BRUNEI CYBERSECURITY ASSOCIATION

EMPOWERING A SECURE DIGITAL FUTURE: BRUNEI CYBER SECURITY ASSOCIATION (BCSA)

MD AZAD ZAKI HAJI MOHD TAHIR
PRESIDENT BCSA

"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."

Welcoming Remark, 1st Brunei Cybersecurity Conference (CYSEC) 2023

The Executive Committees below represents each respective sectors (both public and private)

VICE-PRESIDENT
- Name: Hakim (EGNC)
- Initial 2 years term

SECRETARY
- Name: Serina (UTB)
- Initial 2 years term

TREASURY
- Name: Mira (BSP)
- Initial 2 years term

+VICE-PRESIDENT
- Name: Azizul (BGC)
- Initial 1 year term

ASSISTANT SECRETARY
- Name: Zulfadly (Anak.IT)
- Initial 1 year term

ASSISTANT TREASURY
- Name: Rohani (IBTE)
- Initial 1 year term

ORDINARY COMMITTEE MEMBER
- Name: Nisa (BLNG)
- Name: Nomi (ITPSS)
- Name: Farah (ITPSS)
- Initial 2 years term

NOMINATED MEMBERS
- Name Sazwi - CSB
- Name: Amsyar - MTIC
- Name: Hj Azlan (PA)
- Name:
- Name
- Initial 2 years term

ORDINARY COMMITTEE MEMBER

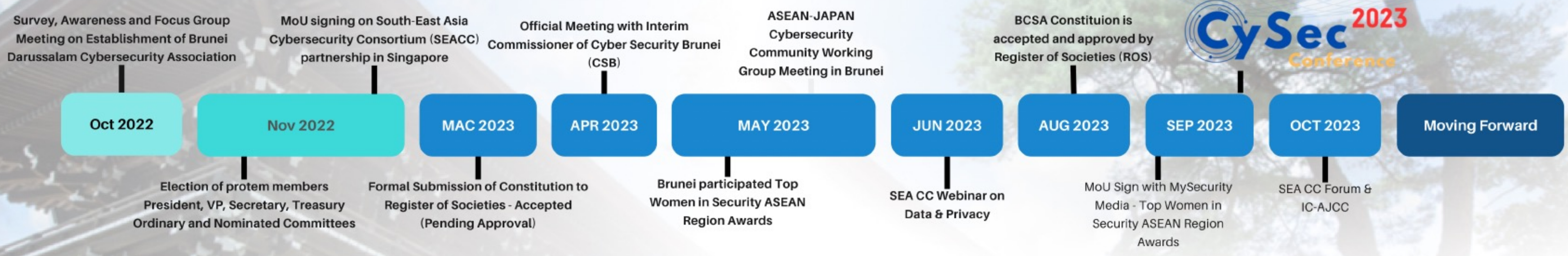
Name: Zack (TAP)
Name: Abdul Rahman (Deloitte)
Name: Yusof Sidek (BIBD)
Name: Hafizah (Dynamik)
Initial 1 year term

* Voting rights
* Assigned to lead particular initiatives as well as the workplan of the association.

50th Year of ASEAN-Japan Friendship and Cooperation

BRUNEI
CYBERSECURITY
ASSOCIATION

OUR VISION: BUILDING A RESILIENT CYBERSECURITY ECOSYSTEM



- Oct 2022: Survey, Awareness and Focus Group Meeting on Establishment of Brunei Darussalam Cybersecurity Association
- Nov 2022: Election of protem members President, VP, Secretary, Treasury Ordinary and Nominated Committees
- Nov 2022: MoU signing on South-East Asia Cybersecurity Consortium (SEACC) partnership in Singapore
- MAC 2023: Formal Submission of Constitution to Register of Societies - Accepted (Pending Approval)
- APR 2023: Official Meeting with Interim Commissioner of Cyber Security Brunei (CSB)
- MAY 2023: Brunei participated Top Women in Security ASEAN Region Awards
- MAY 2023: ASEAN-JAPAN Cybersecurity Community Working Group Meeting in Brunei
- JUN 2023: SEA CC Webinar on Data & Privacy
- AUG 2023: BCSA Constituion is accepted and approved by Register of Societies (ROS)
- SEP 2023: MoU Sign with MySecurity Media - Top Women in Security ASEAN Region Awards
- SEP 2023: CySec 2023 Conference
- OCT 2023: SEA CC Forum & IC-AJCC
- Moving Forward

The Brunei Cybersecurity Association is committed to:

CYBERSECURITY AWARENESS

Promoting Cybersecurity Awareness

CYBER SKILLS AND GROWTH

Facilitating Skill Development

CYBER SHIELD COLLECTIVE

Encouraging Collaboration

Cybersecurity Policy and Regulations

Advocating for Policy and Regulation

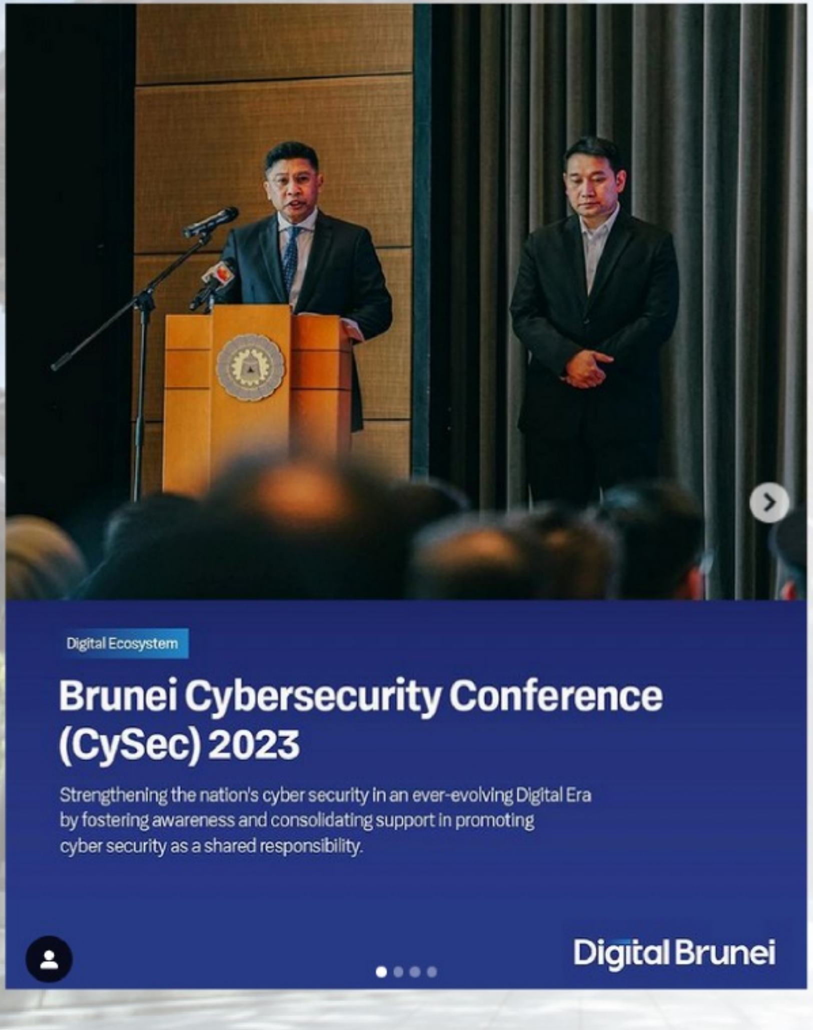
CySec 2023 Conference

Annual Brunei Cybersecurity Conference

50th Year of ASEAN-Japan Friendship and Cooperation

BRUNEI
CYBERSECURITY
ASSOCIATION

JOIN US IN BUILDING A SAFER DIGITAL WORLD

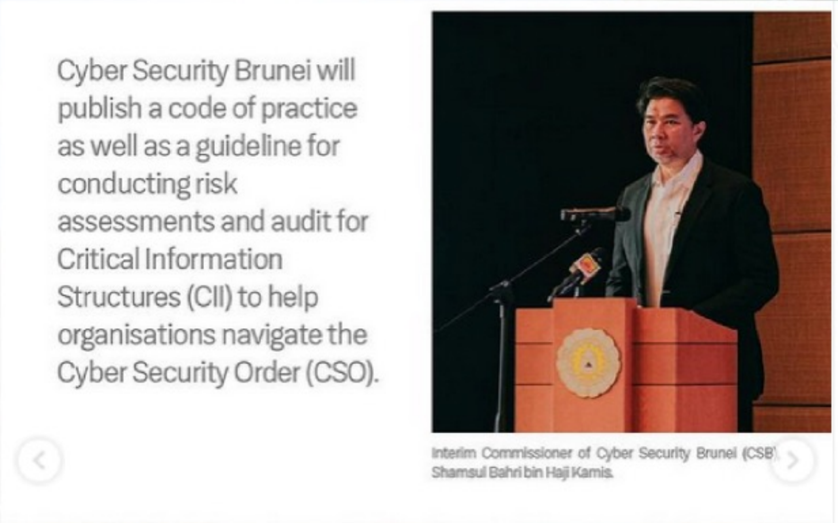


Digital Ecosystem

Brunei Cybersecurity Conference (CySec) 2023

Strengthening the nation's cyber security in an ever-evolving Digital Era by fostering awareness and consolidating support in promoting cyber security as a shared responsibility.

Digital Brunei



Cyber Security Brunei will publish a code of practice as well as a guideline for conducting risk assessments and audit for Critical Information Structures (CII) to help organisations navigate the Cyber Security Order (CSO).

Interim Commissioner of Cyber Security Brunei (CSB) Shamsul Bahri bin Haji Kamis.

CySec
فرسيداڠن كسلامتن سيبير بروني
BRUNEI CYBERSECURITY CONFERENCE (CYSEC)
SECURING THE DIGITAL FRONTIER: NAVIGATING CYBER CHALLENGES

Contact Us

Thank you for your interest in the Brunei Cyber Security Association (BCSA). We value your feedback, inquiries and suggestion. Please feel free to get in touch with us using the information below:

General Inquiries:

✉ Email: pksbrunei@gmail.com

☎ Phone: +6732458000

Address: Simpang 69 Jalan E-Kerajaan,
Kampung Beribi Gadong, BE1110
Brunei Darussalam

Connect with Us:

@bcsa.bn

https://www.linkedin.com/in/bcsabn

50th Year of
ASEAN-Japan
Friendship and Cooperation

Improving Cybersecurity Capacity through Cyber Community

Phannarith OU

Chairman, ISAC-Cambodia

ISAC–CAMBODIA

CYBERSECURITY SHARING PLATFORM

50th Year of ASEAN-Japan Friendship and Cooperation

ISAC-Cambodia

- Founded: 01st January 2016
- The first and biggest Cybersecurity Community in Cambodia
- We have around 10K+ Subscribers and Virtually 80K Members

> “To become trusted platform for cybersecurity professionals in Cambodia.”

50th Year of ASEAN-Japan Friendship and Cooperation

OBJECTIVES

- 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

50th Year of
ASEAN-Japan
Friendship and Cooperation

OUR PROGRAMS

SecuDemy.com

Security Starts with You

CYBER YOUTH CAMBODIA

THANK YOU

Phannarith OU

Chairman, ISAC-Cambodia

ISAC–CAMBODIA

CYBERSECURITY SHARING PLATFORM

50th Year of ASEAN-Japan Friendship and Cooperation

idNSA and the collaboration mindset

Rudi Lumanto

rudi@idnsa

50th Year of ASEAN-Japan Friendship and Cooperation

Our Digital Footprints and Driving Forces

- Started as Cyber Security Research Circle in 2011, registered legally in 2017 as non-profit, community based.

- Three beliefs :

  - The role of community is very important in making safer and secure cyber space
  - keeps on learning because cyber space keeps on growing
  - contribution in strengthening the weakest link

Community Services

- Online Cybersecurity News
- Self Assessment Digital Literacy index
- Secure online video conference
- Every Body Can Hack Workshop Series
- Risk Management and Security Solution seminar Series
- idNSA Academy
- Supporting System of Cyber Jawara National and International Hacking Contest

- International and National cooperation and particpation
  - JNSA
  - Blackhat Asia
  - Communic Asia
  - Big Data and AI Asia
  - Cyber Security Indonesia
  - Codebali
  - World Congress on Innovation and Technology (WCIT)
  - Security Blaze
  - etc

idNSA INDONESIA NETWORK SECURITY ASSOCIATION

50th Year of ASEAN-Japan Friendship and Cooperation

Our thought about "collaboration for a cyber safe ASEAN Japan Community"

- Due to the current cyber threat landscape, collaboration and cooperation is much more needed right now than before.
- G to G collaboration up to now enhance the foundation and C to C will boosting the safer and secure environment, it strengthens the foundation to the outreach layer
- Collaboration also means doing together, It is not what Japan can do for ASEAN but what Japan can do with ASEAN
- Community means people, and people to people ties are source of strength and we strongly believe that this new collaboration is committed to these ties

50th Year of ASEAN-Japan Friendship and Cooperation

RA://SEC

Malaysia Cyber Security Community

ABOUT US

Envision to built a repertoire of Information & Cyber Security Professional as well as providing a platform to groom local cyber security talents.

RA:// SEC
Malaysia Cyber Security Community
RA:// SEC
Malaysia Cyber Security Community

Cyber Security

Outreach Provider

of The Year 2023

ACTIVITIES

We are a community that nurtures and develops talent among our members.

Monthly Meetup

Conference

Technical Workshop

Webinar

PH
CERT
Philippine Computer
Emergency Response Team
Coordinating Center

Philippine Computer Emergency Response Team (PHCERT/CC)

ANGEL S. AVERIA, JR.

President

PH.. WHO?

MANUFACTURING

CONSULTANTS

CIVIL SOCIETY ADVOCATES

FINANCE

VENDORS

TELCO

GOVERNMENT

PH CERT

Philippine Computer
Emergency Response Team
Coordinating Center

INFORMATION SECURITY PROFESSIONALS WITH "DAY JOBS"

PH CERT

Philippine Computer
Emergency Response Team
[Est. 2001]

The Philippine's First Information Security Community of Practice

Primary Purpose & Advocacy

To increase the awareness for Information Security (InfoSec) and Cybersecurity; develop an inclusive Information Security and Cybersecurity Workforce; and adopt InfoSec and Cybersecurity standards, and best practices to uplift their practice in the Philippines and the Asia-Pacific Region.

Platform for Volunteers

It provides its members a platform and venue to learn from each other and hone skills in the field of InfoSec and Cybersecurity, and to serve as a coordinating body in addressing information security incidents. PH-CERT also provides InfoSec advisories and alerts to its community volunteers.

Flagship Initiatives

PH CERT Philippine Computer Emergency Response Team Academy Est. 2001

PH CERT Philippine Computer Emergency Response Team Certified Information Security Essentials Specialist

PRIVACY FRIDAYS & FIGHTBACK CYBERSECURITY

CyberSecConPH

✉ aaveria@phcert.cc

f PHCERT

PHCERT/CC

Organized at the Turn of the Century

- YES. We are THAT OLD! – Today we say ‘LEGACY’
- Registered with the Phil. Securities and Exchange Commission on March 15, 2001

Once Recognized as the National CERT

- VIA the CICT – 2004 ASEAN TELMIN Conference

Founding Member of APCERT

- Asia Pacific CERT established in 2003

Volunteers with Law Enforcement

- NBI: Cybercrime Division
- PNP: Anti-Cybercrime Group

Legislation and Policy Development

- RA 8792 (eCommerce Act)
- ITECC Subcommittee Co-Chair (2001-2004)
- RA 10175 Cybercrime Prevention Act
- RA 10173 Data Privacy Act
- RA10844 DICT Act
- DTI-BPS (Certification of Certification Authorities, National Standards for Information Security Management)
- Congress/Senate: Technology Subcommittees
- Supreme Court eCommerce Sub-committee and Committee on Rules (Rules on Electronic Evidence, Electronic Filing, and eNotary)
- National Competitiveness Council
- National Movement on Free Elections (NAMFREL)
- COMELEC Advisory Council
- Presidential Task Force on Critical Infrastructure (2004)
- National Information and Communication Technology Advisory Council (NICTAC)

Awareness and Education

- JPCERT: IRT Creation and Management (2009,2011), Secure Coding (2010)
- DOJ/US-DOJ (OPDAT): Digital Forensics and Electronic Evidence Training for Prosecutors
- PHILJA/US-DOJ (OPDAT): Technical Aspects of Cybercrime
- DOJ/COE: Global Action on Cybercrime (GLACY) Project for Prosecutors, Judges, and Law Enforcement
- Kingdom of TONGA: Cybercrime, Electronic Evidence, CERT establishment assistance

NADPOP

National Association of Data Protection Officers of the Philippines [Est. 2018]

The Philippine's First Data Privacy & Cybersecurity Community of Practice

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

Flagship Initiatives

PRIVACY FRIDAYS & FIGHTBACK CYBERSECURITY

PRIVACY FRIDAYS
FIGHTBACK CYBERSECURITY
4th ANNUAL DATA PRIVACY & CYBERSECURITY YEAR ENDER PART 2
December 17, 2021 | Friday | 7pm
Data Privacy & Cybersecurity in the
METAVERSE
KEYNOTE SPEAKERS
NADPOP

✉ privacy@nadpop.org   🌐 nadpop.org

Information Security Essentials Certification (ISEC)

ISEC

INFORMATION SECURITY ESSENTIALS CERTIFICATION

Interested to go into or learn more about Information Security but don't know where to start?

