

An aerial night view of a city skyline with numerous skyscrapers. Overlaid on the city are glowing, curved lines representing fiber optic connections or data paths, creating a network-like pattern across the urban landscape.

AiSP

Association of
Information Security Professionals

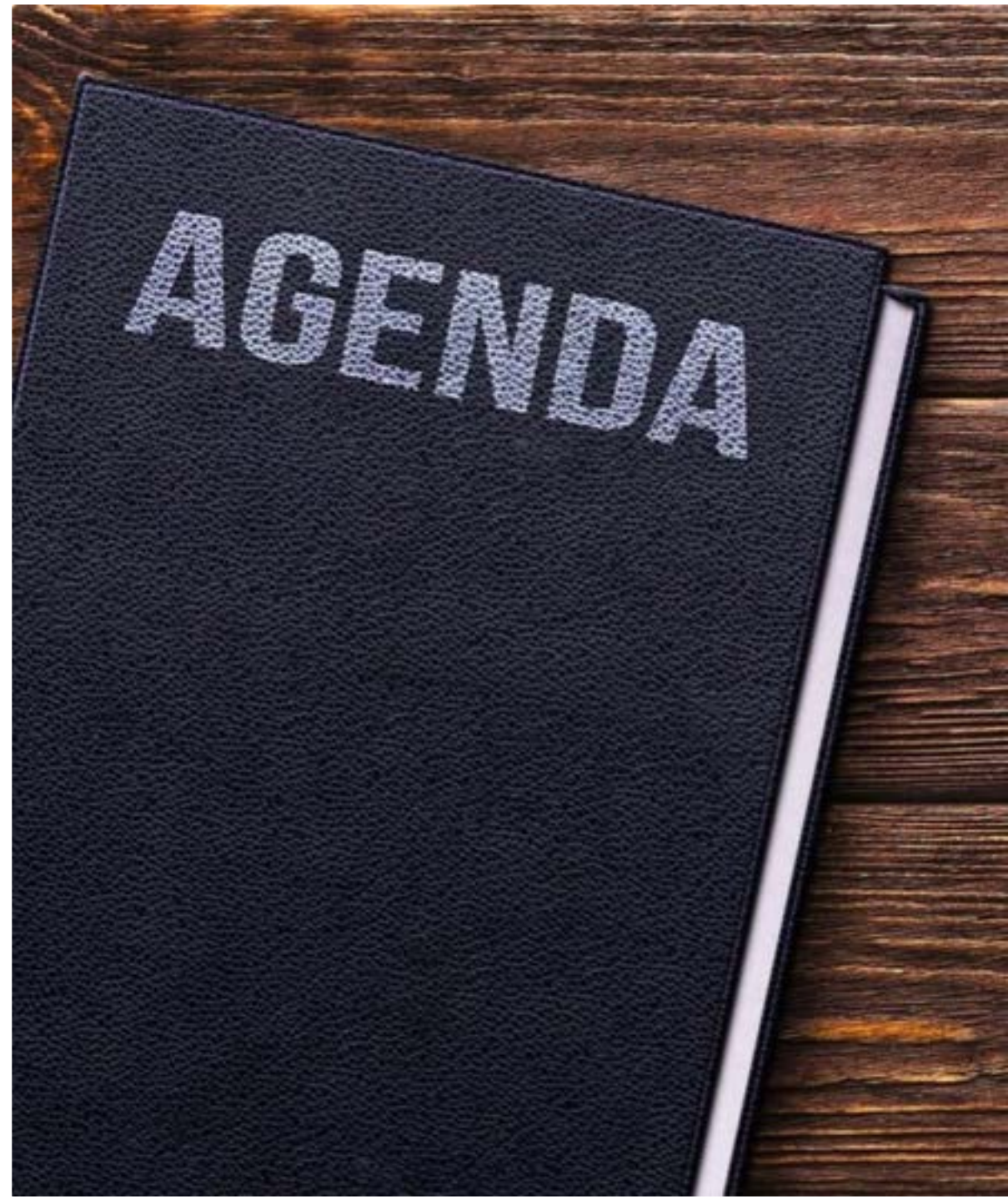
Challenges in building ASEAN Cyber Resilience

Tony Low, AiSP VP

Royalty-free image for Microsoft O365 subscribers.

Today's Agenda

1. State of Digital and Cyber Security of ASEAN
2. What are the countries in ASEAN facing today in Cybersecurity?
3. Looking at a collective community Effort
4. Where are we today?
5. Call to Action



**[Unknown]
Inflation & Recession**

Not Skilled

Journey is rough

**Treacherous Digital + Business
Environment**

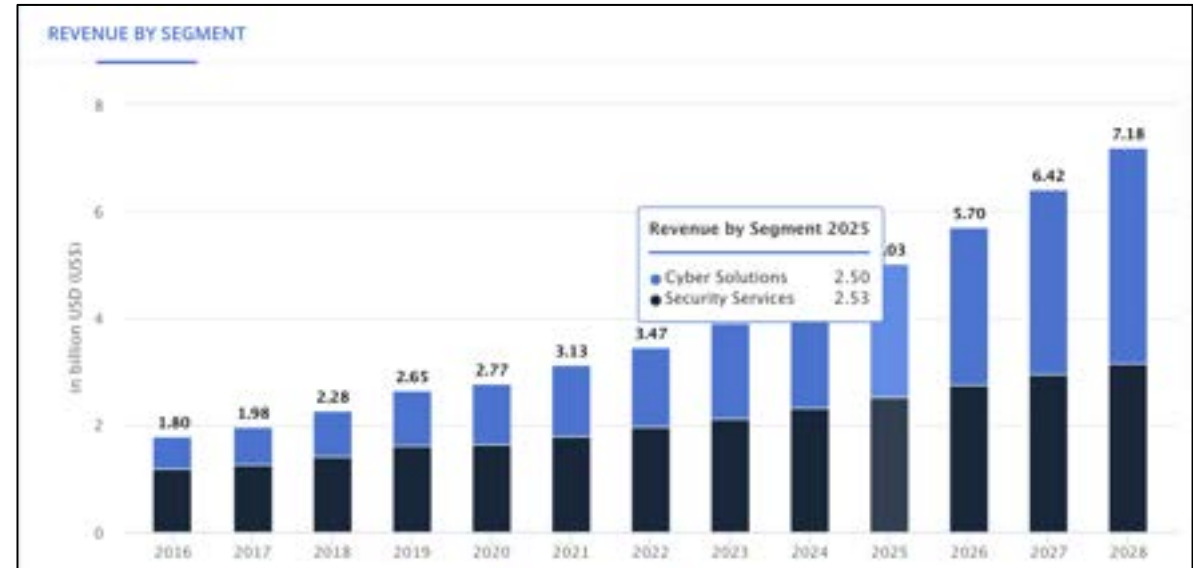
My Business



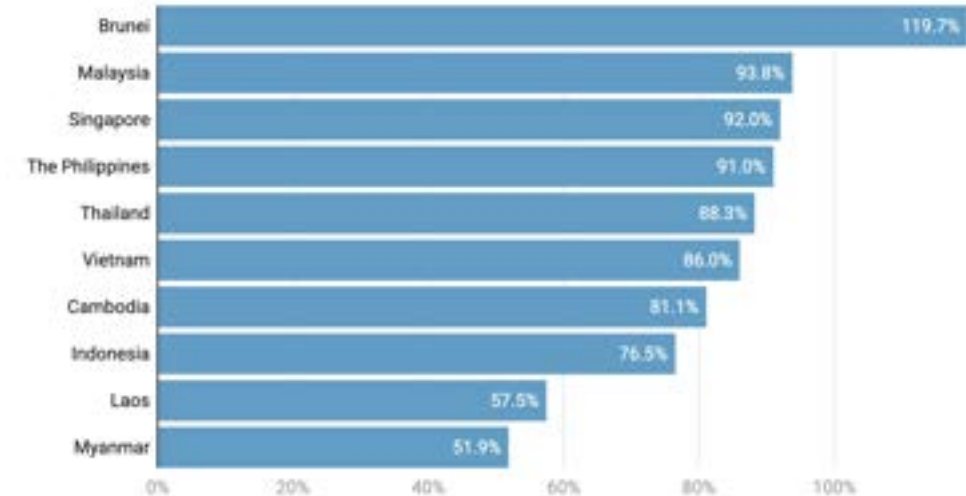
State of Digital and Cyber Security of ASEAN

