integration

Manufacturer should consider the integrability of the communication interface with its security mechanisms such as encryption channel and device identity identification.

TC-E10 Blocking internet debug mode

Access to operating system debug mode via internet should be prevented.

4.4.4. Communication Protocol

TC-E11 Communication protocol security

back to top

Evaluate security of communication protocol ensuring that it conform to standard specification and not impacted by known vulnerabilities.

TC-E12 Communication protocol maintenance

Evaluate the maintainability of the communication through factors such as capability to respond to attacks and capability to fix vulnerability after product release.

TC-E13 Security mechanism integration

Developer should consider the integrability of the communication protocol with its security mechanisms such as encryption channel and device identity identification.

TC-E14 Unauthorized connection

Security mechanism should be in place to prevent unauthorized connection at all Open System Interconnection (OSI) level.

TC-E15 Connection speed limitation

Limit speed of network traffic to reduce the risk of denial of service.

TC-E16 Use proven solutions

Only proven communication protocols and cryptographic algorithms should be used. Such proven solutions could be solutions that are recognized and adopted by the scientific community. Unproven solutions such as customized cryptographic algorithm should be avoided.

4.5. Identification, Authentication and Authorization

4.5.1. Authentication

TC-F01 Identity authentication

Identity authentication mechanism should be designed, and the system should only provide services to users or other devices after they are authenticated. Example authentication mechanism can be device certificate, user certificate, or user account and password matching.

TC-F02 Re-authentication

According to the operating environment of the IoT device, authentication system designs should automatically provide a mechanism requiring re-authentication after a period of inactivity or prior to providing services to users or other devices.

TC-F03 Replay attack protection mechanism

Identify authentication mechanism should have the capability to protect the system against replay attack.

TC-F04 Limited disclosure of personal identifiable information

The device should not disclose personal identifiable information or related messages due to incorrect/improper access.

TC-F05 Multifactor authentication

Multifactor authentication should be implemented to ensure credibility if resource is available and without affecting user experience.

TC-F06 Two-way authentication

Two-way authentication should be implemented to ensure credibility if resource is available and without affecting user experience.

back to top

4.5.2. Password

TC-F07 Password strength requirement

Proper password length and complex composition rules should be used to increase the strength of password.

TC-F08 Incorrect password protection

Proper password protection mechanism such as limiting number of password guesses should be implemented.

TC-F09 Default password differentiation

Each of the developed IoT should have different default password.

TC-F10 Default password management

Default password management mechanisms should be implemented. Enforce mechanism which require users to change password after initial login and limit user access using default password.

TC-F11 Secure authentication credentials

Authentication credentials should be salted, hashed and/or encrypted.

TC-F12 Secure password recovery

Ensure password recovery or reset mechanism is robust and does not leak information indicating a valid account to an attacker. The same applies to key update and recovery mechanisms.

4.5.3. Authorization

TC-F13 Access control policy

In order to maintain data confidentiality and integrity, device access control should be based on the necessity, importance and privacy requirements of the subject to access the object. Authorization schemes based on system-level threat models should also be implemented.

TC-F14 Least privilege

IoT users and devices should be given access to resources or IoT devices following the principle of least privilege according to the operating environment of the IoT.

TC-F15 Blocking privileged mode

Special operation privilege should not be given to users and other device if resource is available and without affecting user experience.

TC-F16 Privileged code isolation

Device firmware should be designed as privileged code and can only be accessed with the presence of privilege authorization. It should also be isolated from application and data.

4.6. Privacy Protection

4.6.1 Assessment of Sensitive Information

TC-G01 Minimize personal data collection

The amount of personal data that is processed should be restricted to the minimal amount possible according to the operating environment of the IoT.

back to top

TC-G02 Hide personal data

Secure personal data storage structure should be implemented to make sure personal data, and their interrelationships, be hidden from plain view during storage and access.

TC-G03 Separate personal data

Secure personal data storage structure should be implemented to make sure personal data is processed in a distributed fashion, in separate compartments whenever possible.

TC-G04 Data deletion right protection

Data deletion right protection should be implemented to allow users to delete their stored personal data.