Information Security is the only field that cuts across all of the IT Disciplines. Be it Networks, Systems, Application Development, Physical Infrastructure and even in the Cloud!

It is ABSOLUTELY important that you start your journey into INFOSEC on the right foot and solid foundation.

FOUNDATIONAL KNOWLEDGE

The topics included in the course will provide you with all the important concept you need to know to effectively understand the rudiments of Information Security.

1. Security and Risk Management
2. Asset Security
3. Security Architecture & Engineering
4. Communication & Network Security
5. Identity and Access Management
6. Security Assessment and Testing
7. Security Operations
8. Software Development Security

* Infosec 8-Common Bodies of Knowledge

https://phcert.cc

PH CERT

Philippine Computer
Emergency Response Team
Coordinating Center

Angel S. Averia, jr.

asaveria@phcert.cc

fb.me/phcert

twitter.com/phcert

どうもありがとうございます　MARAMING SALAMAT PO!

AiSP

Advance Connect Excel

Collaboration for a Cyber-safe ASEAN –Japan Community

Association of Information Security Professionals

AiSP
Advance Connect Excel

OUR VISION A safe cyberspace supported by a strong and vibrant cybersecurity ecosystem

- Founded in 2008, the **Association of Information Security Professionals** (AiSP) is a non profit, independent cybersecurity association that believes in:

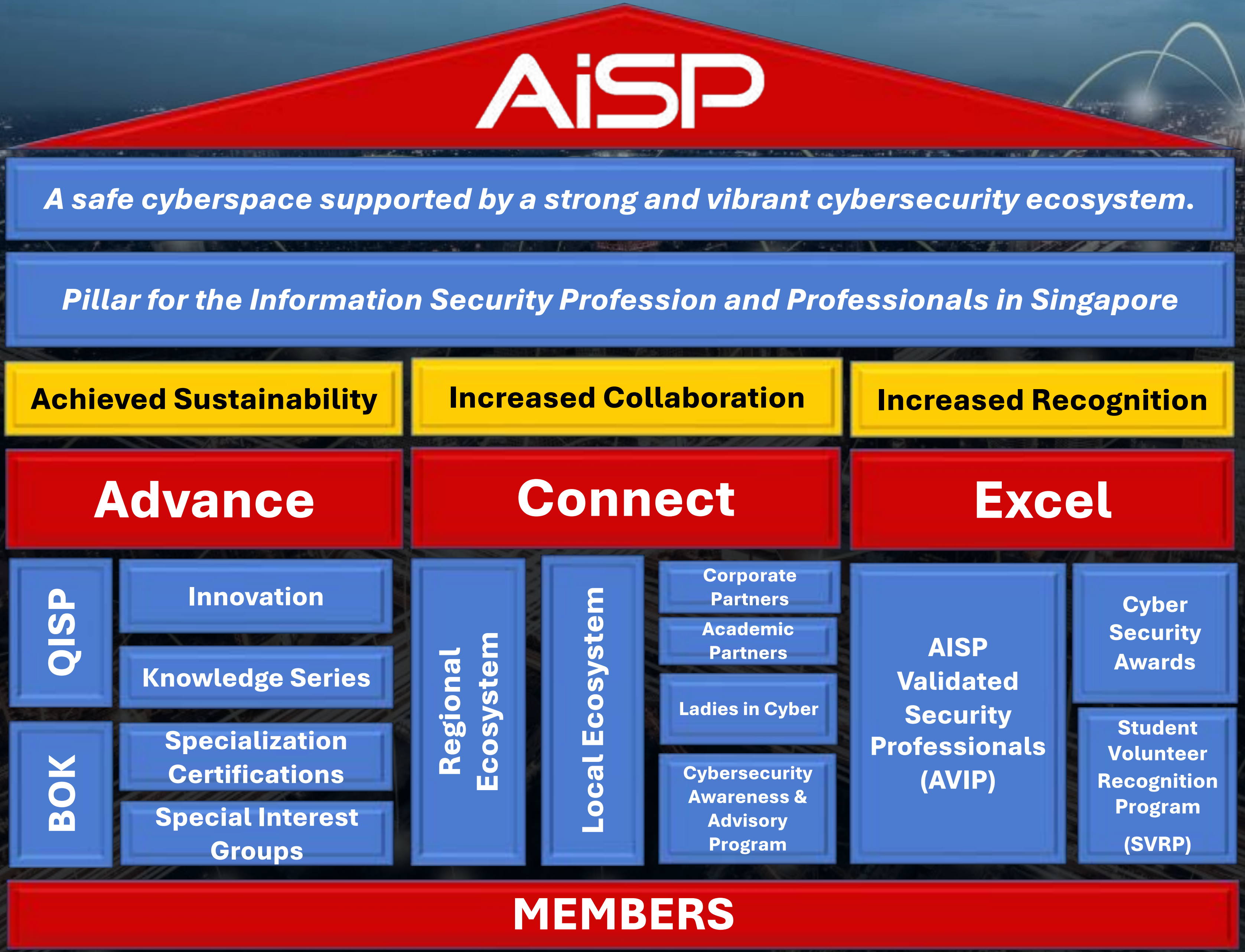
developing, supporting and enhancing industry technical competence and management expertise

promoting the integrity, status, and interests of Information Security Professionals in Singapore

developing, increasing and spreading of cybersecurity knowledge to shape more resilient economies

AiSP

Advance Connect Excel



AiSP

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

Pillar for the Information Security Profession and Professionals in Singapore

Achieved Sustainability | Increased Collaboration | Increased Recognition

Advance

- QISP
- BOK
- Innovation
- Knowledge Series
- Specialization Certifications
- Special Interest Groups

Connect

- Regional Ecosystem
- Local Ecosystem
- Corporate Partners
- Academic Partners
- Ladies in Cyber
- Cybersecurity Awareness & Advisory Program

Excel

- AISP Validated Security Professionals (AVIP)
- Cyber Security Awards
- Student Volunteer Recognition Program (SVRP)

MEMBERS

Vision

Mission

Strategic Goals

Strategic Thrusts

Increased Collaboration

Connect

AiSP
Advance Connect Excel

LOCAL & REGIONAL ECOSYSTEM

- ✓AiSP has established MOU PARTNERSHIP with local and overseas organisations to promote cooperation and collaboration, including co-creating joint initiatives or participating in and benefiting from each other's respective initiatives.
- ✓The aim is to create a vibrant and dynamic international information and cybersecurity ecosystem, and to provide the linkage between government, Industry, communities and Individuals.

Thailand Information Security Association (TISA)

ASEAN Hot IT/Cyber Topics in 2023

Cybersecurity Culture	Generative AI (ChatGPT/Bard)	Data Science	Data Security Data Privacy	Data Governance	Data Resilience
Digital Literacy/ Digital Inequality	Mobile/ Social Media Services	Internet of Things (IoT)	Information of Things	Big Data Analytics	Data Sovereignty
Cyber Literacy	Cloud Service	Cloud Security	Digital Twin	Metaverse	Over-the-Top Regulation (OTT)
Cyber Resilience	Cyber Drill Cyber Range	Cyber Sovereignty	Information & Technology (I&T)	Operational Technology (OT)	Shadow Data Shadow IT

Regulatory Compliance, RegTech, InsurTech

History & Revolution of Cyber Domain

1st Gen : Computer Security (1986)

2nd Gen : Information Security (2005)

3rd Gen : Cybersecurity (2013)

4th Gen : Cyber Resilience (2011/2023)

5th Gen : Cyber Dominance (2020/2030)

UN Global Digital Compact (GDC) 2023

1. Digital inclusion and connectivity
2. Internet governance
3. Data protection
4. Human rights online
5. Digital trust and security
6. AI and other emerging technologies
7. Global digital commons
8. Accelerating progress towards the SDGs

About us

Description:

Thailand Information Security Association (TISA) is the Non-profit association for information security/cybersecurity/cyber resilience professionals in Thailand since 2007

Vision:

Thailand Information Security Society is Trusted Globally

TISA Mission:

Develop Thailand's Information Security processes and professionals to achieve international standards

Vision

TISA Objectives:

- Develop information security best practice and process standards for Thailand situation
- Develop Code of Conduct for Thailand’s **information security/cybersecurity/cyber resilience** professionals
- Develop proficiency test and certify professionals to work in information security roles
- Guide the practice of information security based on Governance, Risk Management, and Compliance (GRC)
- Promote awareness and knowledge relating to information security, cybersecurity & cyber resilience
- Collaborate with other agencies in improving the level of information security in Thailand

TISA Committee 2023

1	Police Colonel Yanaphon Yongyuen	President	
2	Narinrit Prem-Apiwathanokul	Vice President	
3	Chuchai Vachirabanchong	Vice President	
4	Wanawit Ahkuputra	Vice President	
5	Dr.Pattarawan Prasarnphanich	Committee	
6	Pol.Lt.Col. Manupat Sriboonlue	Committee	
7	Pol.Lt.Col.Narin Phetthong, PhD	Committee	
8	Sompop Sukprasong	Committee	
9	Napat Aruntana	Committee	
10	Kasipat Thanitthanakhun	Committee	
11	Associate Professor Pongpisit Wuttidittachotti, Ph.D.	Committee	
12	Mr. Wasasus Chawalitthamrong	Committee	
13	Sommai Fongnamthip	Committee	
14	Asst.Prof. Dr. M.L.Kulthon Kasemsan	Committee and Secretary	

Honorary Advisor 2023

1	Mr. Metha Suvanasarn	Honorary Advisor	
2	General Bunjerd Tientongdee	Honorary Advisor	
3	Ms. Chutima Nimsuwan	Honorary Advisor	
4	Dr. Prinya Hom-anek	Honorary Advisor	
5	Dr. Yunyong Teng-amnuay	Honorary Advisor	

6	Mr. Surachai Chatchalermpun	Honorary Advisor	
7	Dr. Rom Hiranpruk	Honorary Advisor	
8	Dr. Kumpol Sontanarat	Honorary Advisor	
9	Dr. Vites Techangam	Honorary Advisor	
10	Dr. Sutee Tuvirat	Honorary Advisor	

TISA – Event 2007-2023 (17 years)

TISA – Event 2007-2023 (17 years)

กิจกรรมวิชาการ

TISA Pro Talk

โดยสมาคมความมั่นคงปลอดภัยระบบสารสนเทศ

พ.ต.อ. ญาณพล ยั่งยืน

ประธานจัดงาน

ข้อมูลส่วนบุคคล...ดูแลอย่างไรให้ปลอดภัย

พบกับการเสวนาออนไลน์ในหัวข้อ

DNS Security and Privacy in PDPA Compliance Perspective

วิทยากรผู้ทรงคุณวุฒิ

ดร.ธรรอง เต็งอำนวย

อ. ปริญญา หอมเอนก

คุณพีญูกรี อรุณวัฒนามงคล

คุณภาคภูมิ ไตรพัฒน์

คุณชยา ลิมจิตติ

ลงทะเบียน Click

พบกันวันที่ 6 สิงหาคม 2563

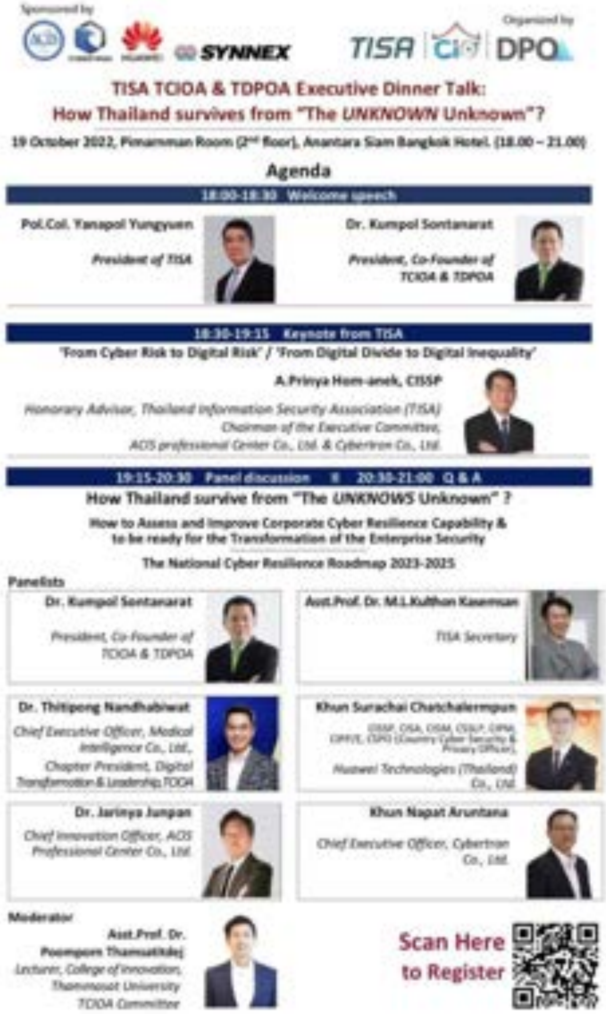
เวลา 19.00 – 21.00 น.

TISA

CSP

TISA
PRO-TALK
TISA Pro-Talk ครั้งที่ 1/2559
"Ransomware Incident Management &
RSA Conference 2016 Experience Sharing"
พุธที่ 27 เมษายน 2559 เวลา 18:00 – 21:00 น.
อง 2201 ชั้น 22 ศูนย์ศึกษาวิภาวดี มหาวิทยาลัยรัง
อาคาร ทีเอสที ทาวเวอร์ ถนนวิภาวดีรังสิต
กำหนดการกิจกร
ทะเบียน

TISA – Event 2007-2023 (17 years)



Sponsored by

SYNNEX

Organized by

TISA | CIO | DPO

TISA TCIOA & TDPOA Executive Dinner Talk:
How Thailand survives from "The *UNKNOWN* Unknown"?

19 October 2022, Pimanmman Room (2nd floor), Anantara Siam Bangkok Hotel. (18.00 – 21.00)

Agenda

18:00-18:30 Welcome speech

Pol.Col. Yanapol Yungyuen
President of TISA

Dr. Kumpol Sontanarat
President, Co-Founder of TCIOA & TDPOA

18:30-19:15 Keynote from TISA

'From Cyber Risk to Digital Risk' / 'From Digital Divide to Digital Inequality'

A.Prinya Hom-anek, CISSP
Honorary Advisor, Thailand Information Security Association (TISA)
Chairman of the Executive Committee,
ACIS professional Center Co., Ltd. & Cybertron Co., Ltd.

19:15-20:30 Panel discussion II 20:30-21:00 Q & A

How Thailand survive from "The *UNKNOWS* Unknown" ?

How to Assess and Improve Corporate Cyber Resilience Capability &
to be ready for the Transformation of the Enterprise Security

The National Cyber Resilience Roadmap 2023-2025

Panelists

Dr. Kumpol Sontanarat
President, Co-Founder of TCIOA & TDPOA

Asst.Prof. Dr. M.L.Kulthon Kasemsan
TISA Secretary

Dr. Thitipong Nandhabiwat
Chief Executive Officer, Medical Intelligence Co., Ltd.,
Chapter President, Digital Transformation & Leadership,TCIOA

Khun Surachai Chatchalermpun
CISSP, CISA, CISM, CSSLP, CIPM, CIPP/E, CSPO (Country Cyber Security & Privacy Officer),
Huawei Technologies (Thailand) Co., Ltd.

Dr. Jarinya Junpan
Chief Innovation Officer, ACIS Professional Center Co., Ltd.

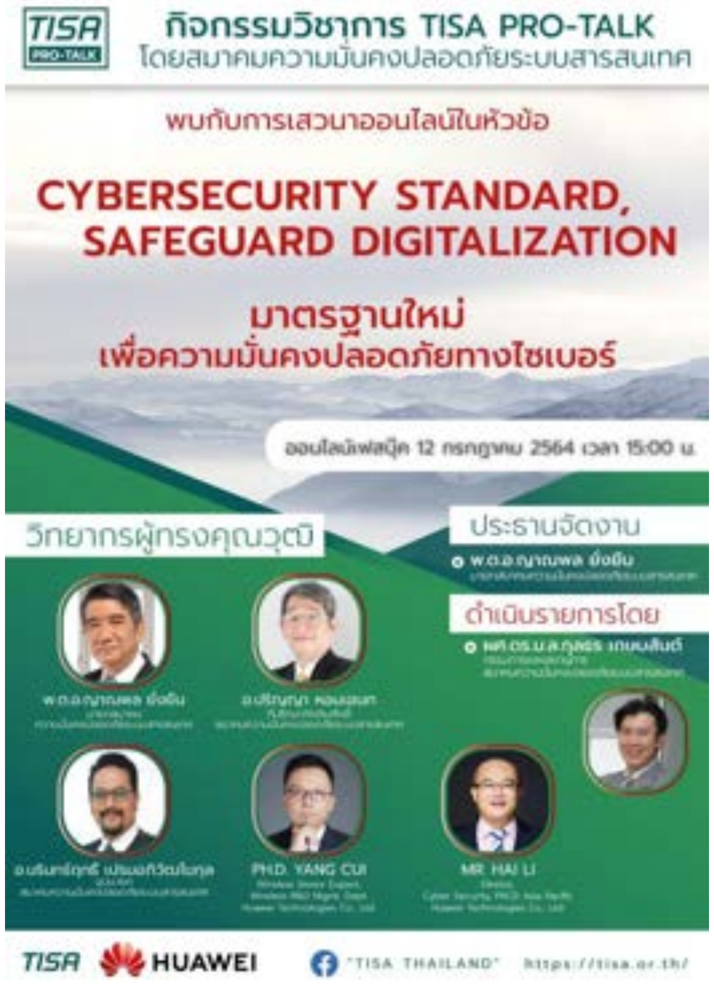
Khun Napat Aruntana
Chief Executive Officer, Cybertron Co., Ltd.