Huge opportunity within Asean Post Pandemic and Beyond

- **Foreign businesses** expect sales in the region to grow by 23.2% in 2023
- ASEAN is on track to become the world's **largest** market by 2030.
- Celebrated young and dynamic population with **34%** of ASEAN's population consists of young people, aged between **15 and 34 years old**
- In 2023, **86%** of tech founders is still looking to expand their head count with engineers and data scientists remaining high in demand.
- Digital economy is projected to triple by the end of the decade through the natural adoption of digital technologies, growing from approximately **US\$300 billion to almost US\$1 trillion by 2030.**



Internet penetration rate in ASEAN



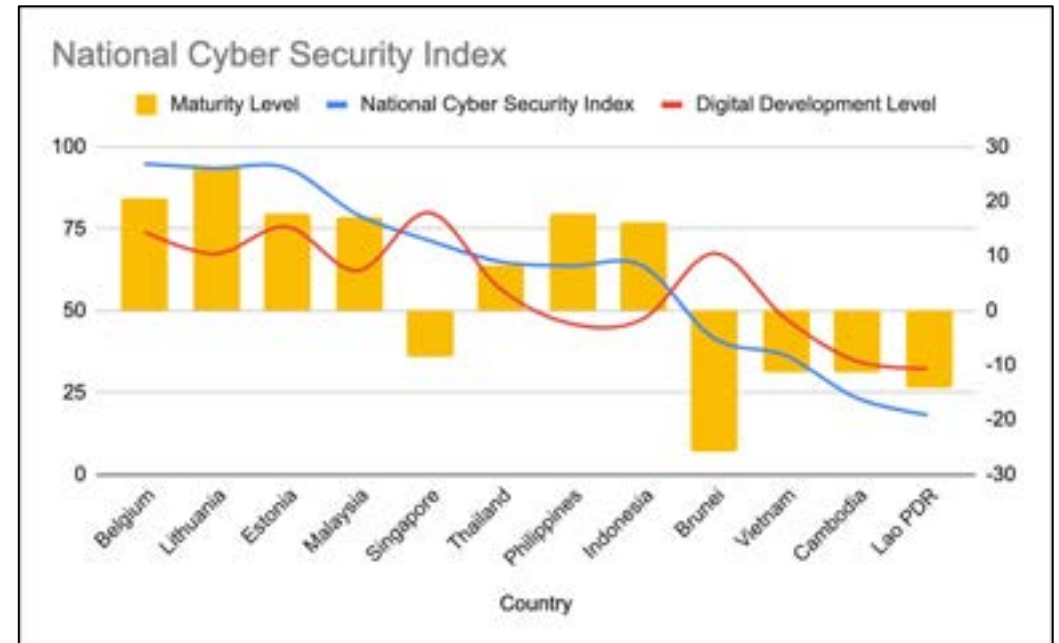
Date as of July 2022

Source: Statista • Get the data • Created with Datawrapper

How ready is the economy in Asean to keep up with the Pace?

Some Examples:

- **Malaysia** - experienced several high-profile cyber breach incidents in 2022 including the data leak of **22.5 million** Malaysians on the dark web. Total estimated of almost RM600 million in losses were recorded throughout 2022 as a result of cybercrimes in the country.
- **Singapore** – The public sector reported **182** data incidents in the year up to March 31 2023, up from 178 cases reported in the year before, as data sharing among agencies accelerated due to increased digitalisation.
- **Bangkok** - The average number of cyber-attacks on organisations in almost double the average rate globally 2,388 times per week on average during the last six months, compared with **2,375 attacks** per week in Southeast Asia.



Source: NCSI ,Survey by: NCSI

Release date

July 2023

ASEAN countries can emerged as launchpads for cyberattacks

1. Large number of vulnerable hotbeds of unsecured infrastructure:
 - a. Personal devices and home networks accessing the corporate network (**47%**)
 - b. Unmonitored IoT devices and unsecured IoT devices (**60%**)
 - c. **94%** of ASEAN organizations had experienced a rise in the number of attacks in 2021.
 - d. ~ 269,533 phishing attempts were targeted against Malaysian SMEs in the first half of 2020.
2. **5%** of IT professionals in the region have the [technical knowledge and experience](#) to analyze attacks on their networks
3. Nascent local cybersecurity industry with shortages of home-grown capabilities and expertise



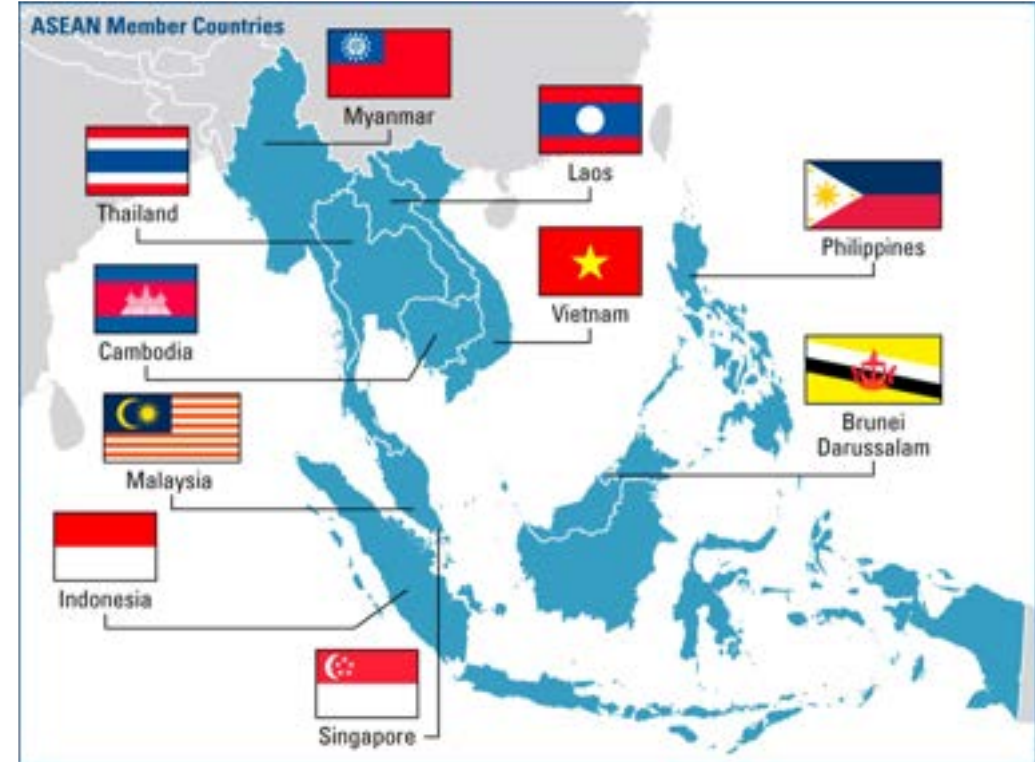


**CHALLENGES
AHEAD**

**What are the countries in
ASEAN facing today in
Cybersecurity?**

ASEAN faces a number of challenges in building cyber resilience in 2023 and beyond

- **Limited resources:** Needed more resources to invest in cybersecurity, implementing necessary security measures and developing a skilled cybersecurity workforce
- **Lack of awareness:** General population must be fully aware of the cybersecurity risks they face, understand careless behavior makes them more vulnerable to attack.
- **Complex regulatory environment:** The cybersecurity regulatory environment in ASEAN is complex and fragmented for organizations to comply with all relevant regulations.
- **Growing sophistication of cyber attacks:** Cybercriminals are becoming increasingly sophisticated in their attacks and better funded.