Bibliographic Citations

[1] European Union Agency For Network And Information Security, *Baseline Security Recommendations for IoT*, November 2017. https://www.enisa.europa.eu/publications/baselinesecurity-recommendations-for-iot/at_download/fullReport (accessed September 4, 2018)

[2] National Institute of Standards and Technology, *Federal Information Processing Standards Publication 140-2: Security Requirements for Cryptographic Modules*, December 2002. https://csrc.nist.gov/publications/detail/fips/140/2/final (accessed September 4, 2018)

[3] Open Web Application Security Project, *Internet of Things Top Ten*, 2014. https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf (accessed September 4, 2018)

Acknowledgements

This report was prepared by Christopher Lek, Ethan Chen, Henry Hu, Mickey Law and Wyatt Lee and members of the Centre for Strategic Cyberspace + Security Science (CSCSS) IoT Security Standard Development Technical Committee. Contributors were David Nordell and Richard Zaluski. Overall guidance was provided by Aloysius Cheang.

This work is a product of the staff and volunteers of CSCSS. The findings, interpretations, and conclusion expressed in this work do not necessarily reflect the views of the donors of the CSCSS or its Board of Directors.

The whitepaper benefitted from close partnership and extensive discussion with staff of the iSyncGroup Inc. that had provided the initial draft of this whitepaper.
In addition, we would like to thank The Association of Information Security Professionals (AISP) in Singapore for the strong support and extensive discussion that made this whitepaper possible.

back to top

Commons Attribution license, you are free to copy, distribute, transmit, and adapt this work, including for commercial purposes, under the following conditions:
Please cite the work as follows: Centre for Strategic Cyberspace + Security Science. 2018. Centre for Strategic Cyberspace + Security Science: Internet of Things (IoT) Security Whitepaper. London, United Kingdom: Centre for Strategic Cyberspace + Security Science. License: Creative Commons Attribution CC BY 3.0 IGO.

Article from our CPP Partner, IronNet

For cybersecurity teams, juggling how the business navigates an increasingly complex, decentralised operating landscape with an expanding and sophisticated threat landscape will become critical success factors in 2022.

To help navigate this complex web of cyber threats, actors, and change drivers, global cybersecurity leader, IronNet, has identified three critical cybersecurity trends set to define Asian enterprises in the year ahead.

THE CLOUD CONNUNDRUM:
The mass adoption of cloud forced by COVID, helped ensure businesses and economies continued to function during an unprecedented global lockdown, but also ushered an explosion of unwanted and inherent vulnerabilities within the enterprise that continue to frustrate and exhaust security teams. And it's set to accelerate in 2022.

<u>Securing the cloud:</u>
Confusion over cloud security, governance, and responsibility will dominate cybersecurity teams. While cloud providers are responsible for their platform, customers are ultimately responsible for protecting their own apps and data running on it - something, many seem unaware of. This uncertainty, and unfamiliarity with cloud's open posture, has meant an attractive and profitable attack surface for hackers - and businesses vulnerable to a variety of malicious threats.

The sheer volume of assets in the cloud also poses vulnerabilities. Traditional security solutions are incapable of enforcing policies at the speed and scale of the cloud, especially given rapidly changing workloads. This lag places immense pressure on security teams as they constantly firefight and scramble to patch holes.

Then there is visibility and control. Because security teams cannot access the cloud provider's infrastructure, it's difficult to identify or visualise their entire cloud environment. This obscurity makes vulnerabilities and threat landscape difficult to assess – and easier for attacks to go undetected.

Ensuring interoperability and seamless integration of hybrid and multi-cloud operations security solutions across all on cloud and off cloud environments will be an ongoing priority as businesses try to balance speed and flexibility with greater security.

back to top

Thus, fully understanding governance, roles, and responsibility for all on and off cloud environments, as well as meticulously configuring, securing, and managing cloud and on-premise solutions and operating environments will be critical over the coming months.

Living with inconsistency:
COVID also ushered in a variety of hybrid working models. Inconsistency across teams, production lines, divisions, and countries, as well as the explosion of personal devices has left SoC teams struggling to find stability and predictability in a constant state of flux.