Moderator

Asst.Prof. Dr. Poomporn Thamsatitdej
Lecturer, College of Innovation, Thammasat University
TCIOA Committee

Scan Here to Register

TISA – Event 2007-2023 (17 years)



กิจกรรมวิชาการ TISA PRO-TALK
โดยสมาคมความมั่นคงปลอดภัยระบบสารสนเทศ

พบกับการเสวนาออนไลน์ในหัวข้อ

CYBERSECURITY STANDARD, SAFEGUARD DIGITALIZATION

**มาตรฐานใหม่
เพื่อความมั่นคงปลอดภัยทางไซเบอร์**

ออนไลน์เฟสบุ๊ค 12 กรกฎาคม 2564 เวลา 15:00 น.

วิทยากรผู้ทรงคุณวุฒิ

- พ.ต.อ.ญาณพล ยั่งยืน
- อ.ปริญญา หอมเอนก
- อ.นรินทร์ฤทธิ์ เปรมอภิวัฒโนกุล
- PH.D. YANG CUI
  Wireless Device Expert,
  Wireless R&D Mgmt. Dept.
  Huawei Technologies Co., Ltd
- MR. HAI LI
  Director,
  Cyber Security, PACD Asia Pacific
  Huawei Technologies Co., Ltd

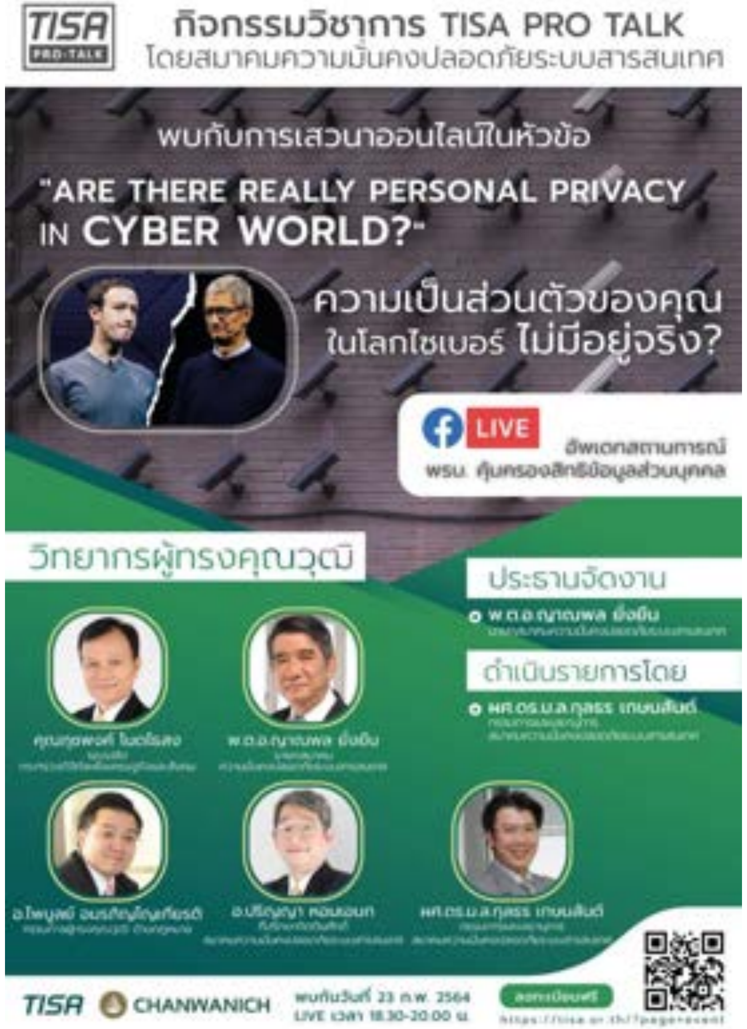
ประธานจัดงาน

- พ.ต.อ.ญาณพล ยั่งยืน

ดำเนินรายการโดย

- ผศ.ดร.ม.ล.กุลธร เกษมสันต์

TISA HUAWEI "TISA THAILAND" https://tisa.or.th/



กิจกรรมวิชาการ TISA PRO TALK
โดยสมาคมความมั่นคงปลอดภัยระบบสารสนเทศ

พบกับการเสวนาออนไลน์ในหัวข้อ

"ARE THERE REALLY PERSONAL PRIVACY IN CYBER WORLD?"

**ความเป็นส่วนตัวของคุณ
ในโลกไซเบอร์ ไม่มีอยู่จริง?**

LIVE
อัพเดทสถานการณ์
พรบ. คุ้มครองสิทธิข้อมูลส่วนบุคคล

วิทยากรผู้ทรงคุณวุฒิ

- คุณภุชพงศ์ โนดไธสง
- พ.ต.อ.ญาณพล ยั่งยืน
- อ.ไพบูลย์ อมรภิญโญเกียรติ
- อ.ปริญญา หอมเอนก
- ผศ.ดร.ม.ล.กุลธร เกษมสันต์

ประธานจัดงาน

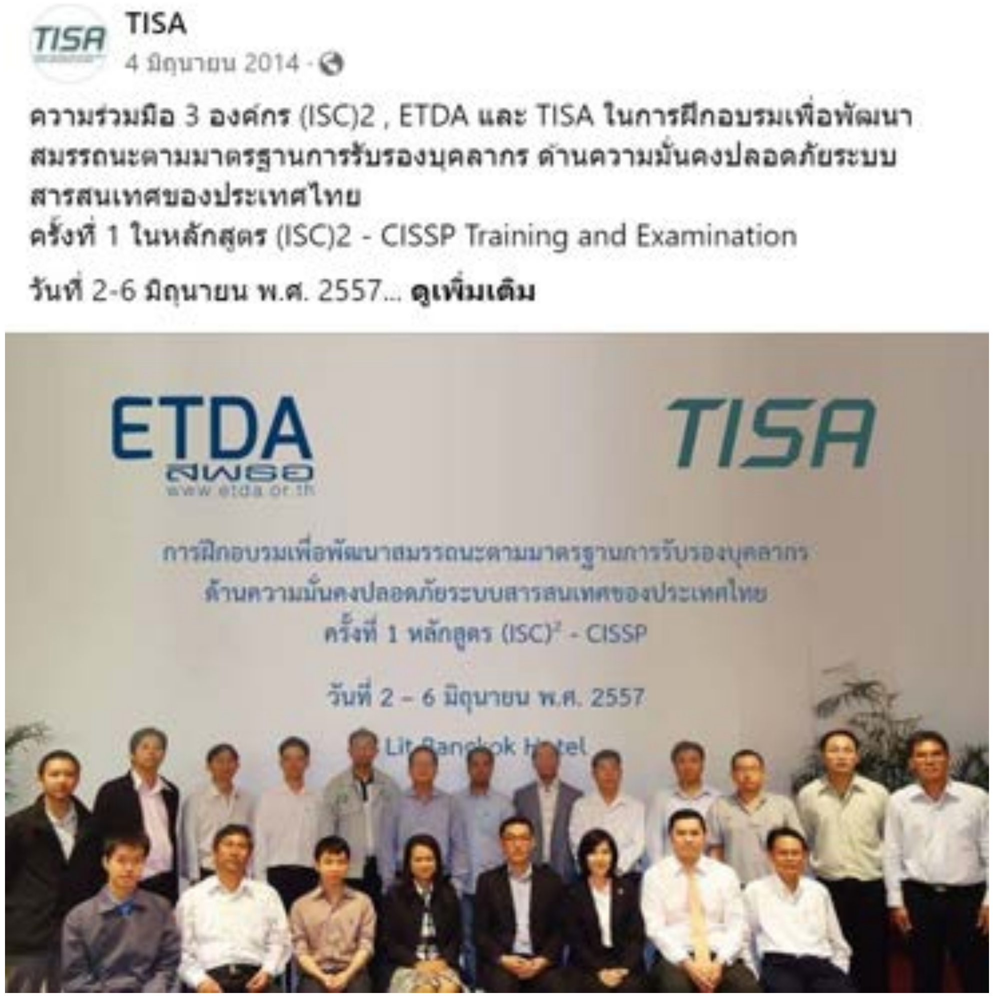
- พ.ต.อ.ญาณพล ยั่งยืน

ดำเนินรายการโดย

- ผศ.ดร.ม.ล.กุลธร เกษมสันต์

TISA CHANWANICH
พบกันวันที่ 23 ก.พ. 2564
LIVE เวลา 18.30-20.00 น.
ลงทะเบียนฟรี
https://tisa.or.th/?page=event

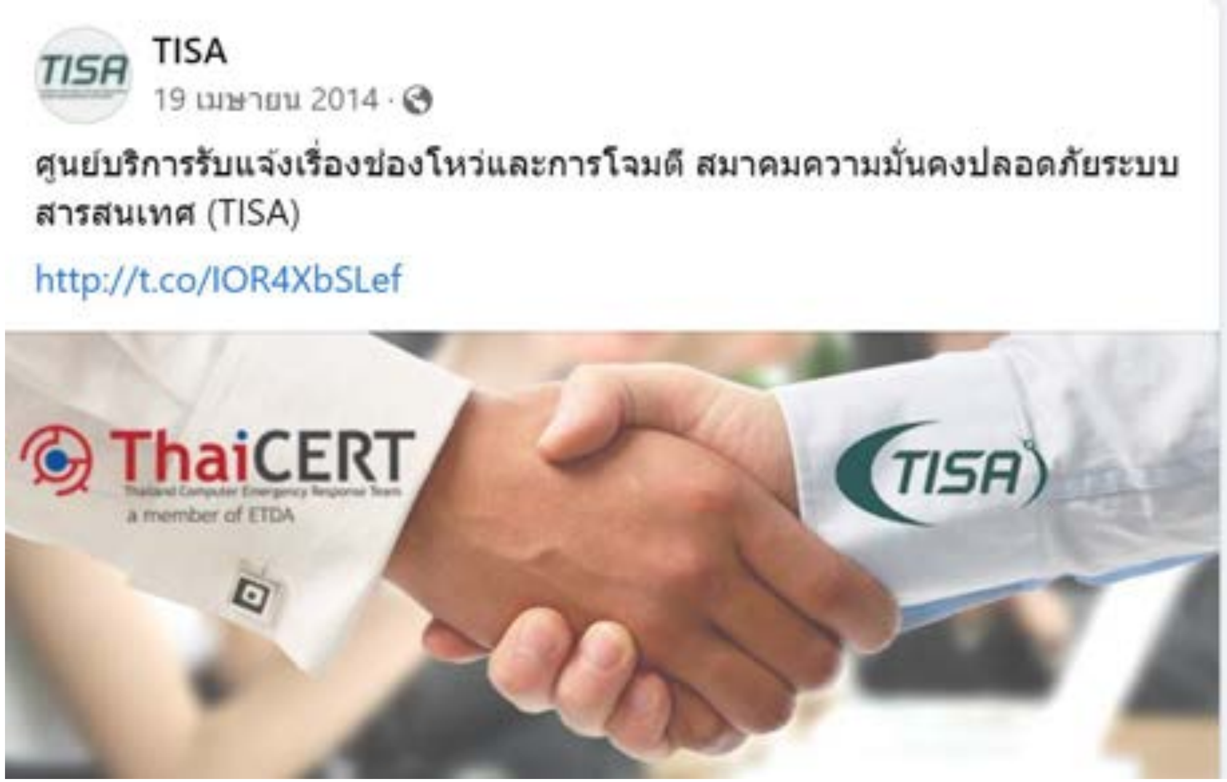
TISA – Event 2007-2023 (17 years)



TISA
4 มิถุนายน 2014 ·

ความร่วมมือ 3 องค์กร (ISC)2 , ETDA และ TISA ในการฝึกอบรมเพื่อพัฒนาสมรรถนะตามมาตรฐานการรับรองบุคลากร ด้านความมั่นคงปลอดภัยระบบสารสนเทศของประเทศไทย
ครั้งที่ 1 ในหลักสูตร (ISC)2 - CISSP Training and Examination
วันที่ 2-6 มิถุนายน พ.ศ. 2557... **ดูเพิ่มเติม**

ETDA
สพธอ
www.etda.or.th
TISA
การฝึกอบรมเพื่อพัฒนาสมรรถนะตามมาตรฐานการรับรองบุคลากร
ด้านความมั่นคงปลอดภัยระบบสารสนเทศของประเทศไทย
ครั้งที่ 1 หลักสูตร (ISC)² - CISSP
วันที่ 2 – 6 มิถุนายน พ.ศ. 2557
Lit Bangkok Hotel

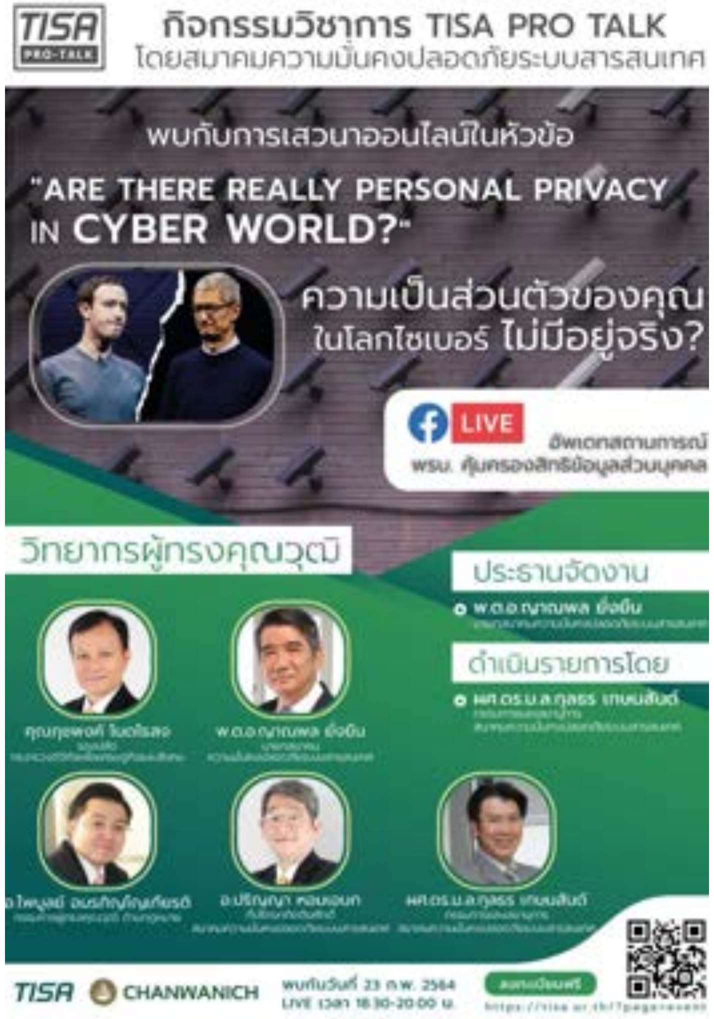


TISA
19 เมษายน 2014 ·

ศูนย์บริการรับแจ้งเรื่องช่องโหว่และการโจมตี สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (TISA)

http://t.co/IOR4XbSLef

TISA activities – PRO TALK



TISA PRO-TALK

กิจกรรมวิชาการ TISA PRO TALK
โดยสมาคมความมั่นคงปลอดภัยระบบสารสนเทศ

พบกันการเสวนาออนไลน์ในหัวข้อ

"ARE THERE REALLY PERSONAL PRIVACY IN CYBER WORLD?"

ความเป็นส่วนตัวของคุณ
ในโลกไซเบอร์ ไม่มีอยู่จริง?

LIVE
อัพเดทสถานการณ์
พรบ. คุ้มครองสิทธิข้อมูลส่วนบุคคล

วิทยากรผู้ทรงคุณวุฒิ

- คุณภุชพงค์ โนดไธสง
- พ.ต.อ.ญาณพล ยั่งยืน
- อ.ไพบูลย์ อมรภิญโญเกียรติ
- อ.ปริญญา หอมเอนก
- ผศ.ดร.ม.ล.กุลธร เกษมสันต์

ประธานจัดงาน

- พ.ต.อ.ญาณพล ยั่งยืน

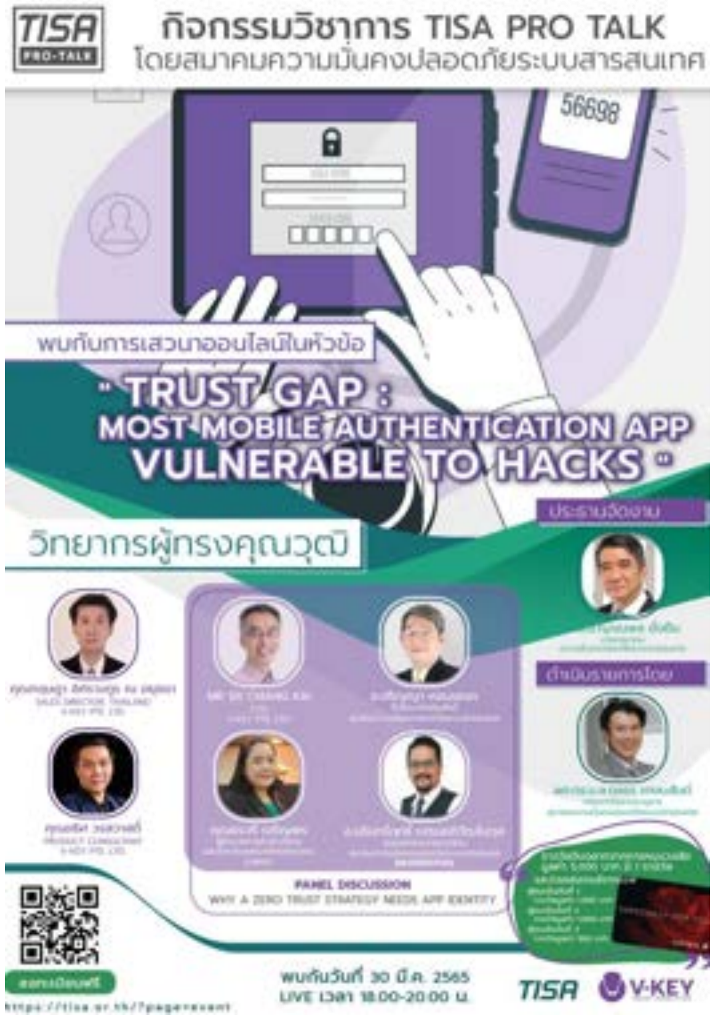
ดำเนินรายการโดย

- ผศ.ดร.ม.ล.กุลธร เกษมสันต์

TISA CHANWANICH

พบกันวันที่ 23 ก.พ. 2564
LIVE เวลา 18.30-20.00 น.