Limited Resources - Talent, Budget & Capabilities

1. Many ASEAN countries, Governments and Enterprises **just started capacity** - Cambodia, Laos, Myanmar and Vietnam are in the early stages of cyber-security capacity building and are also struggling with a lack of resources and technical expertise
2. **97% of the enterprise in Asean are SMBs** who typically does not have the ability to drive large scale security programs, SMEs are unaware of the extent of the damage that a cyberattack can cause.
3. **Acute shortage of cybersecurity talent** in all countries including Singapore - e.g Vietnam has an estimated shortage of around 100,000 engineers

State of global cybersecurity talent

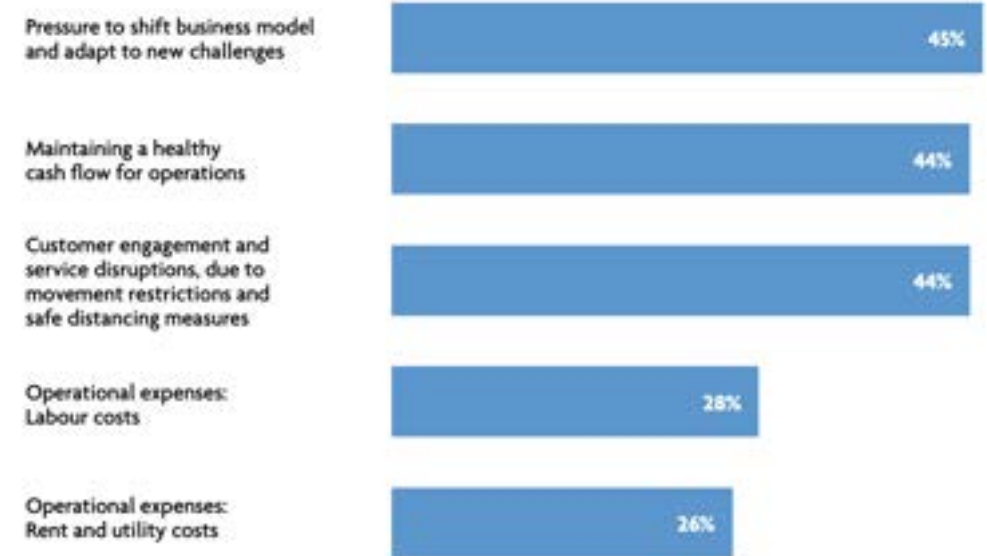


Source: A.T. Kearney analysis

Varying Maturity and approach towards Cybersecurity

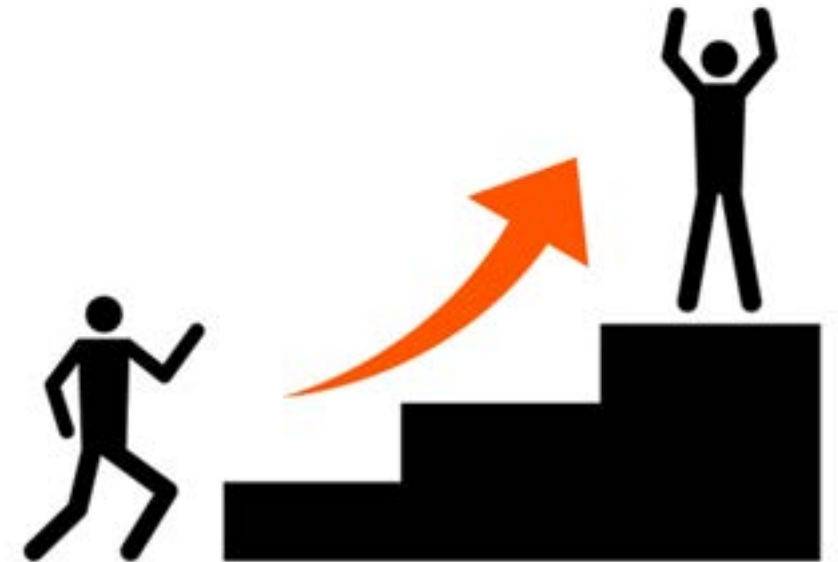
1. **Cisco Cybersecurity Readiness Index** - Only 23% SEA companies ready to defend against cybersecurity threats
2. Countries with a **high degree** of cyber maturity, such as Singapore, are more likely to push for advancing norms adoption, capacity-building measures, and other cyber policy aspects.
3. Countries with a **lower degree** of cyber maturity, such as Myanmar, are more focused on establishing protection measures for their national **infrastructures**.
4. Different **cybersecurity priorities** of ASEAN member states with varying levels of cyber maturity pose a challenge to regional cybersecurity cooperation.

Figure 2: SMEs' immediate business concerns



Complex regulatory environment - Different stages of definition in each economy*

1. **ASEAN intergovernmental** structure - **10 countries x 10 different** sets of cybersecurity regulations to comply with creating challenges for businesses and organizations to comply with all of the relevant regulations
2. The **ASEAN Way** of consensus-based decision-making and non-interference slows the policy-making process and limits regional cyber policies.
3. **Differing views** among ASEAN member states due to their diverse cultural and political contexts and histories hinders the sharing of threat intelligence.
4. **Disparity in cyber-crime laws** and enforcement among ASEAN member states prevents the agreement on an overarching regulation.
5. **Digital divide** among ASEAN member states where issue of a cyber-induced emergency may be a lower priority for developing countries.



Growing sophistication of cyber attacks

1. Cybercriminals are becoming increasingly sophisticated in their attacks, using a variety of new and emerging techniques to **exploit vulnerabilities and gain access to systems and data.**
2. **Cybercrime is a multi-billion dollar industry.** This means that cybercriminals have the resources to invest in research and development to develop new attack techniques.
3. **Digital landscape is constantly evolving.** The rise of mobile technologies and the increase adoption of IoT
4. **Increase difficulty** to defend against cyberattacks and to recover from them. e.g **Ransomware**
5. **The rise of cybercrime-as-a-service.** Cyber Attack Commoditization where attacks can be paid and initiated by anyone. Tools, services and people are out for rental by anyone.

CYBERSECURITY TOOLS: Then, now, and tomorrow.



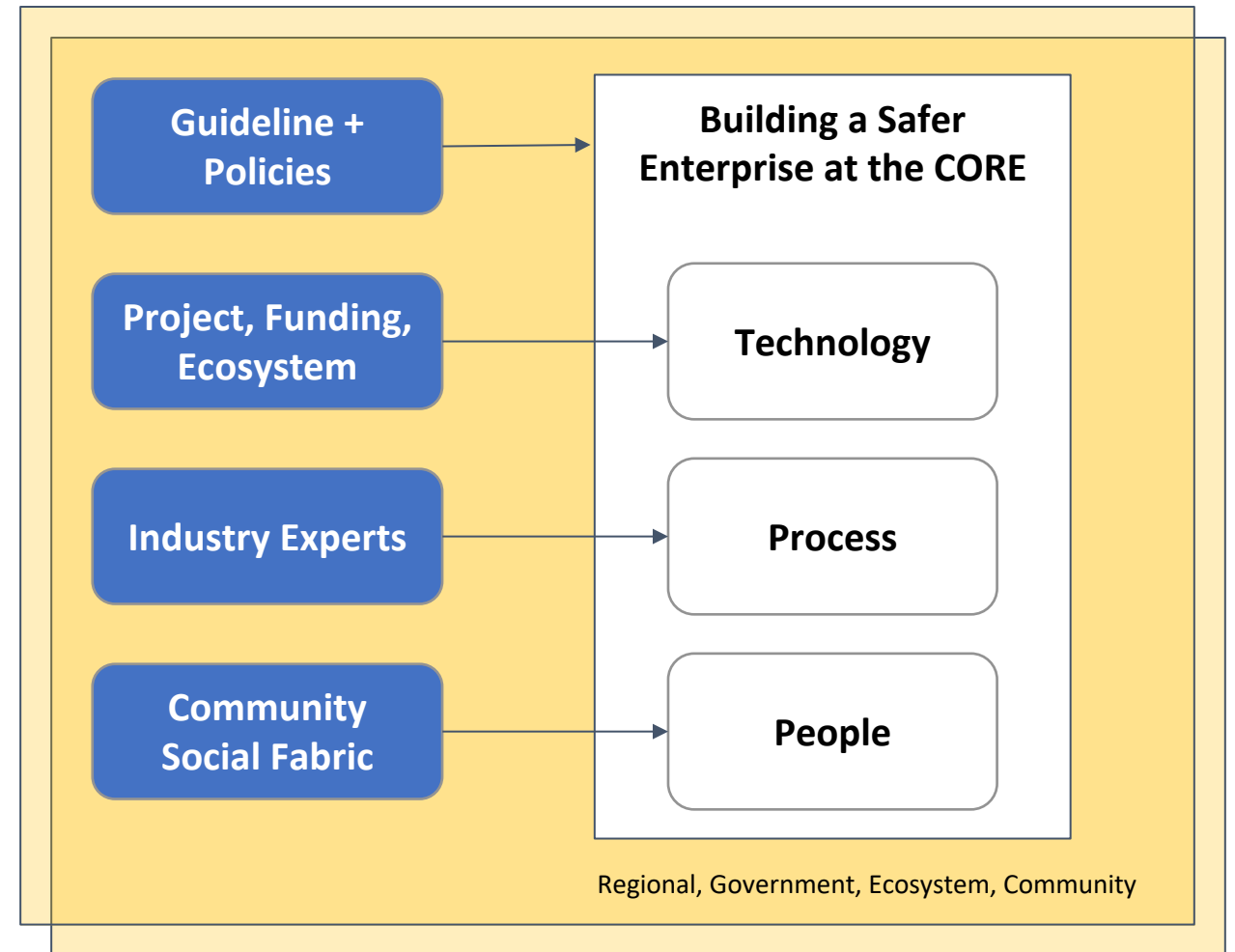
- WiFi**
 - Don't allow your device to auto-join unfamiliar networks.
 - Always turn off WiFi when you aren't using it or don't need it.
 - Never send sensitive information over WiFi unless you're absolutely sure it's a secure network.
- Bluetooth**
 - Disable automatic Bluetooth pairing.
 - Always turn it off when you don't need it.
- Smishing (phishing via SMS)**
 - Don't trust messages that attempt to get you to reveal any personal information.
 - Beware of similar tactics in platforms like WhatsApp, Facebook Messenger Instagram, etc.
 - Treat messages the same way you would treat email, always think before you click!
- Vishing (voice phishing)**
 - Do not respond to telephone or email requests for personal financial information. If you are concerned, call the financial institution directly, using the phone number that appears on the back of your credit card or on your monthly statement.
 - Never click on a link in an unsolicited commercial email.
 - Speak only with live people when providing account information, and **only** when you initiate.
- Apps**
 - Only use apps available in your device's official store - NEVER download from a browser.
 - Be wary of apps from unknown developers or those with limited/bad reviews.
 - Keep them updated to ensure they have the latest security.
 - If they're no longer supported by your store, just delete!
 - Don't grant administrator, or excessive privileges to apps unless you truly trust them.
- Browser**
 - Watch out for ads, giveaways and contests that seem too good to be true. Often these lead to



