Data Collection Survey for Promoting Private-Sector Cybersecurity Cooperation in the ASEAN and the Indo-Pacific Region: Final Report

February 2024

Japan International Cooperation Agency

**Japan Telecommunications Engineering
and
Consulting Service**

Final Report
Table of Contents

Table of abbreviation

Abbreviation	Definition
AFDI	Indonesia Digital Forensic Association
AIM	ASEAN Institute for Management
AiSP	Association of Information Security Professional
AJCCA	ASEAN-JAPAN Cybersecurity Community Alliance
AJCCBC	ASEAN-Japan Cybersecurity Capacity Building Centre
ASPILUKI	Indonesia Telematics Software Association
APICTA	Asia Pacific ICT Alliance
ASOCIO	Asian-Oceanian Computing Industry Organization
ATCI	The Association of Thai ICT Industry
BCS	Bangladesh Computer Samity
BruCERT	Brunei Computer Emergency Response Team
BCSA	Brunei Cyber Security Association
CDTA	Cambodia Digital Technology Association
CII	Critical Information Infrastructure
CSA	Cyber Security Agency of Singapore
CSB	Cyber Security Brunei
CSIRT.ID	Indonesia Cyber Security Independent Resilience Team
CSM	Cyber Security Malaysia
DFFT	Data Free Flow with Trust
FIRST	Forum of Incident Response and Security Teams
FTII	Indonesian Information Technology Federation
GCI	Global Cybersecurity Index
GDPR	General Data Protection Regulation
IBPAP	IT And Business Process Association of The Philippines
IC-AJCC	International Conference on ASEAN-JAPAN Cybersecurity Community
ICSF	Indonesia Cyber Security Forum
ICT-TL	Timor-Leste ICT Association
IFB	Infocom Federation Brunei
idCare	Indonesia Cyber Awareness and Resilient
idNSA	Indonesia Network Security Association
Id-SIRTII/CC	Indonesia Security Incident Response Team on Internet Infrastructure coordination center

ISAC Cambodia	Information Sharing and Analysis Centers
JISA	Japan Information Technology Services Industry Association
JNSA	Japan Network Security Association
JP-CERT	Japan Computer Emergency Response Team/Coordination Center
LIDA	Lao ICT and Digital Association
MIC	Ministry of Information and Communication
MOSA	Mongolian Software Industry Association
MPTC	Ministry of Post and Telecommunications
MPT	Ministry of Technology and Communications
NADPOP	The National Association of Data Protection Officers of the Philippines
NCSA	National Cyber Security Agency
NICP	The National ICT Confederation of the Philippines
NISC	National center of Incident readiness and Strategy for Cybersecurity
PCS	Philippine Computer Society
PH-CERT	Philippine Computer Emergency Response Team
PICSPRO	Philippine Institute of Cyber Security Professionals
PIKOM	The National Tech Association of Malaysia
rawSEC	Malaysia CyberSecurity Community
SCSIA	Singapore Cyber Security Inter Association
SGTech	Singapore's tech industry
SEACC	South East Asia Cybersecurity Consortium
SICW	Singapore International Cyber Week
TISA	Thailand Information Security Association
VINASA	Vietnam Software And IT Services Association
VNISA	Vietnam Information Security Association

List of Figures

List of Tables

1. Survey Contents

Data collection survey for promoting private-sector cybersecurity cooperation in the ASEAN and the Indo-Pacific region (hereinafter referred to as "the Survey").

2. Background of "the Survey"

With the advancement of digitalization, people, goods, money, many organizations including administrative bodies and infrastructure systems have become connected in cyberspace, and it is widely recognized that cybersecurity risks have become enormous in recent years. In many developing countries, the lack of cybersecurity countermeasure systems and capabilities, as well as the lack of human resources, have increased risks, and serious damage has occurred frequently.

- Damage caused by ransomware ran riot worldwide
- Severe damage to critical social infrastructure (energy, finance, telecommunications, health, etc.)
- Leaking of confidential information through the supply chain
- Social disruption caused by disinformation
- Leaking of personal information

Under these circumstances, several development cooperation organizations and governments continue to provide support to strengthen cybersecurity capabilities in developing countries. This serves as a safeguard for countries to promote digital societies in developing countries and to strengthen the security of cyberspace at the regional level, mitigating potential damage across borders.

The Japanese government has proposed "Data Free Flow with Trust (DFFT)" to promote international distribution of data useful for solving business and social issues while ensuring trust in privacy and intellectual property rights from 2019 onward. In 2021, from the viewpoint of reducing international cybersecurity risks, the government formulated the "Basic Policy on Cybersecurity Capacity Building Support for Developing Countries" to promote international cooperation in critical infrastructure protection, cybercrime prevention, international rule making, trust building measures, and human resource development.

In light of the above, in addition to strengthening cybersecurity in each country from the perspective of supply chain risk for Japan's economic security, Japan is promoting cooperation with countries in the Indo-Pacific region, especially ASEAN. While cooperation at the government level is being strengthened, especially through the National center of Incident

readiness and Strategy for Cybersecurity (NISC) of the Cabinet Secretariat, which regularly holds the ASEAN-Japan Cybersecurity Policy Meeting (hereinafter referred to as "the Policy Meeting"), the presence of reliable private companies is important for supply chain risks. However, even in ASEAN countries where many Japanese companies operate, the number of countries where industry associations dealing with cybersecurity have been established and operated is limited, and cooperation with Japanese cybersecurity companies and organizations is insufficient.

3. Overview of "the Survey"

3-1. Purpose of "the Survey"

⑴ To conduct a survey on the actual status of cybersecurity in each country (government, companies, industry associations, etc.) to understand the current state of the public-private partnership environment in ASEAN countries.

⑵ To invite local private associations and organizations (hereinafter referred to as "Selected Organizations") related to cyber security from 9 ASEAN countries to Japan in conjunction with the International Conference on ASEAN-JAPAN Cybersecurity Community (hereinafter referred to as "the Forum") held by NISC in October. Select "target organizations" from among private associations and organizations specialized in cyber security in ASEAN countries (hereinafter referred to as "target organizations") in consultation with NISC (hereinafter referred to as "selected organizations"). In such a case, confirm the participating representatives (hereinafter referred to as "Invitees")

⑶ To conduct a webinar as a follow-up to the ASEAN-Japan Cybersecurity Capacity Building Center (AJCCBC) for current participants and past participants.

⑷ To consider activities that contribute to the promotion of Japanese companies' entry into the market and cooperation with Japanese companies by establishing new target organizations or strengthening their activities based on local wishes.

3-2. Target of "the Survey"

⑴ Countries targeted for on-site surveys ("Target Countries"), 9 countries: Brunei, Cambodia, Indonesia, Laos, Malaysia, Philippines, Singapore, Thailand, Vietnam.

⑵ Desktop (online) survey, 3 countries Bangladesh, Mongolia, East Timor.
   (Order of countries: alphabetical)

3-3. Implementation Schedule of "the Survey"

⑴ Policy

In identifying the contents of the survey, the following survey procedure was adopted considering the urgent need to select "target organizations" and "invitees" to be invited to "the Forum" held by NISC in October, and the difficulty of finding informants from each country at the start of the survey.

⑵ Implementation method

① [First On-site Survey] Invitation negotiation (Until October 2023)
(Purpose)
- in the target countries, conduct interviews to accurately identify relevant private sector organizations and groups, and proceed with the identification, negotiation, and selection of "Selected organizations" and their representatives' "invitees"
- If an invitee is selected through on-site interviews, the private organization will propose a "Cybersecurity event" to promote the target organization and the forum (hereinafter referred to as "local event").

② [Second On-site Survey] Follow-up events (Until October 2023)
(Purpose)
- To assist "local event" as determined in ①.
- Completion of tasks unfinished in ①. *In that case, to hold "local event" (3 times)

③ [Desktop Survey] (From November 2023)
(Purpose)
- Using the partnerships established through ① and ②, specific survey to be conducted through associations in each country.

④ Questionnaire survey of "the Forum" participants

⑤ Annual Report Survey for the ASEAN-JAPAN Cybersecurity Community Alliance (AJCCA), a federation of associations formed through an MOU signed at "the Forum".

4. Cybersecurity Indicators and Collection Methods in Each Country

4-1. Overview

The main focus of the study was desktop survey, and online information was collected from the websites of national CSIRT and other sources for each country.

(1) Reference indicators

Websites of each national CSIRT:
- Brunei: https://www.brucert.org.bn/
- Cambodia: https://www.camcert.gov.kh/en/
- Indonesia: https://idsirtii.or.id/

- Laos: https://laocert.gov.la/
- Japan: https://www.jpcert.or.jp/
- Malaysia: https://www.mycert.org.my/
- Philippines: https://www.ncert.gov.ph/about-us/ncert
- Singapore: https://www.csa.gov.sg
- Thailand: https://www.thaicert.or.th/
- Vietnam: https://vncert.vn/
- Bangladesh: https://www.cirt.gov.bd/
- Mongolia: https://mncert.org/
- East Timor: https://tlcsirt.org/

(2) Collection methods

Received referrals for associations and organizations in the cyber security industry and key persons from the following organizations and conducted interviews with them individually.

- Asian-Oceanian Computing Industry Organization (ASOCIO)
- Asia Pacific ICT Alliance (APICTA)
- Japan Information Technology Services Industry Association (JISA)
- Japan Network Security Association（JNSA）
- Japan Computer Emergency Response Team/Coordination Center (JP-CERT)
- Forum of Incident Response and Security Teams (FIRST)

① Desktop survey
・ Digital data, online information collected over the Internet.
・ Information collected through online meetings with individual referrers and by email.

② Individual interview survey
・ On-site Interview surveys.
・ Interviews with AJCCA members.

5. Status of ICT and Cybersecurity Private Organizations in Each Country

5-1. Brunei

Brunei, with a population of approximately 485,000 and a remarkable real GDP per capita of $60,100, holds a unique position within the ASEAN community. While boasting a respectable Global Cybersecurity Index (GCI) rank of 85 and a regional rank of 16 in the Asia Pacific, the

nation is actively taking steps to bolster its cybersecurity landscape. Recent updates include the establishment of a scam protection center led by banks, efforts to standardize Critical Information Infrastructure (CII) guidelines, and the strengthening of data protection laws. Despite these proactive measures, Brunei faces significant cyber threats, with phishing, identity fraud, and scams dominating the cybersecurity landscape. However, the nation benefits from the presence of an official cybersecurity community, the Brunei Computer Emergency Response Team (BruCERT), which plays a crucial role in engaging stakeholders, raising awareness, and mitigating cyber risks. As Brunei continues to enhance its cybersecurity resilience, initiatives like the BCSA (Brunei Cyber Security Association) underscore the nation's commitment to safeguarding its digital infrastructure and fostering a secure cyber environment for its citizens and businesses.

Country Profile

Population	484,991 (2023 est.)
Real GDP per Capita (USD)	60,100 (2021 est.)
Member ASEAN	1984

ICT and Cybersecurity Profile

Telephones user- fixed lines	122,204 (2022 est.)
Telephones user - mobile cellular	603,486 (2021 est.)
Telecommunication Operator (included VNO)	3
Internet users	441,000 (2021 est.)
Broadband - fixed subscriptions	71,078 (2020 est.)
GCI Index Overall score	56,70
GCI Index Regional Rank (Asia Pacific)	16
GCI Index Global Rank	85

Cybersecurity Community in Brunei

Brunei Cyber Security Association (BCSA): https://www.itpss.com
InfoCom Federation Brunei (IFB): https://www.ifb.org.bn/

See Appendix below for detailed information on ICT and cybersecurity private sector organizations and cybersecurity indicators from the desktop survey.

Appendix1: Survey ICT Organization

Appendix2: Survey Cybersecurity Private Organization

Appendix3: Desktop Survey on Cybersecurity

Table 1 : Brunei - On-site Survey Schedule and List of Interviewees

Brunei	First On-site Survey	Tuesday, May 22nd to Thursday, May 26th, 2023
1	Name	Ms. Pengiran Sarimah Binti Pengiran HJ Abdul Latiff
	Organization	InfoCom Federation Brunei (IFB)
	Job title	Chairwoman
	Notes	Member of ASOCIO
2	Name	Mohamad Azad Zaki Haji Mohd Tahir
	Organization	Brunei Cyber Security Association (BCSA)
	Job title	President
	Notes	

Table 2 : Brunei - "Selected Organization" Information

Organization	Brunei Cyber Security Association (BCSA)
Website	https://www.itpss.com
Status	NGO
Year of Establishment	2022
Purpose & Background	In the pursuit of the growing demand for cybersecurity professionals in Brunei Darussalam, it is my pleasure to announce the official establishment of the Brunei Cyber Security Association (BCSA) as of the 14th of August 2023, and we have outlined our objectives within our constitution the values and mission needed to undertake in order to improve our cybersecurity workforce. Our journey began with a shared desire to create a platform similar to today's conference, that would bring together individuals and organizations who share a common interest in cybersecurity. Insha'Allah, We shall commence the onboarding process of our membership program to prospective members both individual and corporate in 2024.
Chairman	Mohamad Azad Zaki Haji Mohd Tahir
Number of members	20
Government Relations	Cyber Security Brunei（CSB）
Structure	Chairman,2 Vice President, Secretary, Assistant Secretary, Treasury, Assistant Treasury, Executive committee: 18

- "Invitees"：Mr. Mohamad Azad Zaki Haji Mohd Tahir

- Intention to hold "local event"：No

See Appendix below for the results of the "Cyber Security Survey" responses from the "selected organizations".

Appendix4: JICA Cyber Security Questionnaire

(1) Results of On-site Survey

The Brunei Cyber Security Association (BCSA) is committed to protecting the country's digital infrastructure, providing a safe and secure environment, and working with government agencies.

BCSA Chairman Mohammad Azad Zaki Haji Mohd Tahir was briefed about "the Forum" and asked to participate in the event as a speaker. The possibility of strong cooperation among the Japanese and ASEAN cyber communities is also discussed. Through the interview, it is confirmed that BCSA is the only cybersecurity association in Brunei.

5-2. Cambodia

Cambodia, with a population estimated at 38.2 million and a real GDP per capita of approximately $19,899,790, is emerging as a key player in the ASEAN region. Despite its relatively small size, the country is making strides in bolstering its cybersecurity landscape. Plans are underway to establish a governance structure aimed at coordinating a nationwide approach to cybersecurity, alongside the endorsement of comprehensive cybersecurity legislation, including laws addressing personal data protection, cybercrime, and cybersecurity strategy. Additionally, a Digital Security Committee is slated for establishment in the coming months, indicating Cambodia's commitment to enhancing its cyber resilience. However, the nation faces significant cyber threats such as phishing attacks, ransomware, scams, fraud, APT (Advanced Persistent Threats), and supply chain vulnerabilities. Notably, while Cambodia currently lacks an official cybersecurity community, initiatives like ISAC-Cambodia serve as virtual platforms, fostering collaboration and information sharing among stakeholders in the cybersecurity domain.

Country Profile

Population	16,891,245 (2023 est.)
Real GDP per Capita (USD)	1,851 (2022 est.)
Member ASEAN	1999

ICT and Cybersecurity profile

Telephones user- fixed lines	38,284 (2022 est.)
Telephones user - mobile cellular	19,899,790 (2021 est.)
Telecommunication Operator (included VNO)	6
Internet users	1,020,000 (2021 est.)
Broadband - fixed subscriptions	233,732 (2020 est.)
GCI Index Overall score	19,12
GCI Index Regional Rank (Asia Pacific)	26
GCI Index Global Rank	132

Cybersecurity Community in Cambodia

ISAC Cambodia: https://web.facebook.com/groups/242965532481324

Cambodia Digital Technology Association (CDTA):

https://web.facebook.com/CambodiaDigitalTechAssociation

See Appendix below for detailed information on ICT and cybersecurity private sector organizations and cybersecurity indicators from the desktop survey.

Appendix1: Survey ICT Organization

Appendix2: Survey Cybersecurity Private Organization

Appendix3: Desktop Survey on Cybersecurity

Table 3：Cambodia - On-site Survey Schedule and List of Interviewees

Cambodia	First On-site Survey	Saturday, June 3rd to Wednesday, June 7th, 2023
1	Name	Mr. Phannarith Ou
	Organization	Ministry of Post and Telecommunication（MPTC), ISAC Cambodia
	Job title	Chairman
	Notes	
2	Name	Mr. Oknha Chin Ken
	Organization	Cambodia Digital Technology Association (CDTA)
	Job title	Chairman
	Notes	

Table 4：Cambodia - "Selected Organization" Information

Country	Cambodia
Organization	Information Sharing and Analysis Centers (ISAC Cambodia)
Website	https://www.facebook.com/groups/242965532481324

Status	NGO
Year of Establishment	2016
Purpose & Background	• Sharing best practice and know-how on cybersecurity related matters
	• Conduct sharing session, training and workshop • Local and international cooperation on cyber related issues & emerging technologies • Industries and partners collaboration programs
Chairman	Mr. Phannarith Ou
Number of members	80000
Government Relations	Mr. Phannarith Ou, chairman of ISAC Cambodia is also Ministry of Post and Telecommunications (MPTC)
Structure	Chairman

- "Invitees"：Mr. Phannarith Ou
- Intention to hold "local event"：No

See Appendix below for the results of the "Cyber Security Survey" responses from the "selected organizations".
Appendix4: JICA Cyber Security Questionnaire

(1) Results of On-site Survey
Interview with Mr. Phannarith Ou and Mr. Ann Kim of the Ministry of Post and Telecommunications (MPTC) confirmed that Cambodia has no association dedicated to cybersecurity. The relevance of an organization called Innovations for Social Accountability in Cambodia (ISAC Cambodia), which is not yet legally registered, was discussed and it was decided to recommend it as a target organization since Mr. Ou is its representative.

(2) Cooperation with Japanese companies and organizations
There is no collaboration with Japanese private companies or organizations, and although several companies appear to have entered the market on a stand-alone basis, the names of the companies could not be identified. MPTC is the government agency in charge of cyber security in the Kingdom of Cambodia and is a member of NISC's ASEAN-Japan Cyber Security Policy Council. JICA is currently stationed at MPTC for a cyber security project in Cambodia.

(3) Other Reference Information

CDTA is primarily an ICT general association, with some members dedicated to cybersecurity. Multiple requests to attend the October event were received, but after informing them of the requirement to cover their own travel and lodging expenses, they rescinded their intention to attend. They presented software using AI technology at the interview. The association hopes to interact with Japanese ICT associations and companies in the future.

5-3. Indonesia

Indonesia, with a population of over 279 million and a real GDP per capita of $11,900, stands as a significant player in Southeast Asia. In terms of cybersecurity, the nation has been proactive, evidenced by the launch of more than 100 Computer Security Incident Response Teams (CSIRTs) nationwide, an initiative driven by the government. Furthermore, the enactment of the Data Privacy Protection Law in 2022, set to take effect in 2024, reflects Indonesia's commitment to bolstering its cyber defenses. Despite these efforts, the country faces various cyber threats, including big data leaks, malware, ransomware, phishing, scams, and fraud. However, Indonesia's cybersecurity landscape benefits from active engagement from numerous cybersecurity communities dedicated to combating these challenges, indicating a collective effort towards enhancing the nation's cyber resilience.

Country Profile

Population	279,476,346
Real GDP per Capita (USD)	11.900
Member ASEAN	1967

ICT and Cybersecurity profile

Telephones user- fixed lines	8,423,990 (2022 est.)
Telephones user - mobile cellular	365,872,608 (2021 est.)
Telecommunication Operator (included VNO)	7
Internet users	16,740,000 (2021 est.)
Broadband - fixed subscriptions	11,722,218 (2020 est.)
GCI Index Overall score	94,88
GCI Index Regional Rank (Asia Pacific)	6
GCI Index Global Rank	24

Cybersecurity Community in Indonesia

Indonesia Network Security Association (idNSA)：https://idnsa.id

Indonesia Cyber Awareness and Resilient (idCare)：https://idcare.ui.ac.id/

Indonesia Cyber Security Independent Resilience Team (CSIRT.ID)：https://csirt.id/

Indonesia Digital Forensic Association (AFDI)：https://www.afdi.or.id/

Indonesia Cyber Security Forum (ICSF): https://id.linkedin.com/company/indonesia-cyber-security-summit

See Appendix below for detailed information on ICT and cybersecurity private sector organizations and cybersecurity indicators from the desktop survey.

Appendix1: Survey ICT Organization

Appendix2: Survey Cybersecurity Private Organization

Appendix3: Desktop Survey on Cybersecurity

Table 5：Indonesia - On-site Survey Schedule and List of Interviewees

Indonesia	First On-site Survey	Remote Survey
1	Since Dr. Rudi Lumanto, the representative of the association in Indonesia, was participating as a local staff member, the purpose of the first on-site survey, "interview with the association representative and explanation of this forum," were accomplished without visiting the site. Therefore, it was changed to a remote survey.	
Indonesia	**Second On-site Survey**	**Monday, July 17th to Thursday, July 20th, 2023**
1	Name	Mr. Sigit Jarot
	Organization	Indonesia Network Security Association (idNSA)
	Job title	Advisor
	Notes	
2	Name	Mr. Fardan
	Organization	Indonesia Network Security Association (idNSA)
	Job title	Chairman
	Notes	
3	Name	Mr. Andi Budimansyah
	Organization	Federasi Teknologi Informasi Indonesia (FTII)
	Job title	Chairman
	Notes	Member of ASOCIO
4	Name	Dr. Muhammad Salman

	Organization	Indonesia Cyber Awareness and Resilience Center, University of Indonesia
	Job title	Professor
	Notes	
5	Name	Mr. Angel Averia
	Organization	Philippine Computer Emergency Response Team (PH-CERT)
	Job title	President
	Notes	The meeting with Mr. Averia took place during his visit to Indonesia.

Table 6：Indonesia - "Selected Organization" Information

Country	Indonesia
Organization	Indonesia Network Security Association (idNSA)
Website	https://idnsa.id
Status	NGO
Year of Establishment	2011
Purpose & Background	Started as Indonesia Cyber Security Research Circle (ICyReC in 2011) Established as IdNSA in 31/8/2017 , Ministry of Law and Human Right Registration Number : AHU-0013509.AH.01.07.TAHUN 2017 Three purposes : To know, learn and engage in the development of network security which is growing rapidly worldwide Improving community security awareness To contribute and take a part on building a safe and secure network environment through a bottom-up approach and strengthening the weakest links.
Chairman	Mr. Fardan, Chairman
Number of members	800
Government Relations	JNSA (2017)
Structure	Advisory Board, Expert Board, Chairman, Secretary, Head of Capacity Dev, Head of Readiness, Head of RnD、Executive committee: 10

- "Invitees"：Dr. Rudi Lumanto
- Intention to hold "local event"：Yes

See Appendix below for the results of the "Cyber Security Survey" responses from the "selected organizations".
Appendix4: JICA Cyber Security Questionnaire

(1) Results of On-site Survey

The founder of idNSA in Indonesia is Dr. Rudi Lumanto. He has overseen Indonesia's national CSIRT, Indonesia Security Incident Response Team on Internet Infrastructure coordination center (Id-SIRTII/CC), when working for the Indonesian Ministry of Cryptology, and is well acquainted with Japanese ministries and companies. He is also the founder and organizer of "Code Bali", a cyber security event started in 2015 with the support of Japanese industry and government, and is involved as a university official in a JICA project to support the establishment of a POC for SOC at the University of Indonesia.

(2) Cooperation with Japanese companies and organizations

idNSA has an MOU with JNSA, a Japanese private association, for collaboration in September 2017, and has several partnerships with JNSA member companies (LAC Corporation, NEC, NRI Secure, Amiya).

(3) Other Reference Information

idNSA has made the Indonesian SECCON "Cyber Jawara" as an international event from this year, actively inviting participants and speakers from other countries. The goal is to position the event as a qualifier for SECCON organized by JNSA in Japan as a private-sector-led security contest competing with the government-led SECCON "Cyber Sea Game" held at AJCCBC in Thailand.

5-4. Laos

Laos, with a population of approximately 7.85 million and a real GDP per capita of $7,800, faces unique challenges in its cybersecurity landscape. While boasting a Global Cybersecurity Index (GCI) rank of 131 and a regional rank of 25 in the Asia Pacific, Laos is witnessing an increased demand for cybersecurity assessments, particularly from sectors like banking, telecommunications, and small and medium enterprises (SMEs). However, the country grapples with a notable lack of cybersecurity capacity both in the public and private sectors. Additionally, while e-commerce remains in its infancy, socio-commerce continues to dominate in Laos. In these

challenges, the presence of Lao CERT, the government agency responsible for national cybersecurity, as well as LAO HACKER, a private cybersecurity community, underscores efforts towards fostering collaboration and knowledge-sharing within the country. Laos is set to host the ASEAN Leaders Summit and other related events, providing opportunities to accelerate the country's development, including advancements in cybersecurity. Nevertheless, Laos faces significant cyber threats, including scams, virus infections, and data leaks, highlighting the importance of strengthening its cybersecurity infrastructure to mitigate risks and safeguard its digital landscape.

Country Profile

Population	7,852,377 (2023 est.)
Real GDP per Capita (USD)	7,800 (2021 est.)
Member ASEAN	23-Jul-1997

ICT and Cybersecurity profile

Telephones user- fixed lines	1,300,195 (2021 est.)
Telephones user - mobile cellular	4,822,973 (2021 est.)
Telecommunication Operator (included VNO)	4
Internet users	4,588,000 (2021 est.)
Broadband - fixed subscriptions	128,000 (2020 est.)
GCI Index Overall score	20,34
GCI Index Regional Rank (Asia Pacific)	25
GCI Index Global Rank	131

Cybersecurity Community in Laos

Lao Hacker: https://www.laohacker.com/

See Appendix below for detailed information on ICT and cybersecurity private sector organizations and cybersecurity indicators from the desktop survey.

Appendix1: Survey ICT Organization

Appendix2: Survey Cybersecurity Private Organization

Appendix3: Desktop Survey on Cybersecurity

Table 7: Laos - On-site Survey Schedule and List of Interviewees

Laos	First On-site Survey	Friday, February 9th, 2023
1	Name	Mr. Thanousone Phonama

	Organization	Lao ICT and Digital Association (LIDA) Vice President, Lao National Chamber of Commerce and Industry
	Job title	Chairman of LIDA, Vice President of Lao National Chamber of Commerce and Industry
	Notes	
2	Name	Mr. Khamla Sounnalat
	Organization	Department of Cyber Security, Ministry of Technology and Communications (MPT) , LaoCERT Division
	Job title	Director General of Lao CERT
	Notes	
3	Name	Mr. Sengxay Xayachack
	Organization	CYBERRUS sole Co., Ltd.
	Job title	CEO & Founder
	Notes	
4	Name	Mr. Vongvilai Inthasanh
	Organization	Department of Cyber Security, Ministry of Technology and Communications (MPT) , LaoCERT Division
	Job title	Deputy director LaoCERT Division
	Notes	

See Appendix below for the results of the "Cyber Security Survey" responses from the "selected organizations".
Appendix4: JICA Cyber Security Questionnaire

(1) Results of On-site Survey
-Interview with Mr. Thanousone Phonamat (Vice Chairman Lao National Chamber of Commerce and Industry/Chairman of Lao ICT and Digital Association (LIDA))
Mr. Thanousone is also the owner of ALO (e-commerce), Planet (a pioneering broadband ISP for businesses) and four other companies. Planet focuses on large and small businesses that offer broadband through fiber (FTTH). LIDA has around 50 member companies and security chapter is only one company: CYBERRUS sole Co., Ltd. LIDA holds three monthly meeting called Digital Forum, included cybersecurity as one of the themes. According to Mr. Thanousone, starting cybersecurity business is easy in Laos, as it is allowed to foreign people to

build even 100% shares. But other sectors like telecommunication may be restricted by the government.

-Interview with Mr. Frank Sengxay Xayachack (Founder and CEO of CYBERRUS sole Co., Ltd.)
CYBERRUS sole Co., Ltd. has been operating for 2 years with 10 employees. Its primary business is security assessments targeting mainly web applications; cloud and others are not yet covered. Mr. Xayachack has his own community called the "Lao Hacker Club" which meets monthly. Many university students are members of this club, which has about 40 active members. This community helps the government with the infrastructure for the annual CTF convention. The club supervises Student Cybersecurity Club in Lao University and Soutsaka College. As claimed by Mr. Xayachack, many cyber incidents are never publicized and may be controlled by the government.
Mr. Xayachack's community is a self-funded independent organization, receives no government support, and wishes to join the AJCCA.

-Interview with Mr. Khamla Sounnalat (Director General of Lao CERT, Ministry of Technology and Communication, LAO P.D.R)
Cybersecurity in Laos is under Mr. Sounnalat's department, which includes Lao CERT. The total number of employees is between 20 and 30 including the five Lao CERT members. Many of them do not have professional certifications in cybersecurity, so obtaining certifications is currently of utmost importance to them. Mr. Sounnalat would like to obtain JICA's assistance so that his employees can be trained under Indonesia's UI/JICA program.

(2) Other Reference Information
- In the past two years, there has been an increase in demand for cybersecurity assessments from banks, e-communications companies, and SMEs, however, Lao's cybersecurity capabilities lack in both the public and private sectors.
- Social commerce continues to dominate in Laos.
- Laos is the host country of this year's ASEAN Summit, with many other events scheduled in parallel. Therefore, Laos will have many opportunities to accelerate nation-building, including cybersecurity.