ลงทะเบียนฟรี
https://tisa.or.th/?page=event



TISA PRO-TALK

กิจกรรมวิชาการ TISA PRO TALK
โดยสมาคมความมั่นคงปลอดภัยระบบสารสนเทศ

พบกันการเสวนาออนไลน์ในหัวข้อ

" TRUST GAP :
MOST MOBILE AUTHENTICATION APP
VULNERABLE TO HACKS "

วิทยากรผู้ทรงคุณวุฒิ

ประธานจัดงาน

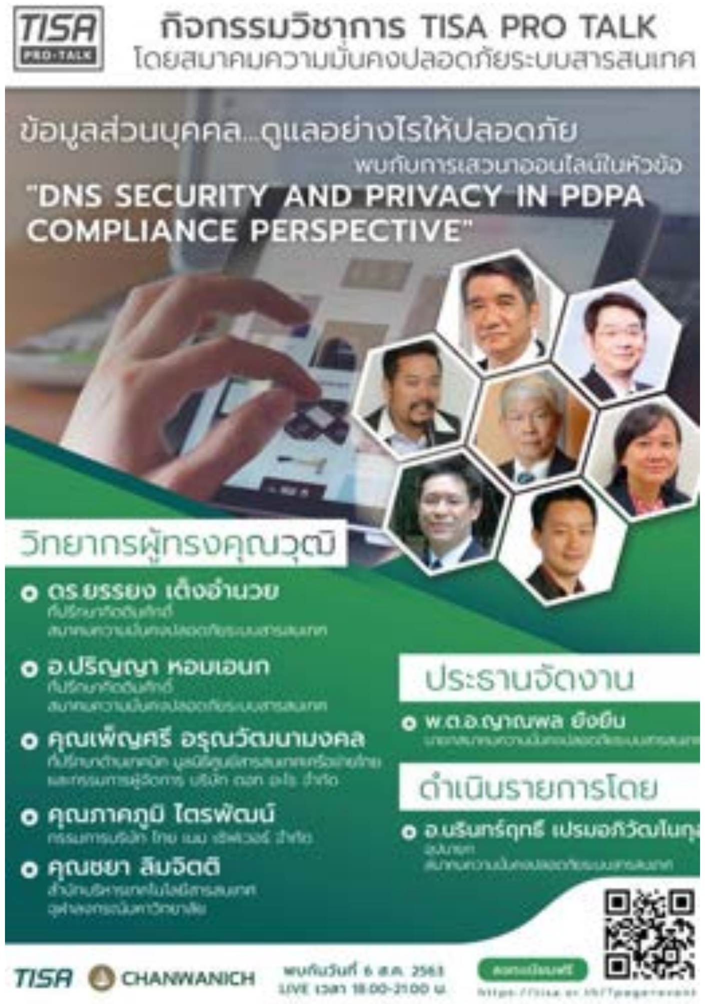
ดำเนินรายการโดย

PANEL DISCUSSION
WHY A ZERO TRUST STRATEGY NEEDS APP IDENTITY

ลงทะเบียนฟรี
https://tisa.or.th/?page=event

พบกันวันที่ 30 มี.ค. 2565
LIVE เวลา 18.00-20.00 น.

TISA V-KEY



TISA PRO-TALK

กิจกรรมวิชาการ TISA PRO TALK
โดยสมาคมความมั่นคงปลอดภัยระบบสารสนเทศ

ข้อมูลส่วนบุคคล...ดูแลอย่างไรให้ปลอดภัย

พบกันการเสวนาออนไลน์ในหัวข้อ

"DNS SECURITY AND PRIVACY IN PDPA COMPLIANCE PERSPECTIVE"

วิทยากรผู้ทรงคุณวุฒิ

- ดร.ยรรยง เต็งอำนวย
  ที่ปรึกษากิตติมศักดิ์
  สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ
- อ.ปริญญา หอมเอนก
  ที่ปรึกษากิตติมศักดิ์
  สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ
- คุณเพ็ญศรี อรุณวัฒนามงคล
  ที่ปรึกษาด้านเทคนิค มูลนิธิศูนย์สารสนเทศเครือข่ายไทย
  และกรรมการผู้จัดการ บริษัท ดอท อะไร จำกัด
- คุณภาคภูมิ ไตรพัฒน์
  กรรมการบริษัท ไทย เนม เซิฟเวอร์ จำกัด
- คุณชยา ลิมจิตติ
  สำนักบริหารเทคโนโลยีสารสนเทศ
  จุฬาลงกรณ์มหาวิทยาลัย

ประธานจัดงาน

- พ.ต.อ.ญาณพล ยั่งยืน
  นายกสมาคมความมั่นคงปลอดภัยระบบสารสนเทศ

ดำเนินรายการโดย

- อ.นรินทร์ฤทธิ์ เปรมอภิวัฒโนกุล
  อุปนายก
  สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ

TISA CHANWANICH

พบกันวันที่ 6 ส.ค. 2563
LIVE เวลา 18.00-21.00 น.

ลงทะเบียนฟรี
https://tisa.or.th/?page=event

JICA-TISA Event 2023 21 Sep 2023

JICA-TISA

CYBERSECURITY AND SUSTAINABILITY SEMINAR

THE UNEXPECTED DUO OF DIGITAL TRANSFORMATION

21 September 2023
Grand Fortune Hotel

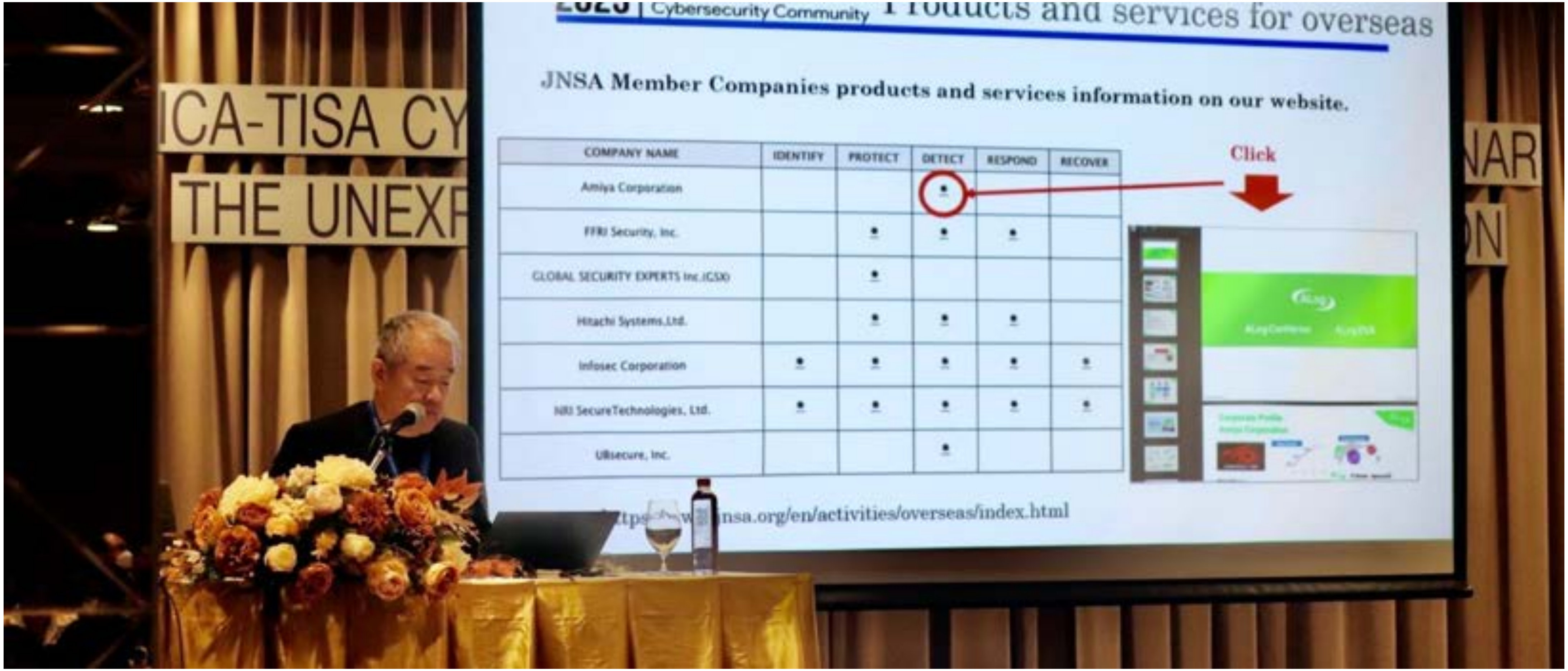
JIC

jica
TISA
SA CYBERSEC ITY AND S TAINABILITY
UNEXPECTED O OF DIGI TRANSFOR
ptemb
Gra gkok

TISA
Y AND SUSTAINABILITY SEMINAR
OF DIGITAL TRANSFORMATION

JIC … SA

JICA-TISA Event 2023 21 Sep 2023



Cybersecurity Community Products and services for overseas

JNSA Member Companies products and services information on our website.

COMPANY NAME	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Amiya Corporation			●		
FFRI Security, Inc.		●	●	●	
GLOBAL SECURITY EXPERTS Inc.(GSX)		●			
Hitachi Systems,Ltd.		●	●	●	
Infosec Corporation	●	●	●	●	●
NRI SecureTechnologies, Ltd.	●	●	●	●	●
Ubsecure, Inc.			●		

https://www.jnsa.org/en/activities/overseas/index.html

JICA-TISA Event 2023 21 Sep 2023

JICA-TISA Event 2023 21 Sep 2023

Please visit us at http://www.tisa.or.th

tisa.or.th
TISA
Thailand Information Security Association
สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ
Home
Vision
Committee
Honorary Advisor
Event
Photo
Links
Download
Alert
Partner
DSI
SOFTWARE PARK THAILAND
สวทช NSTDA
(ISC)²
ISACA
itSMF Thailand

ข่าวอัพเดท จากสมาคมฯ

JICA-TISA CYBERSECURITY AND SUSTAINABILITY SEMINAR
งานสัมมนาความมั่นคงปลอดภัยไซเบอร์สู่การพัฒนาอย่างยั่งยืน

JICA-TISA
CYBERSECURITY AND SUSTAINABILITY SEMINAR
THE UNEXPECTED DUO OF DIGITAL TRANSFORMATION
21 September 2023
Grand Fortune Hotel
jica
TISA
โครงการอบรมการป้องกันความปลอดภัยข้อมูลคอมพิวเตอร์ ครั้งที่ 22
Cyber Defense Initiative Conference 2023
THAILAND CYBERSECURITY DAY
CDIC

Cyber Defense Initiative Conference – CDIC from 2001-2023

โครงการอบรมการป้องกันความปลอดภัยข้อมูลคอมพิวเตอร์ ครั้งที่ 22

Cyber Defense Initiative Conference 2023

งานสัมมนาด้านความมั่นคงปลอดภัยไซเบอร์ที่ใหญ่ที่สุดในประเทศไทย

THAILAND CYBERSECURITY DAY

CDIC

CONFERENCE 2023

29-30 November 2023

Grand Hall, BITEC Bangna, Thailand

Powering **Techno-Drive** in **Digi-Hype** Behaviour towards **Digital Trust**

ผศ.ดร.วีรชัย อาจหาญ
ผู้ช่วยผู้อำนวยการ
สวทช

พล.อ.ต.อมร ชมเชย
เลขาธิการ
สกมช.

ดร.ศิรรักษ์ ศิวโมกษธรรม
เลขาธิการ
สดช.

อ.ปริญญา หอมเอนก
ประธานกรรมการบริหาร
เอซิส โปรเฟสชั่นนัล เซ็นเตอร์

ดร.สุรพันธ์ เมฆนาวิน
ประธานคณะอนุกรรมการ
สำนักงานส่งเสริมเศรษฐกิจดิจิทัล

รศ.ดร.ธนชาติ นุ่มนนท์
ผู้อำนวยการ
สถาบันไอเอ็มซี

ดร.กิตติ โฆษะวิสุทธิ์
ประธานกรรมการ
TB-CERT

คุณวิบูลย์ ภัทรพิบูล
ผู้ช่วยเลขาธิการ
ก.ล.ต.

ดร.ณรงค์ศักดิ์ สุขมา
ผู้ช่วยเลขาธิการ
สำนักงาน คปภ.

คุณภิญโญ ศรีเพชราภรณ์
ผู้อำนวยการ ฝ่ายกำกับฯ
ธนาคารแห่งประเทศไทย

คุณณพงศ์ธวัช โพธิกิจ
ผู้อำนวยการฝ่ายกลยุทธฯ
ธนาคารแห่งประเทศไทย

ดร.มนต์ศักดิ์ โซ่เจริญธรรม
ที่ปรึกษาดิจิทัลอาวุโส
สำนักงานพัฒนารัฐบาลดิจิทัล

พล.ต.ต.นิวัฒน์ อาภรณ์ศิน
รองผู้บัญชาการ
บช.สอท.

ดร.อธิป อัศวานันท์
ผู้อำนวยการ
สมาคมดิจิทัลไทย (DCT)

คุณชัชวัฒน์ อัศวรักวงศ์
กรรมการผู้จัดการ
กสิกร บิซิเนส-เทคโนโลยี กรุ๊ป

คุณจุฬลดา มีจุล
รองผู้อำนวยการ
สถาบันคุณวุฒิวิชาชีพ

Mr.Sam Goh
Chief Information Security Officer
DataX

Mr.Freddy Tan
Managing Director
EPIC Cybersecurity

Mr.Arthur Keleti
Cyber-Secret Futurist
Founder of ITBN

Mr.Dan Houser
Security & Identity Strategist
Board of Directors, (ISC)²

Co-Host

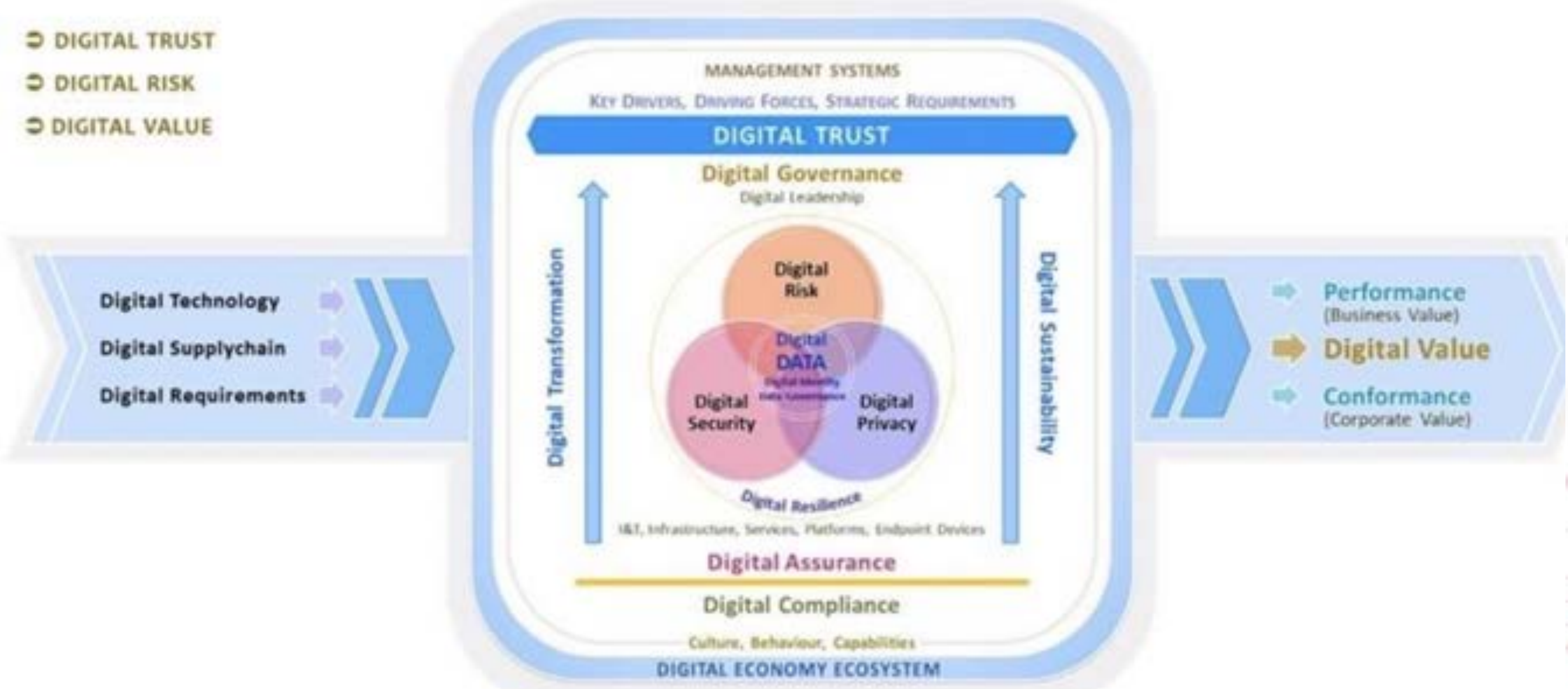
สวทช NSTDA · SOFTWARE PARK THAILAND · ISACA Bangkok Chapter · ACIS · TISA · CIO · (ISC)²

☎ 02-253-4736#2

www.cdicconference.com

DIGITAL TRUST FOUNDATIONAL CONCEPTS

- DIGITAL TRUST
- DIGITAL RISK
- DIGITAL VALUE



Source: "DigiTrust Model: Digital Trust Foundational Concepts", ACIS, 2023

Conference Room

โครงการอบรมการป้องกันความปลอดภัยข้อมูลคอมพิวเตอร์ ครั้งที่ 21
Cyber Defense Initiative Conference 2022
CDiC2022
THAILAND CYBERSECURITY DAY
9-10 November 2022
Grand Hall, BITEC Bangna, Thailand
Co-Host
ISACA
TISA
(ISC)²

Networking

Please join us

www.cdicconference.com

Thank You

VNISA

Introduction to VNISA and Our Corporation

Suggestions on Cyber Security

Nguyen Thanh Hung
Chairman of VNISA – Former Vice Minister of MIC Vietnam

Cybersecurity situation in Vietnam

20th (2020)

8th (2022).