Looking at a collective community Effort

A Point of View: Strengthening Regional Cyber Resilience – One block at a time

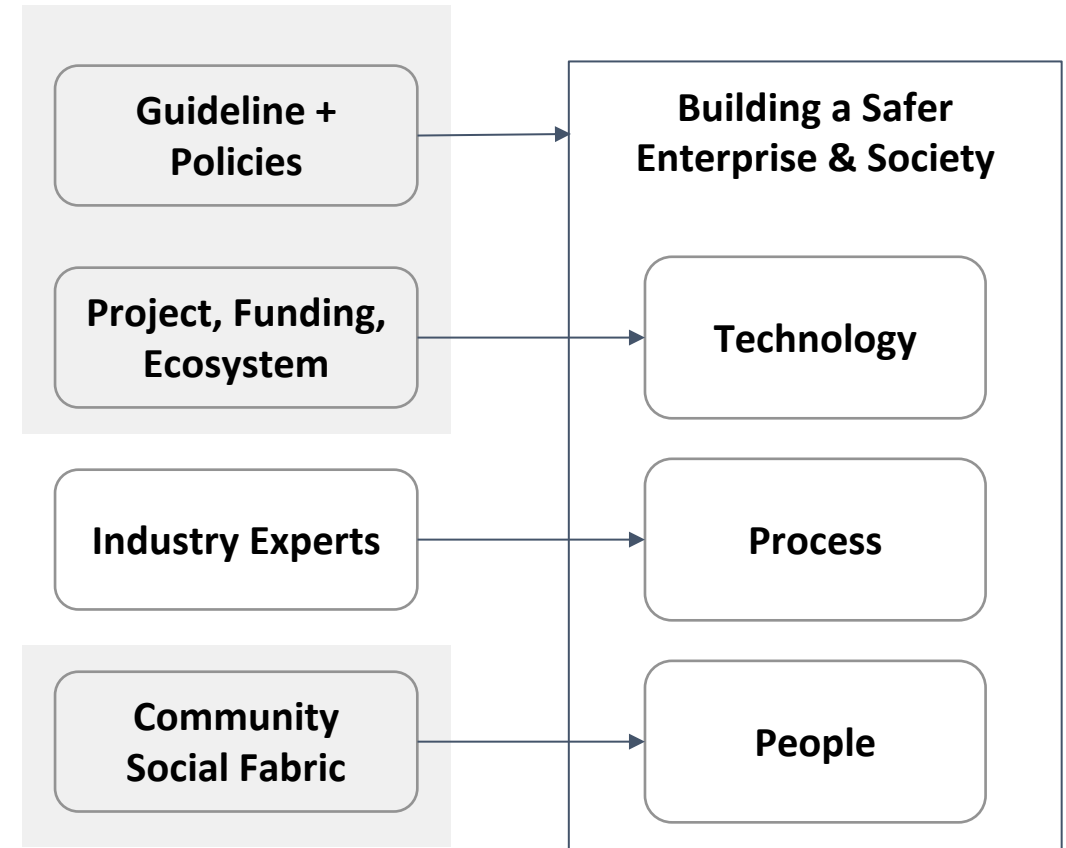
1. Enterprises are built on the structure of **People Excellence, Process Engineering** and **Technology Investments**.
2. Looking at a **Holistic Partnership** between Government, Ecosystem (Industry, Enterprise) and Community.
3. Starting with the Community - Developing a **strong base** within the **Enterprise- Core** through Community and Social Uplift.
4. **Expert Advice:** Cybersecurity is getting complicated, you can do it alone.
5. **Get Involved:** Government Agencies / Ministry are starting to develop policies and guidelines suitable for the country and the economy.



A Point of View: Strengthening Regional Cyber Resilience – One block at a time

Improve your organization's cybersecurity posture and reduce the risk of a cyber attack.

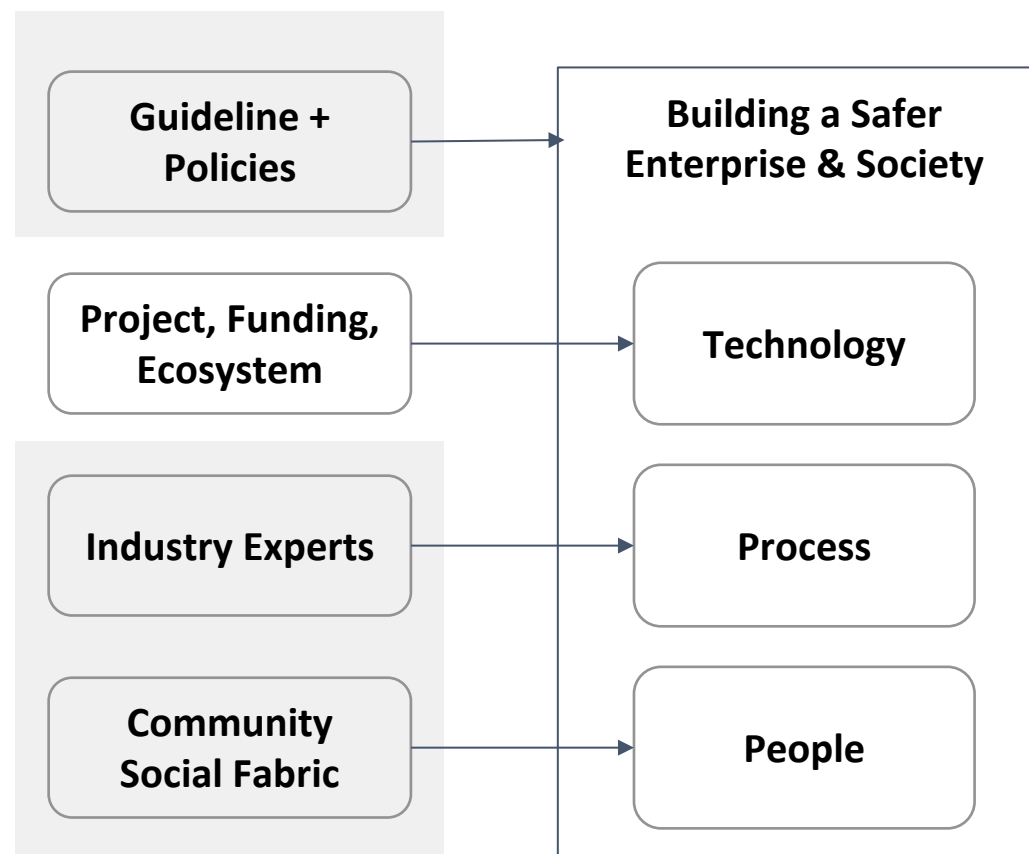
1. **Layered security approach** - Physical and logical (for Cloud) security need assessments.
2. **Systems and software up to date** - Software updates (security patches) can help to protect from known vulnerabilities.
3. **Best practices** - Collaboration can help everyone learn and improve their cybersecurity posture.
4. **Provide technical assistance** - Seek help for specific cybersecurity (Incident response, vulnerability assessment)
5. **Map the cybersecurity regulatory landscape** - Complex and ever-changing to map the cybersecurity regulatory landscape.
6. **Develop a cybersecurity compliance plan** - Help and guide organization meets all applicable cybersecurity regulations



A Point of View: Strengthening Regional Cyber Resilience – One block at a time

Create a more supportive and innovative ecosystem for cybersecurity.