5-5. Malaysia

Malaysia, with a population of over 34 million and a real GDP per capita of $26,300, stands out as a leading force in the ASEAN region. With an impressive Global Cybersecurity Index (GCI)

rank of 5 and a regional rank of 2 in the Asia Pacific, Malaysia demonstrates a proactive approach to cybersecurity. Recent updates indicate significant strides in aligning its data protection legislation with international standards, such as the General Data Protection Regulation (GDPR). Moreover, the forthcoming cybersecurity bill of 2024, slated for parliamentary tabling in Q2 2024, underscores Malaysia's commitment to enhancing its cyber resilience. Despite facing prevalent threats such as ransomware and rootkit attacks, Malaysia benefits from a robust ecosystem of cybersecurity communities and organizations. Notably, rawSEC emerges as an active community, hosting monthly events to promote knowledge-sharing and collaboration within the cybersecurity domain. Moreover, Malaysia's high cybersecurity hygiene and awareness levels are attributed to proactive awareness campaigns by both private and government entities. These efforts reflect Malaysia's dedication to fostering a secure digital environment and positioning itself as a cybersecurity leader within the ASEAN community.

Country Profile

Population	34,219,975 (2023 est.)
Real GDP per Capita (USD)	26,300 (2021 est.)
Member ASEAN	1996

ICT and Cybersecurity profile

Telephones user- fixed lines	8,452,900 (2022 est.)
Telephones user - mobile cellular	47,201,700 (2021 est.)
Telecommunication Operator (included VNO)	16
Internet users	32,980,000 (2021 est.)
Broadband - fixed subscriptions	3,358,800 (2020 est.)
GCI Index Overall score	98,06
GCI Index Regional Rank (Asia Pacific)	2
GCI Index Global Rank	5

Cybersecurity Community in Malaysia

rawSEC: https://www.facebook.com/rawsec.my/

Nanosec : https://nanosec.asia/

See Appendix below for detailed information on ICT and cybersecurity private sector organizations and cybersecurity indicators from the desktop survey.

Appendix1: Survey ICT Organization

Appendix2: Survey Cybersecurity Private Organization

Appendix3: Desktop Survey on Cybersecurity

Table 8：Malaysia - On-site Survey Schedule and List of Interviewees

Malaysia	First On-site Survey	Wednesday, June 7th to Friday, June 9th, 2023
1	Name	Mr. Tahrizi Thareb
	Organization	Malaysia CyberSecurity Community（rawSEC）
	Job title	Co-Founder
	Notes	
2	Name	Dato' Dr Amirudin Abdul Wahab
	Organization	Cyber Security Malaysia (CSM)
	Job title	Chairman
	Notes	
1	Name	Mr. Ong Chin Seon
	Organization	The National Tech Association of Malaysia (PIKOM)
	Job title	Chairman
	Notes	
2	Name	Mr. Alex Loh
	Organization	The National Tech Association of Malaysia (PIKOM)
	Job title	Chairman of CS Chapter, PIKOM
	Notes	*Other executive members
Malaysia	Second On-site Survey	Sunday, July 9th to Thursday, July 13th, 2023
1	Name	Mr. Tahrizi Thareb
	Organization	Malaysia CyberSecurity Community（rawSEC）
	Job title	Co-Founder
	Notes	
2	Name	Dato' Dr Amirudin Abdul Wahab
	Organization	Cyber Security Malaysia (CSM)
	Job title	Chairman
	Notes	
3	Name	Mr. Effendy Zulkifly
	Organization	Blockworq/Crypto Valley Malaysia

	Job title	CEO of Blockworq/ Founder of Crypto Valley Malaysia
	Notes	

Table 9：Malaysia - "Selected Organization" Information

Country	Malaysia
Organization	Malaysia CyberSecurity Community (rawSEC)
Website	https://www.facebook.com/rawsec.my/
Status	NGO
Year of Establishment	2017
Purpose & Background	In summary, rawSEC is a non-profit community effort in Malaysia which intends to provide a strong platform for local information security talents to share and contribute their knowledge to the community. rawSEC existence is to address the current industry gap by bridging the education sector and industry through a series of meetups and discussion sessions which would produce relevant talents for the industry.
Chairman	Mr. Tahrizi Thareb
Number of members	3000
Government Relations	The chairman of rawSEC is a chair of cyber security in Bank Negara Malaysia.
Structure	Chairman, 20 committee including 6 council of elders

- "Invitees"：Mr. Tahrizi Thareb
- Intention to hold "local event"：No

See Appendix below for the results of the "Cyber Security Survey" responses from the "selected organizations".

Appendix4: JICA Cyber Security Questionnaire

(1) Results of On-site Survey

rawSEC facilitates knowledge sharing and cooperation within the Malaysian cybersecurity industry, contributing to the growth of the industry. The rawSEC chairman is the head of the cybersecurity department of the Central Bank of Malaysia and has a leadership role in the

industry, which allows rawSEC to have a close relationship with the industry and develop initiatives that meet the needs of the industry.

(2) Other Reference Information

In Malaysia, the Personal Data Protection Act 2010 (PDPA) is currently under review and is expected to be aligned with the European Union's General Data Protection Regulation (GDPR). The GDPR is one of the strictest data protection laws in the world, and the revised PDPA is expected to be just as stringent.

The GDPR establishes a number of requirements for companies and organizations that collect and process personal data, including:
- Obtaining consent from individuals before collecting their personal data.
- Providing access to personal data and the right to have personal data erased.
- Taking steps to protect personal data from unauthorized access, use, or disclosure.
- Notifying individuals without undue delay in the event of a data breach.

The revised PDPA is expected to include similar matters, and Malaysian companies and organizations will need to modify their data protection policies to comply with the new law.

5-6. Philippines

The Philippines, with a population of over 116 million and a real GDP per capita of $8,100, remains a significant player in the ASEAN region. Despite facing challenges, such as a Global Cybersecurity Index (GCI) rank of 61 and a regional rank of 13 in the Asia Pacific, the country is actively addressing cybersecurity concerns. Recent updates include the consideration of three pending bills focused on enhancing cybersecurity legislation. However, the nation continues to grapple with dominant cyber threats, particularly phishing and ransomware attacks targeting both government systems and private entities. Amidst these challenges, the Philippines benefits from the active engagement of various communities and associations in cybersecurity activities. Notably, PH-CERT stands out as the oldest cybersecurity community in the country, founded in 2001, while Holy Angel University leads the way as the first university to offer both undergraduate and graduate programs in cybersecurity. Additionally, the university's initiative in establishing the PICSPRO chapter in region three underscores its commitment to nurturing cybersecurity talent and fostering a robust cybersecurity ecosystem through events like Capture The Flag (CTF) competitions for students. These efforts reflect the Philippines' dedication to strengthening its cybersecurity resilience and capacity-building initiatives in the face of evolving cyber threats.

Country Profile

Population	116,434,200 (2023 est.)
Real GDP per Capita (USD)	8,100 (2021 est.)
Member ASEAN	1996

ICT and Cybersecurity profile

Telephones user- fixed lines	4,884,608 (2022 est.)
Telephones user - mobile cellular	163,345,244 (2021 est.)
Telecommunication Operator (included VNO)	7
Internet users	5,830,000 (2021 est.)
Broadband - fixed subscriptions	7,936,574 (2020 est.)
GCI Index Overall score	77,00
GCI Index Regional Rank (Asia Pacific)	13
GCI Index Global Rank	61

Cybersecurity Community in Philippines

Philippine Computer Emergency Response Team (PH-CERT):

https://www.facebook.com/PHCERT/

Philippine Institute of Cyber Security Professionals (PICSPRO) :

https://www.facebook.com/PICSProfessionals/

The National Association of Data Protection Officers of the Philippines (NADPOP):

https://nadpop.org/

The National ICT Confederation of the Philippines: https://nicp.org.ph/

Philippine Computer Society (PCS): https://philippinecomputersociety.org/

See Appendix below for detailed information on ICT and cybersecurity private sector organizations and cybersecurity indicators from the desktop survey.

Appendix1: Survey ICT Organization

Appendix2: Survey Cybersecurity Private Organization

Appendix3: Desktop Survey on Cybersecurity

Table 10：Philippines - On-site Survey Schedule and List of Interviewees

Philippines	First On-site Survey	Wednesday, May 31st to Friday June 2nd, 2023
1	Name	Mr. Angel Averia
	Organization	Philippine Computer Emergency Response Team (PH-CERT)

		Job title	Chairman
		Notes	The first registered cybersecurity-related non-profit organization in the Philippines.
	2	Name	
		Organization	Holy Angel University
		Job title	President
		Notes	
	3	Name	Dr. Marlon Tayag
		Organization	Holy Angel University
		Job title	Associate Prof. III, Dean, School of Computing, Holy Angel University
		Notes	*The first university in the Philippines to establish a cybersecurity department
Philippines	Second On-site Survey		Wednesday, September 18th to Friday September 20th, 2023
	1	Name	Mr. Angel Averia
		Organization	Philippine Computer Emergency Response Team (PH-CERT)
		Job title	Chairman
		Notes	
	2	Name	Mr. Samuel Ramon V. Jacoba
		Organization	Philippine Computer Emergency Response Team (PH-CERT), National Association of Data Privacy Officer of Philippine (NADPOP)
		Job title	Vice President of PH-CERT/ President of NADPOP
		Notes	

Table 11：Philippines - "Selected Organization" Information

Country	Philippines
Organization	Philippine Computer Emergency Response Team (PH-CERT)
Website	https://www.facebook.com/PHCERT/
Status	NGO
Year of Establishment	2001

Purpose & Background	Vision: Transform the philippines into a Global Center of Excellence for Data Privacy and Cybersecurity. Mission: Inspire, Empower & Prosper Data Protection Officers and Cybersecurity
	Professionals, then nurture and develop them within a Vibrant Community of Practice.
Chairman	Mr. Angel Averia
Number of members	
Government Relations	Once Recognized as the National CERT • VIA the CICT – 2004 ASEAN TELMIN Conference
Structure	Chairman, Vice Chairman

- "Invitees"：Mr. Angel Averia
- Intention to hold "local event"：Yes

See Appendix below for the results of the "Cyber Security Survey" responses from the "selected organizations".
Appendix4: JICA Cyber Security Questionnaire

(1) Results of On-site Survey
There are several cybersecurity communities in the Philippines, with PH-CERT being the oldest, founded in 2001. Holy Angel University started the first cybersecurity program in the Philippines and has undergraduate and graduate schools. It is the largest university in the province of Pampanga. The ASEAN Institute for Management (AIM) also has a cybersecurity program, but it covers only non-technical subjects.

5-7. Singapore

Singapore, with a population of approximately 5.97 million and a remarkable real GDP per capita of $106,000, stands out as a leader in the ASEAN region. With a stellar Global Cybersecurity Index (GCI) rank of 4 and a top spot in the Asia Pacific region, Singapore continues to prioritize cybersecurity. Recent developments include initiatives like Cyber Professional Accreditation, fostering a skilled workforce, and promoting Research and Innovation to stay ahead in the cybersecurity domain. Additionally, public consultation on the proposed Cybersecurity (Amendment) Bill highlights the nation's commitment to continuously enhancing its cyber defenses. Despite its advanced cybersecurity infrastructure, Singapore is not immune to threats, facing challenges such as DDoS attacks, phishing, ransomware, and an uptick in scam campaigns

like the "Unseen Enemy." However, the country benefits from a robust network of cybersecurity communities and associations, including local chapters of international groups and sectoral associations. Notably, the Singapore Cyber Security Inter Association (SCSIA), formed by the Association of Information Security Professionals (AISP), exemplifies collaborative efforts among like-minded organizations to strengthen the nation's cybersecurity resilience.

Country Profile

Population	5,975,383 (2023 est.)
Real GDP per Capita (USD)	106,000 (2021 est.)
Member ASEAN	1967

ICT and Cybersecurity profile

Telephones user- fixed lines	1,906,200 (2022 est.)
Telephones user - mobile cellular	9,350,700 (2022 est.)
Telecommunication Operator (included VNO)	15
Internet users	53,690,000 (2021 est.)
Broadband - fixed subscriptions	1,509,700 (2020 est.)
GCI Index Overall score	98,52
GCI Index Regional Rank (Asia Pacific)	1
GCI Index Global Rank	4

Cybersecurity Community in Singapore

Association of Information Security Professionals (AiSP): https://aisp.sg/

See Appendix below for detailed information on ICT and cybersecurity private sector organizations and cybersecurity indicators from the desktop survey.

Appendix1: Survey ICT Organization

Appendix2: Survey Cybersecurity Private Organization

Appendix3: Desktop Survey on Cybersecurity

Table 12 : Singapore - On-site Survey Schedule and List of Interviewees

Singapore	First On-site Survey	Thursday, August 17th, 2023
1	Name	Mr. Tony Low
	Organization	Association of Information Security Professionals (AiSP)
	Job title	Vice Chairman

	Notes	
2	Name	Mr. Parvitar Singh
	Organization	Singapore's tech industry (SGTech)
	Job title	Cyber Export Program Assistant Manager
	Notes	
3	Name	Mr. Jezerie Lan
	Organization	Singapore's tech industry (SGTech)
	Job title	Senior Manager, Strategic Programs
	Notes	
Singapore	Second On-site Survey	Tuesday, October 17th to Friday October 20th, 2023
1	Name	Mr. Johny Kho
	Organization	Association of Information Security Professionals (AiSP)
	Job title	Chairman
	Notes	

Table 13 : Singapore - "Selected Organization" Information

Country	Singapore
Organization	Association of Information Security Professional (AiSP)
Website	https://www.aisp.sg
Status	NGO
Year of Establishment	2008
Purpose & Background	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.
Chairman	Mr. Johnny Kho
Number of members	2200
Government Relations	CSA

Structure	Chairman, Vice Chairman, Advisory Council, Executive Committee, Secretariat,Executive committee: 42

- "Invitees"：Mr. Johnny Kho
- Intention to hold "local event"：No

See Appendix below for the results of the "Cyber Security Survey" responses from the "selected organizations".
Appendix4: JICA Cyber Security Questionnaire

(1) Results of On-site Survey

AiSP, Singapore's cybersecurity association, with the support of the government's Cyber Security Agency of Singapore (CSA), signed an MOU with ICT vendor associations from eight ASEAN countries to form the Southeast Asia Cybersecurity Consortium (SEACC) in November 2022. The SEACC, formed at the initiative of AiSP, was confirmed to be business-oriented, calling for cybersecurity business collaboration among ICT vendors not only in ASEAN but also in other Asian countries.

The GovWare Conference & Exhibition 2023, which was attended in the second business travel survey, was not originally an event dedicated to cybersecurity, yet more than 90% of the exhibitors were cybersecurity-related companies, confirming the high level of awareness in this field. This trend can be seen year after year, and the event has now become "the event for cybersecurity".

(2) Cooperation with Japanese companies and organizations

In September 2017, AiSP and JNSA, a Japanese private association, signed an MOU, and since then, JNSA members have been visiting AiSP on occasions such as exhibiting in Singapore, but after the Covid-19 outbreak, there has been no back and forth and they have become estranged.
On a stand-alone basis, a few Japanese companies have already been engaged in activities to expand their business in Singapore, but no successful cases of Japanese companies specializing in cybersecurity was confirmed.

(3) Other Reference Information

This year, the International Cooperation Subcommittee was established within JNSA, and the exchange of information related to "this forum" was resumed.

History of GovernmentWare

- Today GovWare is one of Asia's leading conferences on cybersecurity and is part of Singapore International Cyber Week. It typically focuses on the latest trends, best practices, and innovations in the cybersecurity field.

- GovWare began in the 1990s as part of Singapore International Cyber Week (SICW). Over the years, the conference has grown in size and importance to become one of Asia's premier cybersecurity conferences; in 2022, over 10,000 policy makers, cybersecurity industry leaders, business owners, and practitioners from 65 countries attended the event.

5-8. Thailand

Thailand, with a population exceeding 69 million and a real GDP per capita of $17,100, holds a significant position within the ASEAN community. While boasting a respectable Global Cybersecurity Index (GCI) rank of 44 and a regional rank of 9 in the Asia Pacific, the nation is actively addressing key cybersecurity concerns. Current updates highlight a focus on enhancing cyber resilience and establishing cyber dominance in the digital landscape. However, Thailand faces persistent cyber threats, with ransomware, phishing, and data leaks dominating the cybersecurity landscape. Despite these challenges, Thailand benefits from the active engagement of various communities and associations in cybersecurity activities. Notable entities such as TISA, ISACA Bangkok chapter, and isc2 Bangkok chapter play crucial roles in fostering collaboration, sharing knowledge, and advancing cybersecurity initiatives within the country. These efforts reflect Thailand's commitment to fortifying its cybersecurity posture in an increasingly digital-centric world.

Country Profile

Population	69,794,997 (2023 est.)
Real GDP per Capita (USD)	17,100 (2021 est.)
Member ASEAN	1967

ICT and Cybersecurity profile

Telephones user- fixed lines	43,680,000 (2022 est.)
Telephones user - mobile cellular	1,264,140,000 (2022 est.)
Telecommunication Operator (included VNO)	16
Internet users	61.2 million (2021 est.)
Broadband - fixed subscriptions	11,478,265 (2020 est.)
GCI Index Overall score	86,50

GCI Index Regional Rank (Asia Pacific)	9
GCI Index Global Rank	44

Cybersecurity Community in Thailand

Thailand Information Security Association (TISA): https://www.tisa.or.th/

See Appendix below for detailed information on ICT and cybersecurity private sector organizations and cybersecurity indicators from the desktop survey.

Appendix1: Survey ICT Organization

Appendix2: Survey Cybersecurity Private Organization

Appendix3: Desktop Survey on Cybersecurity

Table 14：Thailand - On-site Survey Schedule and List of Interviewees

Thailand	First On-site Survey	Tuesday, May 16th to Friday May 19th, 2023
1	Name	Mr. Boonchauay Sanguanvorapong
	Organization	Association of Thai ICT Industry (ATCI)
	Job title	Board member of ATCI
	Notes	Member of ASOCIO, Director, Magic Software Corp., Ltd.
2	Name	Dr. Prinya Hom-anek
	Organization	Thailand Information Security Association（TISA）
	Job title	Founder, Special Advisor and Advisor to TISA (Acting Chairman)
	Notes	
3	Name	AVM Amorn Chomchoey
	Organization	National Cyber Security Agency（NCSA）
	Job title	Secretary General
	Notes	
Thailand	Second On-site Survey	(1) Friday, July 14th to Saturday, July 15th, 2023
1	Name	Dr. Prinya Hom-anek
	Organization	Thailand Information Security Association（TISA）

	Job title	Founder, Special Advisor and Advisor to TISA (Acting Chairman)
	Notes	
2	Name	Mr. Bunrak Saraggananda
	Organization	Association of Thai ICT Industry (ATCI)
	Job title	Honorary President of ATCI and ASOCIO
	Notes	*With 15 members from ATCI member companies
3	Name	Dr. Komain Pibulyarojana
	Organization	T-NET Co., Ltd.
	Job title	Information Security Specialist, Founder and Managing Director
	Notes	
4	Name	Ms. Jinda Boonlarptaveechoke
	Organization	Summit Computer
	Job title	Chairman
	Notes	Member of ATCI
Thailand	Second On-site Survey	(2) September 20th to Friday, September 23rd, 2023
1	Name	Mr. Yanaphon Youngyuen
	Organization	Thailand Information Security Association（TISA）
	Job title	Chairman
	Notes	
2	Name	Mr. Yos Kimsawatde
	Organization	The Thai Bankers' Association
	Job title	Chairman
	Notes	

Table 15：Thailand - "Selected Organization" Information

Country	Thailand
Organization	Thailand Information Security Association (TISA)
Website	www.tisa.or.th
Status	NGO
Year of Establishment	2007

Purpose & Background	Vision: Thailand Information Security Society is Trusted Globally Mission: Develop information security processes and personnel to meet internationally accepted standards.
Chairman	Police Colonel Yanaphon Yongyuen, President
Number of members	
Government Relations	NCSA
Structure	President, 3 Vice Presidents, Committees, Honorary Advisors, Executive committee: 14

- "Invitees"：Dr. Prinya Hom-anek
- Intention to hold "local event"：z

See Appendix below for the results of the "Cyber Security Survey" responses from the "selected organizations".

Appendix4: JICA Cyber Security Questionnaire

(1) Results of On-site Survey

Interviews during the visit confirmed that TISA is the only cyber security related organization in Thailand. TISA is an association of information security professionals, researchers, organizations, and related industries that contributes to the promotion of the information security field through information security-related events, seminars, workshops, and research projects, and has links with the national and international information security communities. Thailand has cyber resilience, ransomware, phishing, and data breach challenges.

5-9. Vietnam

Vietnam, with a population exceeding 104 million and a real GDP per capita of $10,600, holds a significant position within the ASEAN community. Despite its growing economy, the nation faces pressing cybersecurity challenges. While Vietnam boasts a commendable Global Cybersecurity Index (GCI) rank of 25 and a regional rank of 7 in the Asia Pacific, it grapples with dominant cyber threats, particularly ransomware and phishing attacks. Recent updates indicate the implementation of data privacy protection policies to address these concerns. Notably, while there are several cybersecurity entities in Vietnam, VNISA emerges as the most active among them. However, the country remains vulnerable, with reports indicating its presence among the top 10 countries suffering from cyber-attacks and dangerous malware infections. Furthermore, Vietnam ranks second among countries most infected with crypto-mining malware. As Vietnam continues

to navigate these challenges, collaborative efforts among government agencies, cybersecurity organizations, and the private sector are crucial in fortifying the nation's cyber resilience and safeguarding its digital infrastructure.

Country Profile

Population	104,799,174 (2023 est.)
Real GDP per Capita (USD)	10,600 (2021 est.)
Member ASEAN	1995

ICT and Cybersecurity profile

Telephones user- fixed lines	2,390,671 (2022 est.)
Telephones user - mobile cellular	1,400,000 (2021 est.)
Telecommunication Operator (included VNO)	5
Internet users	71,780,000 (2021 est.)
Broadband - fixed subscriptions	16,699,249 (2020 est.)
GCI Index Overall score	94,59
GCI Index Regional Rank (Asia Pacific)	7
GCI Index Global Rank	25

Cybersecurity Community in Vietnam

VNISA : vnisa.org.vn

See Appendix below for detailed information on ICT and cybersecurity private sector organizations and cybersecurity indicators from the desktop survey.

Appendix1: Survey ICT Organization

Appendix2: Survey Cybersecurity Private Organization

Appendix3: Desktop Survey on Cybersecurity

Table 16 : Vietnam - On-site Survey Schedule and List of Interviewees

Vietnam	First On-site Survey	Tuesday May 22nd to Thursday, May 26th, 2023
1	Name	Ms. Giang Nguyen
	Organization	Vietnam Software And IT Services Association （VINASA）
	Job title	Chief of the secretariat
	Notes	Member of ASOCIO
2	Name	Mr. Nguyễn Thành Hưng

	Organization	Vietnam Information Security Association（VNISA）
	Job title	Chairman
	Notes	Former Deputy Minister of Information and Communications
3	Name	Mr. Khổng Huy Hùng
	Organization	Vietnam Information Security Association（VNISA）
	Job title	Vice Chairman
	Notes	
4	Name	Ms. Trần Kim Phượng
	Organization	Vietnam Information Security Association（VNISA）
	Job title	
	Notes	
5	Name	Mr. Nguyễn Ngọc Toàn
	Organization	Vietnam Information Security Association（VNISA）
	Job title	Coordinator
	Notes	JICA member
6	Name	Dr. Phan Tam
	Organization	Ministry of Information and Communication （MIC）
	Job title	Deputy Minister
	Notes	
7	Name	Mr. Nguyen Duc Toan
	Organization	Official Multilateral Cooperation Department of International Cooperation, Ministry of Information and Communication （MIC）
	Job title	
	Notes	
Vietnam	Second On-site Survey	Sunday, July 30th to Tuesday August 8th, 2023
1	Name	Mr. Nguyễn Thành Hưng
	Organization	Vietnam Information Security Association（VNISA）
	Job title	Chairman
	Notes	Former Deputy Minister of Information and Communications

2	Name	Mr. Khổng Huy Hùng
	Organization	Vietnam Information Security Association（VNISA）
	Job title	Vice Chairman
	Notes	
3	Name	Mr. Nguyen Van Khoa
	Organization	FPT Software
	Job title	CEO
	Notes	Chairman of VINASA

Table 17：Vietnam - "Selected Organization" Information

Country	Vietnam
Organization	Vietnam Information Security Association (VNISA)
Website	vnisa.org.vn
Status	NGO
Year of Establishment	2007
Purpose & Background	VNISA has the task: Cooperate with Government Agencies: Authority of InfoSec/MIC, VNCERT/MIC, VGISC. Promote Infosec education/training (Organize the information security competitions.) Organize events, conferences, seminar of special subjects Survey on National/Industry information security status Lead up to the meetings among the organizations, businesses, help and cooperate to develop application of information security Promote International Cooperation Develop standards/guidelines.
Chairman	Mr. Nguyen Thanh Hung - Deputy Minister of Information and Communications.
Number of members	More than 160 members
Government Relations	MIC
Structure	Chairman, Vice Chairman, Secretariat, Executive committee: 27

- "Invitees"：Mr. Nguyen Thanh Hung
- Intention to hold "local event"：Yes

See Appendix below for the results of the "Cyber Security Survey" responses from the "selected organizations".

Appendix4: JICA Cyber Security Questionnaire

(1) Results of On-site Survey

The visiting interviews confirmed that VNISA is the only cybersecurity-related association in Vietnam. With 160 member companies, VNISA is the largest association dedicated to cybersecurity in Vietnam and has established extensive partnerships with cybersecurity companies in the country.

(2) Cooperation with Japanese companies and organizations

JNSA and VNISA had not yet signed an MOU, but they signed a relative MOU during this visit. In addition, collaboration among member companies is progressing, such as the example of VNCS and Terilogy.

(3) Other Reference Information

- The follow-up event was held in conjunction with the NISC ASEAN-Japan Cybersecurity Working Group, which resulted in increased participation by the public and private sectors.
- Mr. Khổng Huy Hùng of VNISA is a member of SEACC (South East Asia Cybersecurity Consortium) established by AiSP.
- "The Forum" was introduced at a meeting with MIC (a Vietnamese government agency) coordinated by the ASOCIO Secretariat and VINASA.
- Originally, Vietnamese ICT firms had a good relationship with Japan's ICT software industry, not only because of the deep exchange with Japan's off-shore development, but also because Vietnamese ICT human resources were invited to Japan. However, in recent years, Vietnam's goal in advanced technology has shifted from Japan to Europe and the United States.

Under such circumstances, it is hoped that the success of "the Forum" will be an opportunity to turn the tide not only in Europe and the U.S. but also in Asia. In addition, the tremendous support from ASOCIO was a great help in facilitating this survey.

See Appendix below for the quick report of the On-site survey.

Appendix5：202305 Thailand quick report
Appendix6：202305 Brunei quick report
Appendix7：202305 Vietnam quick report
Appendix8：202306 Philippines Cambodia Malaysia quick report

Appendix9：202307 Malaysia Thailand quick report

Appendix10：202308 Vietnam Singapore quick report

Appendix11：202310 GovWare2023 quick report

Appendix12：202402 Laos quick report

5-10. Bangladesh

A similar desktop survey was conducted for Bangladesh as for the ASEAN countries mentioned above, but there were no disclosures of note, only a Facebook group claiming to be a private cybersecurity organization.

Country Profile

Population	171,180,000 (2022 est.)
Real GDP per Capita (USD)	2,688 (2022 est.)
Member ASEAN	Non-member

ICT and Cybersecurity profile

Telephones user- fixed lines	274,295 (2022 est.)
Telephones user - mobile cellular	181,021,227 (2021 est.)
Telecommunication Operator (included VNO)	1
Internet users	6,630,000 (2021 est.)
Broadband - fixed subscriptions	10,052,819 (2020 est.)
GCI Index Overall score	81.27
GCI Index Regional Rank (Asia Pacific)	11
GCI Index Global Rank	53

See Appendix below for detailed information on ICT and cybersecurity private sector organizations and cybersecurity indicators from the desktop survey.

Appendix1: Survey ICT Organization

Appendix2: Survey Cybersecurity Private Organization

Appendix3: Desktop Survey on Cybersecurity

5-11. Mongolia

A similar desktop survey was conducted for Mongolia as for the ASEAN countries above, but no online information on Mongolian cybersecurity-related organizations was available.

Country Profile

Population	3,450,000 (2022 est.)
Real GDP per Capita (USD)	5,038 (2022 est.)
Member ASEAN	Non-member

ICT and Cybersecurity profile

Telephones user- fixed lines	475,290 (2022 est.)
Telephones user - mobile cellular	4,687,304 (2021 est.)
Telecommunication Operator (included VNO)	12
Internet users	27,720,000 (2021 est.)
Broadband - fixed subscriptions	307,166 (2020 est.)
GCI Index Overall score	26.2
GCI Index Regional Rank (Asia Pacific)	22
GCI Index Global Rank	120

See Appendix below for detailed information on ICT and cybersecurity private sector organizations and cybersecurity indicators from the desktop survey.

Appendix1: Survey ICT Organization

Appendix2: Survey Cybersecurity Private Organization

Appendix3: Desktop Survey on Cybersecurity

5-12. East Timor

A similar desktop survey was conducted for Mongolia as for the ASEAN countries above, but no online information on East Timor cybersecurity-related organizations was available.

Country Profile

Population	1,340,000 (2022 est.)
Real GDP per Capita (USD)	No information
Member ASEAN	Non-member

ICT and Cybersecurity profile

Telephones user- fixed lines	1,840 (2022 est.)
Telephones user - mobile cellular	1,481,007 (2022 est.)
Telecommunication Operator (included VNO)	1
Internet users	507,000 (2021 est.)

Broadband - fixed subscriptions	75 (2020 est.)
GCI Index Overall score	4.26
GCI Index Regional Rank (Asia Pacific)	34
GCI Index Global Rank	173

See Appendix below for detailed information on ICT and cybersecurity private sector organizations and cybersecurity indicators from the desktop survey.

Appendix1: Survey ICT Organization

Appendix2: Survey Cybersecurity Private Organization

Appendix3: Desktop Survey on Cybersecurity

5-13. ASEAN Summary (based on selected countries)

The survey status for each has been summarized under ASEAN.