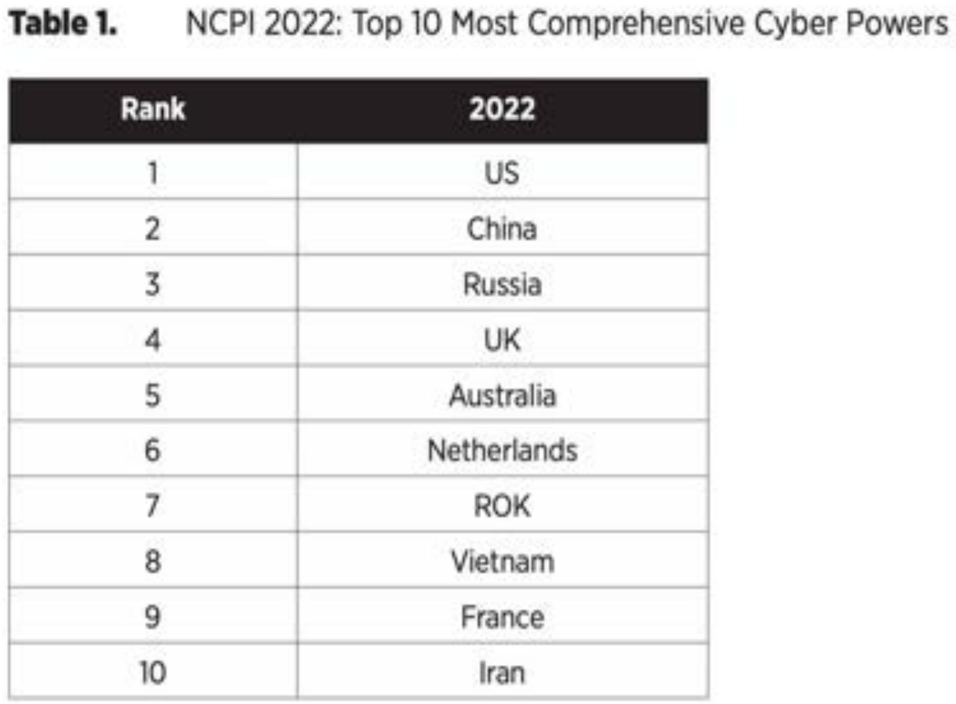


Table 1. NCPI 2022: Top 10 Most Comprehensive Cyber Powers

Rank	2022
1	US
2	China
3	Russia
4	UK
5	Australia
6	Netherlands
7	ROK
8	Vietnam
9	France
10	Iran

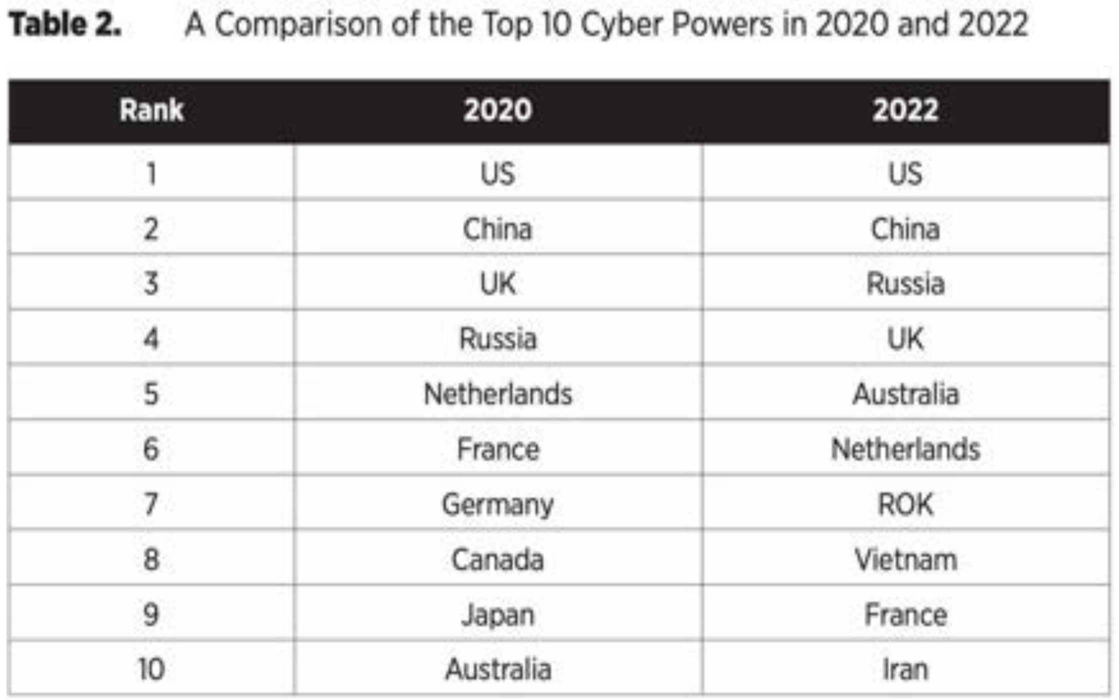
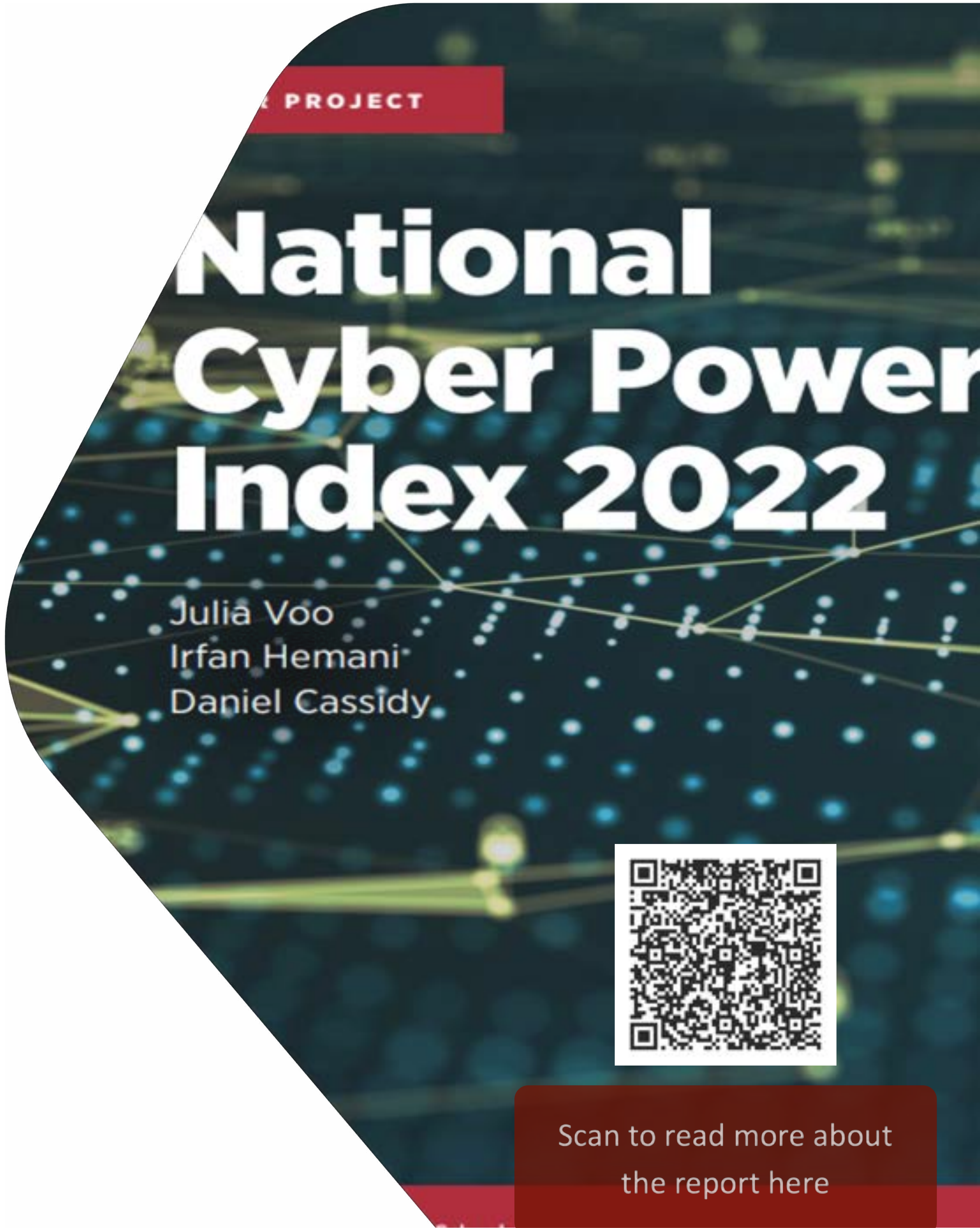


Table 2. A Comparison of the Top 10 Cyber Powers in 2020 and 2022

Rank	2020	2022
1	US	US
2	China	China
3	UK	Russia
4	Russia	UK
5	Netherlands	Australia
6	France	Netherlands
7	Germany	ROK
8	Canada	Vietnam
9	Japan	France
10	Australia	Iran

(National Cyber Power Index 2022 Report - HARVARD Kennedy School)



PROJECT

National Cyber Power Index 2022

Julia Voo
Irfan Hemani
Daniel Cassidy

Scan to read more about the report here

B. About VNISA - Introduction

A. About VNISA:

- Introduction
- Activities

B. About VNISA - Introduction

Vietnam Information Security Association, (VNISA) is the first non-profit organization of Vietnam that operates in the field of Information security (Founded on 2007)

- Cooperate with Government Agencies: Authority of InfoSec/MIC, A05/MPS, VGISC, …
- Promote Infosec education/training (Organize the information security competitions, …)
- Organize events, conferences, seminar of special subjects
- Lead up to the meetings among the organizations, businesses, help and cooperate to develop application of information security
- Promote International Cooperation
- Develop standards/guidelines.

B. About VNISA - Introduction

VNISA

- 15 years of establishment under the Government, approved by Ministry of Internal Affairs.
- Executive committee: 27 members
- The key members:

- VNISA Southern Branch

- Institute of information security technology

- Vietnam Certificate Authority and Digital Transaction Club (VCDC)

- Vietnam Cyber Security Assessment and Audit Club (VSAC)

- Nearly 160 enterprise members

B. About VNISA - Introduction

Activities - Annual event:

- Vietnam Cyber Security Day
- Conference and exhibition
- ASEAN Student Contest on Information Security
- Pupil Contest on Information Security
- VNISA Cyber Security Awards
- Cyber security Training workshops

VIETNAM CYBER SECURITY DAY

CONFERENCE & EXHIBITION

DISCUSSION

VIETNAM INFORMATION SECURITY COMPETENCY ENHANCEMENT SOLUTION:
POLICIES, TECHNOLOGIES AND GLOBAL EXPERIENCE

AWARDs

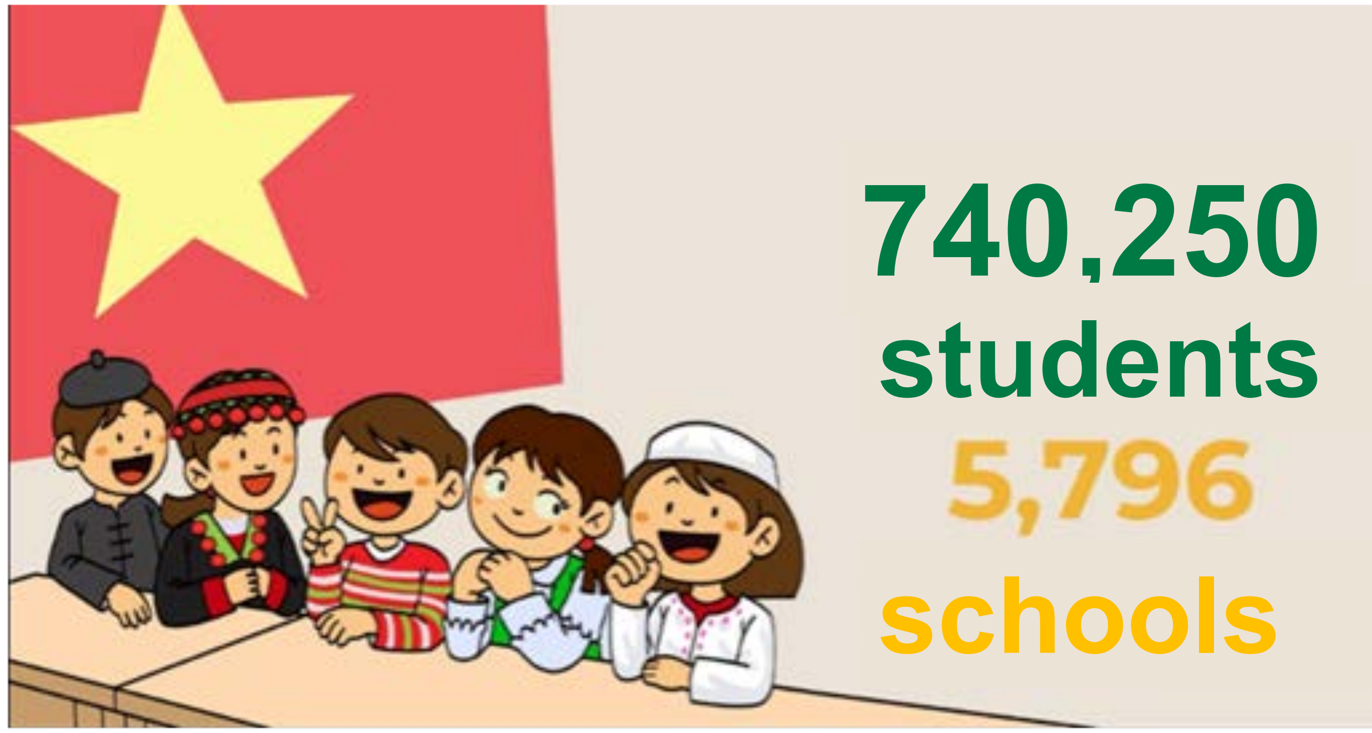
Chủ đề: Kỷ nguyên mới của an ninh mạng
A new era of cyber security
Hà Nội, ngày 02/12/2016
Tài trợ vàng
Google
IBM
Tài trợ bạc
Symantec