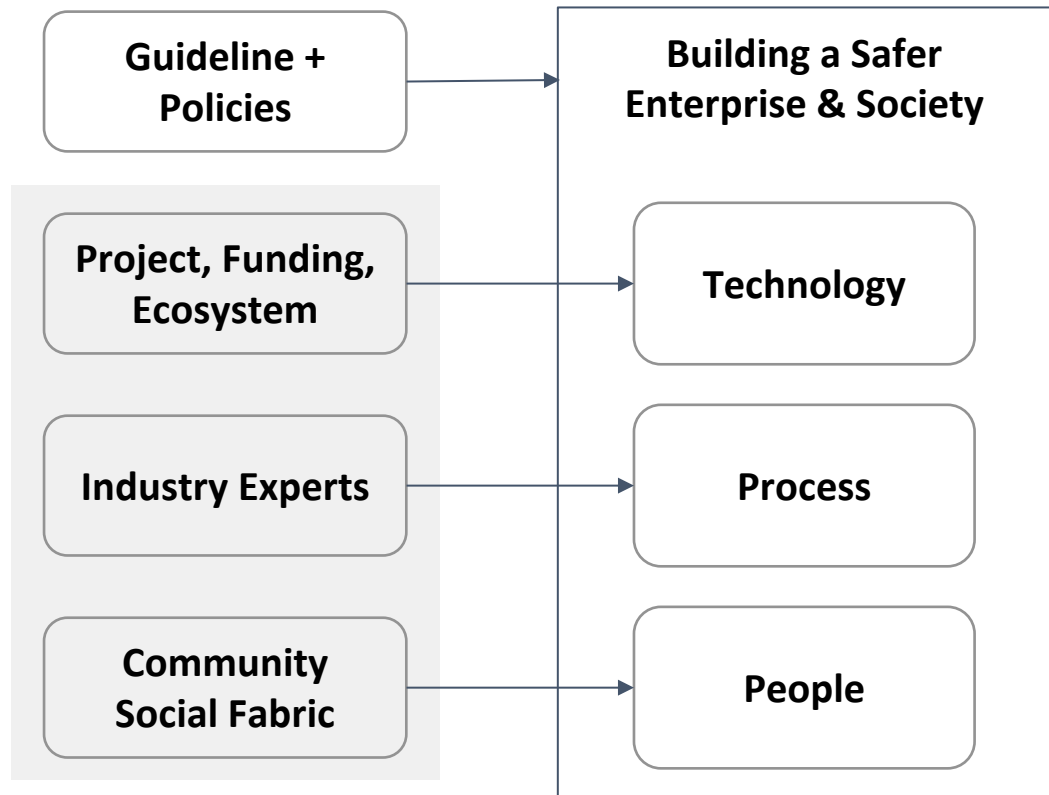
- 1. Prioritize critical Cyber Security projects:**
 - a. Improving tools, technologies & infrastructure.
 - b. Educating people about risks and best practices.
- 2. Clear and concise plan** - project goals, objectives, timeline, budget, and resources required.
- 3. Establish metrics** - for measuring the success of each project to track your progress and adjust accordingly.
- 4. Secure funding for cybersecurity projects** - Could include government grants, project fundings.
- 5. Create a cybersecurity innovation hub** - Gather the community together to collaborate and develop new cybersecurity solutions.
- 6. Create a cybersecurity mentorship program** - Match experienced cybersecurity professionals with new/early-career cybersecurity professionals.



A Point of View: Strengthening Regional Cyber Resilience – One block at a time

Working together, governments, vendors, and industry experts - a vital role in improving cybersecurity

1. **Establish** regional, local, and community cybersecurity cooperation mechanisms.
2. **Identify** the key cybersecurity risks and challenges that need to be addressed.
3. **Develop** guidelines and policies that are SMART (specific, measurable, achievable, relevant, and time-bound).
4. **Engage** with stakeholders to get their feedback and input on the guidelines and policies.
5. **Communicate** the guidelines and policies to all stakeholders.
6. **Monitor** and evaluate the effectiveness of the guidelines and policies, update and revise



A Point of View: Strengthening Regional Cyber Resilience – One block at a time

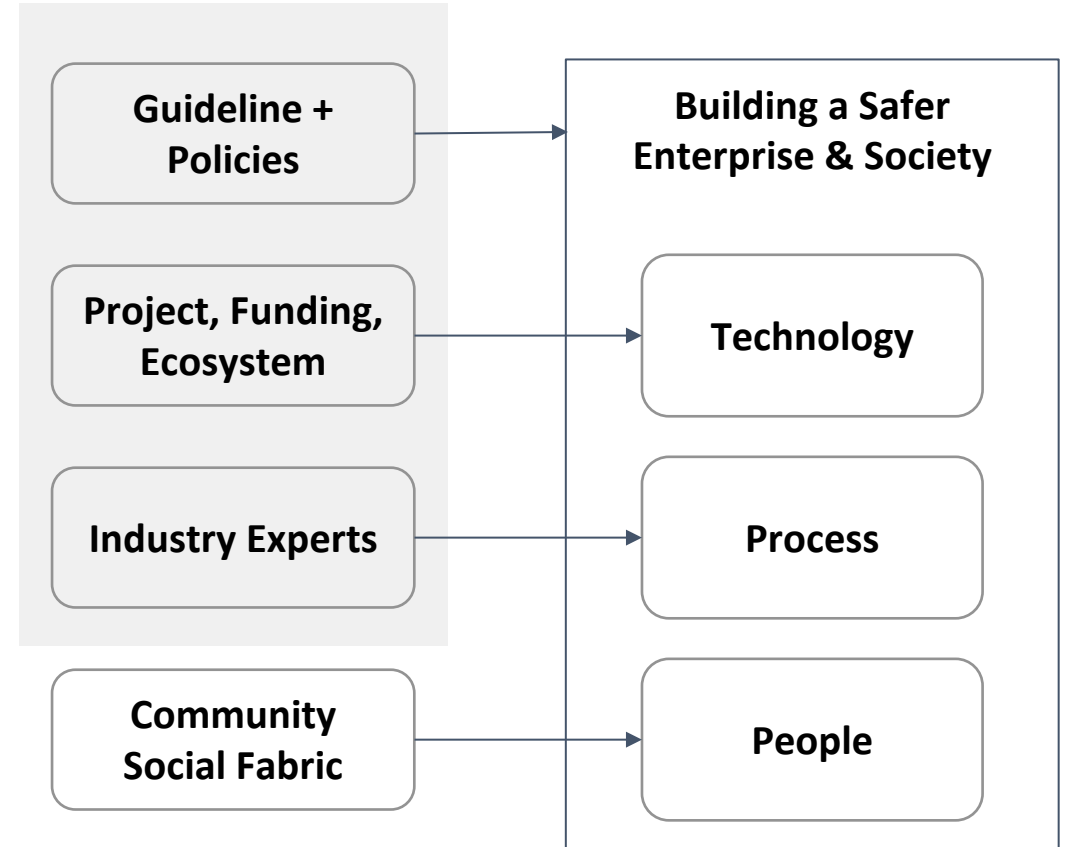
Share best practices and provide technical assistance - Help organizations to improve their cybersecurity posture.

1. Training programs, workshops:

- a. **Educate** people about cybersecurity risks and best practices.
- b. **Public awareness campaigns**, cybersecurity training for employees, and integrating cybersecurity into school curricula.

2. Develop a cybersecurity awareness plan:

- a. Identify the **key cybersecurity risks**.
- b. Best practices for **mitigating** these risks.
- c. **Communication Plan** for educating your employees and customers about cybersecurity risks.