（1）Overview of ASEAN (9 target countries)

　　　Total Population:　635,928,691 (2023 est.)

　　　Average Real GDP: USD 28,033.33

Table 18：ASEAN Member Profile

	Brunei	Cambodia	Indonesia	Laos	Malaysia
Population	484,991 (2023 est.)	16,891,245 (2023 est.)	279,476,346 (2023 est.)	7,852,377 (2023 est.)	34,219,975 (2023 est.)
Real GDP per Capita	$60,100 (2021 est.)	$4,400 (2021 est.)	$11,900 (2021 est.)	$7,800 (2021 est.)	$26,300 (2021 est.)
Member ASEAN	07-Jan-84	30-Apr-99	8 August 196	23-Jul-97	8 August 196

		Philippine	Singapore	Thailand	Vietnam
Population		116,434,200 (2023 est.)	5,975,383 (2023 est.)	69,794,997 (2023 est.)	104,799,174 (2023 est.)
Real GDP per Capita		$8,100 (2021 est.)	$106,000 (2021 est.)	$17,100 (2021 est.)	$10,600 (2021 est.)
Member ASEAN		8 August 196	8 August 196	8 August 196	28-Jul-95

(2) ASEAN Cybersecurity landscape

① ASEAN GCI Index

　　　Overall GCI average score: 71.75

　　　Number of Country above GCI average = 6

　　　Number of Country below GCI average = 3

② GCI position of ASEAN and JAPAN
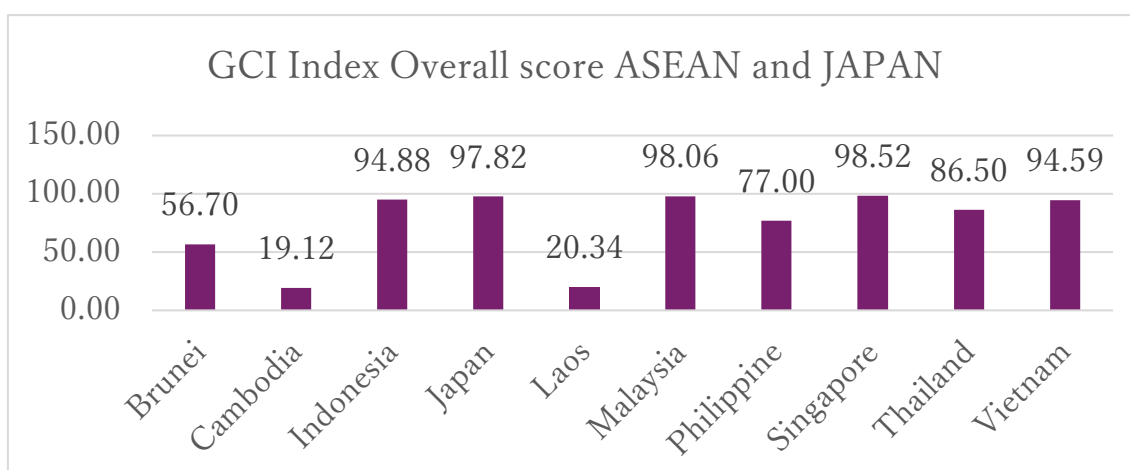
Figure 1 : GCI Index Overall Score ASEAN-JAPAN

Table 19 : ASEAN Member Cybersecurity Profile

	Brunei	Cambodia	Indonesia	Laos	Malaysia
Telephones user- fixed lines	122,204 (2022 est.)	38,284 (2022 est.)	8,423,990 (2022 est.)	1,300,195 (2021 est.)	8,452,900 (2022 est.)
Telephones user - mobile cellular	603,486 (2021 est.)	19,899,790 (2021 est.)	365,872,608 (2021 est.)	4,822,973 (2021 est.)	47,201,700 (2021 est.)
Telecommunication Operator (included VNO)	3	6	7	4	16
Internet users	441,000 (2021 est.)	10.2 million (2021 est.)	167.4 million (2021 est.)	4,588,000 (2021 est.)	32.98 million (2021 est.)
Broadband - fixed subscriptions	71,078 (2020 est.)	233,732 (2020 est.)	11,722,218 (2020 est.)	128,000 (2020 est.)	3,358,800 (2020 est.)
GCI Index Overall score	56,70	19,12	94,88	20,34	98,06
GCI Index Regional Rank (Asia Pacific)	16	26	6	25	2
GCI Index Global Rank	85	132	24	131	5

	Philippine	Singapore	Thailand	Vietnam
Telephones user- fixed lines	4,884,608 (2022 est.)	1,906,200 (2022 est.)	4.368 million (2022 est.)	2,390,671 (2022 est.)
Telephones user - mobile cellular	163,345,244 (2021 est.)	9,350,700 (2022 est.)	126.414 million (2022 es	140 million (2021 est.)
Telecommunication Operator (included VNO)	7	15	16	5
Internet users	58.3 million (2021 est.)	5.369 million (2021 est.)	61.2 million (2021 est.)	71.78 million (2021 est.)
Broadband - fixed subscriptions	7,936,574 (2020 est.)	1,509,700 (2020 est.)	11,478,265 (2020 est.)	16,699,249 (2020 est.)
GCI Index Overall score	77,00	98,52	86,50	94,59
GCI Index Regional Rank (Asia Pacific)	13	1	9	7
GCI Index Global Rank	61	4	44	25
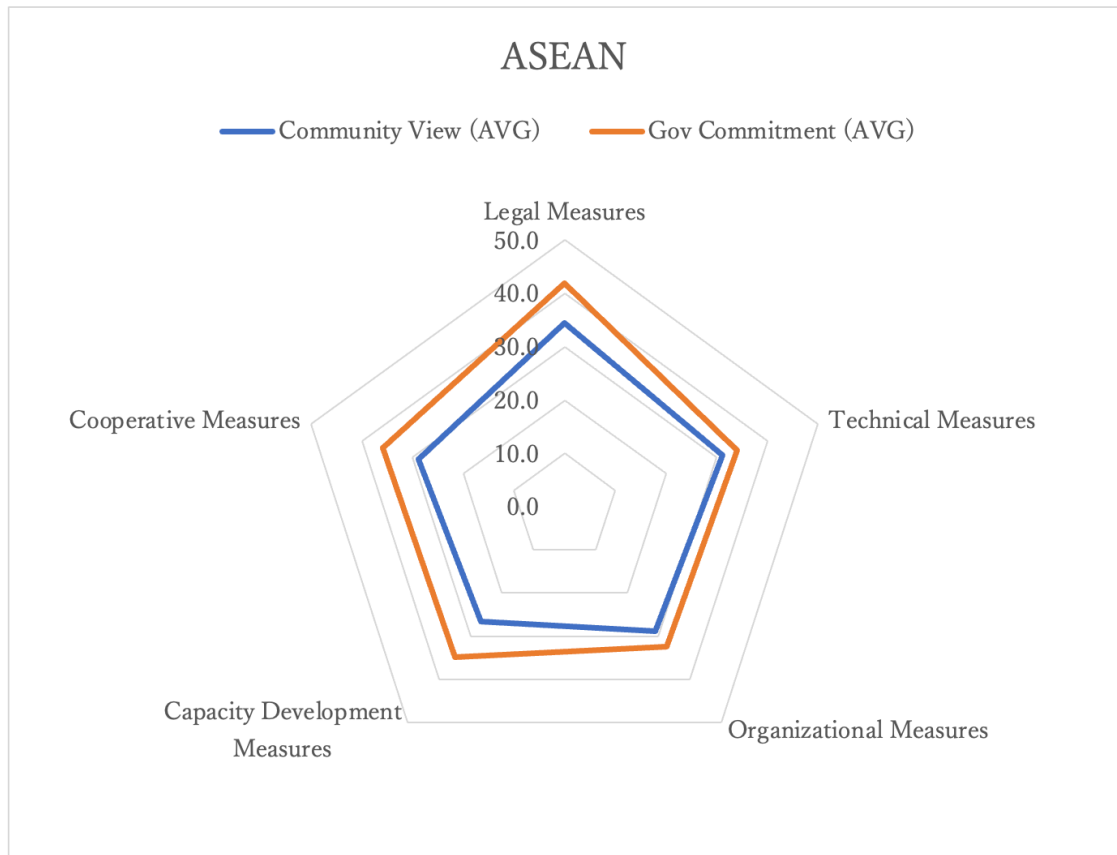
Figure 2：Overview of ASEAN Cybersecurity in GCI Items

ASEAN	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
Gov Commitment (AVG)	41,9	34,0	32,5	34,9	35,9
Community View (AVG)	34,4	31,1	28,9	26,7	28,9

① Development Level: Developing Region

② Areas of Relative Strength:
  - Government Commitment: Legal Measures, Cooperative Measure
  - Community View: Legal Measures, Technical Measures

③ Areas of Potential Growth:
  - Government Commitment: Organizational Measures, Technical Measures
  - Community View: Capacity Development, Organizational Measure, Cooperative Measures

(3) Summary

The ASEAN region, comprising diverse member states, exhibits varying levels of cybersecurity maturity and readiness, as reflected in the Global Cybersecurity Index (GCI) scores. While countries like Singapore and Malaysia demonstrate high GCI scores, indicating robust

cybersecurity infrastructure and measures, others like Laos and Cambodia lag behind despite their efforts. This discrepancy underscores the need for collective action and collaboration within ASEAN to bridge the gap and elevate the region's cybersecurity resilience.

Survey findings highlight areas of potential growth, particularly in organizational and technical measures, indicating opportunities for enhancing cybersecurity capabilities across the region. Conversely, legal measures emerge as a relative strength, suggesting a solid foundation for regulatory frameworks and enforcement mechanisms. However, significant challenges persist, with phishing and ransomware attacks dominating the cybersecurity landscape. Looking ahead, the focus on legal measures presents a key opportunity for ASEAN member states to strengthen cybersecurity governance and address emerging threats effectively, thereby advancing the region's cybersecurity posture and fostering sustainable development.

Reference: https://www.cia.gov/the-world-factbook/

6. Recommended Private Cybersecurity Associations and Organizations in Each Country

6-1. Selected Organizations and their Representatives "Invitees"

In consultation with the STI/DX Office of the Governance and Peacebuilding Department and NISC, the following were selected from the "target organizations" nominated in the survey described in section 5.

Table 20：List of "Selected Organizations" and "Invitees"

Country	Organization/ Title/ Name of Representative
Brunei	Brunei Cyber Security Association (BCSA)
	President, Mr. Mohamad Azad Zaki Haji Mohd Tahir
Cambodia	ISAC Cambodia
	Chairman, Mr. Phannarith Ou
Indonesia	Indonesia Network Security Association (idNSA)
	Founder and Advisor, Dr. Rudi Lumanto
Japan	Japan Network Security Association (JNSA)
	Chairman, Dr. Hiroshi Esaki
Malaysia	Malaysia CyberSecurity Community (rawSEC)
	Co-Founder, Mr. Tahrizi Thareb

Philippines	Philippine Computer Emergency Response Team (PH-CERT) President, Mr. Angel Averia
Singapore	Association of Information Security Professionals (AiSP) President, Mr. Johnny Kho
Thailand	Thailand Information Security Association (TISA) Founder and Special Advisor, Dr. Prinya Hom-anek
Vietnam	Vietnam Information Security Association (VNISA) Chairman, Mr. Nguyen Thanh Hung

6-2. Conditions and Reasons for Selection

The minimum criteria for "selected organizations" among the "target organizations" are as follows:

- They have their own communities or members to serve.
- They have routine activities that they conduct monthly or at least annually.
- They are independent from government intervention.
- They are non-profits and are usually funded by themselves or sponsors.
- They may already have a cooperation agreement or MOU with other international organizations/communities.

(1) BCSA
BCSA was selected because it was the only association dedicated to cybersecurity that existed in Brunei. This was found through meeting with ASOCIO member associations IFB and BCSA and conducting a survey of specialized associations on cybersecurity in Brunei.

(2) ISAC Cambodia
Interview with Mr. Phannarith Ou and Mr. Ann Kim of the Ministry of Post and Telecommunications (MPTC) confirmed that Cambodia has no association dedicated to cybersecurity. The relevance of an organization called Innovations for Social Accountability in Cambodia (ISAC Cambodia), which is not yet legally registered, was discussed and it was decided to recommend it as a target organization since Mr. Ou is its representative.

(3) idNSA
idNSA is the largest professional cybersecurity association in Indonesia. It is actively involved in network security and information security throughout Indonesia.

idNSA has a wide range of partnerships with private cybersecurity companies in Indonesia, and as an industry association of private cybersecurity companies, it has a track record of holding events and seminars, both in Indonesia and abroad. It also has a track record of planning and executing collaborative events with Japan, such as "Code Bali."

(4) rawSEC

It is a White Hat Hacker community recommended by Dato' Dr. Amirudin Abdul Wahab, the CEO of CyberSecurity Malaysia (CSM), and has received the Cybersecurity Award in the ASEAN region.

(5) PH-CERT

PH-CERT was selected because it is the only association in the Philippines with a registered private cybersecurity workforce and no other similar organization exists. It has extensive ties with the private cybersecurity sector in the country.

(6) AiSP

In terms of collaboration among ASEAN countries, which is the objective of this conference, the South East Asia Cybersecurity Consortium (SEACC) was formed in November 2022 under the auspices of the Cyber Security Agency of Singapore (CSA) (a Singaporean government agency) by concluding an MOU among ICT vendor associations from eight ASEAN countries. The alliance formed by the eight ASEAN countries and Japan's cybersecurity associations and organizations at "the Forum" aims to "raise the level of mutual assistance through self-help, mutual aid, and public assistance through public-private partnerships." In contrast, SEACC, which was formed under the leadership of AiSP, is more business-oriented and calls for cybersecurity business collaboration among ICT vendors in Asian countries as well as ASEAN. The differences were mutually confirmed and AiSP's participation in "the Forum" was decided.

(7) TISA

TISA is an association of information security professionals, researchers, organizations, and related industries. In addition, TISA contributes to the promotion of the information security field through information security-related events, seminars, workshops, and research projects, and has ties with the information security community in Thailand and internationally. It has experience in planning and organizing events such as the Cyber Defense Initiative Conference (CDIC), the largest cyber security-related event in Thailand.

(8) VNISA

With 160 member companies, VNISA is the largest professional cybersecurity association in Vietnam. VNISA is an organization that can collaborate with a wide range of domestic private cybersecurity companies and has experience in planning and organizing events, such as the international conference Vietnam Cyber Security Day 2022. It is also a member of SEACC, which was established by AiSP and has signed an MOU with the SEACC.

7. Results of Various Dissemination Activities

7-1. ASEAN Outreach at "the Policy Meeting"

(1) Summary of Activities

Explained "the Forum" at the Industry-Government-Academia Collaboration slot on the last day of "the Policy Meeting".

① June 2023 in Brunei: At the Industry-Government-Academia collaboration slot

Table 21：DAY 1 May 23rd (2023) (excerpt of industry-government-academia collaboration part)

Time	Items	Speaker
13:30 - 14:30	Discussion of CA3: Joint Government- Industry-Academia - J-GIA Overview - Collaboration amongst Industry Associations - Promoting Private-Sector Cybersecurity Cooperation in the ASEAN and the Indo-Pacific region	Japan (lead) Japan (NISC) Indonesia (idNSA) Japan (JICA)
14:30 - 15:30	Discussion of CA4: 50th Year Commemorative Activity - Proposal for the 50th year commemorative activities - Discussion	Japan (lead) Japan (NISC) All participants

② August 2023 in Vietnam: At the Industry-Government-Academia collaboration slot

Table 22：DAY2 Aug 4th (2023) (Excerpt from the industry-government-academia collaboration part)

Time	Items	Speaker
9:30 - 10:00	Reception	Vietnam
10:00 - 11:00	CA8_Joint Government- Industry-Academia - J-GIA overview - Public-Private collaboration in Japan (JNSA and International Relations) - Draft report for 2023 Policy Meeting	Japan (lead) Japan (NISC) Japan (JNSA)
11:00 - 12:00	CA9_50th Commemorative Event - Finalization of distinguished contributors - Draft report for 2023 Policy Meeting	Japan (lead) Japan (NISC)
12:00 - 12:10	Closing Remarks Mr. Junichi Sasaki, NISC Counsellor	Japan

③　October 2023 in Tokyo: At the Industry-Government-Academia collaboration slot

Table 23：DAY 2 Oct 4th (2023) (Excerpt from the industry-government-academia collaboration part)

Session 3: Report of Collaborative Activities in 2023		
09:30 - 10:20 (50min)	[3-5] Report from Joint Awareness Raising - Introduction of video contest entries - Ceremony of Award Winners - Next year's plan	- Brunei Darussalam
10:20 - 10:40 (30min)	[3-6] Report from Voluntary Mutual Notification Program - Report on the results of this year's efforts and future plan	- Japan
Short Break (20min)		
11:00 - 11:30 (30min)	[3-7] Report from Joint Government-Industry-Academia - Report on the results of this year's efforts and future plans	- Japan
11:30 - 12:00 (30min)	[3-8] Report from 50th Commemorative Event - Results of the selection of Award for Merit Recipients - Introduction of IC-AJCC	- Japan
Lunch Break (90min.)		

④ February 2024 in Bangkok, Thailand: At the Industry-Government-Academia collaboration slot

Table 24：DAY2 Feb 7th (2023) (Excerpt from the industry-government-academia collaboration part)

Time	Items	Lead Country / Speaker
09:00 - 09:30	Reception	Thailand
09:30 - 11:30	[9] Joint Government-Industry-Academia - Future Government-Industry-Academia Collaboration Initiatives - Overview of the AJCCA Joint Workshop - Discussion	AJCCA(Lead)

11:30 - 11:40	Closing Remarks
	- Deputy Secretary General of the National Cyber
	  Security Agency of Thailand
	  Major General Teerawut Wittakorn
	- Counsellor, NISC
	  Mr. SASAKI Junichi
		Thailand/Japan

(2) Results of Activities

The Forum was recognized by all governmental participants at the ASEAN-Japan Cyber Security WG Meeting in May and August 2023 and the Policy Meeting in October 2023 through explanations of the Forum and promotion of the progress of its preparation. In addition, at the ASEAN-Japan Cyber Security WG Meeting held in Thailand in February 2024, a workshop on joint promotion of "Public-Private Partnership" was held under the leadership of AJCCA, which was formed at the Forum.

7-2. Webinar for the AJCCBC

(1) Event Outline

Event Name: Webinar AJCCBC Conference 2023

Host: JICA

Date and Time: August 17, 2023, 14:30–16:00

Number of Participants: 68

Method: Zoom Webinar

Participating Countries: Brunei, Cambodia, India, Indonesia, Japan, Laos, Malaysia, Philippines and Thailand.

(2) Program and Abstracts

① 14:30–14:40 (10 min)

Theme: AJCCBC activities

The presentation explained the activities of the AJCCBC and shared the significance and progress of international cooperation in the field of cybersecurity.

Speaker: Mr. Masayuki Furukawa (Senior Deputy Director, Office for STI & DX, Governance and Peacebuilding Department of JICA – Japan International Cooperation Agency)

② 14:40–15:00 (20 min)

Theme: Perspectives on Cybersecurity through International Cooperation

The presentation focused on the importance of cooperation between companies and international organizations in terms of cybersecurity. The speaker discussed specific challenges and possibilities through actual case studies.

Speaker: Mr. Keisuke Kamata (Executive Director and CTO of Financials ISAC Japan/ Executive Director and CTO of Armoris Inc)

③ 15:00–15:30 (30 min)

Theme: Use of the SECBOK in Cybersecurity Workforce Development

The presentation explained the usefulness of the Security Body of Knowledge (SECBOK) and provided suggestions on how it can be used in human resource development.

Speaker: Mr. Toshihiro Hirayama (Professor and Vice Dean of i University/ Director of Education Committee, JNSA)

④ Theme: International Conference on ASEAN-JAPAN Cybersecurity Community (IC-AJCC)

The presentation provided a detailed overview of the importance and progress of the international conference focusing on cybersecurity cooperation with ASEAN countries.

Speaker: Dr. Rudi Lumanto (Founder and Advisor, Indonesia Network Security Association – idNSA)

Closing Remarks

(3) Management on the day of the event

A progression chart was created to manage the entire webinar on the day of the event. In addition, feedback was actively collected from the participants for future improvements.

(4) Production materials

The materials needed to hold the webinar (invitation, registration form, web flyer, questionnaire, etc.) were prepared and a Zoom link for the webinar was created using the "Zoom" online conferencing system. As the webinar was held online, all materials were produced electronically.

① Webinar invitation（Distributed via Zoom）

Figure 3：Webinar invitation（Distributed via Zoom）

② Registration form (via Zoom）

Table 25：Registration form (via Zoom）

	Registration Form Item List
1	First Name
2	Last Name
3	E-mail address
4	Institution
5	Position

③ Web flyer (for PC)

Figure 4：Web flyer (for PC)

Web flyer (for mobile)

Figure 5：Web flyer (for mobile)

④ Web flyer program (for PC)

Figure 6 : Web flyer program (for PC)

Web flyer program (for mobile)

Figure 7 : Web flyer program (for mobile)

⑤　Follow-up email after participation

Figure 8：Follow-Up Email

⑥　Questionnaire (via Zoom)

Table 26：Questionnaire Item List

	Questionnaire Item List
1	Please tell us how satisfied you were with today's seminar.
2	If you have any comments for the lecturers or on the content of the seminar that was particularly helpful, please give them below.
3	Would you like to participate in future webinars like this one?
4	Do you wish to participate in the IC-AJCC (International Conference on ASEAN-Japan Cyber Security Community) to be held in Tokyo in October?
5	Others (questions or concerns)

(5) Questionnaire report

①　Purpose of the questionnaire

The purpose of this webinar was to promote cooperation and knowledge sharing in the field of cybersecurity and to provide useful information to participants. The questionnaire was intended to capture participants' impressions and feedback, which will contribute to improving the quality of future events and webinars.

② Questionnaire content

The questionnaire was structured to focus on the following items.

- Satisfaction with and understanding of the webinar

- Evaluation and feedback on the content of the webinar

- Intention to participate in the International Conference on ASEAN-JAPAN Cybersecurity Community (IC-AJCC)

③ Questionnaire results

Number of responds: 18
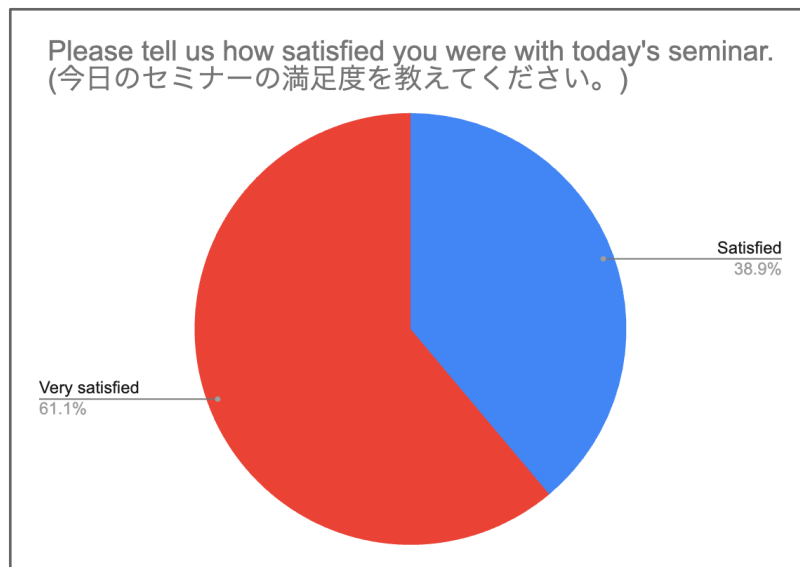
Figure 9：Questionnaire results 1
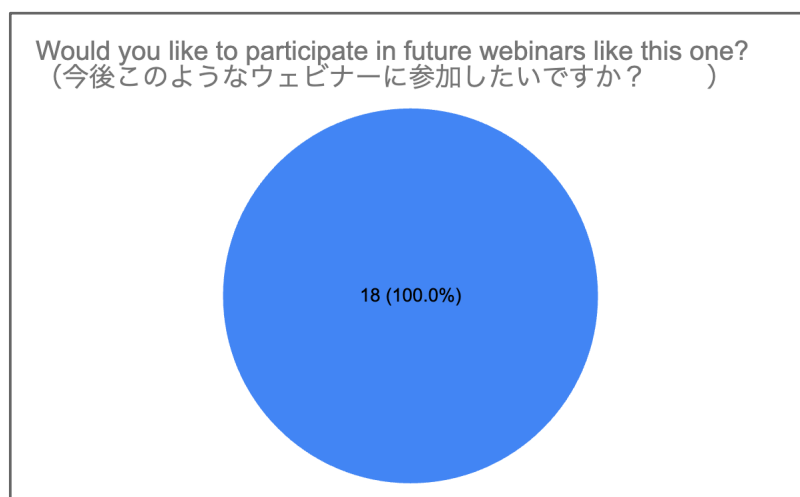
Figure 10：Questionnaire results 2
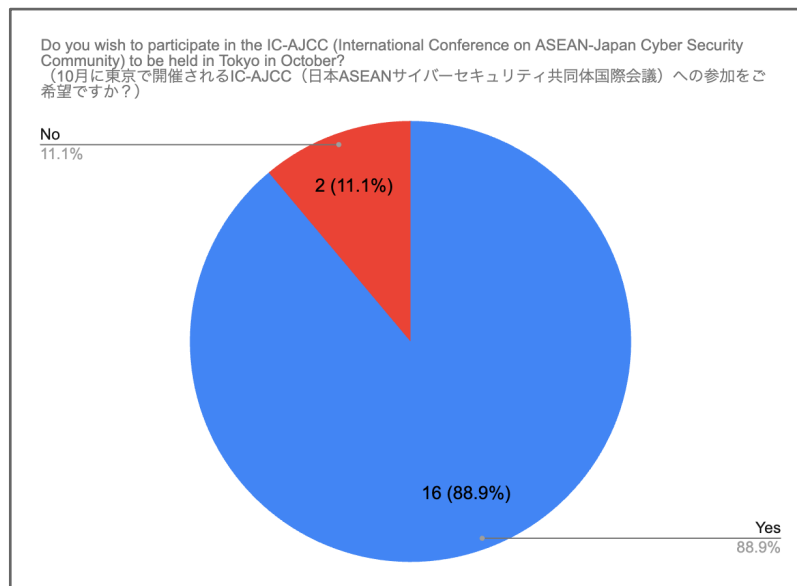
Figure 11：Questionnaire results 3

If you have any comments for the lecturers or on the content of the seminar that was particularly helpful, please give them below.

・All good.

・Nothing in particular. The webinar was detailed.

・The content was very insightful, and I appreciated it very much. However, it was more or less framework-related content, which was a bit different from what I anticipated.

・Please share the presentation materials with participants.

・It would be good if the lecturer could show their presentation in larger fonts for us to see.

・Very Good.

Others (questions or concerns)

・Is there any training in the field of cybersecurity that I can undertake in Japan?

I work as the deputy head of the department for the Institute of Information and Communications Technology. I found that this course is very important for my institute and society.

・Thank you, it was nice. Especially the timing of the webinar.

④　Overview of questionnaire results

The results of the questionnaire showed that many participants highly rated the webinar, and many commented that the knowledge sharing on cybersecurity was particularly beneficial. There was also increased interest in the October event, the International Conference on

ASEAN-JAPAN Cybersecurity Community. The webinar via Zoom was also well received, with a 100% willingness to participate, and it is hoped that this format will continue in the future.

⑤　Impression

The results of this survey can be used to plan and conduct webinars and events that will further satisfy participants.

7-3. Follow-Up Events with Promotion in "Selected Organizations" in Each Country

Follow-up events were held to disseminate JICA projects and the International Conference on ASEAN-JAPAN Cybersecurity Community (IC-AJCC).

(1) Onsite follow-up event work details

In collaboration with local special mercenaries, reconsignment partners were selected from Indonesia, Thailand, the Philippines, and Vietnam. Subcontractors for the follow-up events were selected in consultation with the STI/DX Office of the Governance and Peacebuilding Department. The reconsignment partners are as follows:

① Indonesia Network Security Association (idNSA)
② Vietnam Information Security Association (VNISA)
③ The National Association of Data Protection Officers of the Philippines (NADPOP)
④ Thailand Information Security Association (TISA)

(2) Event summary

① Indonesia Network Security Association (idNSA)

Reconsignment contract amount: IDR 300,000,000.00

Event Name: Cyber Jawara International 2023

Date and Time: July 18, 2023, 9:00–17:00

Venue: Aston Priority Simatupang Hotel and Conference Center

Number of Participants: 128

Main Content:

- International hacking contest

- Keynote speeches by experts

- Workshops on security assessment

- Panel discussions with experts and industry leaders

- Networking and exchange

- Publicity for JICA Cyber Security Project and the International Conference on ASEAN-JAPAN Cybersecurity Community (IC-AJCC)

At this event, panel discussions with experts, practical knowledge sharing, and seminars and workshops aimed at enhancing cybersecurity awareness and defense were conducted. The theme of fostering mutual growth through collaboration within the ASEAN cybersecurity community was highlighted.

During the seminars, renowned cybersecurity experts and key institutions were invited as speakers to share specialized knowledge and insights on new threats, current trends, and effective defense strategies. Participants were provided with knowledge and skills to mitigate risks, protect confidential information, and adopt proactive cybersecurity approaches. Additionally, promotion and explanation of the "International Conference on ASEAN-JAPAN Cybersecurity Community (IC-AJCC)," scheduled for October 5 and 6 and organized by NISC, were carried out.