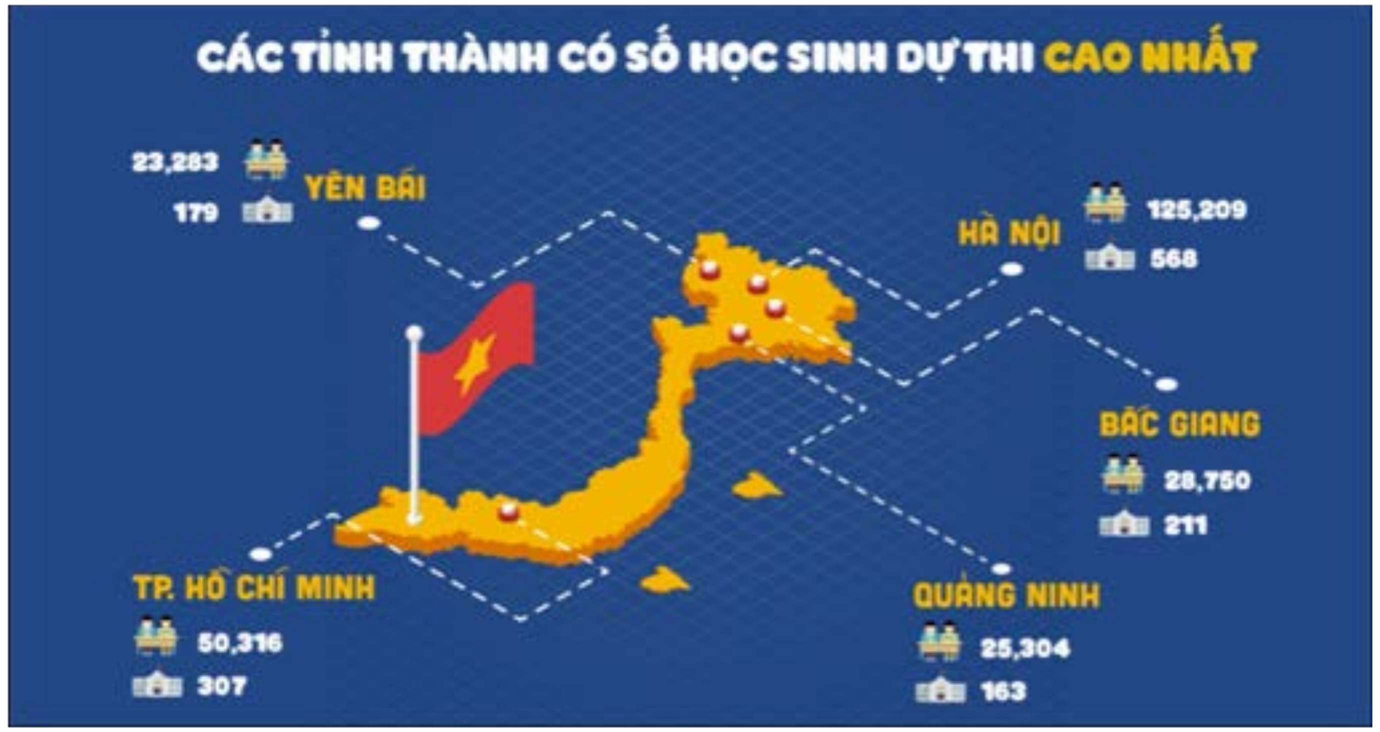
VNISA CYBER SECURITY AWARDS (https://vsa.vnisa.org.vn)

ĐẢNG CỘNG SẢN VIỆT NAM QUANG VINH MUÔN NĂM
VNISA
Hạng mục
"DỊCH VỤ AN TOÀN THÔNG TIN TIÊU BIỂU"

CYBER SECURITY TRAINING WORKSHOPS

PUPIL CONTEST ON INFORMATION SECURITY – ASCIS (https://childsafe.vn)





LỄ PHÁT ĐỘNG VÀ MỞ HỆ THỐNG THI
CUỘC THI HỌC SINH VỚI AN TOÀN THÔNG TIN 2022
PUPIL CONTEST ON INFORMATION SECURITY 2022
Hà Nội, ngày 03/03/2022
Đơn vị phối hợp
Bkav
TikTok
kaspersky
ChildFund
PLAN
World Vision
CMC CORP
JICA

ASEAN STUDENT CONTEST ON INFORMATION SECURITY – ASCIS (https://ascis.vnisa.org.vn)

- Biggest CTF competition in cyber security for Asean students organized by VNISA under the sponsorship of the MIC and MOET
- ASCIS 2022 is the 15th competition for Vietnamese students and the 4th for ASEAN students.
- Nearly 4,000 students attended during 15 years in which there are hundreds of Non-Vietnam students
- Vietnam winning team usually win Cyber Sea Game Asean contest

GIẢI NHẤT
VÒNG SƠ KHẢO KHU VỰC PHÍA BẮC
CUỘC THI SINH VIÊN VỚI AN TOÀN THÔNG TIN ASEAN 2022
ASEAN STUDENT CONTEST ON INFORMATION SECURITY 2022
Hà Nội, ngày 15/10/2022
Principal sponsor

B: Suggestions of International Corporation

Areas of Corporation Improvement	Country Level Actions	Association Level Recommended Actions
Strengthening Regional Cyber Policy Coordination	ASEAN Regional Action Plan (RAP) on the Implementation of Norms of Responsible State Behaviour	Commonly establish cyber security standards among associations
Regional Capacity Building	ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) ASEAN Cyber Shield Project	Exchange experts and share knowledge and experiences through workshops and training regionally.
Advancing Cyber Readiness	Establishment of the ASEAN Regional CERT	Threat Intel or Attack Use Case Sharing
International Cooperation	ASEAN-China Cyber Dialogue ASEAN-Russia Dialogue on ICT Security-related Issues ASEAN-US Cyber Policy Dialogue	- Organizing Regional Conferences and Workshops - Regional Cyber Awards to promote local companies

VNISA
VIETNAM INFORMATION SECURITY ASSOCIATION

THANK YOU!

Nguyen Thanh Hung
Chairman of VNISA – Former Vice Minister of MIC
Vietnam

IC-AJCC

MINISTRY OF
COMMUNICATIONS AND DIGITAL

CyberSecurity
MALAYSIA

CHALLENGES OF RISK MANAGEMENT AND GOVERNANCE IN THE CURRENT CYBERSECURITY LANDSCAPE:

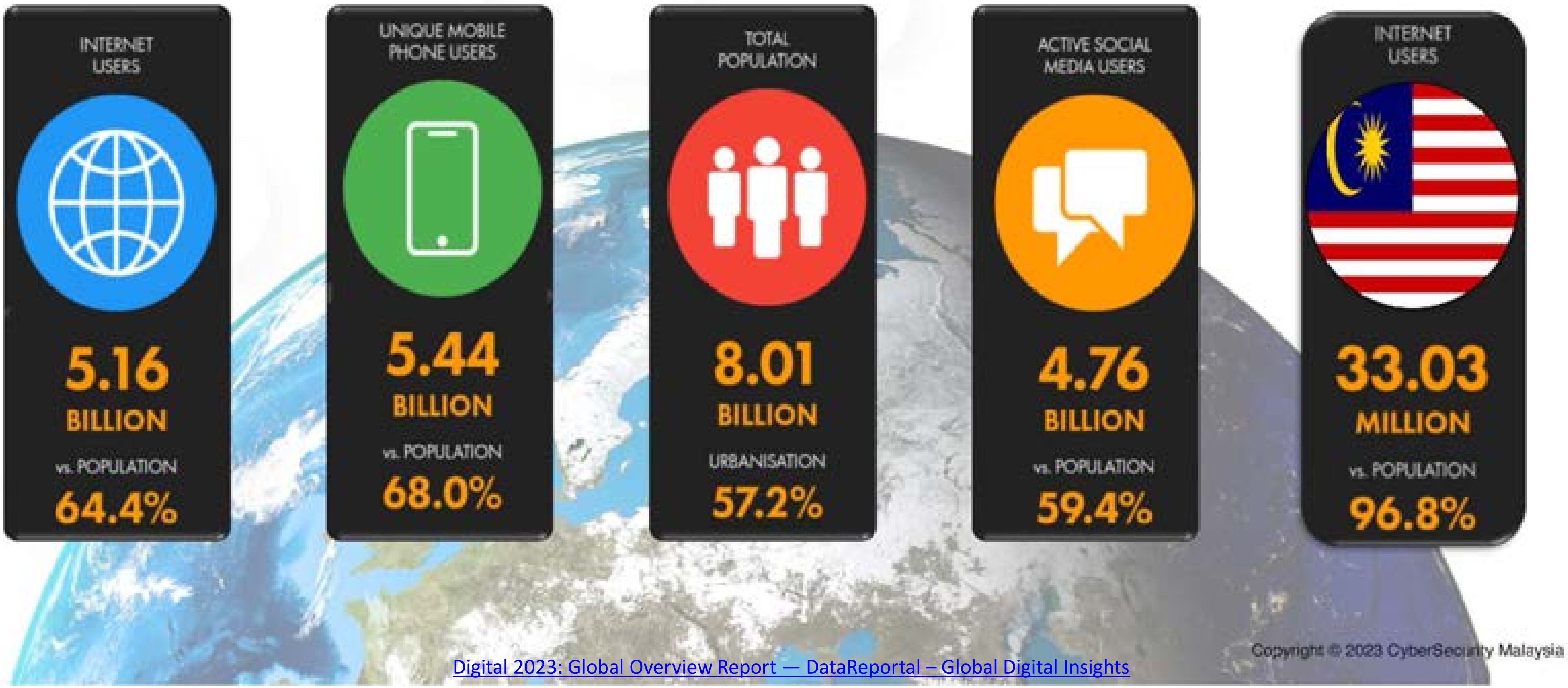
Operational Best Practices

6th October 2023

DATO' TS. DR. HAJI AMIRUDIN ABDUL WAHAB FASc,
Chief Executive Officer
CyberSecurity Malaysia

SECURING
OUR
CYBERSPACE

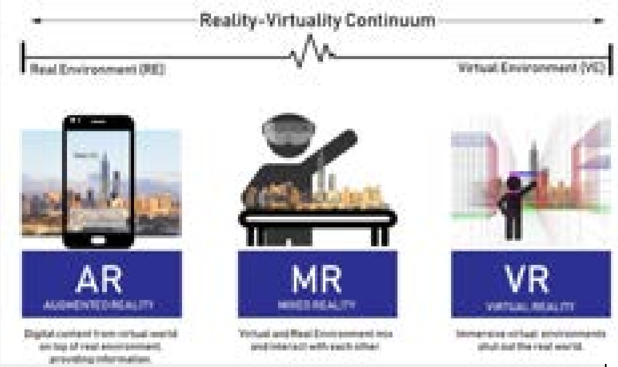
WE ARE MOVING INTO A MORE INTERCONNECTED CYBERSPACE

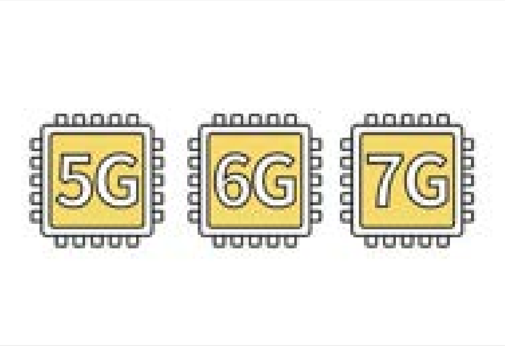


Digital 2023: Global Overview Report — DataReportal – Global Digital Insights

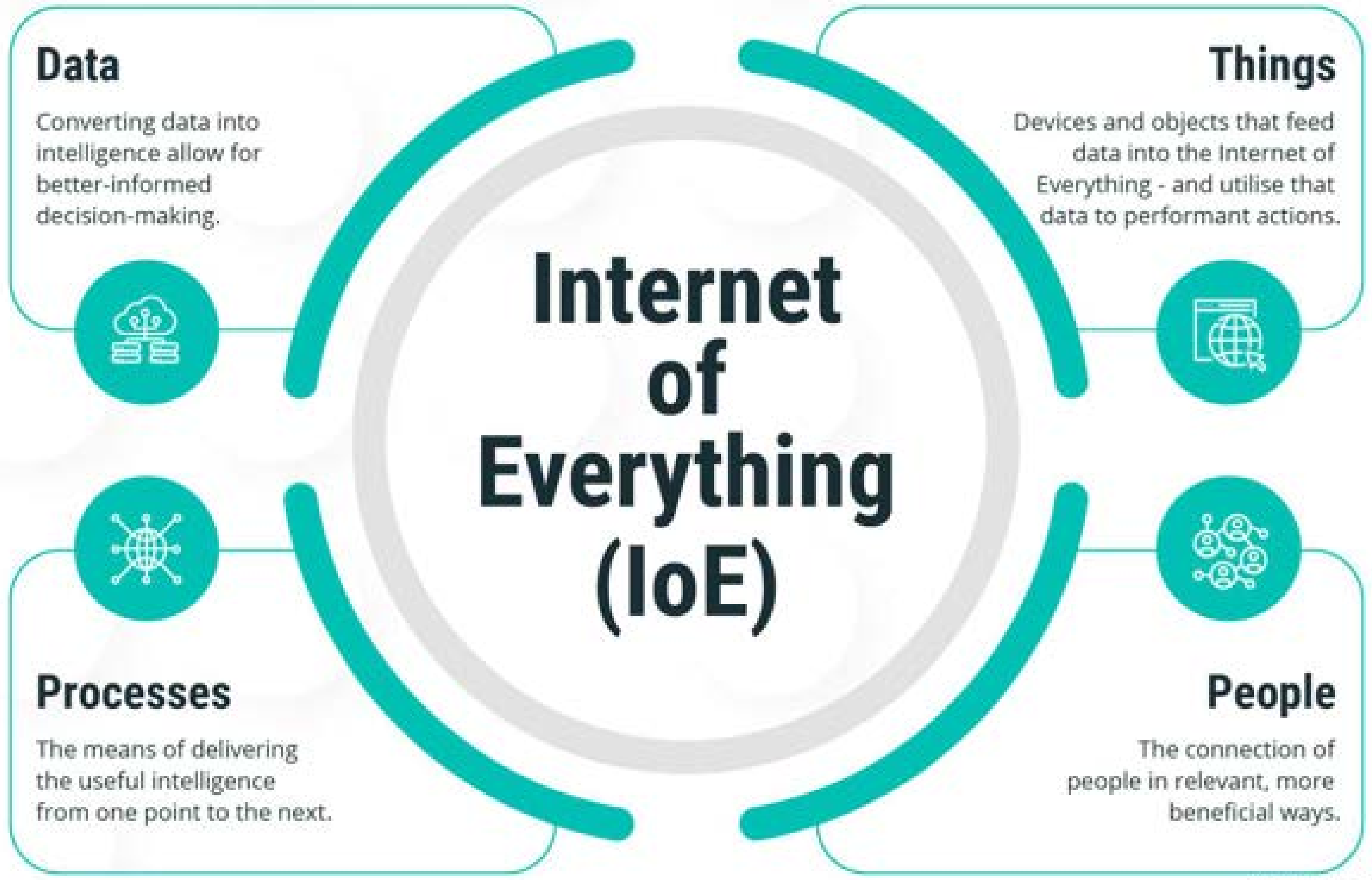
CONVERGENCE OF TECHNOLOGIES

Add More Complexities to Cyber Space and Digital Transformation


Reality-Virtuality Continuum
Real Environment (RE)
Virtual Environment (VE)
AR
AUGMENTED REALITY
Digital content from virtual world on top of real environment providing information
MR
MIXED REALITY
Virtual and Real Environment mix and interact with each other
VR
VIRTUAL REALITY
Immersive virtual environments shut out the real world



The World Has Become Heavily Reliant And Connected To One Another Whether It’s People, Process And Technology



Internet of Everything (IoE)

Data

Converting data into intelligence allow for better-informed decision-making.

Things

Devices and objects that feed data into the Internet of Everything - and utilise that data to performant actions.

Processes

The means of delivering the useful intelligence from one point to the next.

People

The connection of people in relevant, more beneficial ways.

IT VS **OT** VS **IOT** VS **IOE**

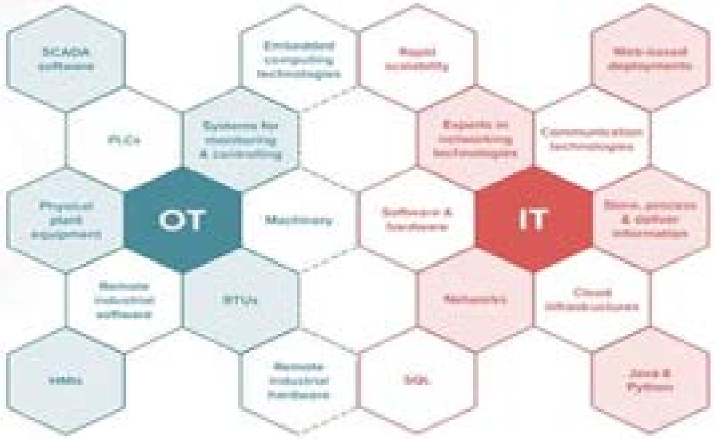
Information Technology (IT): The computer, data storage, and networking infrastructure and processes that are used to create, process, store, secure, and exchange all forms of electronic data. It deals with data, information and communication.

Operational Technology (OT): Traditionally, physical devices in industrial, agricultural, and mission-critical sectors or Industrial IoT networks. It deals with machines.

Internet of Things (IOTs): Networks not specific to a particular sector.

Internet of Everything (IoE): extends beyond IoT by integrating operational technology (OT) and information technology (IT) into a unified ecosystem, enabling seamless communication, data sharing, and intelligent decision-making.