**Where are we
today?**

Collaboration and working across ASEAN Agencies

- On the occasion of the 32nd ASEAN summit, the leaders of ASEAN countries issued a Statement on cybersecurity cooperation.
- The leaders recognised the need to build closer cooperation and coordination among ASEAN Member States on cybersecurity policy development and capacity building initiatives.
- Relevant Ministers are to recommend options of coordinating cybersecurity policy, diplomacy, cooperation, technical and capacity building efforts among various platforms of the three pillars of ASEAN.
- They also tasked Ministers to identify a concrete list of voluntary practical norms of responsible State behaviour in cyberspace that ASEAN could adapt and implement, taking into consideration the report of the UN GGE from 2015.
- The Ministers are further requested to facilitate cross-border cooperation in addressing critical infrastructure vulnerabilities, and encourage capacity building and cooperation for combating criminal and terrorist use of cyberspace.

Full statements: <https://asean.org/wp-content/uploads/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf>

First ASEAN Strategy Paper (2017-2020)

1. Strengthening CERT-CERT cooperation and capacity building
 - ASEAN CERT Maturity Framework
 - Establishment of future ASEAN Regional Computer Emergency Response Team
 - ASEAN Cyber-security Cooperation
 - Targeted Capacity Building Initiatives
2. Key ASEAN Achievements in support of Cyber Cooperation
 - Policy Coordination
 - Incident Response
 - Capacity Building
2. Accelerated Digitalisation:
 - **80%** in Southeast Asia vs **67%** of Asian with access to the Internet
 - High Smartphone usage - **90%** in Malaysia
2. “Digital by default”
3. Sophistication of Cyberattacks and its Implications
4. Complex Interrelation of Cyber and Digital Issues

ASEAN CYBERSECURITY COOPERATION STRATEGY

(2021 – 2025)

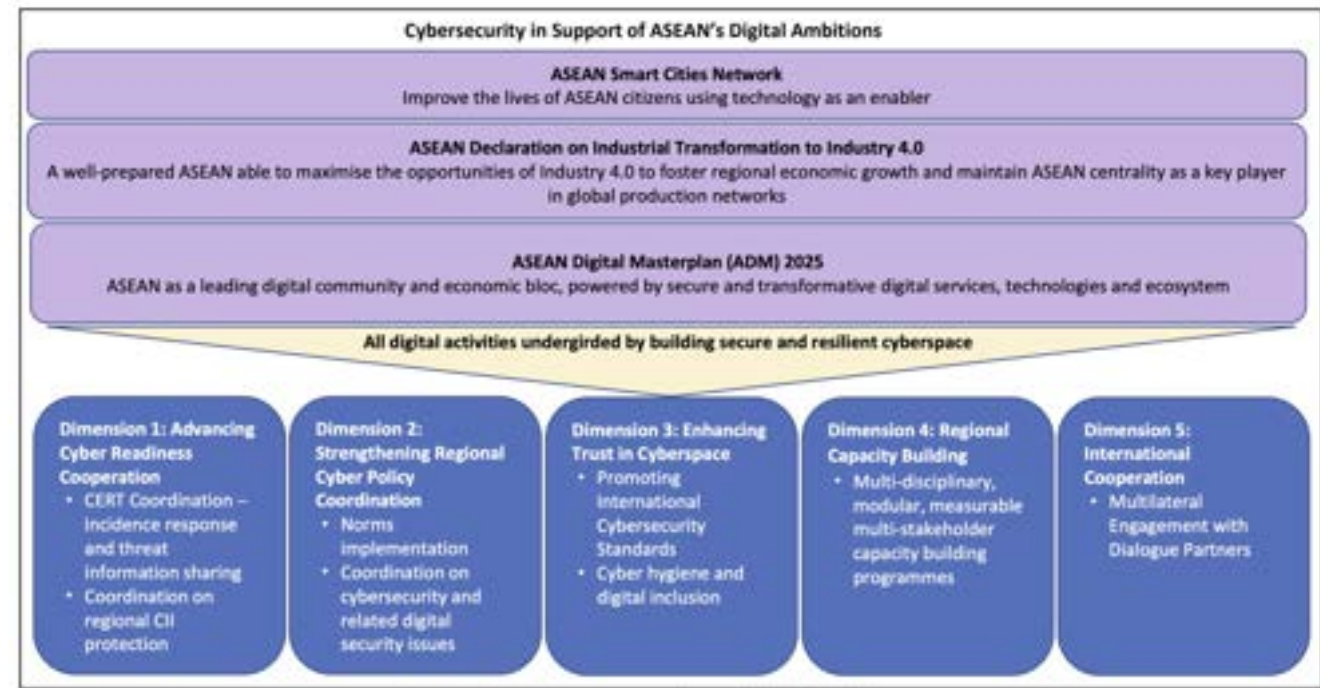


CYBER SECURITY FRAMEWORK (CSF)

ADMM-Plus Experts' Working Group on
Cyber Security

Looking Ahead - OBJECTIVE OF 2021-2025 STRATEGY

1. Advancing Cyber Readiness Cooperation;
2. Strengthening Regional Cyber Policy Coordination;
3. Enhancing Trust in Cyberspace;
4. Regional Capacity Building; and
5. International Cooperation.



AiSP - Leading the formation of Southeast Asia Cybersecurity Consortium (SEACC)

MOU PARTNERSHIP with key overseas organisations to foster cooperation and collaboration

- Participating in and benefiting from each other's respective initiatives and programs.
- To Create a vibrant and dynamic international information and cybersecurity ecosystem.
- Scale and grow our community and partners beyond geographic boundaries

Objective:

- Create a consortium of like-minded individuals and organizations to promote cybersecurity collaboration in the Southeast Asia.
- Drive initiatives and events that bring together a community of industry and academia stakeholders for knowledge exchange, talent development and promotion of diversity and inclusion.
- Drive industry-led initiatives for cybersecurity awareness to elevate the overall security posture for the Southeast Asia region.



Cybersecurity Awareness & Advisory Programme (CAAP)

Targeted for Singapore SMEs, the CAAP aims to drive digital security awareness and readiness. Supported by CSA, our CAAP operating committee focuses on:



Enhance security awareness and training



Create cohesive security knowledge resources



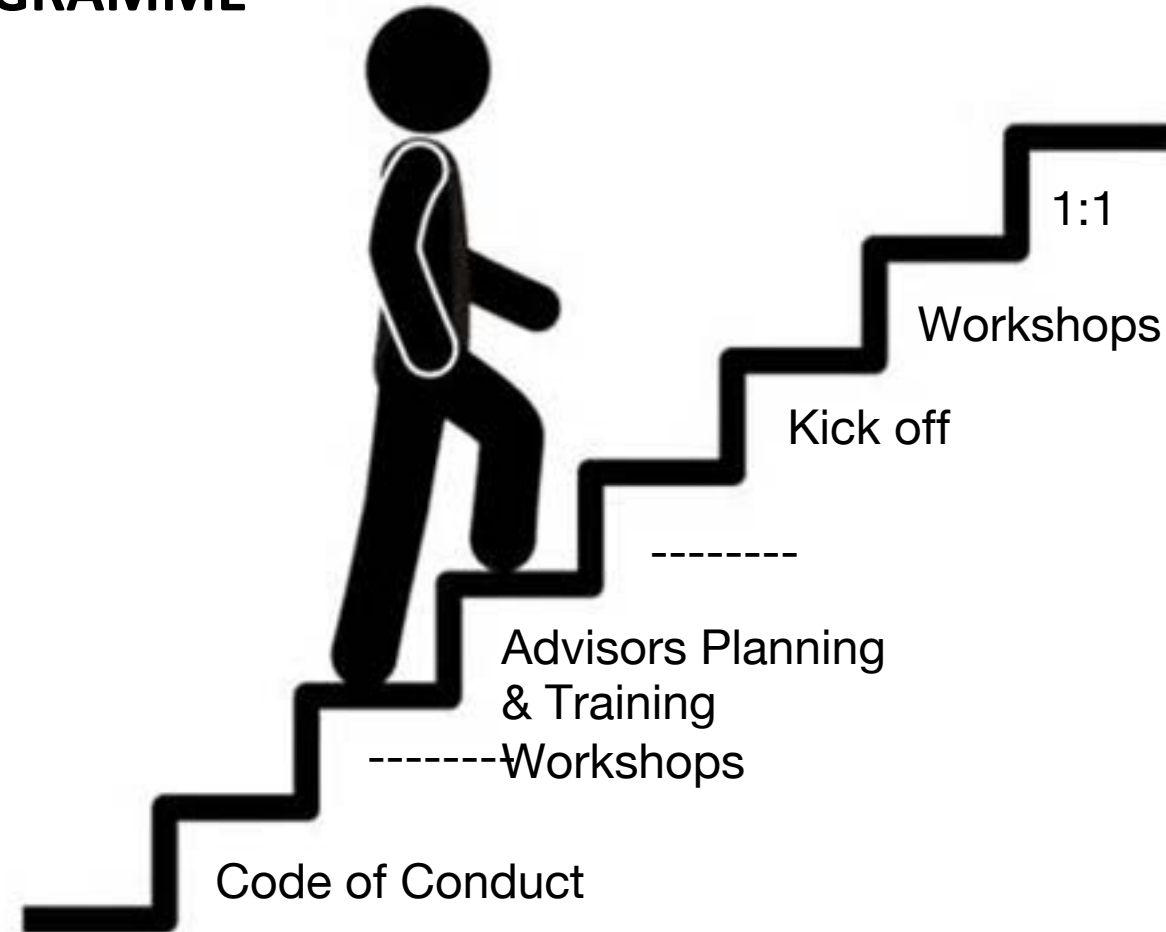
Offer security solutions and services support