Workshops included practical training on Cyber Jawara CTF problem solving, WhatsApp forensics, and security assessment using the new version of the INDONESE Framework. The speakers were as follows:
1. Cyber Jawara International Problems Exploration by Mr. Usman Abdul Halim
(CJI Committee)
2. WhatsApp forensics by Mr. Hamdan Abdul Aziz (idNSA)
3. Security Assessment using the new INDONESE Framework by Mr. Aiman Al Fatih
(Pesantren Siber)

During the panel discussions, experts and industry leaders discussed the challenges that organizations are facing in implementing, managing, and maintaining robust cybersecurity programs. The panelists were as follows:
1. Mr. Angel Averia (Chairman, Philippine CERT)
2. Mr. Ahmad Rully (Security Researcher, Waseda University)
3. Mr. Faisal Yahya (Country Manager, Vantage Point Security)
4. Dr. Bisyron Wahyudi (Vice Chairman, CSIRT.ID)
5. Dr. Muhammad Salman (Chairman, idCare, University of Indonesia)
6. Mr. Muhammad Solahuddien (Vice Chairman, CSIRT.ID)

Feedback from participants was highly positive, with 94% stating that the seminar exceeded their expectations. The quality of the speakers, relevance of topics, and interactivity of the sessions

were highly praised. Many participants expressed that they had gained valuable insights and practical knowledge.

This seminar had a significant impact on the cybersecurity community, resulting in knowledge-sharing and increased awareness. Several participants indicated their intention to implement cybersecurity best practices within their organizations and some shared plans to pursue further research in cybersecurity.

② Vietnam Information Security Association (VNISA)
Reconsignment contract amount: VND 380.226.000
Event Name: Enhance Cooperation and Information Sharing for Information Security and Cybersecurity for Organizations, Government and Enterprises
Date and Time: August 4, 2023, 13:30–16:30
Venue: Pan Pacific Hanoi
Number of Participants: 70
Main Content:
- Keynote speeches by experts
- Workshops
- Panel discussion
- Networking session
- Publicity for JICA Cyber Security Project and the International Conference on ASEAN-JAPAN Cybersecurity Community (IC-AJCC)

This event was held under the theme "Enhancing Cooperation and Information Sharing for Information Security and Cybersecurity for Organizations, Governments, and Enterprises," aiming to strengthen skill development and cooperation in the information security field between Vietnam and Japan. It sought to enhance information sharing and collaboration among national agencies, organizations, and businesses in this field. Targeting both countries as well as national regulatory authorities, experts, and companies in ASEAN, paying particular attention to Vietnam's characteristic of having a majority of small and medium-sized enterprises, the event shared possibilities for technical issues, policies, and cooperation in the digital transformation process among sectors.

The objectives focused on survey results regarding promoting information security cooperation in the private sector in ASEAN and the Indo-Pacific region, information security challenges for private organizations and companies during digital transformation, and policies and resources to

support information security orientation for small and medium-sized enterprises. Additionally, an explanation of the "International Conference on ASEAN-JAPAN Cybersecurity Community (IC-AJCC)," scheduled for October 5 and 6, organized by NISC, was provided.

The event featured speeches from Vietnamese government agencies, companies, and information security enterprises. The speakers were as follows:

1. Mr. Khong Huy Hung (Vice Chairman, VNISA)

2. Mr. Nguyen Xuan Hoang (Vice Chairman, MISA)

3. Mr. Pham Van Duc (General Director, SAVIS)

4. Mr. Nguyen Minh Duc (CEO, CycRadar)

5. Mr. Le Hoang Duong (Director of Network Security Center, FPT)

This event had a significant impact on the cybersecurity community, information security agencies, organizations, and businesses in Vietnam, leading to knowledge-sharing and increased awareness.

③　The National Association of Data Protection Officers of the Philippines (NADPOP)

Reconsignment contract amount: USD 14,016

Event Name: CyberSecConPH (The Philippine Leg of the International Conference on ASEAN-JAPAN Cybersecurity Community (IC-AJCC))

Date and Time: September 19, 2023, 13:00–16:00

Venue: Crowne Plaza Manila Galleria

Number of Participants: 110

Main Content:

- Keynote speeches by experts

- Workshops

- Panel discussion

- Questionnaire for participants

- Networking session

- Publicity for JICA Cyber Security Project and the International Conference on ASEAN-JAPAN Cybersecurity Community (IC-AJCC)

This event was organized to promote networking and knowledge sharing among individuals and organizations in the field of cybersecurity in the Philippines, with a particular focus on fostering collaboration across sectors between public and private entities. Additionally, the "International

Conference on ASEAN-JAPAN Cybersecurity Community (IC-AJCC)," scheduled for October 5 and 6, organized by NISC, was promoted.

The event featured speeches from information security and cybersecurity experts from both government and private organizations. The speakers were as follows:

1. Mr. Samuel Ramon V. Jacoba (Founder and President of NADPOP)

2. Mr. Ito Seiichi (Japan Network Security Association - JNSA)

3. Dr. Rudi Lumanto (Founder of the Indonesia Network Security Association - idNSA)

4. Mr. Jeffrey Ian C. Dy (Undersecretary, Department of Information and Communications Technology)

5. Mr. Angel Averia (Chairman of PH-CERT)

6. Mr. Engels Antonio (Chairman, Advisory Group for Transformation and Development, IT Management Service, Philippine National Police)

At this event, cybersecurity knowledge sharing was facilitated not only among cybersecurity experts but also among participants from government agencies.

④　Thailand Information Security Association (TISA)

Reconsignment contract amount: USD 21,000

Event Name: Cybersecurity and Sustainability (The Unexpected Duo of Digital Transformation)

Date and Time: September 21, 2023, 9:00-16:00

Venue: Grand Fortune Hotel

Number of Participants: 152

Main Content:

- Keynote speeches by experts

- Workshops

- Panel discussion

- Questionnaire for participants

- Networking session

- Publicity for JICA Cyber Security Project and the International Conference on ASEAN-JAPAN Cybersecurity Community (IC-AJCC)

The main objective of this event was to establish cooperation in cybersecurity with Japan and share information such as knowledge and experiences regarding the cybersecurity situation in the region. Additionally, the latest laws in Thailand, including the Personal Data Protection Act, were

discussed among IT personnel from Thai government agencies, state-owned enterprises, and the private sector.

A seminar was held with invited cybersecurity experts from both the domestic and international arenas. The speakers were as follows:

1. Dr. Kawin Boonyapredee (Co-Founder and Advisory Board member, Singaporean CIO Network - SCION/Cyber Risk Subcommittee, Singapore FinTech Association - SFA)

2. Dr. Rudi Lumanto (Founder and Advisor of idNSA)

3. Pol.Col. Yanaphon Youngyuen (President of the Thailand Information Security Association - TISA)

4. Mr. Shuichi Kato (Deputy Counsellor of the National Center of Incident Readiness and Strategy for Cybersecurity - NISC)

5. Mr. Seiichi Ito (Chair of the International Relations Committee, Japan Network Security Association - JNSA)

During the panel discussion led by regulatory specialists from Thai government agencies and leaders in the cybersecurity industry, the following topics were discussed:

1. Top 3 cyber-attacks/privacy breaches/cyber incidents in Thailand.

2. Top 3 best practices by NCSA/PDPC, particularly regarding issues with cybersecurity laws and the Personal Data Protection Act.

3. The impact of generative AI on cybersecurity or data privacy in Thailand.

The panelists were as follows:

1. Mr. AVM Amorn Chomchoey (Secretary General of the National Cyber Security Agency - NCSA)

2. Dr. Siwaruk Siwamogsatham (Secretary General of The Office of the Personal Data Protection Committee, Ministry of Digital Economy and Society)

3. Dr. Prinya Hom-anek (Chairman of the Executive Committee, ACIS Professional Center Co., Ltd./ Honorary Advisor, Thailand Information Security Association - TISA)

4. Mr. Narinrit Prem-Apiwathanokul (Vice President, Thailand Information Security Association - TISA)

5. Dr. M.L. Kulthon Kasemsan (Asst. Prof., Committee and Secretary, Thailand Information Security Association - TISA)

The seminar facilitated knowledge sharing and the exchange of different perspectives and experiences, thereby raising awareness of cybersecurity at the international level. Through

interactions with experts, government officials, and representatives from private companies, extensive discussions were held on the latest trends and countermeasures against cyber threats. Such information exchange and networking helped the participants recognize the importance of future efforts in cybersecurity and international cooperation while promoting mutual learning.

During the panel discussions, participants were able to understand and visualize cyberattacks or incidents and gain insights into best practices regarding cybersecurity laws and the Personal Data Protection Act. Additionally, they acquired knowledge of the impact of generative AI on cybersecurity and data privacy in Thailand.

8. Invitation to Japan for the International Conference on ASEAN-JAPAN Cybersecurity Community (IC-AJCC)

(1) Details of Invitation Work

To commemorate the 50th anniversary of ASEAN-Japan Friendship and Cooperation, NISC hosted the International Conference on ASEAN-JAPAN Cybersecurity Community (IC-AJCC) on October 5 and 6, in 2023 following the ASEAN-Japan Cyber Security Policy Meeting.

The NISC invited local cybersecurity-related private sector officials from five ASEAN countries to participate in "the Forum". The participants were selected upon consultation with the STI/DX Office of the Governance and Peacebuilding Department and NISC.

(2) List of invitees

Indonesia (2), Malaysia (4), the Philippines (3), Thailand (2), Vietnam (2) (a total of 13 persons). The original plan was to invite 14 persons, but Dr. Effendy Zulkifly (No. 14 in the table below) cancelled his visit to Japan at the last minute.

Table 27：List of "Invitees"

	Country	Name	Position, Organization
1	Indonesia	Dr. Rudi Lumanto	Founder and Advisor, Indonesia Network Security Association (idNSA)
2	Malaysia	Mr. Tahrizi Tahreb	Co-Founder, Chairman, Malaysia CyberSecurity Community (rawSEC)

3	Philippines	Mr. Angel Averia	President, Philippine Computer Emergency Response Team (PH-CERT)
4	Thailand	Dr. Prinya Hom-anek	Founder and Special Advisor, Thailand Information Security Association (TISA)
5	Vietnam	Mr. Nguyen Thanh Hung	Chairman, Vietnam Information Security Association (VNISA)
6	Malaysia	Dato' Dr. Amirudin Abdul Wahab	Chief Executive Officer (CEO), CyberSecurity Malaysia (CSM)
7	Indonesia	Dr.-Ing. Kalamullah Ramli	Founder of Id-CARE, University of Indonesia
8	Thailand	Dr. Komain Pibulyarojana	Founder and Managing Director, Former Senior Researcher at NECTEC (NSTDA), T-Net Co., Ltd
9	Philippines	Dr. Marlon Tayag	Associate Prof. III, Dean, School of Computing, Holy Angel University
10	Vietnam	Mr. Khong Huy Hung	Vice Chairman, Vietnam Information Security Association (VNISA)
11	Malaysia	Mr. Alex Loh	Chairman of CS Chapter, The National Tech Association of Malaysia (PIKOM)
12	Malaysia	Dr. Selvakumar Manickam	Senior Lecturer, National Advanced IPv6 Centre of Excellence (Nav6)
13	Philippines	Mr. Samuel Ramon V. Jacoba	President of the National Association of Data Protection Officers of the Philippines (NADPOP), Vice President of Philippine Computer Emergency Response Team (PH-CERT)
14	Malaysia	Dr. Effendy Zulkifly	President, Blockchain expert, Crypto Valley Malaysia

(3) Event summary

Event Name: International Conference on ASEAN-JAPAN Cybersecurity Community (IC-AJCC 2023）

Date: October 5 and 6, 2023

Venue: Meijikinenkan, Tokyo, JAPAN

(4) Itinerary

Organizer: NISC

October 5 (Day 1)   9:30 AM - 17:00 PM

Dinner Reception   18:00 PM – 20:00 PM

October 6 (Day 2)   10:20 AM - 16:30 PM

(5) Event report

The event featured keynote speeches and panel discussions on cybersecurity as well as information on cybersecurity in various countries. 178 people on-site and 167 people online were attended on the event.

The ASEAN Japan Cybersecurity Communities Alliance (AJCCA) was established by nine associations of private organizations and communities from eight ASEAN countries and Japan that signed an MOU. Indonesia was selected as the first host country.

In addition, 19 companies from the ASEAN region and Japan participated in business meetings and exhibition spaces where future customers were acquired and communication between companies took place.

①   Event program

Day 1 – Thursday, October 5

Welcome Speech by the Minister of Cyber Security

Presentations by related organizations about past and future cooperative activities

Speakers:

Ministry of Internal Affairs and Communications (MIC)

Ministry of Foreign Affairs of Japan (MOFA)

Ministry of Economy, Trade and Industry (METI)

Japan International Cooperation Agency (JICA)

Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)

Keynote Panel
Theme: "Collaboration for a Cyber-Safe ASEAN-Japan Community"
Speakers:
(Brunei) - Mr. Mohamad Azad Zaki Haji Mohd Tahir (President of the Brunei Cyber Security Association - BCSA)
(Cambodia) - Mr. Phannarith Ou (Chairman of ISAC Cambodia)
(Indonesia) - Dr. Rudi Lumanto (Founder and Advisor, Indonesia Network Security Association - idNSA)
(Japan) - Dr. Hiroshi Esaki (Chairman of the Japan Network Security Association – JNSA)
(Malaysia) - Mr. Tahrizi Thareb (Co-Founder of the Malaysia CyberSecurity Community - rawSEC)
(Philippines) - Mr. Angel Averia (President of the Philippine Computer Emergency Response Team - PH-CERT)
(Singapore) - Mr. Johnny Kho (President of the Association of Information Security Professionals - AiSP)
(Thailand) - Dr. Prinya Hom-anek (Founder and Special Advisor of the Thailand Information Security Association - TISA)
(Vietnam) - Mr. Nguyen Thanh Hung (Chairman of the Vietnam Information Security Association - VNISA)

Panel 1
Theme: "Past and Future in ASEAN-JAPAN Cybersecurity Cooperation"
Speakers: Selected distinguished contributors
Moderator: (Japan) - Dr. Nobushige Takamizawa (Visiting Professor, University of Tokyo)

Panel 2
Theme: "The Role of the Cybersecurity Community in Supporting National Cyber Space Protection"
Speakers:
(Brunei) - Mr. Mohamad Azad Zaki Haji Mohd Tahir (President of the Brunei Cyber Security Association - BCSA)
(Indonesia) - Dr. Rudi Lumanto (Founder and Advisor, Indonesia Network Security Association - idNSA)

(Singapore) - Mr. Johnny Kho (President of the Association of Information Security Professionals - AiSP)

(Thailand) - Dr. Prinya Hom-anek (Founder and Special Advisor of the Thailand Information Security Association - TISA)

Moderator: (Japan) - Mr. Akihiro Wada (Chair, Working Group on Cyber-Security Enhancement, Committee on Cyber Security, Keidanren)

Panel 3

Theme: "Cyber Security Community Program in Increasing Cyber Security Awareness"

Speakers:

(Cambodia) - Mr. Phannarith Ou (Chairman of ISAC Cambodia)

(Malaysia) - Mr. Tahrizi Thareb (Co-Founder of the Malaysia CyberSecurity Community - rawSEC)

(Philippines) - Mr. Angel Averia (President of the Philippine Computer Emergency Response Team - PH-CERT)

(Vietnam) - Mr. Nguyen Thanh Hung (Chairman of the Vietnam Information Security Association - VNISA)

Moderator: (Indonesia) - Dr. Muhammad Salman (Co-Founder and Chairman of idCARE - Indonesia Cyber Awareness and Resilience Center of University of Indonesia)

Day 2 – Friday, October 6

Keynote 1

Theme: "ASEAN DX Trend and Cybersecurity Challenges"

Speaker: Mr. Brian Shen (Chairman of ASOCIO-The Asian-Oceanian computing industry organization – ASOCIO)

Keynote 2

Theme: "Challenges of Risk Management and Governance in the Current Cybersecurity Landscape: Operational Best Practices"

Speaker: (Malaysia) - Dato' Dr. Amirudin Abdul Wahab (CEO of CyberSecurity Malaysia - CSM)

Keynote 3

Theme: "Standardization in Cybersecurity"

Speaker: Dr. Koji Nakao (Distinguished Researcher of the National Institute

of Information and Communications Technology –NICT)

Keynote 4
Theme: "Challenges in Building ASEAN Cyber Resilience"
Speaker: (Singapore) - Mr. Tony Low (Vice President of the Association of Information Security Professionals - AiSP)

Keynote 5
Theme: "The Current State of the Cybersecurity Market in Japan"
Speaker: Mr. Itsuro Nishimoto (President of LAC Co., Ltd.)

Keynote 6
Theme: "Cybersecurity Preparedness in Critical Infrastructures"
Speaker: Dr. Kenji Watanabe (Professor, Graduate School of Social
Science, Head of Disaster and Safety Management, Risk Management Center, Nagoya Institute of Technology)

Panel 4
Theme: "Cybersecurity Framework for loT/IloT devices "
Speakers:
(Japan) - Dr. Masaki Umeshima (IEC System Committee on Smart Energy(IEC SyC SE) Project Leader/ Associate Professor, Keio University)
(Malaysia) - Dr. Selvakumar Manickam   (Senior Lecturer, National Advanced IPv6 Centre of Excellence - Nav6)
Moderator: (Japan) - Dr. Koji Nakao (Distinguished Researcher of the National Institute of Information and Communications Technology - NICT)

Panel 5
Theme: "Cybersecurity Research Trends for Emerging Cyber Threats"
Speakers:
(Indonesia) - Dr.-Ing. Kalamullah Ramli (University of Indonesia)
(Japan) - Dr. Daisuke Inoue (Director General of the Cybersecurity Research Institute of the National Institute of Information and Communications Technology - NICT)
(Japan) - Dr. Katsunari Yoshioka (Professor at the Graduate School of Environment and Information Sciences/the Institute of Advanced Sciences, Yokohama National University

Moderator: (Thailand) - Mr. Thongchai Sangsiri (Expert Supervisory Policy and Standard Center Electronic Transactions Development Agency)

Panel 6
Theme: "Developing Cybersecurity Human Resources"
Speaker:
(Janan) – Mr. Hiroyuki Ide (Senior Advisor (ICT) Japan International Cooperation Agency)
(Japan) - Mr. Toshihiro Hirayama (Professor and Vice Dean of i University/ Director of Education Committee, JNSA)
(Malaysia) - Mr. Tahrizi Thareb (Co-Founder of the Malaysia CyberSecurity Community - rawSEC)
(Philippines) - Dr. Marlon Tayag (Associate Prof. III, Dean, School of Computing, Holy Angel University)
Moderator: (Indonesia) - Dr. Muhammad Salman (Co-Founder and Chairman of idCARE - Indonesia Cyber Awareness and Resilience Center of University of Indonesia)

Panel 7
Theme: "Cybersecurity Technology Solutions"
Speaker:
(Indonesia) - Dr. Toto Atmojo (Founder & Chief Executive Officer of Defenxor)
(Japan) - Mr. Fumikazu Okuno (Executive Officer, Public Sector, GMO Cybersecurity by Ierae, Inc.)
(Japan) - Mr. Yujiro Hayashi (Senior Architect, Group Director/Vuls Director, Cyber Security Innovation Group, Future Inc.)
(Thailand) - Mr. Chaiyanath Chamoraman (e-Cop (Thailand) Co., Ltd)
(Japan) – Mr. Naoki Kaneda (Japanese Business Development Manager - VNCS Global）
Moderator : (Thailand) - Dr. Komain Pibulyarojana (Information Security Specialist, Founder and Managing Director of T-NET Co., Ltd.)

Panel 8
Theme: "Cybersecurity in Financial Institutions"
Speaker:
(Japan) - Mr. Keisuke Kamata (Executive Director and CTO of   Financials ISAC
Japan/   Executive Director and CTO of Armoris Inc)

(Philippines) - Mr. Samuel Ramon V. Jacoba (President of the National Association of Data Protection Officers of the Philippines - NADPOP/Vice President of the Philippine Computer Emergency Response Team (PH-CERT))

(Vietnam) - Mr. Khong Huy Hung (Chairman of the Vietnam Information Security Association - VNISA)

Moderator : (Malaysia) - Mr. Alex Loh (Chairman of the CS Chapter, The National Tech Association of Malaysia - PIKOM)

Panel 9

Theme: "Current Challenges in Cybersecurity Incidents Response"

Speaker:

(Japan) - Ms. Yukako Uchida (Manager, Global Coordination Division, JPCERT/CC)

(Japan) - Mr. Hikohiro Lin (Managing Director of PwC Technology and Digital Consulting – Digital Trust)

(Philippines) - Mr. Angel Averia (President of the Philippine Computer Emergency Response Team - PH-CERT)

Moderator: Mr. Masato Terada (Chief Coordination Designer, Hitachi Incident Response Team (HIRT), Hitachi Ltd.)

See Appendix below for the materials of the speech given by the above-mentioned invited speakers.

Appendix13：Day1-Keynote Panel-Brunei-BCSA

Appendix14：Day1-Keynote Panel-Cambodia-ISAC

Appendix15：Day1-Keynote Panel-Indonesia-idNSA

Appendix16：Day1-Keynote Panel-Malaysia-Rawsec

Appendix17：Day1-Keynote Panel-Philippines-PHCERT

Appendix18：Day1-Keynote Panel-Singapore-AISP

Appendix19：Day1-Keynote Panel-Thailand-TISA

Appendix20：Day1-Keynote Panel-Vietnam-VNISA

Appendix21：Day2-Keynote2_Dato_ DrAmirudin

Appendix22：Day2-Keynote4_MrTonyLow

Appendix23：Day2-Panel4_Dr. Masaki Umeshima and Dr. Selvakumar Manickam

Appendix24：Day2-Panel5_Dr-IngKalamullahRamli

Appendix25：Day2-Panel6_DrMarlonTayag

Appendix26：Day2-Panel8_MRSamJacoba

② Number of participants

・Onsite 178

Speakers/Moderators: 40 (ASEAN: 20, Japan: 20)

ASEAN Policymakers (Government): 20

ASEAN industry participants (private sector): 26

Japanese Government Officials: 20

Japan Industry Relations 72

・Online 167

③ MOU signed by private organizations and communities in eight ASEAN countries and Japan

Contents of the MOU: "All parties are private and independent organizations related to cyber security, and all parties **agreed** to start exchanges between organizations to deepen mutual understanding and recognition across countries, **to exchange information** about cyber security threats, incidents and their solutions in each country, and **to promote cooperation** between organization members in order **to enhance security awareness and capacity building."**

The nine associations that signed the MOU.

(Brunei): Brunei Cyber Security Association (BCSA)

(Cambodia) : Information Sharing and Analysis Center (ISAC-Cambodia)

(Indonesia) : Indonesia Network Security Association (idNSA)

(Japan) : Japan Network Security Association (JNSA)

(Malaysia) : Malaysia CyberSecurity Community (rawSEC)

(Philippines) : Philippine Computer Emergency Response Team (PH-CERT)

(Singapore) : Association of Information Security Professionals (AiSP)

(Thailand) : Thailand Information Security Association (TISA)

(Vietnam) : Vietnam Information Security Association (VNISA)

Figure 12：MOU Ceremony

Figure 13：Contents of the MOU

④ Establishment of a new organization: AJCCA

The ASEAN Japan Cybersecurity Communities Alliance (AJCCA) was established, a vote was held after the MOU signing ceremony, and Indonesia was chosen as the first host country.

⑤ Business matching negotiation and exhibition space

19 companies from the ASEAN region and Japan participated in the business meeting and exhibition space.

Table 28：List of Exhibitors

Company No.	Name	Country
1	Defender Nusa Semesta (Defenxor)	Indonesia
2	GMO Cybersecurity by Ierae, Inc.	Japan
3	NTT TechnoCross Corporation	Japan
4	Future Inc.	Japan
5	Terilogy Co., Ltd.	Japan
6	VNCS Global Solution Technology	Vietnam
7	NetPro Academy	Vietnam
8	BroadBand Security, Inc.	Japan
9	Armis Inc.	Singapore
10	Blackpanda Japan K.K.	Japan
11	AMIYA Corporation	Japan
12	Vectra AI Japan	Singapore
13	wizlynx group	Singapore
14 & 15	National Association of Data Protection Officers of the Philippines (NADPOP) & Philippine Computer Emergency Response Team - PH-CERT	Philippines
16	ITPSS Sdn Bhd.	Brunei
17	Acronis Asia Pte. Ltd	Singapore
18 & 19	Athena Dynamics & BOS Marine & Offshore Engineering Corporation (BOSMEC)	Singapore

⑥　Questionnaire results
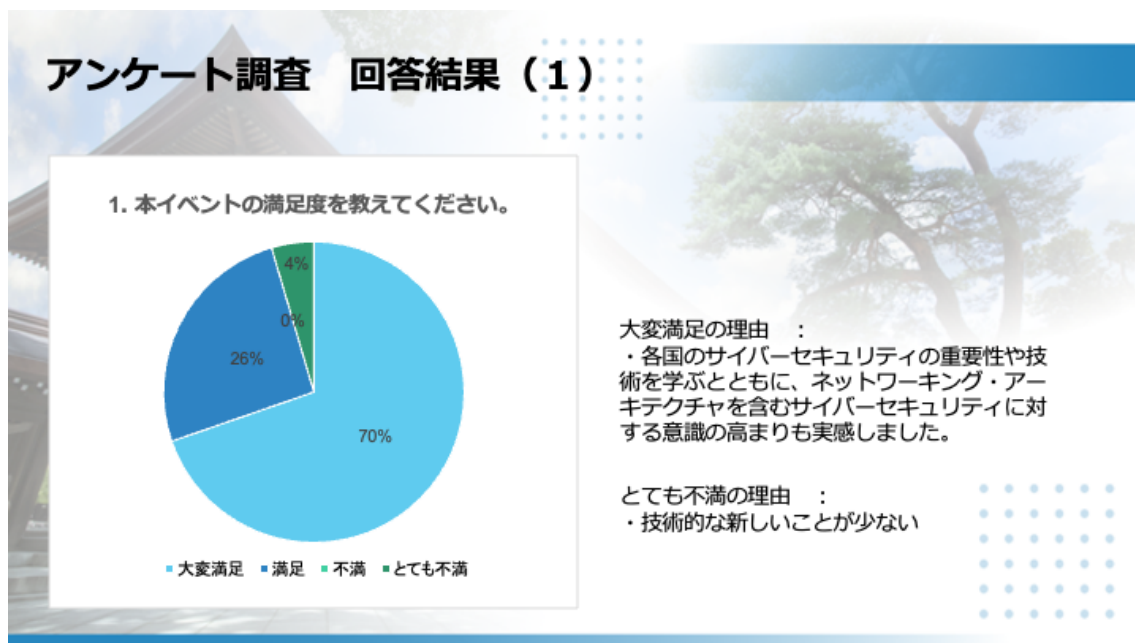
Figure 14：IC-AJCC Survey Response 1
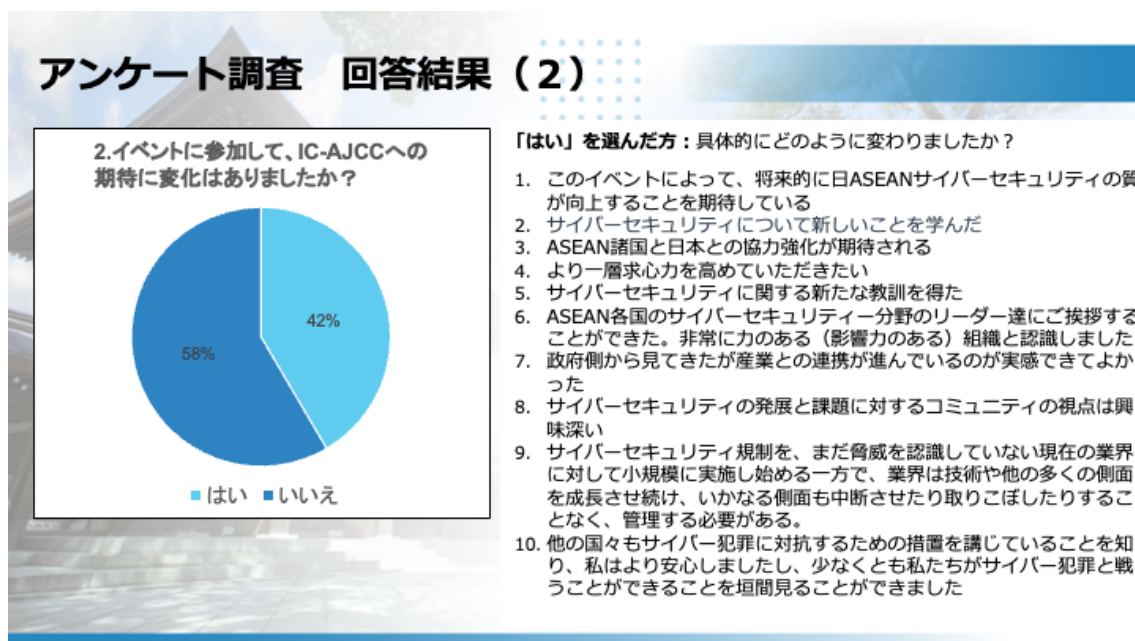
Figure 15：IC-AJCC Survey Response 2

Figure 16：IC-AJCC Survey Response 3
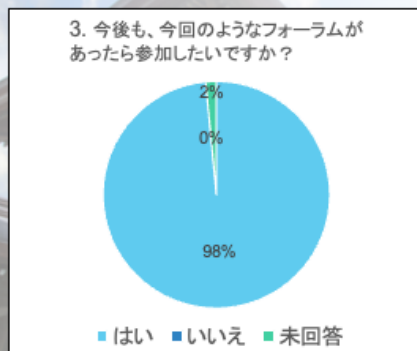
Figure 17：IC-AJCC Survey Response 4
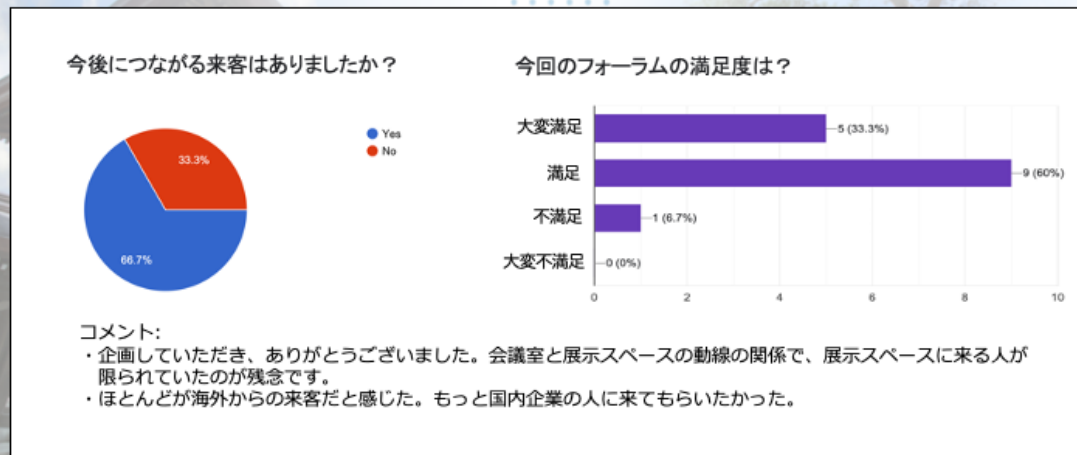
Figure 18：**IC-AJCC Survey Response 5**

9. Status of Follow-Up after "the Forum"

After the signing of the MOU on October 5, 2023, and the subsequent formation of the alliance, Dr. Rudi Lumanto from idNSA was announced as the first chairman at the reception on October 6, 2023.