The World Are More Interconnected, Opening new opportunities

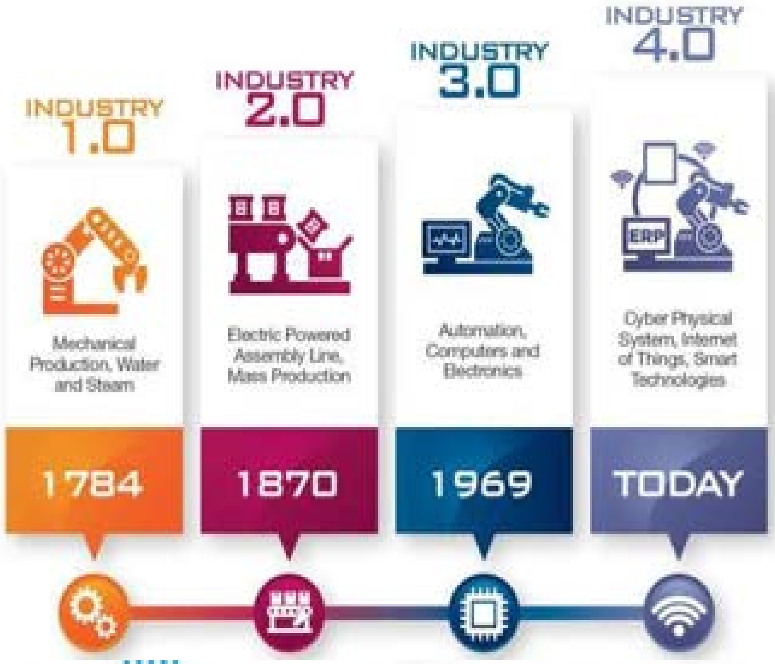

SCADA software
Embedded computing technologies
Rapid scalability
Web-based deployments
PLCs
Systems for monitoring & controlling
Experts in networking technologies
Communication technologies
Physical plant equipment
OT
Machinery
Software & hardware
IT
Store, process & deliver information
Remote industrial software
RTUs
Networks
Cloud infrastructures
HMIs
Remote industrial hardware
SQL
Java & Python

Malaysia

THE LANDSCAPE IS CATALYSED WITH IR4.0 AND DIGITAL TRANSFORMATION

4th INDUSTRIAL REVOLUTION

TO ACHIEVE BY 2030


INDUSTRY 1.0
Mechanical Production, Water and Steam
1784
INDUSTRY 2.0
Electric Powered Assembly Line, Mass Production
1870
INDUSTRY 3.0
Automation, Computers and Electronics
1969
INDUSTRY 4.0
Cyber Physical System, Internet of Things, Smart Technologies
TODAY
ERP

Jendela

Jalinan Digital Negara

MALAYSIA'S DIGITAL TRANSFORMATION: MALAYSIA DIGITAL ECONOMY BLUEPRINT AND THE NATIONAL 4IR POLICY

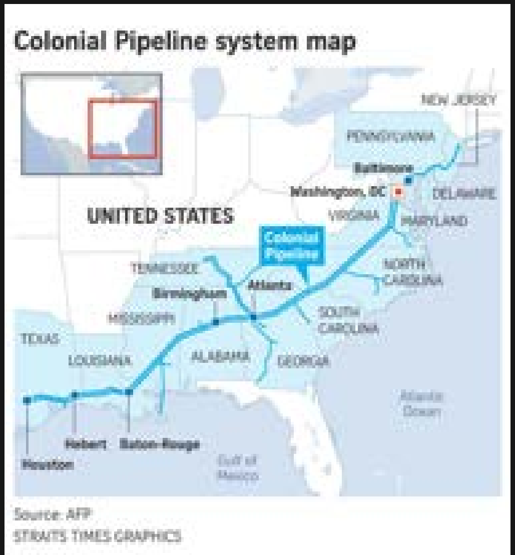
MyDIGITAL

MINISTRY OF ECONOMY
WORLD ECONOMIC FORUM
Malaysia Centre for the Fourth Industrial Revolution
Shaping the Fourth Industrial Revolution
Building a Better Future for All
15 May 2023
THE STRAITS TIMES

In Phase 2 (2023-2025), inclusive digital transformation will be prioritized.

In Phase 3 (from 2026 to 2030) will position Malaysia as a regional leader in digital content and cyber security. MyDIGITAL's mission is to ensure that all Malaysians benefit from the opportunities of the digital revolution.

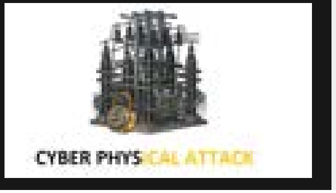
CYBER-ATTACKS MAY HAVE PHYSICAL CONSEQUENCES



Source: AFP
STRAITS TIMES GRAPHICS

Chinese cyber attack on power grid
Status of cyber security in India
#UPSC #IAS
by Rahul Saigaonker

Cyberattacks On Vehicles Pose A Threat To Drivers And Manufacturers



DIGITAL TRANSFORMATION IS NOT WITHOUT ITS RISK

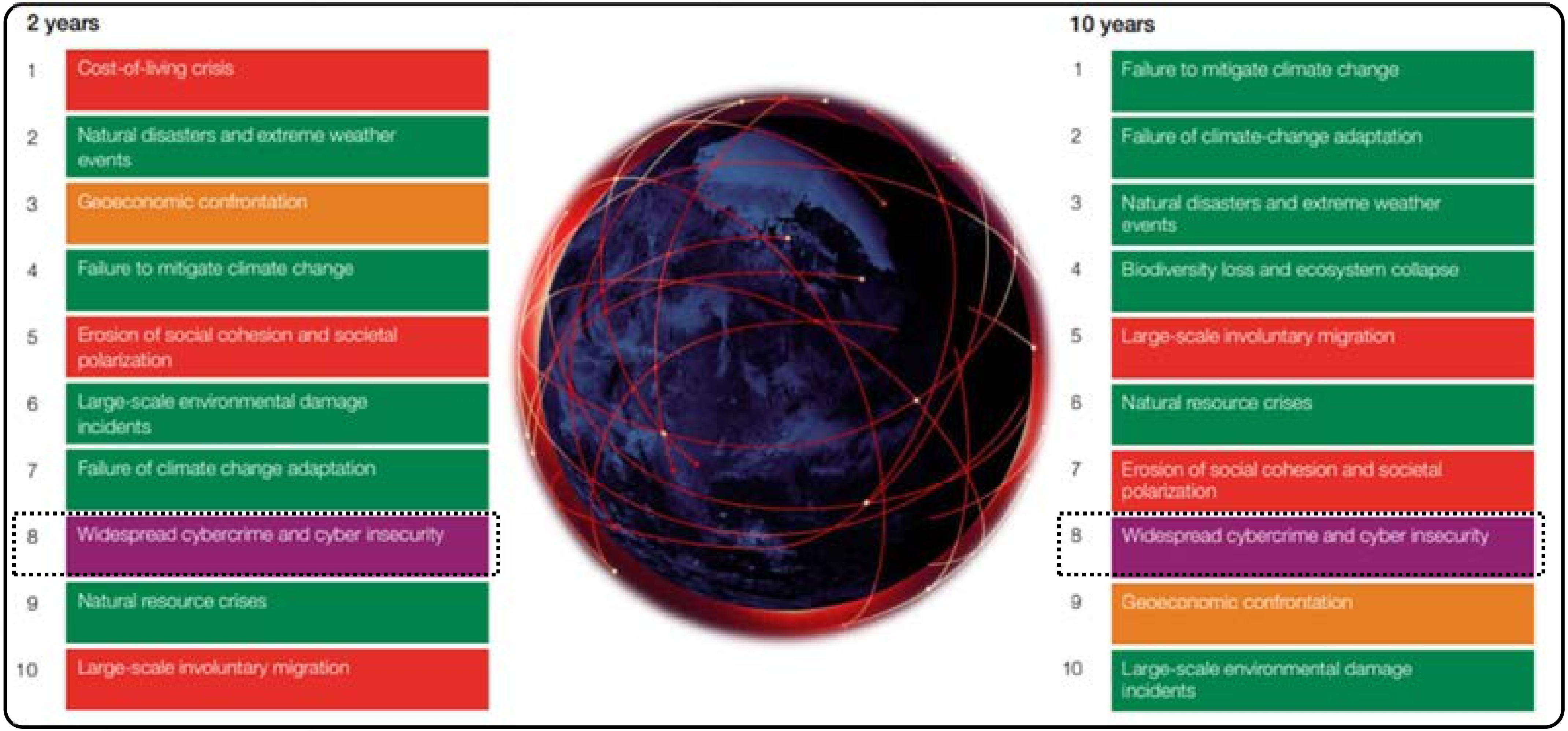
- Technology such as wireless technology has changed the way we conduct business, offering workers with constant access to business-critical applications and data.

- While this flexibility is convenient and expands productivity, it introduces complexity and security risk as these new technology and devices become new target for hackers looking to infiltrate a corporate network.

CYBER RISK

‘Cyber risk’ means any **risk of financial loss, disruption or damage to the reputation** of an organization from some sort of **failure of its information technology systems**. Hence, **CYBER RISK MANAGEMENT** is needed!

GLOBAL RISK 2023



	2 years		10 years
1	Cost-of-living crisis	1	Failure to mitigate climate change
2	Natural disasters and extreme weather events	2	Failure of climate-change adaptation
3	Geoeconomic confrontation	3	Natural disasters and extreme weather events
4	Failure to mitigate climate change	4	Biodiversity loss and ecosystem collapse
5	Erosion of social cohesion and societal polarization	5	Large-scale involuntary migration
6	Large-scale environmental damage incidents	6	Natural resource crises
7	Failure of climate change adaptation	7	Erosion of social cohesion and societal polarization
8	Widespread cybercrime and cyber insecurity	8	Widespread cybercrime and cyber insecurity
9	Natural resource crises	9	Geoeconomic confrontation
10	Large-scale involuntary migration	10	Large-scale environmental damage incidents

Source: WEF_Global_Risks_Report_2023.pdf (weforum.org)

UNDERSTANDING HOW TO HANDLE EACH RISK

AVOID

- Action is taken to do something different.
- The threat is eliminated

ACCEPT

- No actions are taken.
- Risk is acceptable.

MITIGATE

- Actions taken to reduce the probability and impact of risk.
- Implementing relevant controls.

TRANSFER

- Shifting the responsibility and impact to a third party.

SHARE

- Sharing risk with the higher authority or with a third party.

RISK MANAGEMENT AND GOVERNANCE

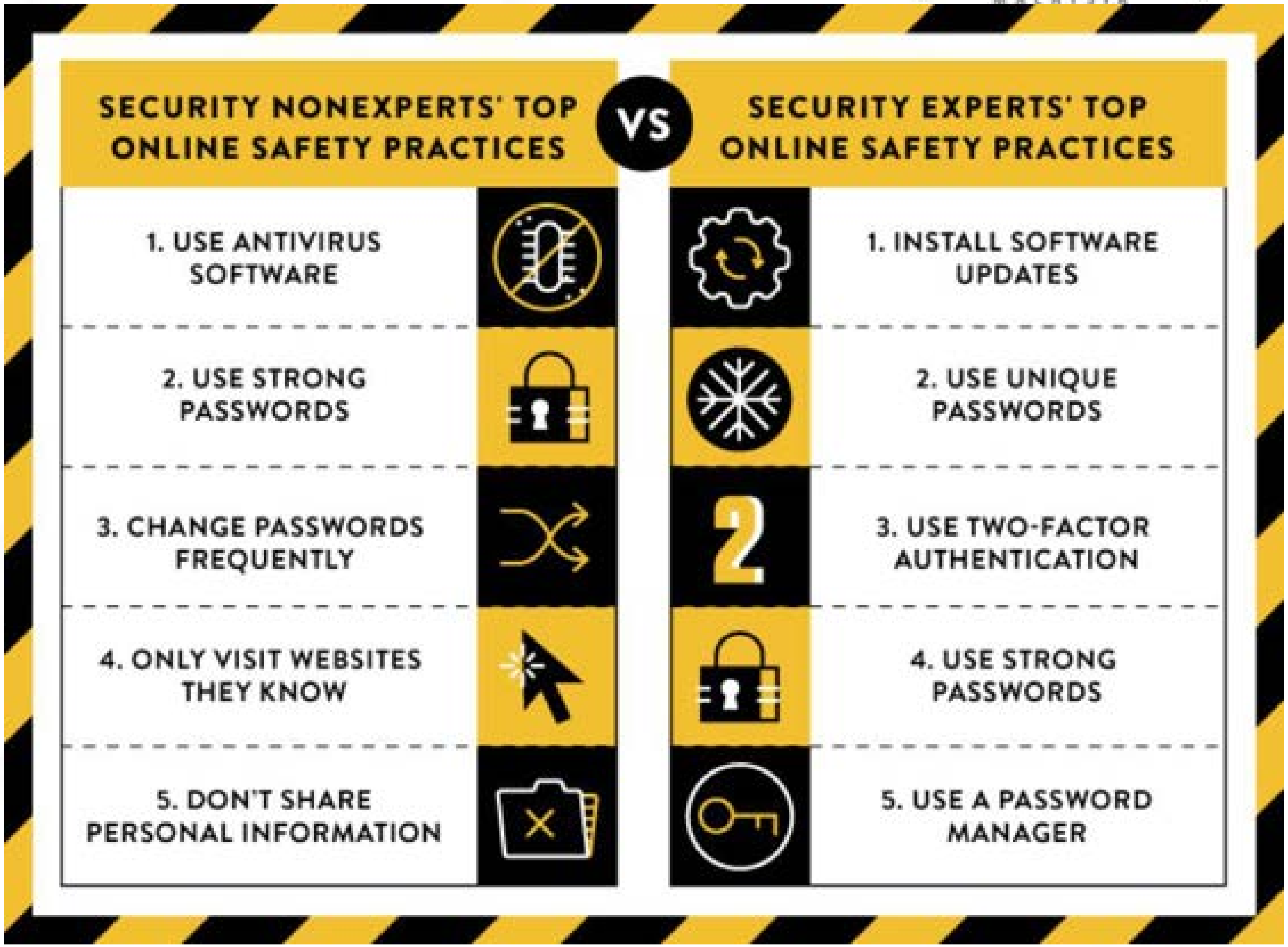
BEST PRACTICES

Risk Management And Governance

Best Practices

CYBER HYGIENE

Refers to fundamental cybersecurity **best practices** that an organization's security practitioners and users can undertake.



SECURITY NONEXPERTS' TOP ONLINE SAFETY PRACTICES	VS	SECURITY EXPERTS' TOP ONLINE SAFETY PRACTICES
1. USE ANTIVIRUS SOFTWARE		1. INSTALL SOFTWARE UPDATES
2. USE STRONG PASSWORDS		2. USE UNIQUE PASSWORDS
3. CHANGE PASSWORDS FREQUENTLY		3. USE TWO-FACTOR AUTHENTICATION
4. ONLY VISIT WEBSITES THEY KNOW		4. USE STRONG PASSWORDS
5. DON'T SHARE PERSONAL INFORMATION		5. USE A PASSWORD MANAGER

Practice Great Cyber Hygiene - Cyber Risk Opportunities

RISK MANAGEMENT BEST PRACTICES

INTEGRATED AND CONSISTENT CONTROLS AND POLICIES	A consistent, systemic and integrated approach to risk management can help determine how **best to identify, manage and mitigate significant risks**.
GAIN BOARD AND MANAGEMENT SUPPORT	Ensure strategic **direction are aligned** and resource are **allocated properly**

RISK MANAGEMENT BEST PRACTICES

MONITOR THE RISK ENVIRONMENT

Management can act promptly if and when the nature, potential impact, or likelihood of **the risk goes outside acceptable levels**

IDENTIFY AND UNDERSTAND ONE'S RISK ENVIRONMENT

A process of **documenting any risks** that could **keep an organization or program from reaching its objective**

COLLABORATION WITH EXTERNAL PARTIES

Collaborating with external parties can help **identify** and **mitigate supply chain risks** that can disrupt operations.

CyberSecurity MALAYSIA

GOVERNANCE BEST PRACTICES

HOLISTIC APPROACH

A holistic approach to governance includes various elements within an organization or government in a comprehensive manner.

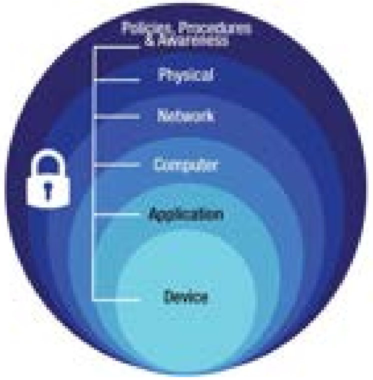
ADAPTIVE APPROACH

Adaptive security is a security approach that's used to respond to potential cyberthreats in real-time by continually monitoring user sessions.

TRUSTED
Firewall
Firewall
UNTRUSTED

ZERO TRUST

Continuous verification. Always verify access, all the time, for all resources or simply put it as "Trust No One".



DEFENCE-IN-DEPTH

A multifaceted approach to safeguard the organization's overall well-being, compliance, and ethical standards.

SOURCE: https://www.datamation.com/big-data/data-governance-trends/

GOVERNANCE BEST PRACTICES

TRAINING & AWARENESS

Promote awareness and training programs to inform the clients or shareholders of their responsibilities and functions within an organisation.

COLLABORATION

Sharing of information, resources, and expertise among various national and international entities to collectively address cyber threats.