For employees – the desire to increase productivity has meant third party apps may be downloaded and deployed without appropriate devopps, security, or sandbox considerations – further increasing corporate exposure. Simultaneously, WFH meant insecure home networks, IoT, and millions of personal devices became potential attack vectors, many still invisible to security teams.

The outcome is a threat landscape that extends from secure servers to the connected fridge. Finding balanced operating models and practical working policies will therefore be critical in managing the business and employee expectations. As a result, security will become more granular, with a greater focus on Zero Trust Network Access.

In Zero Trust, the system, by default, automatically distrusts anyone or anything, inside or outside the network, and restricts and controls access to resources. Zero Trust also utilises micro-segmentation, which isolates specific areas within the database or cloud, automatically providing separation of workloads, and restricting infection and access while improving connectivity.

So, 2022 looks set to be a consuming battle of change, inconsistency, contradictory demands and expectations, and an expanded threat landscape. That said, help is at hand.

Smart Tech for a Smarter Business
Currently, many enterprises are being out-fought and out-thought when it comes to cybersecurity - fighting a modern war with outdated tools and tactics. A struggle intensified by the wholesale adoption of cloud.

The traditional business mindset scans for threats and then reacts once an attack is detected. And while artificial intelligence (AI) and machine learning (ML) have mitigated impact, this back foot posture and philosophy hasn't. Conventional technology continues to undermine business integrity.

Meanwhile, cyberattackers have evolved: from nuisance, attention seekers to organised criminal gangs using industrial scale resources, technology, and networks that span sectors, countries, and continents.

back to top

The only way for under resourced security teams to combat this sophisticated threat is to think and act smarter - with much greater use of smart(er) technology and AI and ML deployed proactively.

AI analyses large volumes of risk data to provide intelligence for real-time response and guide critical decisions. Combined with solutions like behaviour analytics, this allows overstretched security teams to identify patterns, behaviours, and intent, and then automatically anticipate, alert, and respond. All the time growing in strength, intelligence, and anticipation.

By pivoting from defence to offence, enterprises can shift from rigid, rules-based model to behavioural and intent based solutions - heralding the arrival of a smarter, tech savvy function focused on real-time defence.

Rethinking Cybersecurity

This outward facing posture will lead to the final trend for 2022. A surge in collaboration and cooperation between companies, ecosystems, and even sectors.

Historically, corporations have defended in isolation: unwilling to share attack and threat intelligence due to a misbelief they'd be revealing their most prized IP and business data.

The rise, sophistication, and frequency of the threat, the demand for efficiency, overworked and burdened SoCs, and the greater importance of governance and risk will usher a rethink. One that combines technology and collaboration to provide a modern defence and security infrastructure.

A problem shared

This will prioritise intelligence and advanced early warning, identification and tracking patterns and behaviour, and automated alerting and response.

By combining the technologies mentioned earlier with selective intelligence from an extensive network of partners, peers, and even competitors - enterprises will be able to increase visibility and early warning, reduce workloads, and improve efficiency, productivity, and cost. SoC teams will be able to focus on adding value rather than day to day firefighting.

Harnessing these capabilities will help move the entire "intelligence" community onto the front foot: improving efficiency and productivity by sharing and streamlining resources in real time. (Imagine 30 companies with three analysts each. With Collective Defense, you now have 90 people working together on a common set of problems.)The natural conclusion will be the connection of sectors as government and business coalesce around mutual survival and a joint threat.

A Tough Year Ahead:

Thus, while 2022 presents challenges, there are grounds for optimism. From advanced, automated tech to real-time intelligence and threat sharing across networks and ecosystems, a more comprehensive and adaptable cybersecurity model will be

back to top

available. A model that can navigate the complex operational and threat landscape accelerated by COVID and the agility and flexibility demanded by the business.

For any enquiries, please email to info_apj@ironnet.com

Article from SME Sponsor, Thales

What is Modern Authentication and Its Role in Achieving Zero Trust Security?

Danna Bethlehem | Director, Product Marketing | Thales

The evolving business and technology landscape and the need for secure, yet convenient, ways of logging into applications are driving the quest for more effective authentication.