Following the conclusion of the Forum, representatives from each relevant association convened for a meeting to discuss the formation of the alliance. They agreed to name the alliance "ASEAN-Japan Cybersecurity Community Alliance" (AJCCA). The objectives and activities of the alliance were discussed in two online meetings.

Ultimately, the decisions were finalized during the AJCCA Council Meeting ("C9") in Bangkok, Thailand on February 5 and 6, 2024. Subsequently, a workshop on public-private collaboration was conducted on the 7th as part of "the Policy Meeting," providing an opportunity to exchange views after the establishment of AJCCA.

9-1. Establishment of the AJCCA Organization

(1) AJCCA Mission

① Facilitate Exchanges Among Organizations:

Recognizing the importance of diverse perspectives and experiences in tackling cyber threats,

the AJCCA aims to deepen mutual understanding, interactions and collaborations across member countries about cybersecurity governance and operations.

② Exchange Information on Cyber Threats for better cyber resilience:
A critical component of the alliance is the sharing of intelligence regarding cybersecurity threats, incidents, and solutions prevalent in each member country. This information exchange is pivotal in pre-empting and mitigating cyber-attacks.

③ Improve and Enhance Sustainable Cybersecurity Capacity:
The alliance focuses on building trust, nurturing capacities and enhancing security awareness among its members. This involves joint training programs, workshops, and seminars to equip members with the latest cybersecurity knowledge and skills.

(2) Setting goals for AJCCA's activities.
① Capacity building
   - Themes: ICS, CTI, etc.
   - Training and certification
   - Local startup incubation
② Cyber threat intelligence sharing
③ Annual events and meetings
   - Off-site meetings and annual general meetings:
       - Annual general meetings and semi-annual board meetings
   - 2024 Annual Program/Party linking to "Policy Meeting"
       - Semiannual board meeting in Cambodia in May 2024
       - Annual General Meeting in Singapore in October 2024
   - Hosting the Second Annual Event in 2024
       - Annual event following last October's "the Forum"
       - The annual event for 2024 is planned to coincide with the annual general meeting
         scheduled in Singapore.
④ Commendation activities
   - Awards for contributions to cybersecurity community development and activities
   - Community awards for local cybersecurity solution products
⑤ Collaboration strategy and communication activities
   - Interaction, collaboration, and information sharing with AJCCA member associations and
     organizations
   - Collaboration with "the Policy Meeting"

- Partnership and collaboration with relevant organizations: ASOCIO Global Partners

⑥ Operation-related activities

    - Promotion, branding

    - Publications: Events, annual reports, and article-publishing activities

    - Research and development, investigative tools

⑦ Fundraising/management/audit activities

(3) Drafting of AJCCA Articles of Association

① Articles of organization are part of a formal legal document used to establish a limited liability company (LLC) at the state level.

② They are "organization rules and standards" to define rights, powers, duties, liabilities, and other obligations between each member of an LLC and between the LLC and its members.

③ Following basic information are required to be filed regarding all articles:

    - Organization's business name and address

    - The names and addresses of members

    - The statement of the organization's purpose: Vision and Mission

    Article I – Vision, Mission, and Purpose

    Article II – Offices and Mailing Address

    Article III – Member Organizations of AJCCA

    Article IV – Board of Trustees

    Article V – Donation and Contribution

    Article VI – Liability

    Article VII – Miscellaneous

    Article VIII – Amendments

④ AJCCA's operational policies and organizational structure

    - Trustees and Elections:

The affairs of the AJCCA shall be directed by the Board of AJCCA (the "Board"), comprising the Board of Trustees (the "Trustees"). Each AJCCA member organization assigns a trustee. The Chair of AJCCA (the "Chair") shall be elected at the Annual Board Meeting (the "AGM") every two years. The officers shall be as follows:

Chairman: Dr. Rudi Lumanto (idNSA)

Vice Chair (General Affairs): Prof. Hiroshi Esaki (JNSA)

Vice Chair (Annual Event): Mr. Johnny Kho (AiSP)

Secretary: Mr. Seiichi Ito (JNSA)

⑤　AJCCA logo and website

Design Concepts:

- First 'A' for ASEAN and Japan: This 'A' is designed to represent the partnership or alliance between the ASEAN countries and Japan, indicated by its prominent position and the use of red and blue colors referencing the colors found in many ASEAN nations' flags as well as the Japanese flag.
- The Two 'C's: These letters are stylized to represent a chain or a secure connection, which aligns with the cybersecurity focus of the alliance. Interconnected circles symbolize unity, strength, and the interconnected nature of cybersecurity efforts across nations.
- Color Scheme: The red, blue, and black chosen because of their strong visual impact, with red and blue often associated with trust, security, and authority, which are key aspects of cybersecurity.
- Typography and Style: The bold and modern typeface of the 'AJCCA' acronym conveys a sense of professionalism and modernity, which is fitting for a cybersecurity alliance.
- Overall Shape and Balance: The design is balanced with a mix of angular and rounded elements, which convey a sense of dynamism and adaptability, which are important traits for cybersecurity.

website : https://ajcca.net

Figure 19：AJCCA LOGO

9-2. Promotion and Consideration of Public-Private Collaboration

(1) Conference Title: "Public-Private Collaboration Workshop

(2) Agenda:

Table 29：Day 2, Wednesday, February 7 (excerpt from the Industry-Government-Academia Collaboration part)

Time	Items	Lead Country / Speaker
09:00 - 09:30	Reception	Thailand
09:30 - 11:30	[9] Joint Government-Industry-Academia - Future Government-Industry-Academia Collaboration Initiatives - Overview of the AJCCA Joint Workshop - Discussion	AJCCA(Lead)

11:30 - 11:40	**Closing Remarks**
	- Deputy Secretary General of the National Cyber
	  Security Agency of Thailand
	  Major General Teerawut Wittakorn
	- Counsellor, NISC
	  Mr. Junichi Sasaki
		Thailand/Japan

(3) Objective:

Through a questionnaire survey of AJCCA members, the actual status of their awareness of the promotion of "public-private collaboration" was summarized, and "mutual cooperation," "division of roles," and "activity plans" for the promotion of "public-private collaboration" were discussed with the "the Policy Meeting" members.

(4) Date and Time: February 7, 2024, 9:30-11:30 am

(5) Venue: Pathuwman Princess Hotel, Bangkok, Thailand

(6) Participants from AJCCA:

(Online participants) *Dr. Prinya Hom-anek from TISA, Mr. Toan from VNISA, and Ms. Yuko Nagano from JNSA

(Onsite participants) Countries in alphabetical order.

Table 30：List of AJCCA Participants in the Public-Private Workshop

Name	Org	Position
Mr. Muhammad Hakim bin Haji Bakri	(BCSA) Brunei Cyber Security Association	Vice President

Mr. Phannarith Ou	ISAC Cambodia	Chairman
Dr. Rudi Lumanto (MC)	(idNSA) Indonesia Network Security Association	Founder and Advisor
Mr. Fardan	(idNSA) Indonesia Network Security Association	Chairman
Dr. Hiroshi Esaki	(JNSA) Japan Network Security Association	Chairman
Mr. Seiichi Ito	(JNSA) Japan Network Security Association	Chair of International Relations Committee
Mr. Tahrizi Thareb	(rawSEC) Malaysia CyberSecurity Community	Co-Founder
Mr. Angel Averia	(PH-CERT) Philippine Computer Emergency Response Team	President
Mr. Samuel Ramon V. Jacoba	(PH-CERT) Philippine Computer Emergency Response Team	Vice President
Mr. Johnny Kho	(AiSP) Association of Information Security Professionals	President
Dr. Prinya Hom-anek	(TISA) Thailand Information Security Association	Special Advisor
Mr. Vincent Toh	(AiSP) Association of Information Security Professionals	Secretariat
Mr. Setyono	(idNSA) Indonesia Network Security Association	Secretariat
Ms. Aki Takemori	(JNSA) Japan Network Security Association	Secretariat

(7) Specific promotion procedure

① First Step: The promotion discussions on "Public-Private Collaboration" were conducted following the steps outlined below:

Implementation of "Public-Private Collaboration" awareness survey questionnaires for selected AJCCA organizations.

② Second Step: Unification of views at the C9 meeting.

③ Third Step: Exploration of the ideal form of "Public-Private Collaboration" through a joint workshop between NISC's Policy Meeting and C9.

(8) Survey Results

① Survey Results Report

② Minutes of Meeting

See Appendix for the Survey Results Report and the Minutes of Meeting.
Appendix27：AJCCA Profile and PPP community report
Appendix 28：Minutes of Meeting ASEAN-JP WG in Bangkok

10. Summary of "the Survey" Activities

10-1. Impressions on "the Survey"

During the initial phase of the investigation, which involved collaboration with local industry associations, there was a lack of access to private sector information on cybersecurity within ASEAN countries. Quantitative surveys of "market conditions," "industry information," "incident information," and "level of response personnel" relied primarily on desktop research using information available on the websites of some association bodies and various country CERTs.

Owing to the preliminary stage of the investigation, identifying the presence of local associations or communities and searching for their websites proved to be challenging.
The first investigative trips to the target countries began to provide insights into the actual situation in each country. A networking approach was employed to understand the realities of each country by facilitating introductions to "key persons" or "stakeholders" in cybersecurity from the member associations of ASOCIO, a federation of ICT associations in 24 countries in Asia.

As a result of these activities, progress was made in obtaining information on the existence of groups and organizations (communities) in each country and their selection (evaluation). Candidate organizations were selected to participate in the "Forum" to be held in October, and after consultation with the STI/DX Secretariat, the Governance and Peacebuilding Department, and NISC, they were registered as selected organizations.

Although the specifications of the Survey initially mentioned "about five countries," in reality, there were associations or groups in eight countries. By the second investigative trip, all these entities had expressed agreement with the purpose of "the Forum" and their intention to participate. Additionally, among the "selected organizations," four association bodies cooperated to promote follow-up events.

Subsequently, at "the Forum," the MOU was signed by the nine countries' "selected organizations," and AJCCA was formed. However, obtaining information regarding private-

sector activities in cybersecurity, especially the level of response of countries and critical infrastructure companies, remains challenging because of the conservative nature of this theme, which affects the credibility of the industry and companies involved.

During the latter half of the Survey, representative meetings were held after the formation of AJCCA, providing more opportunities to discuss its full scope and policies. This strengthened trust relationships among representatives of various country associations, making it easier to obtain previously difficult-to-obtain information through AJCCA.

Moreover, despite the initial desktop research and online inquiries suggesting the absence of target organizations, an investigative trip in February confirmed the existence of a cybersecurity community in Laos. This indicated the emergence of not only a collective body as a reserve force for associations or groups but also the emergence of cybersecurity business players, following in the footsteps of ASEAN's economic leaders (Singapore, Thailand, Malaysia, Indonesia, etc.).

10-2. Overall Survey Activities

The title of the Survey is "Data collection survey for promoting private-sector cybersecurity cooperation in the ASEAN and the Indo-Pacific region". To identify selected organizations to be invited to the Forum held by NISC to commemorate the "50th Anniversary of ASEAN-Japan Friendship" and promote cooperation between private associations and organizations in each country, the "circumstances of promoting collaboration with the private sector" in cybersecurity was investigated. Existing "target groups" were identified from private organizations specializing in cybersecurity, from which appropriate groups (selected groups) were determined and invited to participate in October 2023 "the Forum". The information collected through the activities was compiled into a "survey report," which attempted to identify "needs" for "cooperation and support from local public organizations" and "cooperation and support from the Japanese government," which are essential for the development of the cybersecurity environment in ASEAN. However, countermeasures for cybersecurity issues such as incidents/accidents, threats, markets, and the enactment of laws and regulations (hereinafter referred to as "Current Countermeasures") have rapidly expanded in recent years, despite having a short history. Furthermore, considering the many variations in policies and progress toward Current Countermeasures depending on the circumstances of each country, most research is conducted using publicly available data from public institutions, such as governments and government-related organizations (websites such as ministries and agencies in charge in each country and national CERTs). Therefore, "desktop research" has qualitative limitations. Even during the "travel research," it is difficult to collect actual information because the exact persons and circumstances involved are not known. However,

by taking a "promotion" and "invitation" approach to the "ASEAN-Japan 50th Anniversary Friendship Event" (the Forum) led by the Japanese government, it has made it possible to expand the network of local public and private sector experts and key personnel. This has become the basis for obtaining information from ICT associations in various countries (such as the ASOCIO) and AJCCA member associations. Information that is initially difficult to find in Japan through the "desktop research" was found from "travel research" through interviews.

10-3. Composition and Characteristics of Organizations in Each Country

There are officially registered "associations" and naturally occurring collective bodies known as "communities," both featuring prominent individual activities. The membership system includes both "corporate membership" and "individual membership," or a combination of both. The names of these bodies have evolved over time. Some, such as JNSA and idNSA, changed from network security-related associations to their current forms. Others, such as TISA and VNISA, originated from information security management systems. In addition, communities and organizations have emerged from the gathering of SOC or CERT operators, such as PH-CERT, ISAC-Cambodia, and rawSEC. The differences in the characteristics of organizations (JNSA, AiSP, rawSEC, PH-CERT, idNSA, VNISA, TISA) are those that maintain a distance from the government, are less dependent on the government, and engage in independent activities while cooperating with the government, and those (BCSA and ISAC-Cambodia) that are established through support from government policies and have a higher rate of involvement by government agencies. Many of the former existed before cybersecurity policies were introduced in each country and most already had established economic zones and operating funds. The latter have recently been hastily organized to meet the needs of establishing private organizations considering the circumstances in each country, and it can be seen that they have not yet reached the point of establishing an economic zone.

10-4. Business Development of ASEAN Cyber Security Industry

On the other hand, the business development of the cybersecurity industry is actively progressing in each country and is not limited to the traditional import and sales model of products from European and American manufacturers; it also employs consultants with advanced knowledge, forensics, and incident analysis experience. Additionally, products and services using new technologies developed by universities and venture companies, such as blockchain, thread intelligence, and log analysis, are also appearing. Most public and private sectors have adopted standards based on the US NIST standards for cybersecurity evaluation. Using the phrase "global

standard" to emphasize their expertise and superiority, they have received orders for Security Operation Center (SOC) and consulting services from critical infrastructure companies. Vietnam has a company that provides SOC services to six of the eight financial institutions. Surprisingly, in Laos, the only cybersecurity service company has entered consulting contracts with four banks. However, there remain very few companies, including those in Cambodia and Brunei, that have established themselves as specialized companies in this field. Generally, as part of providing ICT services, they also sell "security services" such as UntiVirus license sales. This situation does not involve more than one model. There is still a sense of disparity in knowledge and technical abilities regarding cybersecurity.

Consequently, companies that are good at overseas information, have extensive knowledge about cybersecurity, and have excellent human resources have little competition and can enjoy a first-mover advantage.

10-5. Contributions of the Japanese Government and Public Institutions' Activities

In the Survey, we interview the private sector and government-affiliated key personnel from each ASEAN country. Many of those who received support from the Japanese government and public institutions or had participated in activities were friendly and cooperative.

11. Summary

11-1. Results of "the Survey"

Unlike conventional quantitative surveys based on general data collection, the Survey traced the on-the-ground personal connections in each ASEAN country, elicited the true feelings of each stakeholder, explained the necessity of cooperation, and encouraged the establishment of a federation to build a foundation for collaboration. If you search for "ASEAN Cybersecurity Association/Organization" on the search site, the results will include the "International Conference on ASEAN-JAPAN Cybersecurity Community" or "IC-AJCC." You can also see articles such as "Japan and 8 ASEAN countries conclude MOU'" and "AJCCA launch" occupy the top rankings. Searching for the "ASEAN Cybersecurity community" from an overseas perspective yields similar results.

Furthermore, if you search for the "ASEAN Cybersecurity Public-Private Partnership," you will find similar articles from the private sector. These keywords have been used in the "International Conference on ASEAN-JAPAN Cybersecurity Community (IC-AJCC)" and by the ASEAN-Japan Cybersecurity Alliance (AJCCA), which was established after an MOU was signed at the

conference. Thus, it can be said that, in the past, there were not many articles on the Internet about cybersecurity associations and organizations in ASEAN or public-private collaboration between Japan and ASEAN.

According to the aforementioned results, in ASEAN, there have been exchanges between private cybersecurity associations in each country, including personal and lecture requests. However, it can be assumed that there has been little collaboration in standardizing guidelines for mutual improvement or comparing the levels of skill improvement programs. However, the "Japan-ASEAN Cybersecurity Policy Meeting" held every year by NISC is a platform for governmental collaboration ("government-to-government collaboration") among ASEAN countries. It seems that the private sector would not participate in the conference until the "Industry-Academia Collaboration Framework" was established at the Bali Conference in August 2022. In other words, in terms of cybersecurity in ASEAN, collaboration between the public and private sectors has not substantially progressed apart from public-private relationships that exist in each country. We believe that by establishing a "public-private partnership" system that combines ASEAN's "government-to-government collaboration" and "private-sector collaboration," we can ensure a high level of cybersecurity for ASEAN.

There is an urgent need to "improve the level of cybersecurity in supply chains across ASEAN countries," which the Japanese government has recognized as an important risk factor. To achieve this, collaboration among private businesses in each country's industries is essential. The "AJCCA" launched through the Survey project has the potential to become key to "private-sector collaboration" and "public-private collaboration" in ASEAN.

Appendix

Appendix1: Survey ICT Organization

Appendix2: Survey Cybersecurity Private Organization

Appendix3: Desktop Survey on Cybersecurity

Appendix4: JICA Cyber Security Questionnaire

Appendix5: 202305 Thailand quick report

Appendix6: 202305 Brunei quick report

Appendix7: 202305 Vietnam quick report

Appendix8: 202306 Philippines Cambodia Malaysia quick report

Appendix9：202307 Malaysia Thailand quick report

Appendix10: 202308 Vietnam Singapore quick report

Appendix11: 202310 GovWare2023 quick report

Appendix12: 202402 Laos quick report

Appendix13: Day1-Keynote Panel-Brunei-BCSA

Appendix14: Day1-Keynote Panel-Cambodia-ISAC

Appendix15: Day1-Keynote Panel-Indonesia-idNSA

Appendix16: Day1-Keynote Panel-Malaysia-Rawsec

Appendix17: Day1-Keynote Panel-Philippines-PHCERT

Appendix18: Day1-Keynote Panel-Singapore-AISP

Appendix19: Day1-Keynote Panel-Thailand-TISA

Appendix20: Day1-Keynote Panel-Vietnam-VNISA

Appendix21: Day2-Keynote2_Dato_ DrAmirudin

Appendix22: Day2-Keynote4_MrTonyLow

Appendix23: Day2-Panel4_Dr. Masaki Umeshima and Dr. Selvakumar Manickam

Appendix24: Day2-Panel5_Dr-IngKalamullahRamli

Appendix25: Day2-Panel6_DrMarlonTayag

Appendix26: Day2-Panel8_MRSamJacoba

Appendix27: AJCCA Profile and PPP community report

Appendix28: Minutes of Meeting ASEAN-JP WG in Bangkok

List of References and Websites

- References1: security_info
- The World Factbook: https://www.cia.gov/the-world-factbook/
- ITU Global Cybersecurity Index Report 2020:
  https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf
- Asian-Oceanian Computing Industry Organization (ASOCIO): https://www.asocio.org/
- Asia Pacific ICT Alliance (APICTA): https://apicta.org/
- InfoCom Federation Brunei (IFB) : https://www.ifb.org.bn/
- Authority for Info-communications Technology Industry of Brunei Darussalam (AITI)
  https://www.aiti.gov.bn/
- ICT Federation of Cambodia (ICTF) : www.ictfederation.org
- Indonesian Information Technology Federation (FTII) : https://ftii.id/
- Indonesia Telematics Software Association (ASPILUKI) : https://aspiluki.or.id/
- The National Tech Association of Malaysia (PIKOM) : https://pikom.org.my/
- IT And Business Process Association of The Philippines (IBPAP) : https://ibpap.org/
- Philippine Computer Society (PCS) : https://philippinecomputersociety.org/
- The National ICT Confederation of the Philippines (NICP) : https://nicp.org.ph/
- Singapore's tech industry (SGTech) : https://www.sgtech.org.sg/
- The Association of Thai ICT Industry (ATCI) : https://www.atci.or.th
- Vietnam Software And IT Services Association   (VINASA) : https://www.vinasa.org.vn
- Lao ICT and Digital Association (LIDA) : https://lida.la/
- Myanmar Computer Industry Association (MCIA) : https://mcia-yangon.org.mm/
- Timor-Leste ICT Association (ICT-TL) :
  https://digitalreview.org/uploads/files/pdf/2009-2010/chap-41_timor-leste.pdf
- Mongolian Software Industry Association : https://www.slideshare.net/MGL_MOSA
- Bangladesh Computer Samity (BCS) : WWW.BCS.ORG.BD
- Brunei Cyber Security Association (BCSA) :https://www.itpss.com
- Information Sharing and Analysis Centers (ISAC Cambodia) :
  https://www.facebook.com/groups/242965532481324
- Cambodia Digital Technology Association (CDTA) :
  https://web.facebook.com/CambodiaDigitalTechAssociation
- Indonesia Network Security Association (idNSA) : https://idnsa.id
- Indonesia Cyber Security Forum (ICSF) : https://www.facebook.com/ICSF.or.id/
- Indonesia Digital Forensic Association (AFDI) : https://www.afdi.or.id/
- Indonesia Cyber Security Independent Resilience Team (CSIRT.ID) : https://csirt.id

- Indonesia Cyber Awareness and Resilient (IDCARE) : https://idcare.ui.ac.id/
- Lao Hacker : https://www.laohacker.com/
- The World Factbook : https://www.cia.gov/the-world-factbook/countries/laos/
- LaoseSIM : https://laosesim.com/operators/
- Malaysia CyberSecurity Community (rawSEC) : https://www.facebook.com/rawsec.my/
- Nano Security Conference (NanoSec) : https://nanosec.asia/
- Philippine Computer Emergency Response Team (PH-CERT) :
  https://www.facebook.com/PHCERT/
- Cybersecurity Association of the Philippines (CAP) :
  https://www.facebook.com/PICSProfessionals/
- Information System Security Association (ISSA) Philippine Chapter :
  https://www.facebook.com/issaphilippines/
- Philippine Institute of Cyber Security Professionals (PICSPRO) :
  https://www.facebook.com/PICSProfessionals/
- The National Association of Data Protection Officers of the Philippines (NADPOP) :
  https://nadpop.org/
- Association of Information Security Professional (AISP) : https://www.aisp.sg
- Cloud Security Alliance Singapore (CSA) :
  https://circle.cloudsecurityalliance.org/singapore/home
- Singapore Cybersecurity Consortium (SGCSC) :
  https://www.nrf.gov.sg/tech-consortia/cybersecurity-consortium/
- Information Systems Security Association (ISSA) Singapore : https://www.issa.org
- Thailand Information Security Association (TISA) : www.tisa.or.th
- Vietnam Information Security Association (VNISA) : vnisa.org.vn
- Bangladesh Cyber Security Community :   https://www.facebook.com/groups/bdcybersec/
- Brunei : https://www.brucert.org.bn/
- Cambodia : https://www.camcert.gov.kh/en/
- Indonesia   : https://idsirtii.or.id
- Laos : https://laocert.gov.la/Home
- Malaysia : https://www.mycert.org.my/
- Philippine : https://www.ncert.gov.ph/about-us/ncert/
- Singapore : https://www.csa.gov.sg/
- Thailand : https://www.thaicert.or.th/
- Vietnam :   https://vncert.vn/
- Bangladesh : https://www.cirt.gov.bd/
- Mongolia : https://mncert.org/#/mn

・Timor Leste : https://tlcsirt.org/

Reference: Each Organization's website

Asian-Oceanian Computing Industry Organization (ASOCIO): https://www.asocio.org/

Asia Pacific ICT Alliance (APICTA): https://apicta.org/

Country			CyberSecurity chapter	Keyman	Year of Establishment	Background of Establishment	Chairman's Name	Number of members	Number of Community (mainly)
Brunei	InfoCom Federation Brunei (IFB)	https://www.ifb.org.bn/	No		2007	The formation of the InfoCom Federation Brunei was an initiative by then the BAG Networks Sdn Bhd, realising the need for Brunei Darussalam to have an ICT Federation that could look after its industry players. BAG Networks hosted a gathering comprising Infocom organisations on May 30, 2007 at the Business Centre, Empire Hotel, to pitch the idea which had garnered good support at the time. This was then followed up by an informal discussion chaired by the then chairman of BAG Network, Dato Seri Setia Haji Ali Apong who was also the Permanent Secretary at the Ministry of Finance at the time. Ten local organisations attended the discussion including Alif Technologies, Syabas Technologies, DST Group, Telbru, ITIS Wescot, KPF Comserve, BAG Networks, Xecutech, E-Prime Networks and Komputer Wisman. Post meeting, a pro-team committee consisting of these companies was then formed with a goal of registering the organisation and establishing the initial Executive Committee.	Ms. Pengiran Sarimah Binti Pengiran HJ Abdul Latiff, Chairwoman, IFB	29	3
Brunei	Authority for Info-communications Technology Industry of Brunei Darussalam (AITI)	https://www.aiti.gov.bn/			2003	We aim to propel the nation towards achieving the vision of a Connected Smart Nation. · To develop towards a thriving digital industry · To develop digital capacity for all · To enable conducive regulatory environment · To enable organisational excellence through its people, processes and technology	Yang Berhormat Pengiran Dato Seri Setia Shamhary bin Pengiran Dato Paduka Haji Mustapha		
Cambodia	ICT Federation of Cambodia (ICTF)	www.ictfederation.org	No		2016	In April of 2016, the ICT Federation of Cambodia (ICTF) was relaunched with a new Board of Directors, represented by industry leaders, and a new vision was set forth: "Empowering Cambodia's Digital Economy." For the first time, Cambodia's top ICT companies have united with a common cause: empowering small to large ICT related businesses to expand Cambodia's digital economy into a multi-billion dollar industry. The current board members of ICTF is representing six major ICT sectors: Software Development, Telecom, ISP, Hardware, New Media and Services & Solutions. We plan to add more board members from other sectors soon. ICTF is independently managed by the private sector but it is strongly endorsed by the Ministry of Post and Telecom (MPTC) as the only recognized ICT association in Cambodia. There are various opportunities for ICTF and MPTC to collaborate on strategic ICT initiatives and events.	Mr.Steven Path, CEO of Pathmazing, Software Development		6
Indonesia	Indonesian Information Technology Federation (FTII)	https://ftii.id/					Mr. Andi Budimansyah,Chairman	15	
Indonesia	Indonesia Telematics Software Association (ASPILUKI)	https://aspiluki.or.id/			1990	· Helping the government to condition the right atmosphere for the development of Copyright Works in the field of software and computers, namely by supporting and implementing consequently the Copyright Law. · Organizing and or participating in scientific activities such as education, training, seminars, lectures, workshops, discussions and so on related to the field of Information Technology and Software industry. · Collect, manage and develop library materials in accordance with existing capabilities. · Publish newsletters, journals and other documents both for the benefit of members and the general public. · Establish and develop cooperation with similar organizations both at home and abroad, as long as the aims and objectives of the organization do not conflict with the aims and objectives of APSILUKI. · Organizing efforts and establishing other institutions deemed necessary by ASPILUKI as long as they do not conflict with the Articles of Association and Bylaws.	Djarot Subiantoro	141	
Malaysia	The National Tech Association of Malaysia (PIKOM)	https://pikom.org.my/	Yes	Mr. Alex Low, Chairman of CS Chapter	1986	As a non-profit organization, PIKOM is managed by a council elected by its members every year during its AGM. PIKOM works to improve the business climate in the interests of all of its member companies and to promote industry growth in line with national aspirations.	Mr. Ong Chin Seong PIKOM Chairman	Over 1000 companies	7
Philippines	IT And Business Process Association of The Philippines (IBPAP)	https://ibpap.org/	No information		2004	With over 400 members and six partner associations—the Animation Council of the Philippines, Inc. (ACPI), Global In-House Center Council (GICC) Philippines, Contact Center Association of the Philippines (CCAP), Game Developers Association of the Philippines (GDAP), Healthcare Information Management Association of the Philippines (HIMAP), and the Philippine Software Industry Association (PSIA)—IBPAP plays a pivotal role in sustaining the growth of the IT-BPM industry by working with stakeholders in the government and academe to ensure an enduring supply of high-quality labor, support service innovation, and provide country visibility.	Jack Madrid President and CEO	400	
Philippines	Philippine Computer Society (PCS)	https://philippinecomputersociety.org/			1967	The Philippine Computer Society (PCS) is the longest-existing professional association of computing and information technology professionals in the country. From its special interest groups (SIGs) have spun off today's more specialized computing and IT-related organizations, many of which have evolved into national organizations themselves.			
Philippines	The National ICT Confederation of the Philippines (NICP)	https://nicp.org.ph/							
Singapore	Singapore's tech industry (SGTech)	https://www.sgtech.org.sg/	Yes	Parvitar Singh (Parv)	1982	SGTech is the leading trade association for Singapore's tech industry. Representing over 1,000 member companies ranging from top multinational corporations, large local enterprises, vibrant small and medium-sized enterprises, and innovative startups, it is the largest community in Singapore where companies converge to advocate for change and drive what enables tech innovation and accelerates tech adoption to spur greater sustainability in the sector.	Mr Wai Meng Wong, Chairman	Over 1000 companies	8
Thailand	The Association of Thai ICT Industry (ATCI)	https://www.atci.or.th	Yes	Dr. Komain Pibulyarojana, Chairman of CS Chapter	1998	The Association of Thai ICT Industry (ATCI) is Thailand's first Information Technology professional association. Its members include computer hardware and software manufacturers, distributors and service providers, together representing over 80% of Thailand's Information and Communication Technology market. With such strong representation, ATCI plays a significant role in the development of National ICT Policy and the ICT Master Plan.	Mr. Supak Lailet, President	23	6

Country	Association	Website	Member of ASOCIO?	Contact	Year Established	Description	President	Members	Branches
Vietnam	Vietnam Software And IT Services Association (VINASA)	https://www.vinasa.org.vn	No	Ms. Giang Nguyen	2002	Vietnam Software and IT Services As (VINASA) is a professional society organizations, non-profit activities, representing the software industry and IT services in Vietnam. Established on 4/27/2002, VINASA active role as a bridge between the government and business community of software and IT services; between local communities and international companies; support and promote the development and ensure benefits for members thereby promoting the development of the software industry and IT Vietnam.