The three thrusts are driven by the respective working groups of credible and passionate infosec professionals, supported by AiSP secretariat. We are looking for more companies to tap on CAAP and also, partners and professionals to support the cybersecurity ecosystem.



CYBERSECURITY AWARENESS & ADVISORY PROGRAMME


- **Current Focus:** Improving Readiness of SMEs through outreach programs and webinars
- **NEW!:** Providing basic (pro bono) guidance on improving their Cybersecurity Journey
 - Matchmaking between SMEs needs with Advisors
 - Time box and only specific topics engagement to prevent abuse and effort



Next Steps: Awareness  **Advisory**

Working with Community - AiSP Cyber-wellness under IMDA Digital for Life


Career Advice, Hygiene Tips, Game & Quiz



The AiSP Cyber Wellness Programme aims to educate citizens, especially reaching out to the youths and elderly on the importance of Cybersecurity and learn how to stay safe online. There has been an increase in cyber threats, online scams and COVID-19 related phishing activities. With reduced Face-to-Face engagements, the elderly and those with special needs have become more vulnerable to cyber threats. We will reach out to different community groups to raise awareness on the topic of cyber wellness and cybersecurity and participants can pick up cyber knowledge through interactive learning. It is supported by the Digital for Life Fund, an initiative by the Infocomm Media Development Authority (IMDA), that supports digital inclusion projects and activities to help all Singaporeans embrace digital technology.

Join us in our monthly knowledge series to learn and pick up tips on Cybersecurity. Visit our website to get updates on the latest Cyber tips, Cyber news, activities and happenings related to Cybersecurity.

Supported by:







Get #CyberFit with #Acronis

AiSP FAIRPRICE

Prevent Scam



Singapore Cyber Day Quiz will be held throughout the month of December for the students to take part in during the December school holidays. The online quiz competition is opened to primary, secondary and tertiary students (aged 20 years and below) in Singapore with the support from Cyber Security Agency of Singapore & Finland. This competition aims to pique interest in students and equip them with knowledge on Cyber Security. The quiz links will be available from the launch date onwards.

Week 1 Quiz - Launch on 1st Dec	Week 2 Quiz - Launch on 8th Dec
	

Hygiene Tips

- 1 A strong password consists of 12 letters, upper and lower case, as well as special characters.
- 2 Always enable multi-factor authentication (MFA) to keep your accounts more secure
- 3 Unless your device is offline and physically inaccessible by the rest of the world, there is no such thing as "secure enough".
- 4 It is good practice to regularly backup your data on the cloud or a local storage device, at least once a month.
- 5 Always scan external devices for malware before accessing them.
- 6 You can reduce your vulnerability by ensuring you have an anti-virus and at least one anti-malware installed on your computers.

虽然有一部分的人认为 社交媒体的故事 是真实的 有一些虚假故事还是可能会对我们的生活产生真正的影响。 所谓的“反疫苗 [vaxxers](#)运动和最近 [假莫莫恐慌](#) 都是假新闻让我们情绪不佳。

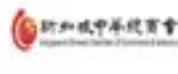
往往你们上网时不知道该 信任谁, 以及 什么是真实的, 现在几乎 所有人都上网, 但其中许多人在情感上却没有能力应对 假新闻 网络文化 的挑战。 我们不能阻止使用互联网, 我们也不应该, 应为 这是一种不可思议的资源。 那么重要的是我们教给你们一些 基本 规则, 以便您对在网上找到的事实充满信心。



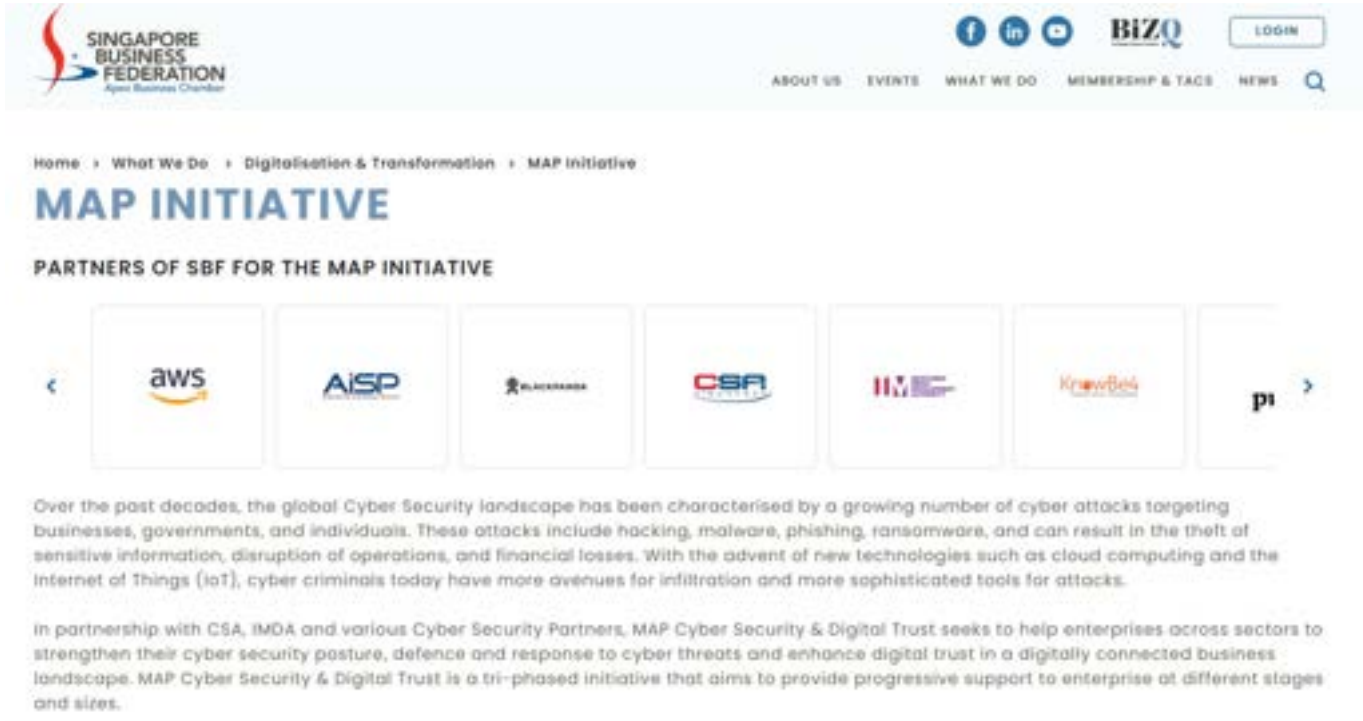
Annual AiSP SME Conference - Bringing the community together



Supported by:



Partnering with Agencies - Singapore Business Federation




The screenshot shows the Singapore Business Federation (SBF) website. The header includes the SBF logo, social media icons for Facebook, LinkedIn, and YouTube, the BIZQ logo, and a LOGIN button. Navigation links include ABOUT US, EVENTS, WHAT WE DO, MEMBERSHIP & TAGS, and NEWS. The main content area features a breadcrumb trail: Home > What We Do > Digitalisation & Transformation > MAP Initiative. Below this is the heading "MAP INITIATIVE" and a sub-heading "PARTNERS OF SBF FOR THE MAP INITIATIVE". A carousel of partner logos is displayed, including AWS, AISP, BLACKPANDA, CSA, IMDA, and KnowBe4. Below the carousel, there is a paragraph of text describing the global Cyber Security landscape and the goals of the MAP Initiative.