The changing landscape
As we are slowly getting into a post pandemic world, the greatest lesson learnt from this turbulent period is that businesses need to have the ability to adapt to changing forces. Adaptability is what separates successful businesses from those that are still struggling to survive whilst working remotely. Besides the challenges of securing remote workforces, businesses have to adapt to the changing legislative landscape. Privacy and security regulations and laws being introduced in many countries mean data sovereignty is becoming a top requirement across many regions.

Surveys indicate that two-thirds of global enterprises will continue to support work from home arrangements for the foreseeable future, while hybrid working environments will pose further security challenges. This is because remote work disperses employees, increases the threat landscape and the inherent business risk.

To reduce the overall risk, organizations are investing in access security. Despite their efforts, they seem to be failing to protect an enterprise's most valuable assets – data. Data is now located outside the traditional perimetry, rendering all legacy data protection and access controls ineffective. Without a defined perimeter to defend, it is time for businesses to redefine their access security strategy.

From static authentication…
The key reason why access security efforts are disjointed from the current threat landscape is because they are not adequate. Many businesses are still relying on single factor, insecure passwords, that are a source of increased risks. Even if they use knowledge questions to provide further protection, passwords are still easily compromised.

back to top

Other businesses are moving away from single factor authentication, embracing multi-factor authentication based on hardware or software tokens and credentials. However, even in this case, the authentication relies on text passwords, which are inherently insecure.

What is important to note is that both methods are binary ones – go or not go. Access is granted based on a static authentication decision which is not affected by the environment where the user is located. In an environment where users are changing devices and networks, accessing data from either business premises or their home, the access decision cannot be static.

… to dynamic, context based authentication
In modern business environments, where users and endpoints are dispersed, authentication cannot be a single, discrete, binary event. Modern authentication needs to be a continuum based on three key concepts:

- Passwordless – move away from insecure passwords that create many security risks and contribute to fatigue and friction.
- Adaptive – adapt the authentication mechanism to the changing risk environment based on defined policies. Higher risk environments require step up authentication based on contextual data.
- Continuous and intelligent – modern authentication must not be a static decision, but it should continuously evaluate the risk environment using analytics such as User and Entity Behavior Analytics (UEBA), risk assessments and identity validation.

An authentication scheme that supports these concepts becomes a key part of strong access management to safeguard authorizing access to valuable yet dispersed data and resources.

Why do you need modern authentication?
Besides securing your assets, modern authentication has become a necessity because employees in digital-first enterprises travel multiple authentication journeys and have different authentication needs. While each user belongs to the same enterprise, there are several factors that differentiate their authentication requirements, including:

- Their personas: the role they have within the organization
- Location: on site, remote or roaming
- Devices they use: business laptops, personal devices, mobile devices
- Resources they need to access either on-premises or in the cloud
- Corporate security policy requirements and regulatory compliance

Therefore, businesses need to support multiple authentication journeys, and to do that, they need to establish and enforce modern authentication. Modern authentication allows for policy based contextual access, based on risk assessments, and passwordless identity validation.

How modern authentication helps Zero Trust security?

back to top

The authenticity of identities supported by modern authentication is at the core of an identity-centric approach to Zero Trust security. Access to enterprise resource is based on identity and assigned attributes. The primary requirement to access corporate resources is based on the access privileges granted to an authenticated user, service, or device. To cater for a more adaptive authentication, access policy enforcement may consider other factors as well, such as device used, asset status, threat intelligence and compliance requirements.

back to top

Article from The Cybersecurity Awards 2021 Winner – Acronis Asia Pte Ltd

Acronis is extremely honored to receive The Cybersecurity Award 2021 for the second year in a row.

Acronis, the global leader in cyber protection and a Singapore unicorn founded here in 2003, we understand that there is a situation in Singapore: fast-growing demands for cybersecurity professionals, not enough qualified cybersecurity professionals around. It's clear that the talent gap can't be solved by one side alone, this will take a joint effort. Acronis works closely with our partners to help change the situation and fix the security talent gap.