Members of VINASA are mostly of leading enterprises in Vietnam operating in the field of software and IT services such as FPT, CMC, CSC, TMA, Harvey Nash, Microsoft, NEC ... By December 20th 2015 VINASA has more than 300 member companies. With over 60% of national programmers, VINASA members provide over 70% of software products and IT services in Vietnam.

VINASA have very strong relations with international organizations, IT associations in different regions and around the world. VINASA is an active member of the Association of Computer Industry in Asia - Oceania (ASOCIO) with 22 members representing 22 countries and economies in the region and Union IT services world (WITSA) with more than 70 member organizations, IT and service associations from countries around the world.

VINASA is linked very closely with other agencies, relevant ministries, especially the Ministry of Information and Communication in activities to promote the development of the software industry & Vietnam IT in general and businesses of VINASA members in particular. | Mr. Nguyen Van Khoa | 300 | 8 |
Laos	Lao ICT and Digital Association (LIDA)	https://lida.la/	No	Mr. Thanousone Ka, President		LIDA (Lao ICT and Digital Association) is a business association under the supervision of the Ministry of Technology and Industry; It is a national level organization that is linked with all parties both domestically and abroad to promote the use of digital technology and innovation in economic-social development in a progressive and sustainable manner.	Mr. Thanousone Ka, President		
Myanmar	Myanmar Computer Industry Association (MCIA)	https://mcia-yangon.org.mm/	No	Myo Naing	1998	To Organize ICT- related business owners within the Yangon Region. To strive toward goals, defined by the Myanmar Computer Science Development Law. To perform domestic, regional, and international activities, lead by MCIA for the Development of ICT	Mr.U Myint Zaw, President	268	4
East Timor	Timor-Leste ICT Association (ICT-TL)	https://digital-review.org/uploads/files/pdf/2009-2010/chap-41_timor-leste.pdf			2007	Timor-Leste ICT Association (ICT-TL) was founded in November 2007 by a group of ICT activists to develop the pro- fessional skills of its members, to promote ICT applications to support the national development process, and to promote the interests of consumers in the ICT sector in Timor-Leste.			
Mongolia	Mongolian Software Industry Association	https://www.slideshare.net/MGL_MOSA	No information		2007	The Mongolian Software Producers Association was established on January 15, 2007 with the mission of bringing the development of the software industry to an international level and developing it into a leading economic sector of Mongolia and contributing to the creation of an economic structure based on intelligence and knowledge.	B. Uuganbayar		
Bangladesh	Bangladesh Computer Samity (BCS)	WWW.BCS.ORG.BD	No	Abdullah H. Kafi	1987	Bangladesh Computer Samity, popularly known as BCS, was formed three decades ago with a vision to become the guiding light of the Bangladesh ICT sector and safeguard the interest of all industry stakeholders. With its relentless and sincere service since its inception in 1987, BCS has established itself as the apex ICT business and trade industry association of organization of the country. After becoming the first registered ICT trade association of Bangladesh in 1992 with 15 member companies, BCS now has 2,630 ICT companies as its members. BCS has 10 branches— Barishal, Chattogram, Cumilla, Jashore, Khulna, Mymensing, Rajshahi, Rangpur, Sylhet & Tangail - across Bangladesh to spread the awareness of ICT services and products among the rural people.	ENGR. SUBRATA SARKAR President, BCS	3025	

Cyber Security Organization List

Country	No.	Community Name	Website	NGO/NPO	Year of Establishment	Background of Establishment	Keyman	Chairman's Name	Number of members	Government	Structure	Cooperation with Japanese Companies
Brunei	1	Brunei Darussalam Information Security Association (BDISA)		NGO								
	2	Brunei Cyber Security Association (BCSA)	https://www.bcsa.com	NGO	2022	In the pursuit of the growing demand for cybersecurity professionals in Brunei Darussalam, it is my pleasure to announce the official establishment of the Brunei Cyber Security Association (BCSA) as of the 14th of August 2023, and we have outlined our objectives within our constitution the values and mission needed to undertake in order to improve our cybersecurity workforce. Our journey began with a shared desire to create a platform similar to today's conference, that would bring together individuals and organizations who share a common interest in cybersecurity. InshaʼAllah, We shall commence the onboarding process of our membership program to prospective members both individual and corporate in 2024	Mohamad Azad Zaki Haji Mohd Tahir	Mohamad Azad Zaki Haji Mohd Tahir	20	Cyber Security Brunei (CSB)	Chairman,2 Vice President, Secretary, Assistant Secretary, Treasury, Assistant Treasury, Executive committee: 18	
Cambodia	1	Khmer-Cambodia Vulnerability Research Team (KVRT)										
	2	Information Sharing and Analysis Centers (ISAC Cambodia)	https://www.facebook.com/groups/242963553481324	NGO	2016	• Sharing best practice and know-how on cybersecurity related matters • Conduct sharing session, training and workshop • Local and international cooperation on cyber related issues & emerging technologies • Industries and partners collaboration programs	Phannarith Ou	Phannarith Ou	60000	Ministry of Post and Telecommunications (MPTC)の OU氏が会長	Chairman	
	3	Cambodia Digital Technology Association (CDTA)	https://web.facebook.com/CambodiaDigitalTechAssociation									
Indonesia	1	Indonesia Network Security Association (idNSA)	https://idnsa.id	NGO	2011	Started as Indonesia Cyber Security Research Circle (ICyReC in 2011) Established as IdNSA in 31/8/2017 , Ministry of Law and Human Right Registration Number : AHU-0013509.AH.01.07.TAHUN 2017 Three purposes : to know, learn and engage in the development of network security which is growing rapidly worldwide Improving community security awareness to contribute and take a part on building a safe and secure network environment through a bottom-up approach and strengthening the weakest links.	Rudi Lumanto	FARDAN, Chairman	600		Advisory Board, Expert Board, Chairman, Secretary, Head of Capacity Dev, Head of Readiness, Head of RnD. Executive committee: 10	JNSA (2017)
	2	Indonesia Cyber Security Forum (ICSF)	https://www.facebook.com/ICSF.or.id/	NGO	2017	The various ICSF activities include matters relating to the cyber world or cyberspace, actively promoting increased security and resilience in the cyber world, as well as encouraging the development of a positive culture of society in using the Internet wisely, safely and ethically.		Ardi Sutedja K.				
	3	Indonesia Digital Forensic Association (AFDI)	https://www.afdi.or.id/	NGO	2015	The Indonesian Digital Forensic Association, hereinafter referred to as AFDI or in English also called the "Indonesian Digital Forensic Association", was founded on November 17 2015. The aim of forming AFDI is to gather and coordinate analysts and digital forensics enthusiasts in an Association forum so as to produce benefits for the progress of the Association members themselves as well as for the nation and state.						
	4	Indonesia Cyber Security Independent Resilience Team (CSIRT.ID)	https://csirt.id	NGO	2020	Background The rapid development of technology, the Internet, and industry 4.0 resulting in the transformation of the human lifestyle in the cyber era. It was impacted by increasing threats and risks within various sectors that are essential and strategic for a country. A failure to prevent cyberattacks will disrupt a wide range of services, resulting in social and economic losses of unprecedented severity. Thus, the ability to detect cyber threats and attack, with early warning capabilities in place is strongly needed. Effective and efficient countermeasures to respond to an incident will reduce risks and impacts. Then synergic cooperation between communities, professionals, experts, and academia is needed to raise public awareness, build cyber resiliencies, and to protect national cyber resources and assets continuously. History CSIRT.ID initiatives were founded on June 1st, 2020 by professionals, experts, and academia as an association organization. Registered as a legal entity at the Ministry of Law and Human Rights of Indonesia, under the (formal) name "Perkumpulan Ahli Keamanan Siber Independen Indonesia" with known abbreviation as "Perkumpulan AKSI Indonesia".					A. Advisory Board B. Oversee Committee C. Board of Executive - Chairman of CSIRT.ID - Deputy of CP and Resilience - Deputy of Operation and Security - Deputy of Research and Development - Deputy of Interagency Collaboration D. General Secretary / Secretariat E. Department / Division / Staff	
	5	Indonesia Cyber Awareness and Resilient (IDCARE)	https://idcare.ui.ac.id/	NGO	2020	Indonesia Cyber Awareness and Resilience Center (IdCARE.UI) is established under Faculty of Technology University of Indonesia (FTUI) in 2020 to provide the following activities: Postgraduates Program in Cybersecurity Cybersecurity Related Research Collaboration and Partnership Capacity Building and Certifications						
Laos	1	Lao Hacker	https://www.laohacker.com/			This platform is open to those interested in security to train their skills in solving cyber security problems, or simply called CTF play.			514			
Malaysia	1	Malaysia CyberSecurity Community (rawSEC)	https://www.facebook.com/rawsec.my/	NGO	2017	In a summary, rawSEC is a non-profit community effort in Malaysia which intends to provide a strong platform for local information security talents to share and contribute their knowledge to the community. rawSEC existence is to address the current industry gap by bridging the education sector and industry through a series of meetups and discussion session which would produce relevant talents for the industry.	Tahriri Thareb	Mr. Tahriri Thareb	3000	The chairman of rawSEC is a chair of cyber security in Bank Negara Malaysia.	Chairman, 20 committee including 6 council of elders	
	2	Nano Security Conference (NanoSec)	https://nanosec.asia/		2018	NanoSec is a newly created security community who organises events that focuses on all things security for Asia Pacific region based in Kuala Lumpur, Malaysia.		Mr. Kamal Hilmi		SIVA5 BOSS		
Philippines	1	Philippine Computer Emergency Response Team (PH-CERT)	https://www.facebook.com/PHCERT/	NGO	2001	Vision:Transform the philippines into a Global Center of Excellence for Data Privacy and Cybersecurity. Mission: Inspire, Empower & Prosper Data Protection Officers and Cybersecurity Proffessionals, then nurture and develop them within a Vibrant Community of Practice.	ANGEL S. AVERIA, JR.	ANGEL S. AVERIA, JR.		Once Recognized as the National CERT • VIA the CICT – 2004 ASEAN TELMIN Conference	Chairman, Vice Chairman	3PCERT: IRT Creation and Management (2009,2011), Secure Coding (2010)
	2	Cybersecurity Association of the Philippines (CAP)	https://www.facebook.com/PECSProfessionals/	NGO		PECSPro is a non-profit organization advocating for a secure Philippine Cyberspace						
	3	Information System Security Association (ISSA) Philippine Chapter	https://www.facebook.com/issaphilippines/	NGO		ISSA PH is the community of choice for Philippine cybersecurity professionals who share information						
	4	Philippine Institute of Cyber Security Professionals (PICSPRO)	https://www.facebook.com/PECSProfessionals/									
	5	The National Association of Data Protection Officers of the Philippines	https://nadpop.org/	NGO		Financial Management of PH-CERT		Mr. Samuel Ramon V. Jacoba			President, Vice president	
Singapore	1	Association of Information Security Professional (AISP)	https://www.aisp.sg	NGO	2008	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.	Tony Low	Johnny Kho	2200	CSA	Chairman, Vice Chairman, Advisory Council, Executive Committee, Secretariat,Executive committee: 42	JNSA
	2	Cloud Security Alliance Singapore (CSA)	https://circle.cloudsecurityalliance.org/singapore/home	global chapter	2008		President Alex Siow	Vice President Jim Lim				
	3	Singapore Cybersecurity Consortium (SGCSC)	https://www.nus.org.sg/tech-consortia/cybersecurity-consortium/	NGO	2016		Professor Abhik Roychoudhury					
	4	Information Systems Security Association (ISSA) Singapore	https://www.issa.org	global chapter	1984	To promote a secure digital world.		Dr. Shawn Murray President				
Thailand	1	Cybersecurity Thailand		NGO	2019							
	2	The Ethical Hackers Club (TEHC)		NGO								
	3	Thailand Information Security Association (TISA)	www.tisa.or.th	NGO	2007	Vision:Thailand Information Security Society is Trusted Globally Mission:Develop information security processes and personnel to meet internationally accepted standards.	Dr. Prinya Hom-anek, Honery Adviser	Mr. Police Colonel Yanaphon Yongyuen, President		NCSA	President, 3 Vice Presidents, Committees, Honorary Advisors,Executive committee: 14	
Vietnam	1	Vietnam Information Security Association (VNISA)	vnisa.org.vn	NGO	2007	VNISA has the task: Cooperate with Government Agencies: Authority of InfoSec/MIC, VNCERT/MIC, VGISC, … Promote Infosec education/training (Organize the information security competitions, …) Organize events, conferences, seminar of special subjects Survey on National/Industry information security status Lead up to the meetings among the organizations, businesses, help and cooperate to develop application of information security Promote International Cooperation Develop standards/guidelines.	Vice Chairman and General Secretary: Dr. Vu Quoc Thanh Chief of office: Tran Thi Kim Phuong	Mr. Nguyen Thanh Hung - Deputy Minister of Information and Communications.	more than 160 members	MIC	Chairman, Vice Chairman, Secretariat. Executive committee: 27	
Bangladesh		Bangladesh Cyber Security Community	https://www.facebook.com/groups/bdcyber.sec/			A community who are already working in information risk and cyber security field and for those who are interested to become one! Share, exchange, learn and grow together to make safer IT Infra in Bangladesh			7,426 followers			
Mongolia	1	No information (Government only)										
Timor Leste	1	No information (Government only)										

Desktop Survey Based on Cluster Strategy for Cybersecurity

Results of the survey

	Information from desktop survey
	Information added or modified by the local association after reviewing the information from the desktop survey
	Information from hearings with the local association

GCI

Item	GCI Ranking	GCI Score
Brunei	56 (86)	56.07
Cambodia	26 (132)	19.12
Indonesia	6 (24)	94.88
Laos	25 (131)	20.34
Malaysia	2 (5)	98.06
Philippines	13 (61)	77
Singapore	1 (4)	98.52
Thailand	9 (44)	86.5
Vietnam	7 (25)	94.55
Bangladesh	11 (53)	81.27
Mongolia	22 (120)	26.2
Timor Leste	34 (173)	4.36

Cyber Security Cooperation Network

Item	CS cooperation network	Partner country/
Brunei	Commonwealth – Model Law on Computer and Computer Related Crimes	Commonwealth
Cambodia	Workshop on International Cyber Security Policy and Diplomacy for CLMV countries (Second); Cambodia-Malaysia ICT-Cooperation; Mekong-Australia Partnership; Agreement on Cooperation in the Field of International Information Security, Shanghai Cooperation Organisation; Cambodia-India Cybercrime Training; Cybersecurity Alliance for Mutual Progress - CAMP Initiative, Member; ASEAN Ministerial Conference on Cybersecurity	Vietnam, Laos, Cambodia and Myanmar; Cambodia-Malaysia; Mekong-Australia; Shanghai Cooperation Organisation; Cambodia-India; ASEAN
Indonesia	Trilateral Meeting on Security, Indonesia-Malaysia-Philippines; Australia-Indonesia Cyber Policy Dialogue; Indonesia-Russia Cyber Bilateral Dialogue; (draft) Memorandum of Understanding, Indonesia-Solomon Islands; Memorandum of Understanding, India-Indonesia; Cybersecurity Alliance for Mutual Progress - CAMP Initiative, Member; Memorandum of Understanding (MoU), Indonesia and Australia	Indonesia-Malaysia-Philippines; Australia-Indonesia; Indonesia-Russia; Indonesia-Solomon Islands; India-Indonesia; CAMP Initiative, Member; Indonesia and Australia; ASEAN
Laos	Workshop on International Cyber Security Policy and Diplomacy for CLMV countries (Second); Memorandum of Understanding, China-Laos; CLMV ASEAN - ICT+Peace Cybersecurity Policy and Diplomacy Workshop; Cybersecurity Alliance for Mutual Progress - CAMP Initiative, Member	Vietnam, Laos, Cambodia and Myanmar; China-Laos; ASEAN
Malaysia	Trilateral Meeting on Security, Indonesia-Malaysia-Philippines; Memorandum of Understanding, Malaysia-Philippines; Memorandum of Agreement, Malaysia-Republic of Korea; Cybersecurity Alliance for Mutual Progress - CAMP Initiative, Member; EU-Malaysia Partnership and Cooperation Agreement (PCA); Memorandum of Understanding, India-Malaysia; Memorandum of Understanding, Malaysia-Oman; Memorandum of Understanding, Australia-Malaysia; Memorandum of Understanding, Malaysia-Morocco; Commonwealth – Model Law on Computer and Computer Related Crimes	Indonesia-Malaysia-Philippines; Malaysia-Philippines; Malaysia-Republic of Korea; CAMP Initiative, Member; EU-Malaysia; India-Malaysia; Malaysia-Oman; Australia-Malaysia; Malaysia-Morocco; Commonwealth
Philippine	Convention on Cybercrime (Budapest Convention); Regional Conference on Cybercrime (Council of Europe and South-East Asian countries); Trilateral Meeting on Security, Indonesia-Malaysia-Philippines; Memorandum of Understanding, Malaysia-Philippines; Cybersecurity Alliance for Mutual Progress - CAMP Initiative, Member; Global Forum on Cyber Expertise, Member	(Budapest Convention); (Council of Europe and South-East Asian countries); Indonesia-Malaysia-Philippines; Malaysia-Philippines
Singapore	Memorandum of Understanding (MoU) with Information Systems Audit and Control Association; Memorandum of Understanding (MoU) on Cybersecurity Cooperation, Singapore-Canada; Memorandum of Understanding (MoU), Singapore-Australia; Global Forum on Cyber Expertise (GFCE), Member; Memorandum of Understanding (MoU), Singapore – US; Commonwealth – Model Law on Computer and Computer Related Crimes; ASEAN Ministerial Conference on Cybersecurity (AMCC); ASEAN Cyber Capacity Programme (ACCP); ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE); UN-Singapore Cyber Programme: Senior Executives Cyber Fellowship; Global Commission on the Stability of Cyberspace (GCSC) Norm Package Singapore; (By hearing) Please see all the government MOU that was signed between Singapore and other countries at https://www.csa.gov.sg/News-Events/News-Articles	ISACA; Singapore-Canada; Singapore-Australia; Global Forum on Cyber Expertise (GFCE), Member; Singapore – US; Commonwealth; ASEAN; UN-Singapore
Thailand	Cooperation, Thailand-Russia; Agreement on cooperation, Iran-Thailand; Strengthening and Enhancing Cybersecurity Cooperation in the ASEAN Region: Towards an Integrated Approach in Addressing Transnational Crimes; Cybercrime Agreement, Australia-Thailand; Digital Cooperation, Portugal-Thailand; Regional Workshop on Cybersecurity: Norms in Cyberspace - ASEAN; Framework Cooperation Memorandum of Understanding, Bangladesh-Thailand; Memorandum of Understanding in the field of ICT, Singapore-Thailand; Cybersecurity Alliance for Mutual Progress - CAMP Initiative, Member; Global Forum on Cyber Expertise (GFCE), Member; ICT Cooperation Agreement, Montenegro-Thailand; Memorandum of Understanding on Cyber and Digital Cooperation, Thailand-Australia	Thailand-Russia; Iran-Thailand; ASEAN Region; Australia-Thailand; Portugal-Thailand; ASEAN; Bangladesh-Thailand; Singapore-Thailand; Montenegro-Thailand; Thailand-Australia
Vietnam	Agreement to enhance coordination, Japan-Vietnam; Workshop on International Cyber Security Policy and Diplomacy for CLMV countries; Memorandum of Understanding, India-Vietnam; Cybersecurity Alliance for Mutual Progress - CAMP Initiative, Member; Global Forum on Cyber Expertise, Member	Japan-Vietnam; Vietnam, Laos, Cambodia and Myanmar; India-Vietnam
Bangladesh	Memorandum of Understanding, Bangladesh-Sri Lanka; Memorandum of Understanding, Bangladesh-India; Framework Cooperation Memorandum of Understanding, Bangladesh-Thailand; Cybersecurity Alliance for Mutual Progress - CAMP Initiative, Member; Global Forum on Cyber Expertise, Member; Commonwealth – Model Law on Computer and Computer Related Crimes	Bangladesh - Sri Lanka; Bangladesh - India; Bangladesh - Thailand; CAMP Initiative; Commonwealth
Mongolia	Joint Statement for India-Mongolia Strategic Partnership; Cybersecurity Alliance for Mutual Progress - CAMP Initiative, Member; Agreement on Cooperation in the Field of International Information Security, Shanghai Cooperation Organisation	India - Mongolia; CAMP Initiative; Shanghai Cooperation Organisation
Timor Leste	Community of Portuguese Speaking Countries (CPLP) Conference on E-Government https://cyberpolicyportal.org/states/timor-leste	CPLP: Angola, Brazil, Cape Verde, Guinea-Bissau, Mozambique, Portugal, Sao Tome and Principe and Timor-Leste

Laws and Regulations

Item	Enactment status of CS-related laws/Update status	CS-responsible ministry/agency	Types of CS laws	Satisfaction with CS laws (by hearing with experts)
Brunei	Enacted	E-Government National Centre (EGNC); Brunei National Computer Emergency Response Term (BruCERT); Cyber Security Brunei	Electronic Transactions Act No. 196 (revised in 2008) , Computer Misuse Act, Revised in 2007	Satisfied
Cambodia	Draft	Director of ICT Security, Ministry of Posts and Telecommunications (MPTC); National Anti-Cybercrime Committee (NACC); Cyber War Team (CWT) Council of Ministers' Press and Quick Reaction Unit; Cambodia CERT; (By hearing) 1. Ministry of Post and Telecommunications (MPTC); 2. Ministry of Interior	Draft Cybercrime law, under review (as per March 2020) , Draft law on Cybersecurity (by MPTC), Draft Law on Personal Data Protection (by MPTC), Law on E-Commerce (enacted on 02 November 2019) ,	Satisfied
Indonesia	Enacted	(BSSN) Badan Siber dan Sandi Negara	Law No. 19 of 2016 on Electronic Information and Transactions (EIT Law), Law No. 27 of 2022 on Personal Data Protection (PDP Law)	Not satisfied. In some cases still need amendment in punishment and law enforcement, especially in cyber incident etc.
Laos	Enacted	National Steering Committee on Cybersecurity (In Progress/ Proposed); Ministry of Public Security; Ministry of Technology and Communications; Lao CERT	Electronic Signature Law, The Law on Prevention and Combating Cybercrime, Law on Electronic Data Protection, Bill - Consumer Protection decree on E-Commerce in 2020	
Malaysia	Enacted	Cyber Security Malaysia; Malaysia Computer Emergency Response Team (MyCERT); National Cyber Coordination and Command Centre (NC4)	Computer Crimes Act 1997, Digital Signature Act 1997, Telemedicine Act 1997, Communications and Multimedia Act 1998, Electronic Commerce Act 2006, Electronic Government Activities Act 2007, Personal Data Protection Act 2010, Anti-Fake News (Repeal) Act 2020	
Philippine	Enacted	Cybercrime Investigation and Coordination Center (CICC); Office of Cybercrime, Department of Justice; Anti Cybercrime Group (PNP-ACG), Philippines National Police; Department of Information and Communications Technology (DICT); Philippine CERT	Electronic Commerce Act of 2000, Data Privacy Act of 2012, Cybercrime Prevention Act 2012	
Singapore	Enacted	The Cyber Security Agency of Singapore (CSA); Minister for Communications and Information; Cyber Security Advisory Panel (CSAP); Defence Cyber Organisation (DCO); Government IT Security Incident Response (GITSIR); Cybercrime Command Singapore Police Force's Criminal Investigation Department; Cybercrime Command; Singapore Police Force's Criminal Investigation Department	Cybersecurity Act 2018, Personal Data Protection Act 2012, Computer Misuse Act 1993, Copyright Act 2021, Strategic Goods (Control) Act 2002	Satisfied
Thailand	Enacted	Electronics Transactions Development Agency (acting National Cybersecurity Agency); Ministry of Information and Communication Technology (MICT); National Cyber Security Committee (NCSC); Thai CERT; (proposed) National Cybersecurity Agency and Hacking Training Centre; Ministry of Digital Economy and Society	The Personal Data Protection Act B.E. 2562 (2019), Computer Crime Act 2007, Electronic Transactions Act 2001, Consumer Protection Act 1979	
Vietnam	Enacted	Cyber Security Department, Ministry of Public Security; Vietnam CERT, Ministry of Information and Communications	Law on E-Transactions No.51/2005/QH11, Law on Protection of Consumers' Rights 2010, Law on information technology 2006, Law on cyber information security 2015, Law on cyber information security, 2015 (In English) Law on network information security 2015 Cybersecurity Law 2018	Satisfied
Bangladesh	Enacted	Information & Communication Technology Division Ministry of Posts, Telecommunications and Information Technology; Bangladesh Computer Council (BCC); Bangladesh e-Government Computer Incident Response Team (BGD e-GOV CIRT); Bangladesh Computer Emergency Response Team (bdCERT)	The Information and Communication Technology Act, 2006. Amended in 2008 and 2013, Consumer Rights Protection Act, 2009, National Digital Security laws Act No.46/2018	
Mongolia	Enacted	Cyber Security Department (Кибер Аюулгүй Байдлын Газар) General Intelligence Agency; Cybercrime Unit (Кибер гэмт хэрэгтэй тэмцэх алба) National Police Agency; Mongolian Cyber Emergency Response Team / Coordination Center (MNCERT/CC); TLCSIRT	Law on Electronic Signatures, Law on information transparency and right to information, 2011 (updated in 2015), Criminal Code 2002	
Timor Leste	Enacted	National Special Advisor, Ministry of State and the Presidency of the Council of Ministers	Decree-Law No. 15/2014 Organic Law of the Scientific Police , Decree-Law No. 11/2003, Establishing the Bases for the Telecommunications Sector Section 23	

Strategic and Organizational Structure

Item	Publication status on each ministry website
Brunei	https://www.csb.gov.bn/
Cambodia	https://www.camcert.gov.kh/
Indonesia	https://bssn.go.id/
Laos	https://laocert.gov.la/
Malaysia	https://www.mampu.gov.my/
Philippine	https://cicc.gov/
Singapore	https://www.csa.gov.sg/
Thailand	https://www.thaicert.or.th/
Vietnam	https://vietnamnet.vn/
Bangladesh	https://www.cirt.gov.bd/
Mongolia	https://mncert.gov.mn/
Mongolia	https://mncert.gov.mn/
Timor Leste	https://tlcirt.com/