Home > What We Do > Digitalisation & Transformation > MAP Initiative

MAP INITIATIVE

PARTNERS OF SBF FOR THE MAP INITIATIVE



Over the past decades, the global Cyber Security landscape has been characterised by a growing number of cyber attacks targeting businesses, governments, and individuals. These attacks include hacking, malware, phishing, ransomware, and can result in the theft of sensitive information, disruption of operations, and financial losses. With the advent of new technologies such as cloud computing and the Internet of Things (IoT), cyber criminals today have more avenues for infiltration and more sophisticated tools for attacks.

In partnership with CSA, IMDA and various Cyber Security Partners, MAP Cyber Security & Digital Trust seeks to help enterprises across sectors to strengthen their cyber security posture, defence and response to cyber threats and enhance digital trust in a digitally connected business landscape. MAP Cyber Security & Digital Trust is a tri-phased initiative that aims to provide progressive support to enterprise at different stages and sizes.



Official Venue Partner:

- Lifelong Learning Institute
- SKILLSfuture SG

MAP Cyber Security & Digital Trust is Supported By:

- aws
- AISP
- BLACKPANDA
- CSA
- IMDA
- KnowBe4
- pwc
- SGTECH
- Singtel
- sptel
- Stone Forest IT

Summary - Call to Action

1. These challenges are likely to become more acute in the coming years, as the region becomes more **digitalized and interconnected**.
2. **Increase investment in cybersecurity**: ASEAN countries need to increase their investment in cybersecurity.
3. **Raise awareness**: ASEAN countries need to raise awareness of cybersecurity risks and best practices among the public and private sectors.
4. **Streamline the regulatory environment**: ASEAN countries need to work together to streamline the cybersecurity regulatory environment.
5. **Continue to develop and collaborate a regional cybersecurity strategy at all levels**: This should include measures to improve cooperation on threat intelligence sharing, incident response, and capacity building.



AiSP

Advance Connect Excel

Thank You for Your Participation!

Please contact secretariat@aisp.sg for any queries.

[https://www.ptsecurity.com/ww-en/analytics/asia-cybersecurity-threatscape-2022-2023/#:~:text=Asia%20Pacific%20\(APAC\)%20was,vulnerable%20as%20digital%20transformation%20continues.](https://www.ptsecurity.com/ww-en/analytics/asia-cybersecurity-threatscape-2022-2023/#:~:text=Asia%20Pacific%20(APAC)%20was,vulnerable%20as%20digital%20transformation%20continues.)

<https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Challenges%20and%20Opportunities%20for%20Cyber%20Norms%20in%20ASEAN%20Revised%20Final.pdf>

<https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/06/asean-cyber-security-cooperation.pdf>

<https://itsnews.widener.edu/2021/10/21/20-ways-to-stop-mobile-attacks/>

<https://www.rsis.edu.sg/rsis-publication/idss/asean-moves-to-strengthen-digital-defence-cooperation/>

CO23101 | ASEAN MOVES TO STRENGTHEN DIGITAL DEFENCE COOPERATION

Empowering ASEAN Cyber Resilience

<https://opengovasia.com/empowering-asean-cyber-resilience/pa>

Enterprise level

<https://techwireasia.com/2021/11/cybersecurity-are-challenging-asean-businesses/>

Cybersecurity is still challenging for ASEAN businesses

What the world can learn from ASEAN's cyber cooperation

1. It is the only regional organization to have subscribed to the UN's 11 voluntary, non-binding norms of responsible state behaviour in cyberspace.
2. Working to develop a regional community with a coordinated approach to cybersecurity. This includes initiatives such as the establishment of the ASEAN Cybersecurity Centre of Excellence and the development of a regional cyber security strategy.
3. Cooperation is based on the principles of mutual trust, respect, and sovereignty. This has allowed ASEAN to build a strong foundation for cooperation in this important area.
4. Challenges still exist in cybersecurity cooperation, such as the need to improve capacity building and to develop a more harmonized regulatory environment.

CYBERSECURITY CROSS-BORDER INNOVATION RESILIENCE

Bookmark

What the world can learn from ASEAN's cyber cooperation

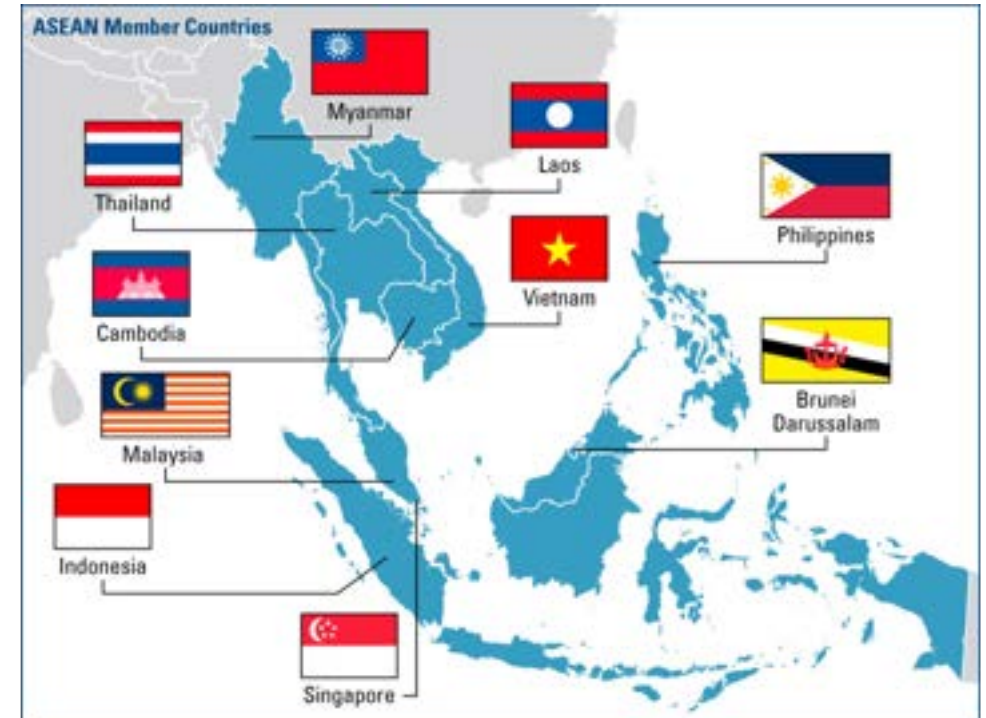
By Amit Roy Choudhury Nov 15, 2021

ASEAN Ministers meet at the Singapore International Cyber Week amidst calls for more cooperation to tackle sophisticated cyber threats.



AiSP - Actively driving collaboration across ASEAN

1. Launched the regionalisation programme to foster closer relationships with other regional cybersecurity associations and organisations.
2. Organized and invited associations / organisations from the Southeast Asia for this key milestone to be distinguished founding members of the South-East Asia Cybersecurity Consortium (SEACC)
3. Launch of the inaugural Southeast Asia Cybersecurity Consortium Forum Nov 2022



South East Asia Cybersecurity Consortium (SEACC)

Country	Association
Brunei	Brunei Cyber Security Association (BCA)
Cambodia	ISAC-Cambodia (InfoSec)
Indonesia	Association Of National Information and Communication Technology Entrepreneurs (APTIKNAS)
Malaysia	Malaysia Board of Technologists (MBOT)
Myanmar	Myanmar Information Security Association (MISA)
Singapore	Association of Information Security Professionals (AiSP)
Philippines	Women in Security Alliance Philippines (WiSAP)
Thailand	Thailand Information Security Association (TISA)
Vietnam	Vietnam Information Security Association (VNISA)



Association of Information Security Professionals



WiSAP

Women in Security Alliance Philippines
Empowering Women in the Cyber Ecosystem



APTIKNAS
Asosiasi Pengusaha TIK Nasional
Indonesian ICT Business Association



VIETNAM INFORMATION SECURITY ASSOCIATION