Already part of our DNA and actively pursued in our daily work: participate in workshops to build awareness on cybersecurity, and educate businesses and the public on the importance of implementing security as part of their operations and daily lives. Acronis will continue to contribute to Singapore's cybersecurity ecosystem, training up a pool of cybersecurity talent and the next wave of cybersecurity leaders in Singapore.

Take a sneak peek at how cyber protection is growing in 2022
The Acronis #CyberFit Summit Singapore goes live on **February 17, 2022** with a day full of insights, networking opportunities available for free online.

back to top

Top-notch experts sharing their cybersecurity outlook for 2022: future of tech & science, cybercrime trends in APAC, Singapore's Cybersafe masterplan, ransomware to be paid or not, how to fix the cybersecurity talent gap & much more.

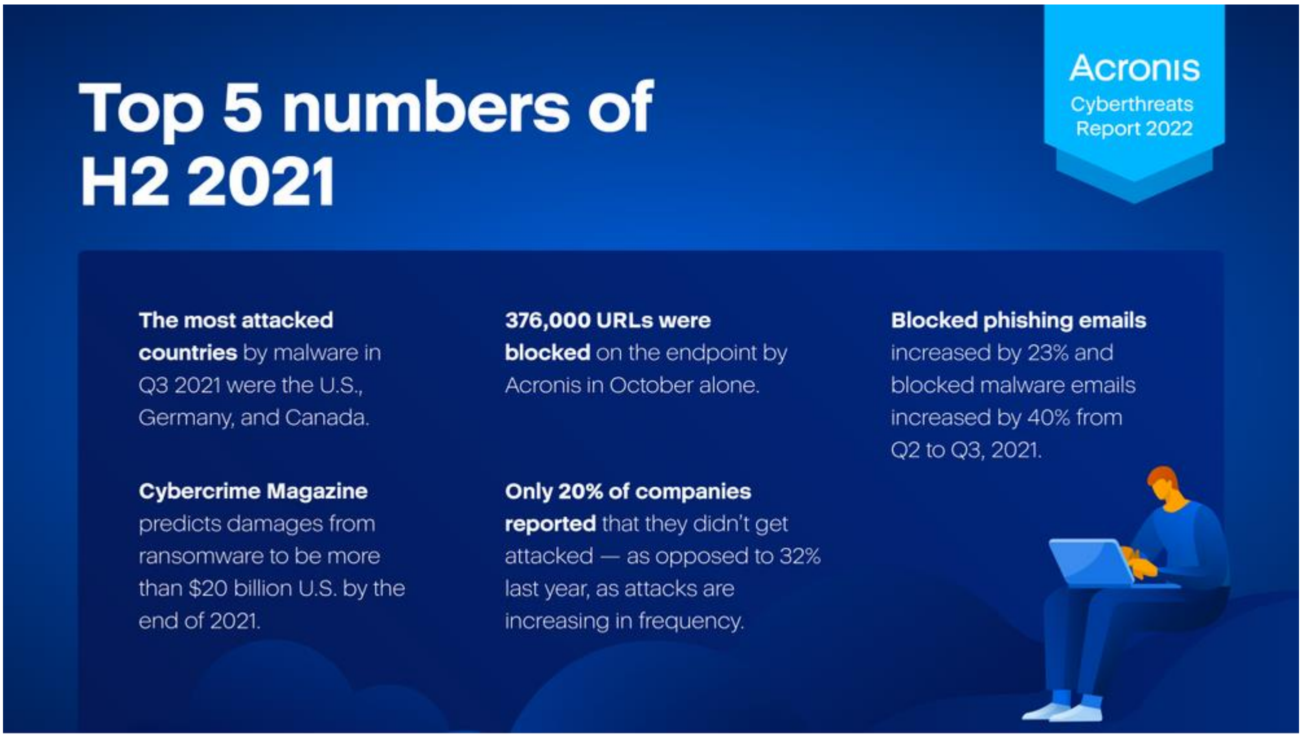
Join hundreds of cybersecurity experts gathering from around the world to learn, grow, and build their businesses together! Hear it from top experts at INTERPOL, CSA, Acronis, NUS, and many others. Check out the agenda & register here for the virtual event: https://acronis.events/summit2021/singapore/

Acronis Cyberthreats Report 2022

Acronis researches and releases reports to educate the public of the cyberthreat situation. In the Acronis Cyberthreats Report 2022, an in-depth review of cybersecurity trends and threats worldwide. The report warns that managed service providers (MSPs) are particularly at risk — having more of their own management tools, such as PSA or RMM, used against them by cybercriminals, and thus are becoming increasingly vulnerable to supply chain attacks.