Technical skill

Item	Basis for setting up a national CSIRT	National CSIRT Service Contents and Achievements
Brunei	https://www.brucert.org.bn/services BruCERT was established with the vision of enhancing the security of Brunei ICT through proactive prevention and effective response. BruCERT became the nation's most trusted one-stop referral agency dealing with computer-related security incidents in Brunei Darussalam.	https://www.brucert.org.bn/services BruCERT runs an awareness program called Secure Verify Connect, aimed at raising awareness of Internet safety and information security among the Bruneian public, though education, seminars and workshops.
Cambodia	Cambodia Computer Emergency Response Team (CamCERT) is the National Computer Emergency Response Team for Cambodia and provides a point of contact for dealing with computer security incidents affecting the Internet community in Cambodia.	Study, research and develop a document of the attack on National Information Infrastructure and Government servers Develop the early warning system on ICT security Managing and update CamCERT's Website and E-mail system Monitoring and collecting attack traffic on servers of Government Research on new technologies in order to raise security issues Coordination and Cooperation with international cybersecurity agencies regionally and globally Managing National Cybersecurity Center
Indonesia	https://www.cert.or.id/tentang-kami/en/ ID-CERT (Indonesia Computer Emergency Response Team) is an independent team which is from and for community. ID-CERT is the first CERT in Indonesia and founded by DR. Budi Raharjo in 1998. ID-CERT wishes to remain standing as a non-governmental organization, independent, but received an allocation of government funding as a contribution to the CERT. ID-CERT is just being reactive (not active) in responding and handling a case of incoming or reported incident by complainers. ID-CERT does not have the authority to investigate a case thoroughly, but just become a liaison who can be trusted, especially by those who reported incident.	1. ID-CERT's purpose is to coordinate the incidents handling involving community locally and internationally. 2. ID-CERT does not have operational authority to its constituency, it only informs a variety of complaints to network incidents, and depends entirely on the cooperation with all those involved in incidents related networks. 3. ID-CERT is built from community and the results will be given back to the community. 4. ID-CERT helps increasing the internet security awareness in Indonesia. 5. ID-CERT has research in internet security which is needed by the Indonesia internet community.
Laos		
Malaysia	https://www.mycert.org.my/portal/full?id=d80322bf-04b2-4ba0-9a46-62c9860a4983 Malaysia Computer Emergency Response Team (MyCERT) is operating from the office of CyberSecurity Malaysia. MyCERT is a point of reference for the Internet community in Malaysia to address computer security incidents. MyCERT assist and gives advices on incidents handling such as intrusion, identity theft, malware infection, and other computer security related incidents.	MyCERT - Core Functions - National point of contact for reporting computer security incidents. - Provide technical analysis of computer security incidents. - Assist Malaysian Internet users in escalating abuse reports to relevant parties. - Conduct operational research and development work in the area of malware and emerging threats. -Issue relevant alerts and advisories on emerging threats to our constituency. - Co-ordination of computer security incident responses with trusted parties at the national and international arena.
Philippine	Cybersecurity Philippines CERT® is a non-profit Computer Security Incident Response Team (CSIRT) recognized as the first registered Computer Emergency Response Team (CERT®) in the Philippines. (By hearing) The Computer Emergency Response Program shall be composed of the National CERT, Government CERTs, and the Sectorial CERTs. The National CERT is the highest body for cybersecurity-related activities. All CERTs, Government CERTs, Sectoral (or Private) CERTs, as well as organizational CERTs shall coordinate and report incidences to the National CERT. The CERTs all over the country shall also conduct real-time coordination with CICC as provisioned in the law. (https://www.ncert.gov.ph/about-us/ncert/)	A Computer Security Incident Response Team (CSIRT) is a service organization responsible for receiving, reviewing, and responding to computer security incident reports and activities. We study and solve problems with widespread cybersecurity implications, conduct research & development and provide advisories on security compromises under the Philippine Autonomous System Number (ASN). We are also collaborating with various local government units, law enforcement, schools, and universities to help improve our country's cybersecurity advocacy to develop cyber defense skills and future employment. As part of our vision, we help determine their security-related practices' effectiveness and take them to the next level of the cybersecurity maturity curve. Concurrently, we collaborate closely with other computer security incident response teams and the different cybersecurity initiatives in the Philippines and abroad.
Singapore	https://www.csa.gov.sg/Explore/who-we-are/our-identity/about-singcert The Singapore Cyber Emergency Response Team (SingCERT) responds to cybersecurity incidents for its Singapore constituents. It was set up to facilitate the detection, resolution and prevention of cybersecurity related incidents on the Internet.	https://www.csa.gov.sg/Explore/what-we-do To underpin National Security, CSA continuously monitors our cyberspace for cyber threats, and protects and defends our Critical Information Infrastructure (CII) to ensure the continuous delivery of essential services to Singapore residents. CSA analyses the risks that the threats pose, and take appropriate mitigation measures to prevent them from affecting us. CSA is also responsible for creating a safer cyberspace for enterprise and individual end-users. CSA advocate and practises security-by-design, provides security consultancy services to other government agencies, certified products and validates systems' security assurance.
Thailand	Cybersecurity Act, B.E. 2562 (2019) grants a mandate of establishment of the Thailand Computer Emergency Response Team (ThaiCERT) as an internal department of the Office of National Cyber Security Agency (NCSA). According to Section 22 of the Cybersecurity Act along with the approval of the National Cyber Security Committee on June 26th (2020), ThaiCERT is tasked with monitoring the risk of occurrence of Cyber Threats, follow, analyze, and process information in relation to the Cyber Threats and the alerts on the Cyber Threats.	1. Stay a step ahead of detected and undetected cyberthreats and stop them in their tracks with threat prevention, detection and response capabilities. 2. Investigate and respond to a detected security incident by leveraging capabilities such as incident triage, incident response, threat intelligence curation and management, compliance monitoring and management. 3. Enforce legal safeguards to ensure the security of cyberspace.
Vietnam		
Bangladesh	Bangladesh Government's e-Government Computer Incident Response Team (BGD e-GOV CIRT); Bangladesh Computer Council (BCC) serving as the National CIRT of Bangladesh (N-CIRT) with responsibilities including but not limited to receiving, reviewing, and responding to computer security incidents and activities in the territory of Bangladesh as well as keeping close collaboration with international partners to secure the cyberspace of Bangladesh. BGD e-GOV CIRT reviews and takes necessary measures to resolve the issues with broad cybersecurity ramifications, conducts research & development, and provides guidance on security threats & vulnerabilities. BGD e-GOV CIRT also works with various Government Agencies, Critical Information Infrastructures (CII), Financial Organizations, Law Enforcement Agencies (LEAs), Academia & Civil Societies to help improve the cybersecurity landscape of Bangladesh. BGD e-GOV CIRT has a very strong tie with international organizations and cybersecurity communities and works as a focal point for Bangladesh for trans-border cyber issues.	INCIDENT HANDLING UNIT DIGITAL FORENSIC UNIT CYBER AWARENESS & CAPACITY DEVELOPMENT UNIT CYBER SENSOR UNIT CYBER RANGE UNIT CYBER RISK ASSESSMENT UNIT CRITICAL INFORMATION INFRASTRUCTURE UNIT CYBER AUDIT UNIT
Mongolia	Mongolian Cyber Emergency Response Team / Coordination Center. Founded in 2014.	MNCERT CC aims to spread awareness of information security to the public and create cooperation between experts.
Timor Leste	No information	No information

Capacity Buildings

Item	Status of CS Curriculum Development at Educational Institutions	CS Curriculum Introduction Status at Educational Institutions	Number and content of CS awareness activities conducted by public institutions	Research institutes conducting research and development in the CS field	Research content	International Recognition Status
Brunei						
Cambodia	Cambodia Digital Academy of Technology (CADT) www.cadt.edu.kh	https://www.cit.edu.kh/bachelor-of-telecoms-and-networking/specialized-in-cyber-security/	https://www.camcert.g.ov.kh/category/activities/awareness/			
Indonesia	22 universities that have cybersecurity study programs and almost all of them are in Java. (https://www.eccouncil.org/ec-council-in-newjolor-council-collaborates-with-indonesias-ministry-of-communication-and-information-to-facilitate-cybersecurity-training/		https://openguveais.com/campaign-to-raise-cybersecurity-awareness-for-indonesian-youth/ Indonesia's National Cyber and Crypto Agency (BSSN) held a digital cybersecurity literacy campaign for Indonesian youth. The cybersecurity awareness movement is designed to raise awareness and educate Indonesia's young generation on cybersecurity issues and to ensure good behaviour when surfing in cyberspace.		https://www.researchgate.net/publication/347111955_Analysis_of_College_Students%27_Cybersecurity_Awareness_In_Indonesia - Analysis of College Students' Cybersecurity Awareness In Indonesia - Cybersecurity awareness among polytechnic student population - Students' Cybersecurity Awareness at a Private Tertiary Educational Institution - THE IMPORTANCE OF CYBERSECURITY AWARENESS FOR CHILDREN	
Laos						

Malaysia	As a body entrusted to ensure the security of Malaysia's cyberspace, Cyber Security Malaysia expertise and services are widely needed to provide training and consultancy in the area of cyber security domains:
	  Digital Forensics
	  Incident Handling and Response
	  Security Assurance
	  Cryptography
	  Cybersecurity Management - Governance, Risk and Compliance
	(By hearing)
	CS module by Ministry of Education (MOE)
	CS Courses by Ministry of Higher Education (MOHE)
		The list of programmes offered by CyberSecurity Malaysia includes:
		  Competency Trainings
		  Security Essential
		  Business Continuity Management
		  Common Criteria
		  Digital Forensics
		  Incident Response and Handling
		  ISO 27001
		  Network Security Assessment
		  Web Application Security Assessment
		  Server & Desktop Security Assessment
		  Wireless Security
		  Certified Training under Global AGE Certification:
		  Certified Digital Forensic for First Responder (CDFFR)
		  Certified Information Security Management System: Internal Auditor (CISMS)
		  Certified Penetration Tester (CPT)
		  Certified Secure Application Professional (CSAP)
		  Certified Information Security Awareness Manager (CISAM)
		(By hearing)
		National Cyber Security Awareness Module in 300 schools nationwide.
		Cybersecurity courses offered by 30 Universities in Malaysia
		- 18 public universities
		- 12 private universities
			https://www.malaysia.gov.my/portal/content/30868
			CyberSAFE (Cyber Safety Awareness for Everyone)
			Program is one of the initiatives from Cybersecurity Malaysia aimed at promoting cyber and internet security awareness and to cultivate a positive culture on the use of internet among Malaysians from all walks of life.
			(By hearing)
			• NACSA has published the 10 Easy Steps for Cyber Security Awareness that outlines all of the most sensible practices in cyberspace;
			• Malaysian Modernization and Management Planning Unit (MAMPU) has been organising cyber security awareness programmes for public sector such as the Cyber Security Awareness Month and Public Sector ICT Security Conference;
			• Royal Malaysia Police through the Be Smart campaign ensure the community are more aware and cautious about cybercrime;
			• Malaysian Communications and Multimedia Commission has organised various programmes under the Klik Dengan Bijak initiative, a media and digital literacy initiative to nurture positive and responsible Internet use among ICT users
			• Ministry of Health also has come out with female Selamure Klik campaign;
			• Chief Government Security Office (CGSO) through the Protective Security Training Centre provides ICT security awareness courses to government officer as part of its annual cybersecurity awareness programme;
			• CyberSecurity Malaysia in collaboration with MOE and DIGI Telecommunications Sdn. Bhd. runs the CyberSAFE campaign to nurture positive internet use among ICT users; and
			• Central Bank of Malaysia has been raising awareness to all banking users on online fraud and safety tips for Internet bankingservices.
					The Strategic Research Division of CyberSecurity Malaysia focused on these 3 pillars
					- Strategic Research and Advisory (SRA),
					- Knowledge Management Center (KMC), and
					- Cyber Action & Intelligence Team (CAIT)
						Global Cybersecurity Index by International Telecommunications Union (ITU):
						Top 5 globally, Top 2 Asean.

Philippine	https://edurank.com/cs/cybersecurity/ph/	More than twelve Colleges and Universities already have college and post-college level Cybersecurity courses	October is Cybersecurity Month in the Philippines and the DICT takes the lead in conducting cybersecurity activities for the whole country at this time. Throughout the year, the private and public sector also conducts various cybersecurity activities, including awareness campaigns.	We expect that the current crop of Colleges and Universities offering Cybersecurity degree courses will also be conducting cybersecurity research and development	Here are some notable cybersecurity research conducted recently: (1) Cybersecurity Workforce Study (2022) by IBM and the USAID Better Access and Connectivity (BEACON) Program (https://www.nathaninc.com/usaid-dict-and-ibm-launch-ph-cyber-talent-report-to-counter-high-risk-to-ph-govt-and-economy-if-cyber-staff-shortages-continue/); (2) Cybersecurity in the Philippines: Global Context and Local Challenges (2022) by The Asia Foundation and Secure Connections (https://asiafoundation.org/publication/cybersecurity-in-the-philippine-global-context-and-local-challenges/);	
Singapore	MOE recognises the importance of equipping students to use technology safely and responsibly. Cybersecurity education is delivered as part of Cyber Wellness lessons within the Character and Citizenship Education (CCE) Curriculum. As part of CCE, all primary students are taught how to keep themselves safe in the online environment, including how to identify dangerous online content like phishing emails and online fakehoods.	These lessons are supported by digital literacy resources, covering cybersecurity-related topics such as safeguarding personal information when using internet and social media and hosted on the Student Learning Space online platform (SLS). These resources are available to all students. Beyond the formal curriculum, the Cyber Security Agency of Singapore (or CSA) supports MOE's efforts by providing assembly talks and other enrichment programmes in schools. A cybersecurity module is also incorporated into the Code for Fun programme for all Upper Primary students, where they are exposed to concepts like encryption and ways to protect oneself against cyberattacks. MOE will continue to ensure that students are equipped with cybersecurity knowledge and skills to use technology safely and responsibly in their day-to-day lives.	We also have the IMDA Scholarship to focuses on developing future leaders for Singapore's technology and media ecosystem. URL: https://www.imda.gov.sg/how-we-can-help/singapore-digital-scholarship/utm_source=google&utm_medium=cpc&utm_campaign=2024_SGDScholarship2024&utm_content=generic_phrase_cybersecurity_adcopy>			
Thailand						
Vietnam						
Bangladesh						
Mongolia						
Timor Leste						

Inter-Organizational Cooperation

Item	Status of participation in international CS cooperation frameworks	CS company invitation and establishment promotion status	Number of participants in seminars, etc. related to organizations	Understanding of seminars, etc.	Number of domestic and international conferences held, invited, and attended	Number of CS bilateral collaborations
Brunei						No information
Cambodia	ASEAN, ASEAN Regional Form, ANSAC, Cyber-CC, ASEAN-CERT					Cambodia-Malaysia Mekong-Australia Cambodia-India Cambodia-Thailand Cambodia-Japan
Indonesia						Australia-Indonesia Indonesia-Russia Indonesia-Solomon Islands India-Indonesia
Laos						China-Laos
Malaysia	National CS Consultation Regional cybersecurity awareness programme Capture The Flag competitions Speakers at CS talks	Normal average - Online: 100 attendees above - Phisical seminars: 150 attendees above - Conference: 250 attendees above	Various topics, including but not limited to - Cybersecurity awareness - CS Threats & Trends - Data Security and Integrity - Privacy Concerns in AI - Incident Response Plan - Combating Cyber Bully - CS in Emerging Technology - CS in Healthcare	There are numerous initiatives from government, private, and NGO sectors aimed at developing cybersecurity awareness through various events and agendas, such as conferences, road tours, and public sessions.		Malaysia-Philippines Malaysia-Republic of Korea India-Malaysia Malaysia-Oman Australia-Malaysia Malaysia-Morocco
Philippines						Malaysia-Philippines
Singapore						Singapore-Canada Singapore-Australia Singapore – US
Thailand						Thailand-Russia Iran-Thailand Australia-Thailand Portugal-Thailand Bangladesh-Thailand Singapore-Thailand Montenegro-Thailand Thailand-Australia
Vietnam						Japan-Vietnam India-Vietnam

Cyber Cybersecurity Questionnaire 2023

Country	Brunei	Cambodia	Indonesia	Laos	Malaysia	Philippines	Singapore	Thailand	Vietnam
Question	**Answer**	**Answer**	**Answer**	**Answer**	**Answer**	**Answer**	**Answer**	**Answer**	**Answer**
(1) Are there any big chances in cyber security environment in the country within this 1-2 year, for example new law, new regulation, new agency etc.?	Yes there are few in the pipeline. -Introduction scam protection center lead by bank -Standardize CII guideline -Strengthening data protection law	Governance structure will be established to coordinate nation-wide approach on cybersecurity Cybersecurity law will be endorse Personal Data Protection law Cybercrime law Cybersecurity Strategy Digital Security Committee is going to be established in the next few months	yes there are. Data Privacy Protection Law is enacted in 2022 and will be effective 2024	There are still very few companies operating cybersecurity service. Public awareness is still very low and the demand to pay for such service is low, partly is because of the digitalisation is still at the entry level.	Yes, since Malaysia is currently will be finalising the new cybersecurity bill 2024 and will be tabled out in parliament in Q2 2024.	Three pending bills on cybersecurity	Cyber Professional Accreditation; Research and Innovation Public Consultation on the Proposed Cybersecurity (Amendment) Bill	Issue of Cyber resilience and Cyber Dominance	Data privacy protection policy has been in placed
(2) Is there any big threats or cyber-attacks that bothering the people? What are current popular cyber-attacks? of versions of	Phishing , identity fraud, scam	Phishing attack, Ransomware, Scam and Fraud, APT and Supply chain	Big data leak, malware, ransomware, phishing, scam and fraud	Big threats are scams, virus infection and data got stolen.	Ransomware, Rootkit still dominance threats	Phishing and ransomware; govt systems are being hacked	DDOS, Phishing, Ransomware, Increased in Scam campaign - Unseen Enemy	Ransomware , phishing and data leaks	Ransomware and phishing is biggest issue in Vietnam. Information from Department of Cybersecurity and High-Tech Crime Prevention (Ministry of Public Security) also said: that Vietnam is in the top 10 countries suffering from cyber-attacks and dangerous malware infections, ranked 7th in the number of victims of cyberattacks, and ranked 2nd among countries. most infected with crypto-mining malware.
(3) Are there communities or association involved in cyber security activities in the country? How many?	Currently one official Brunei Computer Emergency Response Team (BruCERT) and one non-government entities BCSA	As of now, there is no official cybersecurity community to do it. ISAC-Cambodia is a virtual platform in Cambodia to serve as a cybersecurity community.	There many cybersecurity communities involved in cyber security activities and also more than 100 CSIRT have been launched nationally initiated by government	Public sector has set up one department specifically looking after cyber security. From the private sector, there are only two companies within our association focusing on this subject.	There are multiple community funded organisation in Malaysia. rawSEC is among the active community which always holding monthly event for the community.	There are several. PH-CERT is the oldest cybersecurity community founded in 2001	Yes, Local Chapters of International Groups, Cybersecurity Chapters of Sectoral Associations. AISP forms a local community called Singapore Cyber Security Inter Association (SCSIA) with like-minded groups	TISA, ISACA Bangkok chapter , isc2 Bangkok chapter	few like VNISA and other associations
(4) How is the acceptance of the people to cyber security solutions?	Need improvement and assurance	N/A	very good, but depend on the sectors.	Currently, not so many people in Laos are aware of the importance of cyber security and prepare to spend some of they money to pay for the cybersecurity solution. Many large companies are still keeping their sentive data offline or in a private cloud.	Malaysian currently has high cybersecurity hygiene and awareness on cybersecurity due to proactive awareness campaign by the private and government entities.	Awareness is high but solutions are still expensive for MSMEs	This is gaining awareness but still needing more awareness and appreciation of value for adoption to increase	Moderate but it needed	very good
(5) Who is the famous or popular person or institution in the country if we are talking about cyber security ?	Cyber security Brunei	Mr. OU Phannarith	BSSN (National Cyber and Crypto Agency)	For private side is Mr. FRANK, FOR PUBLIC SECTOR SIDE IS Mr. KHAMLA THE DG in ministry of technology and communications	Dr Amirudin Abdul Wahab (CEO Cybersecurity Malaysia)	Government officials of course; Lito Averia of PH-CERT; Engels Antonio of Bluepoint	Cyber Security Agency of Singapore is most prominent.	Dr Prinya (TISA) and Gen Amorn (NCSA)	can't tell as there are many

Preliminary report of the first On-site survey - Thailand

The following is a preliminary report of the travel survey conducted.
Purpose of the Survey:
To meet with key persons from government and industry associations in Thailand to hear about the status of industry associations related to cyber security in Thailand, and to explain and request their participation in the "ASEAN-Japan Cyber Security 50th Anniversary Event" hosted by NISC in October.

Survey period: Tuesday, May 16 - Friday, May 19, 2023
Survey method: On-site survey
Survey person in charge: Rudi Lumanto and Seiichi Ito
Survey targets: Industry associations and others related to cyber security in Thailand.
-   ATCI(Association of Thai ICT Industry)Mr.Bunrak Mr. Boonchuay
-   TISA(Thailand Information Security Association) Dr.Prinya
-   NCSA(National Cyber Security Agency)Mr.Amorn

Results of the Survey:
Interviewees and interview content

Mr. Bunrak and Mr. Boonchuay, ATCI (ASOCIO Member Association)
* On the day of the meeting, Mr. Bunrak was hospitalized due to Covid-19 infection, so we met later in Vietnam.
<u>Q1 Mr. Boonchuay</u>
The main ASOCIO members will not be able to participate in the event because it will coincide with the WCIT event period in Malaysia.
<u>A1 Ito</u>
It is not necessary for the head of each ASOCIO association to come to Japan, but we would like the head and members of each association's cyber security chapter to participate.

Dr. Prinya, TISA(Vice President of Cyber Security Associations)
<u>Q1 Dr. Prinya</u>

What is the difference between this consortium and the one formed last October under the leadership of the Singaporean association AiSP with the support of the Singaporean government?

A1 Rudi Lumanto

The AiSP-led ASEAN consortium has the following characteristics.

(1) It is a business-oriented organization with vendor sponsors and does not limit its members to cybersecurity professional associations. It also invites a wide range of participants and aims to expand its scale due to its unique characteristics.

(2) The upcoming MOU and its cooperation between private organizations in ASEAN-Japan related countries is for public-private partnership with the ASEAN-Japan Policy Council. Server security associations (if there is more than one, only one association will be selected) in each country will be selected and invited to participate in the JICA and other support programs. The consortium will not be directly involved in the business activities of each country, but will help develop the industry in each country through the target association. In addition, as this is an ASEAN-Japan program, a Japanese association (JNSA) that is not part of ASEAN will also participate in the program.

Q1 Ito

Who is the right person to invite as the representative of the association?

A1 Dr. Pyinya

The president of TISA exists but has no real authority. I will participate and give a lecture as a representative of TISA. I will secure the schedule.

Result:

TISA will participate in IC-AJCC – OK

MOU singing – OK

Speaker - OK

Preliminary report of the first On-site survey – Brunei

The following is a preliminary report of the travel survey conducted.
Purpose of the Survey: It is to meet with member associations of ASOCIO (Asian-Oceanian computing industry organization), IFB (InfoCom Federation Brunei) and BCA (Brunei Cybersecurity Association), Conduct a survey of professional associations on cybersecurity in Brunei. Also, to explain NISC's project "ASEAN-Japan Cybersecurity 50th Anniversary Event" in October to key persons in Brunei and request their participation.

Survey period: Tuesday, May 22 - Thursday, May 26, 2023
Survey method: On-site survey
Survey person in charge: Ludi Lumanto
Survey targets: Industry associations and others related to cyber security in Brunei.
      Visited Brunei Government(CSB)
      BCA (Brunei Cybersecurity Association)
      IFB (Infocom Federation Brunei)

Result of the Survey:

1. Conducted informal meetings with BCA committee members and BCA president; made official visits to BCA and IFB offices to meet with their presidents; and held informal meetings with academics from Brunei University of Technology.

2. I explained the October event at the BCA office and requested BCA's participation to make the event a success. The chairman is to be the speaker and the others are to be general participants. We also discussed possibilities of cooperation between BCA's Japanese and ASEAN cyber communities.

3. I explained the October event at the IFB office and requested I FB's participation to ensure the success of the event. In this case, I informed them that IFB's participation is business matching, which is possible if there is a solution from Brunei. I also told them that IFB members can be general participants.

Findings:

❶ Send invitations to the BCA president in advance

❷ Update information about the event on the website as soon as possible.

Photo:

1. Informal dinner with BCA committee member and chairman.

2. After meeting at BCA office.

Preliminary report of the first travel survey – Vietnam

The following is a preliminary report of the travel survey conducted.

Purpose of the Survey: Taking advantage of the ASOCIO Board Meeting and DX Summit 2023, we meet with key persons in Vietnam to hear about the status of industry associations related to cyber security in Vietnam. In addition, we will explain about NISC's "ASEAN-Japan Cyber Security 50th Anniversary Event" in October and request their participation.

Survey period: Tuesday, May 22 - Thursday, May 26, 2023

Survey method: On-site survey

Survey person in charge: Seiichi Ito and Yuko Nagano

Survey targets: Industry associations and others related to cyber security in Vietnam.

[1] VNISA (Vietnam Information Security Association) 2023/5/25

[2] MIC（Ministry of Information and Communications）2023/5/25

[3] PIKOM, The National ICT Association of Malaysia 2023/5/23

[4] CISA, Information Service Industry Association of R.O.C. 2023/5/23

[5] ATCI, Association of Thai ICT Industry 2023/5/24

Result of the Survey:

[1] VNISA (Vietnam Information Security Association)

Coordinated by ASOCIO member Mr. Giang, Vice President of VINISA, we met with the VNISA President and others.

Participants:

Ms. Nguyễn Thu Giang - Vice chairwoman cum President of VINASA

Mr. Nguyễn Thành Hưng - Chairman of VNISA

  - Deputy Minister of Information and Communications.

Mr. Khổng Huy Hùng - Vice chairman of VNISA

Ms. Trần Kim Phượng - Chief of Office of VNISA

Mr. Nguyễn Ngọc Toàn - Coordinator

- VNISA was established in 2007.
- There may be other cybersecurity associations, but VNISA is the only one that is in communication with the Vietnamese government.

- In cooperation with Authority of InfoSec/MIC, VNCERT/MIC, VGISC.
- VNISA has 160 members including Government agencies, defense and police departments, banks and financial institutions, telecommunications and utility companies, companies providing information security solutions, consultants, and education, information security experts.
- We briefed NISC "ASEAN-Japan Cyber Security 50th Anniversary Event" in October and requested Mr. Nguyễn Thành Hưng, Chairman of VNISA, to attend. He is willing to attend. (invitation letter required)
- Since the NISC ASEAN-Japan Cyber Security Working Group is scheduled to meet in Vietnam in August, we proposed, and they agreed to organize a follow-up event around that time. (Need invitation as soon as possible). The Japanese side will prepare an invitation to VNISA with specific time, venue, cost, and target audience for the August event. VNISA then makes a proposal to MIC and obtains permission.
- We will receive answers to the questions we submitted in advance (Attachment 1) at a later date. VNISA has conducted a survey on the information security situation in Vietnam and its industries, and the results of the survey will cover half of the questions we have asked.
- We explained about SEACC (South East Asia Cybersecurity Consortium) established by AiSP.
- Vietnam Cybersecurity Day (event) will be held in November this year.
- Winner of last year's security contest (next one to be held in Vietnam)
- Introduction and explanation of JNSA

Result:
VNISA will participate in IC-AJCC – OK
Organizing Follow-up Event - OK

[2] Coordinated by ASOCIO secretariat and VINISA, we visited Vietnam governmental organization – MIC.
Dr. Phan Tam, Deputy Minister
Mr. Nguyen Duc Toan, Official Multilateral Cooperation Department of International Cooperation

- We explained about the "ASEAN-Japan Cyber Security 50th Anniversary Event" and asked the head of the Authority of Information Security to participate in the event.
- We confirmed the progress of the "ASEAN-Japan Cyber Security WG" hosted by NISC to be held in Vietnam and requested that the event be held as scheduled.

[3] Meeting with Mr.Ong Kian Yew, PIKOM -The National ICT Association of Malaysia
- We explained about the "ASEAN-Japan Cyber Security 50th Anniversary Event" and asked for their participation and request to speak at the event.
- Mr. Ong Kian Yew suggested to reserve a slot for "NISC" and "JICA" in the CYDES Malaysia program.
- CYDES Malaysia, to be held in Malaysia from July 10 to 13, is a major cyber security event. https://www.cydes.my
- How about a follow-up event as a side event?

[4] Meeting with CISA - Information Service Industry Association of R.O.C.
Participants:
Mr. Brian Shen, Chairman, CISA
Mr. Lucas Lim, Secretary General, CISA
Ms. Ivy Chang, Deputy Secretary General, CISA
Ms. Louise Li, Project Manager, CISA
- We explained the "ASEAN-Japan Cyber Security 50th Anniversary Event" and asked ASOCIO members to support the ASEAN regional associations.
- How about Mr. Brian Shen, Chairman of ASOCIO, to speak at the event?

[5] Meeting with Mr.Bunrak, ATCI - Association of Thai ICT Industry
- Already met last week.
- Speaker candidates selected.
- Received profiles.

Philippines Cambodia Malaysia preliminary quick repot

May 31st – Jun 9th

Manila Visit

– Survey period: May 31st, 2023 – Jun 2nd, 2023

– Survey method: On-site travel survey

– Survey targets:

  1. HOLY ANGEL UNIVERSITY, where first cybersecurity programs established in the Philippines.
  2. Chairman of Philippine Cert（PH-CERT)

– Survey results:

  1. HOLY ANGEL UNIVERSITY visit:
     – Interviewed Dr Leopardo Jaime (President)、Dr. Marlon Tayag (Cybersecurity and IT Program Chair)
     – Largest university in Pampanga Province.
     – The first university in the Philippines to establish cybersecurity programs (undergraduate and graduate). The ASEAN Institute for Management (AIM) also has a cybersecurity program, but no program in technology.
     – The cybersecurity programs are supported by USAID.
     – There is an association called PICSPRO（Philippines Institute for Cyber Security Professionals）and the leader of PICS PRO in three area (there are twelve areas in Philippines) is Dr. Marlon.
     – Actively conducting cybersecurity events (including CTFs) for students.

  2. Philippine Cert（PH-CERT) visit:
     – Interviewed Mr. Lito, chairman of Philippine Cert.
     – CERT is the first registered non-profit organization in the Philippines.
     – The Philippine government established CERT-Philippines (CERT-Ph) as the national CERT.
     – There are NADPOP（National Association of Data Privacy Officer of the Philippines）, NICP（National IT Confederation of the Philippines）, and PCS（Philippine Computer Society）in the Philippines.
     – PH-Cert works with NADPOP and PCS (Philippine Computer Society).