Cybercriminals are using MSPs' own internal tools against them

Supply-chain attacks on MSPs are particularly devastating, since attackers gain access to both their business and clients — as seen in the SolarWinds breach last year and the Kaseya VSA attack earlier in 2021, one successful attack means crippling hundreds or thousands of SMBs. The report also shows that during the second half of 2021, only 20% of companies reported not having been attacked — as opposed to 32% last year — indicating that attacks are increasing in frequency across the board.



Top 5 numbers of H2 2021

Acronis Cyberthreats Report 2022

The most attacked countries by malware in Q3 2021 were the U.S., Germany, and Canada.

376,000 URLs were blocked on the endpoint by Acronis in October alone.

Blocked phishing emails increased by 23% and blocked malware emails increased by 40% from Q2 to Q3, 2021.

Cybercrime Magazine predicts damages from ransomware to be more than $20 billion U.S. by the end of 2021.

Only 20% of companies reported that they didn't get attacked — as opposed to 32% last year, as attacks are increasing in frequency.

Key cyberthreat trends of 2021 — and predictions for 2022

back to top

Beyond the growing efficiency of cybercriminals and the impact on MSPs and small businesses, the Acronis Cyberthreats Report 2022 shows:

Phishing remains the main attack vector. 94% of malware gets delivered by email — using social engineering techniques to trick users into opening malicious attachments or links, phishing has been topping the charts even before the pandemic. It still continues to grow rapidly: just this year, Acronis reported blocking 23% more phishing emails and 40% more malware emails in Q3, as compared with Q2 of the same year.

Phishing actors develop new tricks, move to messengers. Now targeting OAuth and multifactor authentication tools (MFA), these new tricks allow criminals to take over accounts. To bypass common anti-phishing tools, they will use text messages, Slack, Teams chats and other tools for attacks such as business email compromise (BEC). One recent example of such an attack was the infamous hijacking of the FBI's own email service, which was compromised and started sending spam emails in November 2021.

Ransomware is still the #1 threat — to big companies and SMBs alike. High-value targets include the public sector, healthcare, manufacturing and other critical organizations. But despite some recent arrests, ransomware continues to be one of the most profitable cyberattacks these days. Cybercrime Magazine predicts ransomware damages will exceed $20 billion before the end of 2021.

Cryptocurrency among the attackers' favorite tools. Infostealers and malware that swaps digital wallet addresses are the reality today. We can expect more such attacks waged directly against smart contracts in 2022 — attacking the programs at the heart of cryptocurrencies. Attacks against Web 3.0 apps will also occur more frequently, and new and increasingly sophisticated attacks, such as flash loan attacks, will allow attackers to drain millions of dollars from cryptocurrency pools.

The Acronis Cyberthreats Report 2022 is based on examining attack and threat data collected by the company's global network of Acronis CPOCs, which monitor and research cyberthreats 24/7. Malware data was collected by more than 650,000 unique endpoints around the world running Acronis Cyber Protect — either as a client of an MSP using the solution or a business running the solution. The end-of-year update covers attacks targeting endpoints detected between July and November 2021.

The full report provides in-depth insights into the top cybersecurity and threat trends the CPOCs observed during the second half of 2021; a review of malware families and related statistics; a deep dive into ransomware's most dangerous groups; the vulnerabilities that contribute to successful attacks; and Acronis' security recommendations for 2022 and beyond. You can download a copy of the full Acronis Cyberthreats Report 2022 here.

About Acronis

Acronis unifies data protection and cybersecurity to deliver integrated, automated cyber protection that solves the safety, accessibility, privacy, authenticity, and security (SAPAS)

back to top

challenges of the modern digital world. With flexible deployment models that fit the demands of service providers and IT professionals, Acronis provides superior cyber protection for data, applications, and systems with innovative next-generation antivirus, backup, disaster recovery, and endpoint protection management solutions powered by AI. With advanced anti-malware powered by cutting-edge machine intelligence and blockchain based data authentication technologies, Acronis protects any environment – from cloud to hybrid to on premises – at a low and predictable cost.

Founded in Singapore in 2003 and incorporated in Switzerland in 2008, Acronis now has more than 1,700 employees in 34 locations in 19 countries. Our Acronis Cyber Protect solution is available in 25 languages in over 150 countries and is used by over 20,000 service providers to protect over 750,000 businesses.

Visit https://www.aisp.sg/publications for more contributed contents by our partners.

back to top

PROFESSIONAL DEVELOPMENT

Listing of Courses by Wissen International

Exam Preparation Workshop
26 Feb 2022
9am to 6pm
Virtual live training

Calling all CEH holders!
Attend our 1-day workshop to prepare you for CEH Practical Exam and attain the coveted CEH Master credential!

Only **SGD 950** for 1-day training by EC-Council CEH Master trainer, CEHv11 iLab for 6 months access and CEH Practical exam voucher valid for 12 months

Email cehmaster@wissen-intl.com to register!

Click here to find out more

back to top

Qualified Information Security Professional (QISP®) Course

STEPPING UP ON INFORMATION SECURITY
AiSP
Advance Connect Excel
QUALIFIED INFORMATION SECURITY PROFESSIONAL COURSE

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

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

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

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

back to top

COURSE DETAILS

2022 Course dates can be found on https://www.aisp.sg/qisp_training.html
Time: 9am-6pm
Fees: $2,500 (before GST)*
**10% off for AiSP Members @ $2,250 (before GST)*
*Utap funding is available for NTUC Member

TARGET AUDIENCE

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

COURSE CRITERIA

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

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

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

Program Partner

Transformists NETWORK

Delivery Partners

Ai Network 360

OPUS ACADEMY

NET ASSIST

STEPPING UP ON INFORMATION SECURITY
AiSP Advance Connect Excel
CYBERSECURITY ESSENTIALS COURSE

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

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

Course Objectives

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

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

back to top

COURSE DETAILS

Training dates for year 2022 can be found on
https://www.aisp.sg/cyberessentials_training.html
Time: 9am-6pm
Fees: $ $1,600 (before GST)*
**10% off for AiSP Members @ $1,440 (before GST)*
*Utap funding is available for NTUC Member

TARGET AUDIENCE

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

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

Program Partner

Transformists NETWORK

Delivery Partners

Ai Network 360

OPUS ACADEMY

NETASSIST

back to top

MEMBERSHIP

AiSP Membership

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

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

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

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

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

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

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

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

back to top

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

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

Please check out our website on Job Advertisements by our partners.

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

AiSP Corporate Partners

back to top

MICRO FOCUS

MINDEF SINGAPORE

NUMEN

Privasec

RAJAH & TANN CYBERSECURITY

Recorded Future

Responsible Cyber

SAVIYNT

SecurID
An RSA Business

ST Engineering

TANIUM

ThriveDX
Formerly Cybint

TREND MICRO

xcellink.pte.ltd.
completing your technology chain

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

AiSP Academic Partners

ITE
Institute of Technical Education

NYP NANYANG
THE INNOVATIVE POLYTECHNIC

NGEE ANN POLYTECHNIC

NUS
National University of Singapore

REPUBLIC POLYTECHNIC
DISCOVER. TRANSFORM. ACHIEVE

SIT SINGAPORE INSTITUTE OF TECHNOLOGY

SP Singapore Polytechnic

SMU
SINGAPORE MANAGEMENT UNIVERSITY

SUTD
SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

SUSS
SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

Temasek POLYTECHNIC

back to top

Our Story…

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

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

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

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

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

AiSP
Advance Connect Excel

www.AiSP.sg
secretariat@aisp.sg
☎ +65 8878 5686
116 Changi Road, #04-03 WIS@Changi, S419718
Please email us for any enquiries.

back to top