Manila Visit

– Visiting Photos

※With Dr. Leopardo Jaime (President) and Dr. Marlon Tayag
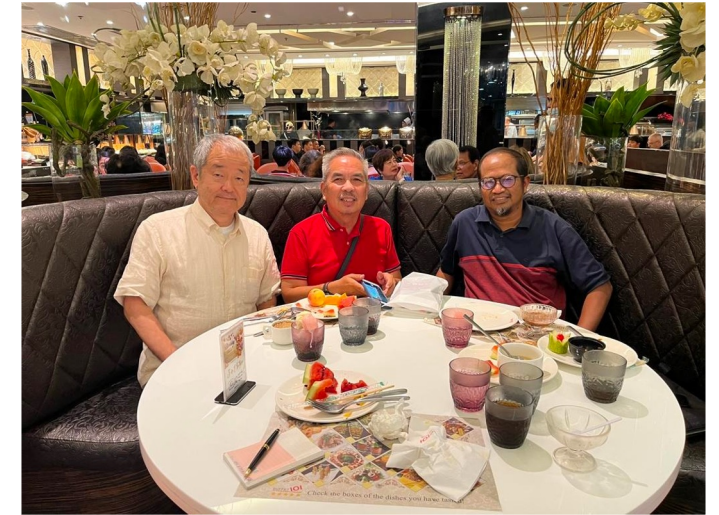
※With Mr. Lito, chairman of Philippine Cert

Phnom Penh Visit

– Survey period: Jun 3rd, 2023 – Jun 7th, 2023

– Survey method: On-site travel survey

– Survey targets:
  1. Mr. Phannarits Ou , Director of Cybersecurity, Ministry of Post and Telecommunication
  2. Mr. Oknha Chin Ken, Chairman of CDTA (Cambodia Digital Technology Association)

– Survey results:
  1. Mr. Phannarits Ou visit:
     – Interviewed Mr. Phannarits Ou, MPT, and Mr. Kim.
     – There is no association dedicated to cyber security in Cambodia.
     – There is a cybersecurity related community called ISAC Cambodia led by Mr. Phannarits Ou (Not legally registered, but active).
     – Participating in October event as ISAC Cambodia and agreed to sign MOU.
     – Helping the October event. Suggested that something like the October event be held annually.
     – Hoping CDTA will also participate.
  2. Mr. Oknha Chin Ken (CDTA) visit:
     – Interviewed Mr. Oknha Chin Ken, Chairman of CDTA and CDTA board members.
     – Members are primarily from the IT industry, but there are also members who specialize in cybersecurity.
     – Wish to participate in the October event. Would like to bring participants from Cambodia.

Phnom Penh Visit

– Visiting Photos

Kuala Lumpur Visit

- Survey period: Jun 7th, 2023 – Jun 9th, 2023

- Survey method: On-site travel survey

- Survey targets:
    1. Mr. Tahrizi Tahreb, who is a co-founder of rawSEC - Malaysia Cybersecurity Community and the head of cybersecurity department at Bank Negara Malaysia.
    2. Dr. Amirudin Abdul Wahab (CEO Cyber Security Malaysia)
    3. PIKOM

- Survey results:
    1. rawSEC visit:
        - Interviewed Mr. Tahrizi Tahreb and others.
        - Non-profit organization.
        - Participated in October event and agreed to sign MOU.
        - Helping the October event.
        - Good connections with the government, especially
        - with the banking industry.

    2. CSM visit:
        - Interviewed Dr. Amirudin Abdul Wahab （CEO of CSM）
        - Can be participated as a speaker by invitation.
        - As a cybersecurity community, called yayasan kesalamatan.

    3. PIKOM visit:
        - Interviewed Mr. Ong Chin Seon, chairman of PIKOM and Mr. Alex Loh, the head of cybersecurity chapter on 8th.
        - WCIT (World Congress) will be held in Malaysia on Oct 5th and 6th. Because Malaysia is the host country of that event and visitors will be gathered from ASOCIO countries, basically PIKOM members are participating WCIT, however, promoted the October event to those in the cybersecurity industry.
        - Mr. Alex Loh himself will also try to make adjustments.
        - Had a meal with PIKOM chairman and board members on 8th.
        - Because Mr. Ong Chin Seon is chairman of PIKOM, he has to prioritize participating WCIT.
        - He is interested but due to overlap with WCIT, he would like to have documents as soon as possible.
        - Had a meal with 10 people of PIKOM members (local service vendors) on 10th.
        - They are interested but due to overlap with WCIT, they would like to have documents as soon as possible.

Kuala Lumpur Visit

With Mr. Tahrizi Tahreb and others

With Mr. Alex Loh at PIKOM

With Dr. Amirudin Abdul Wahab
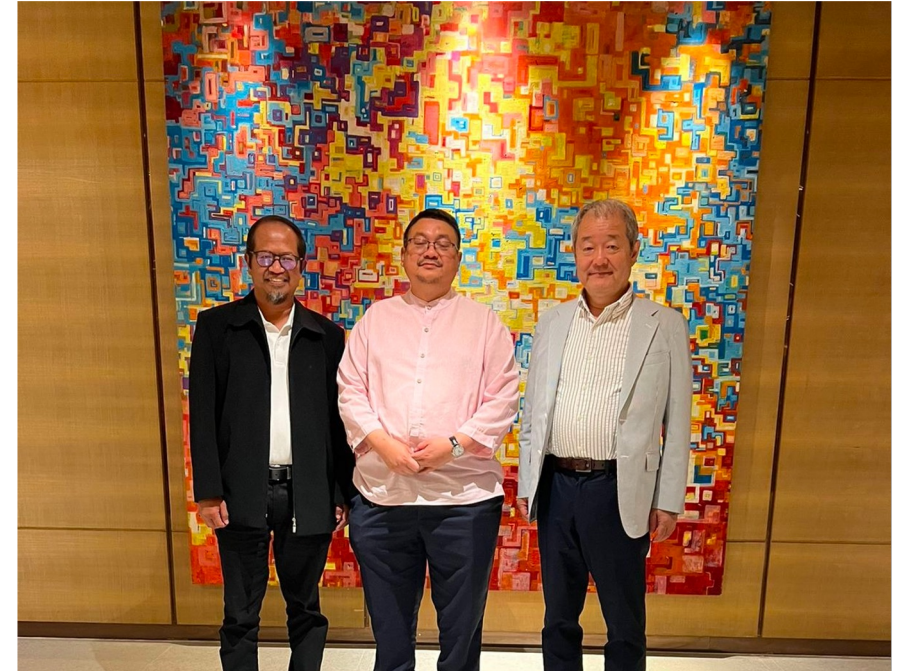
With PIKOM board members

July Executive Summary Report

– Attending CYDES

  – Some Information : NACSA Announcement, Brunei CSB promotion on SEA-CC

– Meet with key person in cybersecurity community in Malaysia

  – Nanosec

  – Rawsec

  – CSM CEO

  – Mr Effendy (Block Chain, IOT asscociation)

– Meet with Mr Prinya and Mr Bunchai, Mr Komain

  – Community Speaker Confirmation and plan about event promotion

  – Business Solution Representative and speakers

– Preparation of Event Promotion in Indonesia and CJI, and welcoming Guest from Philippine

  – Indonesia Event Promotion Seminar Report

Vietnam Singapore preliminary quick repot

Aug 1st – 8th: Hanoi, Vietnam
ASEAN WG, Seminar, Company visit

Aug 16th – 17th: Singapore

August Executive Summary Report

– Attending ASEAN WG, VNISA Seminar, AIS Visit and Local Company Visit in Hanoi
  – Some Information : a question from NACSA about rawSEC
– Update from CyberDSA conference Malaysia
– Meet with SG Tech Security Chapter and AISP Board in Singapore
  – Promoting and presenting IC-AJCC to SG Tech board
  – Inviting and asking for support of SG Tech in term of local solutions
  – Promoting and presenting IC-AJCC to AISP board
  – Confirmation about day 1 attendance and day 2 keynote
– Attending Hack in Taiwan Conference (HITCON) by Taiwan Hacker Association Community
  – How Community make some contribution – Taiwan team rank top 3 in the world (DEFCON 2023)
  – Students get all benefit
– IC-AJCC update

Hanoi Visit:
Aug 1st – 8th

– Photos of ASEAN WG and VNISA Seminar

# Singapore Visit: Aug 16th – 17th

– Photo of SGTECH meeting

Singapore Visit: Aug 16th – 17th

– Photos of CSS and AISP visit
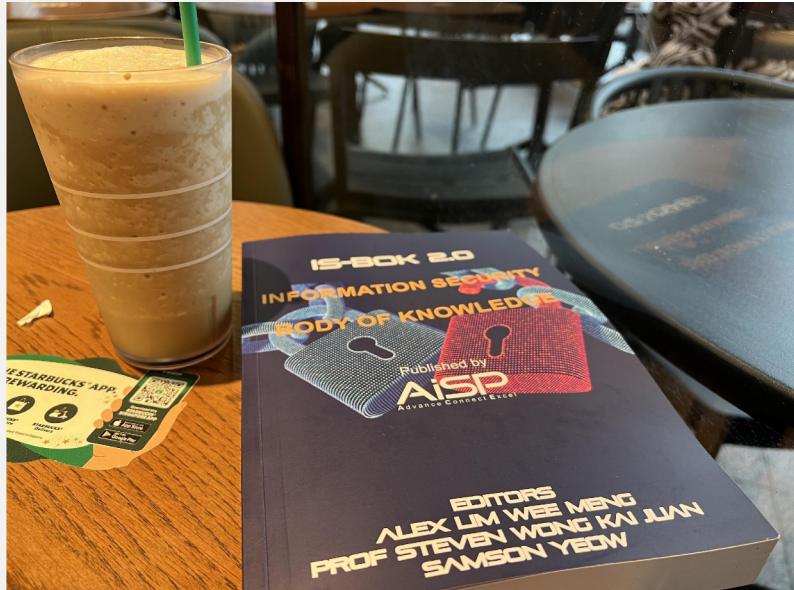
August Executive Summary Report
## Update from CYBER DSA Kuala Lumpur on Aug 6th – 8th
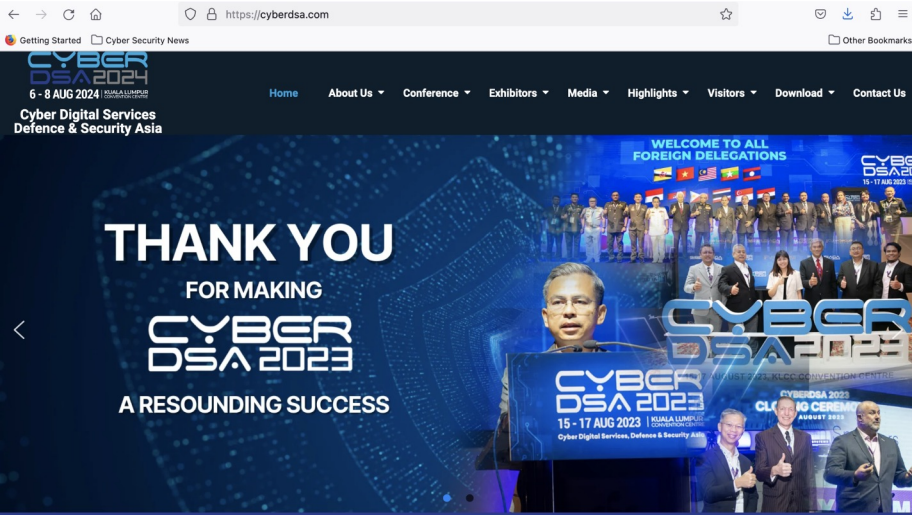
GovWare 2023 Participation Report

Rudi Lumanto

17,18,19 October 2023

GovWare history

- GovWare is one of Asia's premier conferences on cybersecurity and is part of Singapore International Cyber Week. It typically focuses on the latest trends, best practices, and innovations in the field of cybersecurity.

- GovWare, as part of Singapore International Cyber Week (SICW), began in the 1990s. Over the years, it has grown in stature and significance, evolving into one of the premier cybersecurity conferences in Asia.

- GovWare provides various programs and topics so everybody can take benefits for their needs.

- in 2022, The event concluded with unprecedented participation from over 10,000 policymakers, cybersecurity leaders, and cyber practitioners across 65 countries!

GovWare

2023

12,000+	**80+**	**80+**	**130+**
Attendees	Countries	Expert-led Sessions	Global Speakers

2022

10,000+	**35%**	**100+**	**300+**
Total Participants from **65** Countries	Senior Management in Participation	Global Expert Speakers across 90+ Sessions	Exhibitors and Community Partners

2021

2,400+	**60+**	**86%**
Attended GovWare 2021	Countries	Met their objectives

Held In
SG Singapore Passion Made Possible

A Part of
SICW Singapore International Cyber Week

Organised By
image engine

Key Supporting Partner
CSA SINGAPORE

Supporting Organisations
CyberPeace Institute · Cyber Youth Singapore · Singapore Exhibition & Convention Bureau

Supporting Associations
WiSAP Women in Security Alliance Philippines · AiSP Advance Connect Excel · CSA cloud security alliance · APTIKNAS Asosiasi Pengusaha TIK Nasional Indonesian ICT Business Association

APTIKNAS

SFA Singapore Fintech Association · CSCIS Centre for Strategic Cyberspace + International Studies · Brunei Cybersecurity Association · SGTECH Cyber Security Chapter

ISC2 · SCS Singapore Computer Society · ISACA Singapore Chapter · IASA The Business Technology Architect Association

GovWare 2023 key Sponsor : 41

Platinum Plus

Cisco Systems (USA) Pte Ltd
Booth: J08

CrowdStrike Singapore Pte Ltd
Booth: J12

Huawei International Pte Ltd
Booth: H08

M.Tech Products Pte Ltd
Booth: M08

Mandiant
Booth: M12

NCS
Booth: P06

Palo Alto Networks
Booth: G06

PCS Security
Booth: L02

Singtel
Booth: M02

ST Engineering
Booth: H12

Trellix
Booth: L12

Trend Micro
Booth: H02

Platinum

Check Point Software Technologies Ltd.
Booth: L18

F5
Booth: R06

Fortinet
Booth: J18

HPE Aruba Networking
Booth: G02

IBM Corporation
Booth: H18
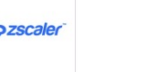
Lenovo Singapore Pte Ltd
Booth: P02

Menlo Security
Booth: G10

NTT
Booth: M18

SentinelOne
Booth: N18

Tanium Singapore Pte Ltd
Booth: P10

Gold

Aqua
Booth: E14

Cloudflare, Pte. Ltd.
Booth: E22

Eclypsium
Booth: O02

ExtraHop
Booth: F08

Imperva
Booth: F01

Infoblox Inc
Booth: E08

LogRhythm
Booth: P14

National Cyber Security Agency - Qatar
Booth: C10

Rubrik
Booth: P18

Samsung
Booth: F17

ServiceNow
Booth: B12

SolarWinds
Booth: Q14

Symantec by Broadcom
Booth: E01

VMware Singapore Pte. Ltd.
Booth: B01

Votiro Cybersec Ltd.
Booth: Q10

XM Cyber
Booth: E09

Zscaler
Booth: E10

GovWare Program Map

Conference Programme

Breakout Track Legends

Refer to the colours below for the corresponding breakout track title.

● Track 1   ● Track 2   ● Track 3

● 2023 Keynote   ● SICW 2023 Open Session   ● CLOUDSEC @GovWare 2023   ● Developments in the Zero Trust Environment

● Cybersecurity Ops Centre   ● Recent Developments in ML/AI Engines   ● How Can Collaborative Partnerships Forge Impactful Synergies In Cybersecurity?

● Endpoint, Mobile & Network Security   ● Governance and Assurance in AI   ● Cybersecurity and Digital Transformation

● Organisational Cybersecurity Culture; The Role of Leadership and Management   ● Managing Crossroads of Data Security, Data Privacy and AI Adoption

● Developing the Cybersecurity Ecosystem, Talent Pipeline and Professionalism   ● Security by Design: Risk Assessment, Avoidance and Mitigation

● Cyber Threat Landscape & Intelligence   ● Darkweb, Cybercrime, Cyberwarfare   ● Operational Technology Threat and Vulnerabilities Landscape

● Building Resilience: Securing Critical Infrastructures and IT Supply Chains   ● Cloud Native Security

17 Oct 2023   **18 Oct 2023**   **19 Oct 2023**

GovWare 2023 Programme Highlights

Benefit for all segments related to cybersecurity

- What is the benefit for the government?
- What is the benefit for private industries, especially local industries?
- What is the benefit for the communities?
- What is the benefit for the people?
- What is the benefit for national and regional security?

What is the benefit for the government?

- **Knowledge Sharing**: GovWare provides a platform for governments to share best practices, strategies, and learnings with their counterparts.

- **Global Networking**: It's an opportunity to form partnerships and collaborations with other nations.

- **Insights into Industry**: The government can gain firsthand knowledge of the latest technologies and solutions in cybersecurity.

- Ecosystem for strengthen national security

What is the benefit for private industries, especially local industries?

- **Business Opportunities**: Private industries can showcase their products and solutions to a global audience.

- **Collaboration**: They can forge partnerships with other businesses or governments, leading to potential joint ventures or projects.

- **Staying Updated**: Industries can stay abreast of the latest threats, technologies, and solutions, ensuring they remain competitive.

What is the benefit for the communities?

- **Awareness**: Communities become more informed about cybersecurity threats and the importance of staying secure online.

- **Education**: Through various events, there's an opportunity for community leaders and members to be educated about best practices.

- **Resilience**: As communities are more informed, they can better defend themselves against cyber threats, leading to a more resilient digital society.

What is the benefit for the people?

- **Education and Awareness**: People gain knowledge about personal cybersecurity, leading to safer online behaviors.

- **Opportunities**: Many events associated with GovWare and SICW offer training, workshops, and certifications, leading to potential job opportunities in the cybersecurity sector.

What is the benefit for national and regional security?

- **Strengthened Defenses**: With knowledge sharing and collaboration, nations can fortify their cyber defenses.

- **Regional Collaboration**: Through GovWare, regional countries can form collaborations to collectively defend against cyber threats, enhancing regional security.

- **Response Mechanisms**: The event helps in formulating better incident response mechanisms through joint exercises and simulations, ensuring quicker and more efficient responses to cyber threats.

GovWare and GCI

GovWare	GCI
1990s | 2023	**2014**: Singapore was ranked 19th. **2016**: Singapore was ranked 6th. **2017**: Singapore achieved 1st place. **2020**: Singapore retained its position at 1st place.

GovWare and GCI relationship

- Interrelated and mutually reinforcing.

- Relationship and relevancy between the two:
    - Demonstration of Commitment
    - Platform for Collaboration
    - Policy and Strategy Formation
    - Promotion of Capacity Building
    - Showcasing Technical Prowess
    - Boosting Confidence

- While the event showcases and reinforces the nation's commitment to cybersecurity, its high GCI rank affirms the effectiveness of its efforts, including the significance of such events.
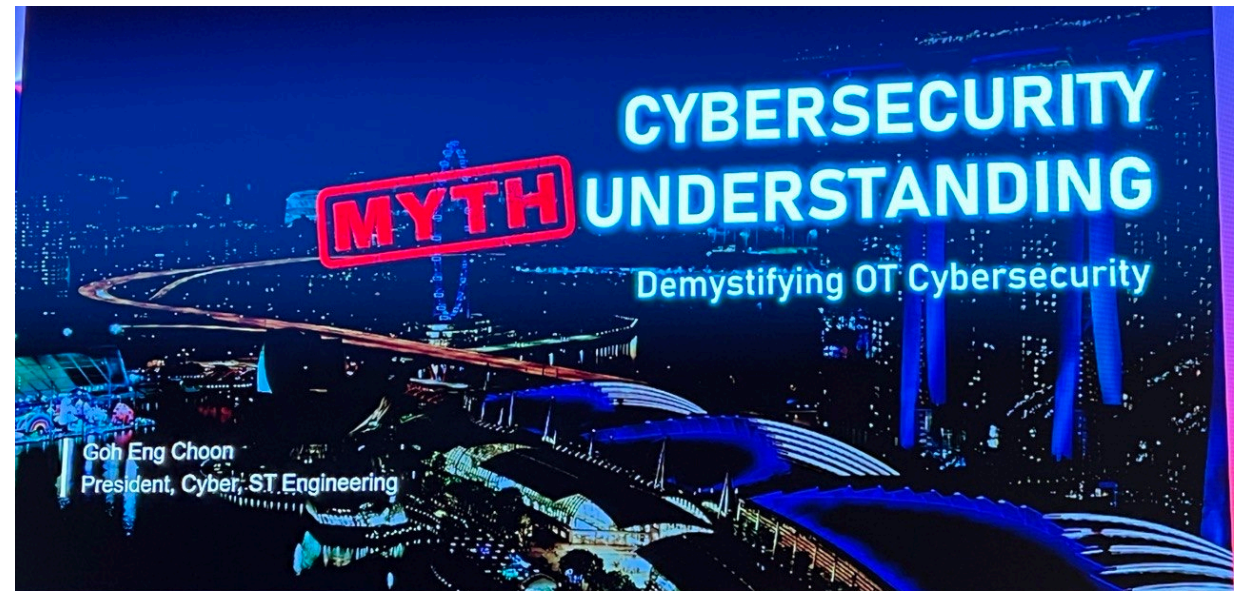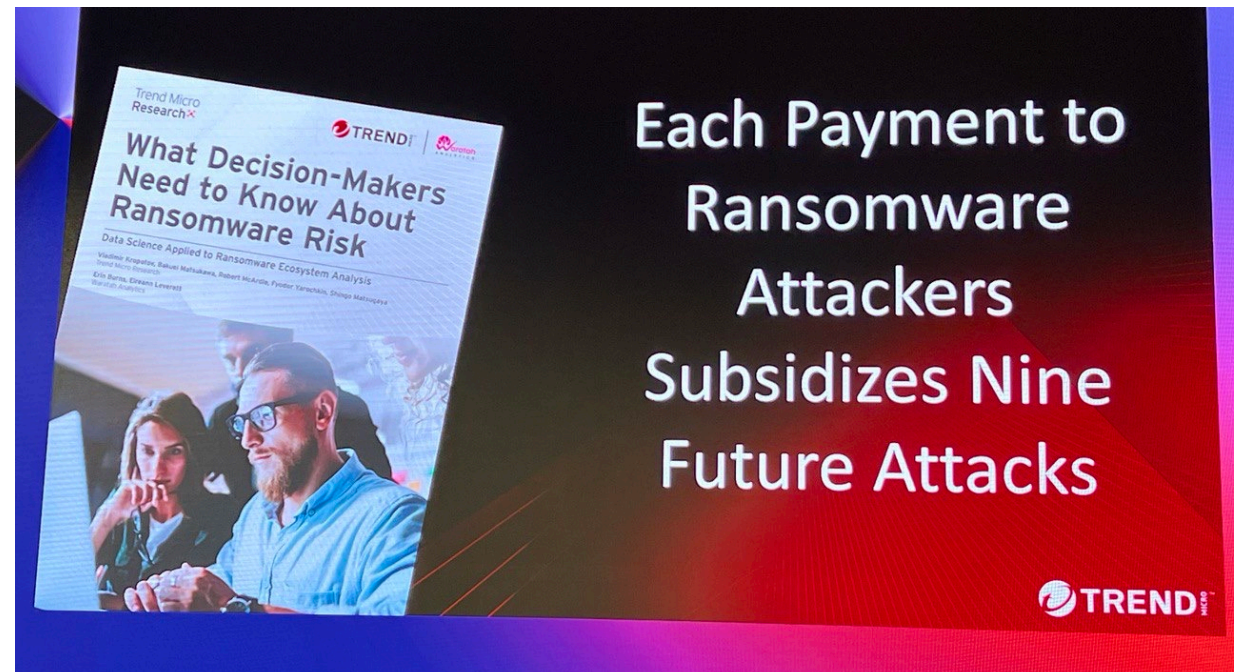
2023 Trends

Cyberwarfare threat

- Japanese respondents exhibited significantly less confidence (33%) in their government's ability to defend against cyberwarfare. (average confidence level was 71%.)

- 66% of Japanese respondents said their organization has programs and practices currently in place specifically designed to respond to cyberwarfare threats. Global average (84%).

Thank you

Survey Report on the Current Cybersecurity Landscape in Laos.

Date: 13 Feb 2024
Prepared for: JICA
Prepared by: Rudi Lumanto and Ito Seiichi (JTEC)

(1) Public and Private View Comments

(1.1) Interview with **Mr Thanousone Phonamat**, Vice President, Lao National Chamber of Commerce and Industry and President, Lao ICT and Digital Association (LIDA)

- Mr Thanousone also the owner of ALO company (E-commerce), Planet (the first ISP for enterprise,broadband), and four more other company. Planet is only focus to enterprise and SME providing broadband through Fiber (FTTH).
- Lida have around 50 member (company) and security chapter is only one company : cyberus
- have three monthly meeting called Digital Forum, included cybersecurity as one of the theme.
- Based on the Law in Lao, to establish association need min 40 member (company)
- E-commerce grow slowly because people still like using socio commerce (direct chat)
- Mr Thanousone also very busy this year preparing ABIS (ASEAN Business Investment Summit) that will be held on October this year, in conjunction with ASEAN leader's summit.
- open cyber security business is easy in Lao, as it is allowed to foreign people to build even 100% share. But the other sector like telecommunication may be restricted by government.

(1.2) Interview with Frank Sengxay Xayachack: Founder and CEO of Cyberus Company

1. Cyberus company already running 2 years. owned by Frank himself and now have 10 employees.
2. Core business is security assessment, before he already made a company with same core business but not running well. Now he owns this business alone and fortunately since last year the business is growing very well. more than 10 clients from bank, telecom operator to SMEs. Security assessment cover mainly web applications not yet to cloud or other.
3. Frank have his own community called Lao Hacker Club, which have gathering meeting every month. Many university students become member of this club, but come and go, and active members are around 40. This community also help government in making infrastructure for annual CTF competition.
4. Via Lao Hacker Club, they also supervising Student Cybersecurity Club in Lao University and Soutsaka College.
5. Frank and the other 3 member of his company has OSCP certification, they can afford the exams and also sometime attending course using scholarship program of BAF (Europe, help 50% donation of the cost)

6. Frank is independent and self-funded, not rely on government in his community activities, really happy if his community can join AJCCA.

7. He does not know about number of cyber incidents or big cyber incidents in Lao because he said most of the incident does not publish, and maybe controlled by government.

8. In case of ransomware, he suggests his customer to prepare back up and give guidance about how to do back up. if ransomware happen, then they just must accept the consequences.

(1.3) Interview with Mr Khamla Sounnalat, Director General of Lao CERT of Ministry of Technology and Communication, LAO P.D.R

1. Cybersecurity in Lao is under his department which included Lao CERT.

2. Now his department is located in LaNIC building (Lao Network Internet Center). LaNic as it serve for public, their office also then easily can be accessed by public and make them think it is not good for them as operating Lao Cybersecurity Services. Kamla think it is better if they can have annother financial support to have their own building separate from public services.

3. Total Empoyee he has around 20-30 people included in Lao Cert is 5 people. most of them does not have professional cyber security certification so certification is important needed right now. He would like to get JICA support in training his staff in JICA program with UI in Indonesia.

4. Regarding the community that can be recommended to join to AJCCA, he would like to get an email inform the need, criteria, and benefit so he can ask permission to department to recommend or supervising the local community to AJCCA

(2) KEY FINDINGS

- There is a cybersecurity community in Laos called LAO HACKER
- There is an increase demand of cybersecurity assessment in last two years from bank, telecommunication and SMEs
- Lack of cybersecurity capacity both in public and private
- Socio Commerce is still dominant
- Laos will host ASEAN LEADERS Summit with many other events in conjunction that. This open Laos many opportunities to speed up Country Development included in Cybersecurity

(3) RESULT ON CURRENT STATUS OF CYBERSECURITY IN LAOS
Public and Private View on Five Important Issues

no	Questions	Public (DG Cybersecurity MTC)	Private (LIDA)
1	Are there any big chances in cyber security environment in the country within this 1-2 year, for example new law, new regulation, new agency etc. ?	Yes	There are still very few companies operating cybersecurity service. Public awareness is still very low and the demand to pay for such service is low, partly is because

			of the digitalisation is still at the entry level.
2	Is there any big threats or cyber-attacks that bothering the people? What are current popular cyber-attacks?	Doesn't have yet	Big threats are scams, virus infection and data got stolen.
3	Are there communities or association involved in cyber security activities in the country? How many?	Commonly no	Public sector has set up one department specifically looking after cyber security. From the private sector, there are only two companies within our association focusing on this subject.
4	How is the acceptance of the people to cyber security solutions?	Need more awareness	Currently, not so many people in Laos are aware of the importance of cyber security and prepare to spend some of their money to pay for the cybersecurity solution. Many large companies are still keeping their sensitive data offline or in a private cloud.
5	Who is the famous or popular person or institution in the country if we are talking about cyber security?	Suggest to have meeting with team in Department of cybersecurity	For private side is Mr. FRANK FOR PUBLIC SECTOR SIDE IS Mr. KHAMLA THE DG in ministry of technology and communications

6. SUMMARY

The survey findings underscore the emergence of a nascent cybersecurity community in Laos, exemplified by the presence of LAO HACKER, indicative of growing grassroots interest and expertise in combating cyber threats. Over the past two years, there has been a noticeable surge in demand for cybersecurity assessments across key sectors such as banking, telecommunications, and SMEs, reflecting heightened awareness of cyber risks and the imperative to fortify digital defences. However, these aspirations are hampered by a glaring deficiency in cybersecurity capacity, both within public institutions and the private sector, highlighting an urgent need for concerted efforts to enhance expertise and infrastructure.

Furthermore, amidst the prevailing socio-commerce landscape, characterized by the fusion of social media and e-commerce platforms, Laos stands at a pivotal juncture poised to leverage digital advancements for economic development. The upcoming ASEAN LEADERS Summit and associated events present a unique opportunity for Laos to accelerate its cybersecurity agenda and broader national development objectives. By capitalizing on these platforms to foster

collaboration, knowledge exchange, and resource mobilization, Laos can position itself as a regional leader in cybersecurity, catalysing sustainable growth and resilience in the digital age.