SOURCE: https://www.datamation.com/big-data/data-governance-trends/

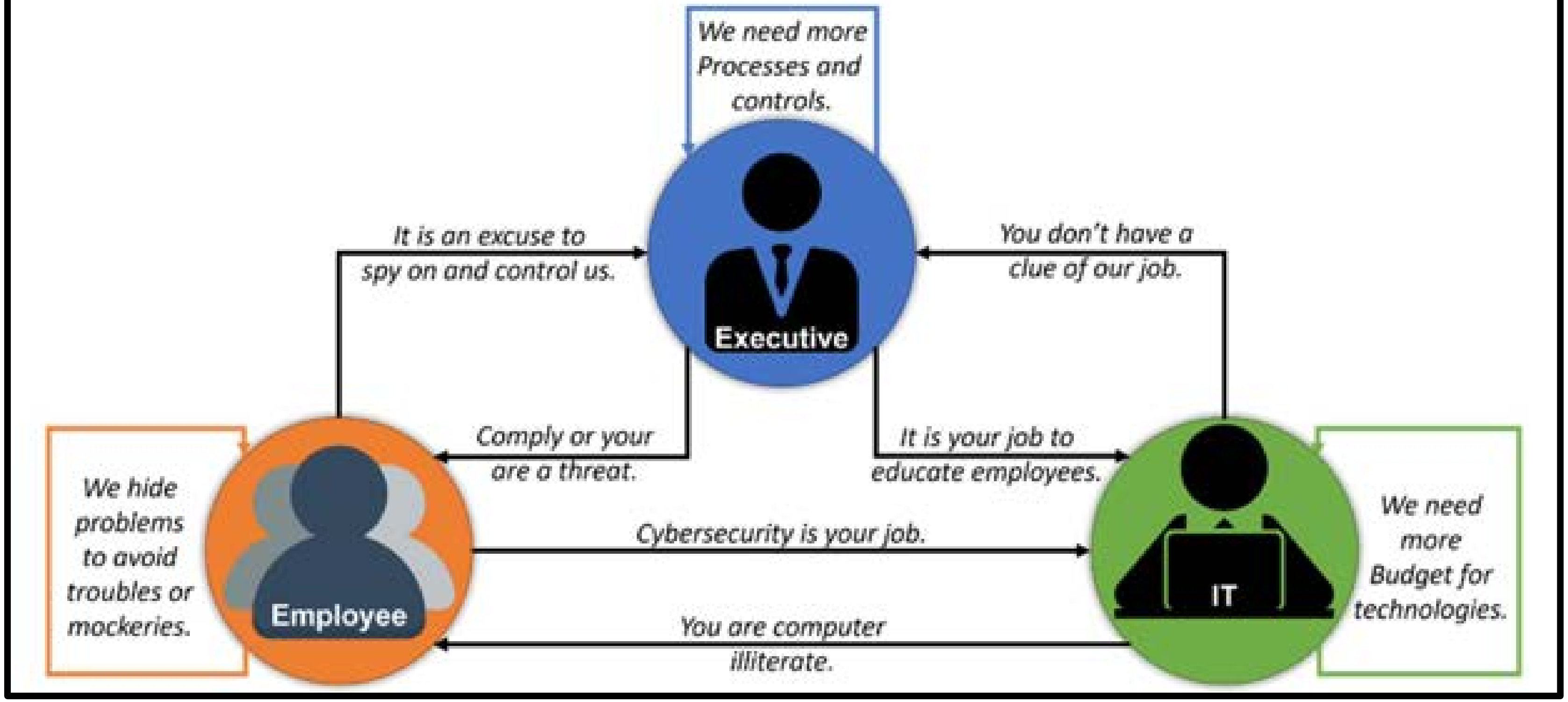
RISK IS EVERYBODY'S RESPONSIBILITY

CYBERSECURITY DOES **NOT** OPERATE IN **SILO!**

THE MANAGEMENT MUST SHOW THE EXAMPLE, BY LEADING THE ORGANISATION IN ENHANCING CYBERSECURITY

CYBERSECURITY, RISK MANAGEMENT, AND GOVERNANCE:

A SHARED RESPONSIBILITY



We need more Processes and controls.
Executive
It is an excuse to spy on and control us.
You don't have a clue of our job.
Comply or your are a threat.
It is your job to educate employees.
We hide problems to avoid troubles or mockeries.
Employee
Cybersecurity is your job.
You are computer illiterate.
IT
We need more Budget for technologies.

CYBERSECURITY MALAYSIA'S INITIATIVES

SiberKASA

OFFICIAL LAUNCH ON 23 MARCH 2021

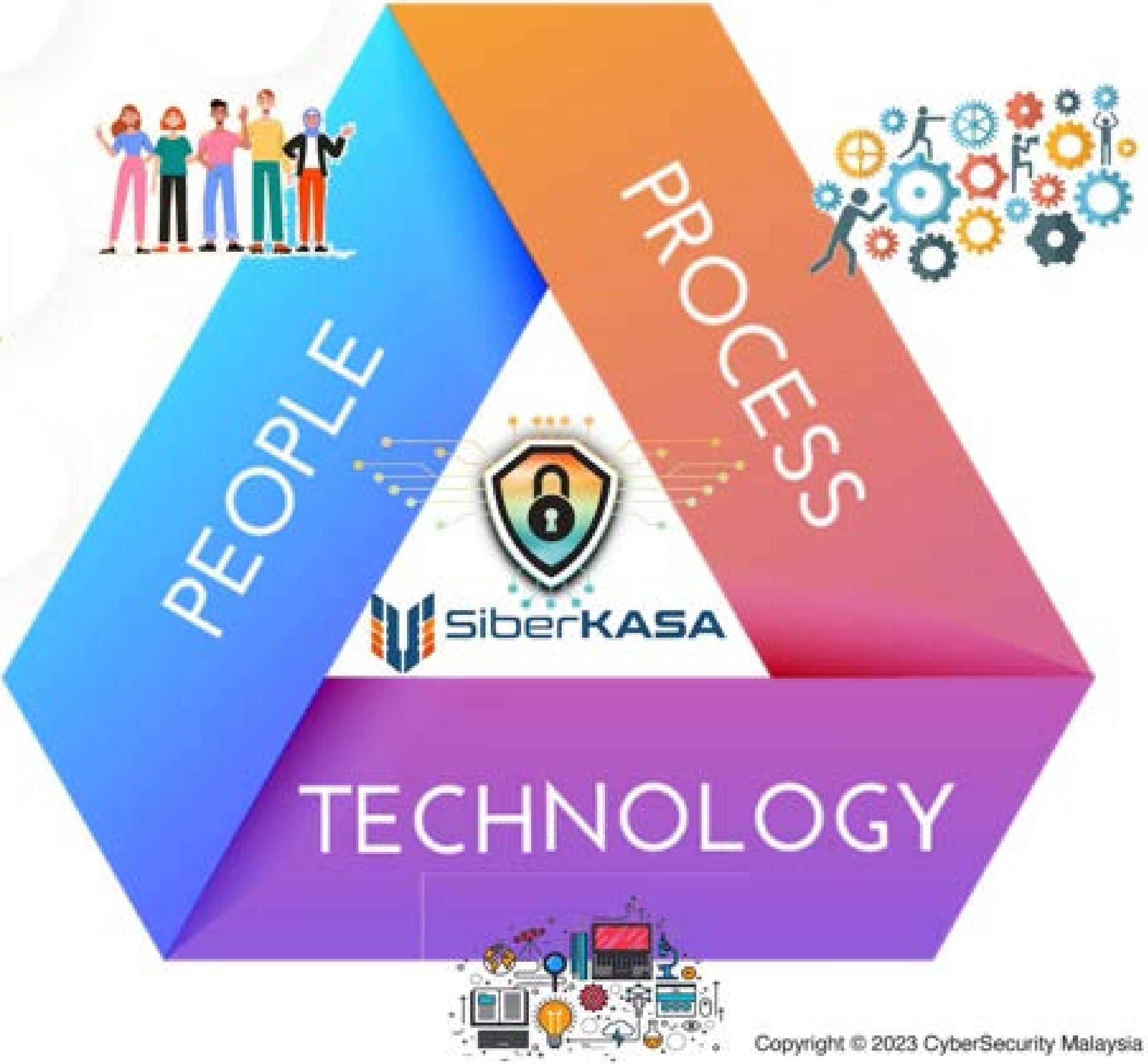
CSM initiatives aimed at developing, empowering, sustaining and strengthening cybersecurity infrastructure and ecosystem in Malaysia to ensure network security preparedness.

CYBERSECURITY MALAYSIA'S INITIATIVES

HOLISTIC APPROACH

Adoption of holistic approach that **identifies potential threats** to organization and **impacts to the national security & public well-being ; and**

To develop the nation to become cyber resilience having the **capability to safeguard the interests** of its **stakeholders, reputation, brand and value creating activities.**



SiberKASA

(Program PemerKASAan Keselamatan Siber)

Objective: Empowering, strengthening and preserving the cyber security infrastructure and ecosystem in Malaysia so that it is always sustainable, protected and resilient.

HUMAN

Covers aspects of skills, knowledge, ethics, behavior and talent

PROCESS

Covers aspects of policy development, strategy, Standard Operating Procedure (SOP), recognition of international standards

TECHNOLOGY

Involves technology in particular matters related to minimizing vulnerabilities, digital forensic analysis, malicious code (malware) and data

PRODUCTS AND SERVICES

PRODUCT

1. Global Accredited Cybersecurity Education (ACE)Scheme
2. CyberSAFE L.I.V.E Gallery
3. Cybersecurity Competency Training (CyberGuru)

1. Information Security Governance, Risk & Compliance Health Check Assessment (ISGRiC)
2. ISMS Guidance Series
3. Information Security Management System(ISMS)

1. Crypto Random Test Tool
2. X-Forensics Tools
3. PenDua Tool
4. Coordinated Malware, Eradication, and Remediation Platform (CMERP)
5. LebahNet
6. CamMuka (Facial Recognition)

SERVICE

1. CyberDrill Exercise
2. Behavioral Competency Assessment (BCA)
3. Cyber Safety Awareness for Everyone (CyberSAFE)
4. CyberSecurity Malaysia Awards, Conference & Exhibition (CSM-ACE)

GLOBAL ACE CERTIFICATION

1. Business Continuity Management System (BCMS) Certification
2. Digital Forensics (DF) Case Management
3. Incident Handling Case Management
4. Cyber Discovery
5. MyTrustSEAL
6. Penetration Testing Service Provider(PTSP) Certification
7. Technology Security Assurance (TSA)
8. ICT Product Security Assessment (IPSA)
9. Security Posture Assessment (SPA)
10. SCADA Security Assessment (SSA)
11. PHP Secure Code Assessment (PSCA)
12. Malaysian Common Criteria Scheme (MyCC)
13. Cybersecurity Strategic and Technical Advisory

1. MyCyberSecurity Clinic (MyCSC)- Data Recovery and Data Sanitization Services
2. Lab Quality Management
3. Cybersecurity Lab Services
4. CyberSecurity Malaysia Cryptographic Evaluation Lab (MyCEL)
5. CCTV Forensics Service
6. Cyber Threat Intelligence Service
7. Cloud Security Compliance Audit
8. Cloud Security Assessment Audit
9. Cloud Security Audit for ISMS
10. Security Operation Centre Service
11. Red Teaming Service

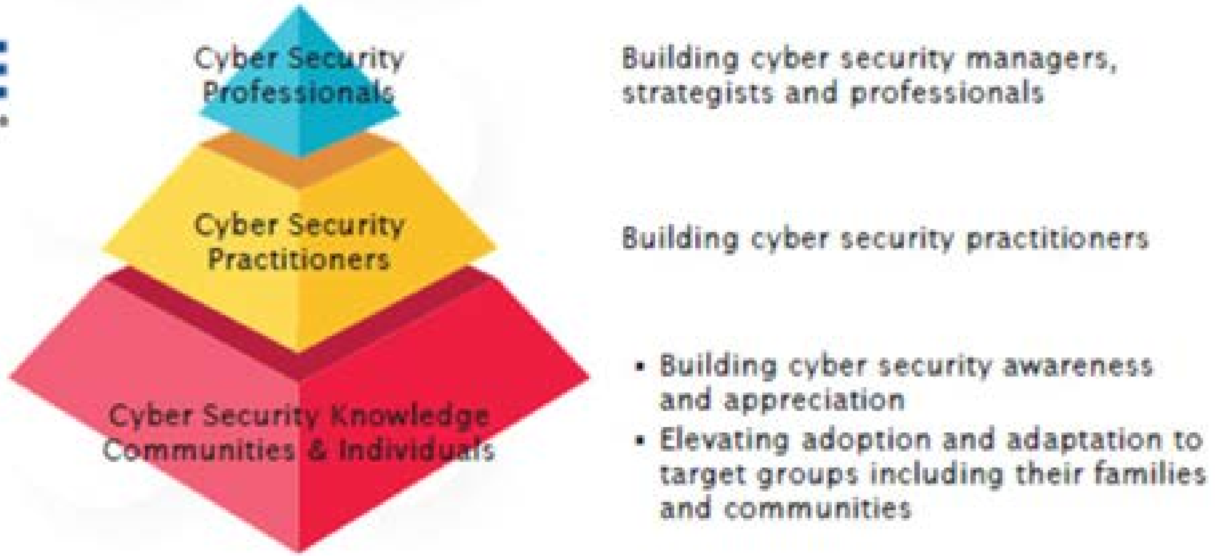
PEOPLE

CYBERSECURITY CAPACITY BUILDING FRAMEWORK

Global ACE Scheme
https://www.cybereducationscheme.org

Cyberguru
https://www.cyberguru.my

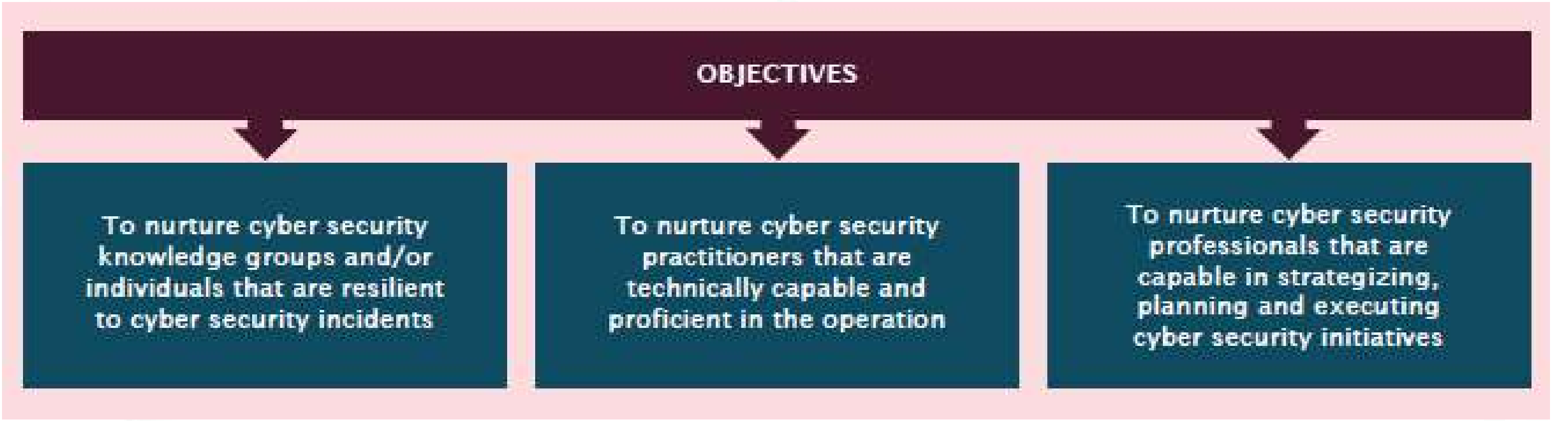
Cybersafe
https://www.cybersafe.my


Cyber Security Professionals
Cyber Security Practitioners
Cyber Security Knowledge Communities & Individuals

Building cyber security managers, strategists and professionals

Building cyber security practitioners

- Building cyber security awareness and appreciation
- Elevating adoption and adaptation to target groups including their families and communities



OBJECTIVES

To nurture cyber security knowledge groups and/or individuals that are resilient to cyber security incidents

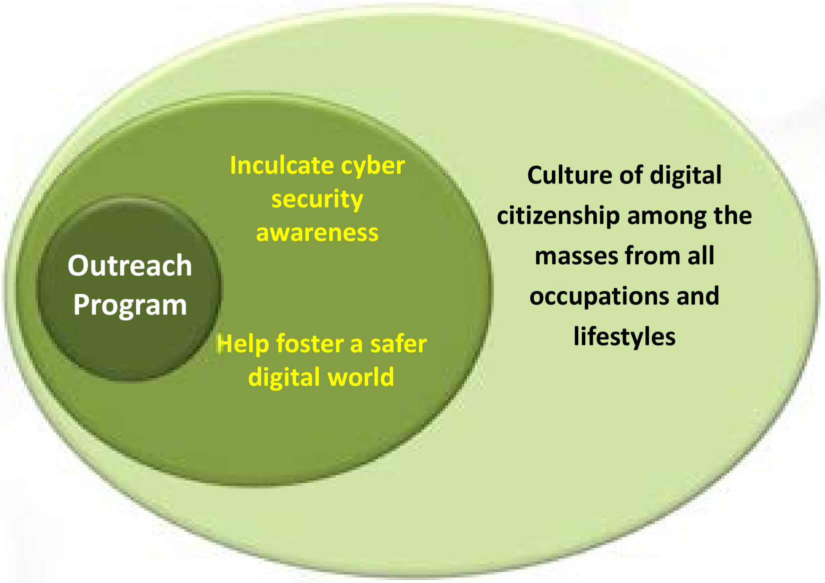
To nurture cyber security practitioners that are technically capable and proficient in the operation

To nurture cyber security professionals that are capable in strategizing, planning and executing cyber security initiatives

CYBERSECURITY AWARENESS FOR EVERYONE (CyberSAFE)

- **CyberSAFE** launched **YAB Deputy Prime Minister**
- Reached out to more than **34,000** students, teachers, adults and more than **190** schools / organisations
- Awareness program referred to by **Australian Communications** and **Media Authority**

Make it a priority to provide those on the frontlines with the information, tools and resources necessary to increase the national awareness level on the importance of cyber security.



Outreach Program

Inculcate cyber security awareness

Help foster a safer digital world

Culture of digital citizenship among the masses from all occupations and lifestyles

CyberSAFE Ambassador
CyberSAFE Mentor
CyberSAFE
Cyber Security Awareness For Everyone
In Schools
Safer Internet Day (SID)
SID :
EDISI MALAYSIA
NICTSeD
NATIONAL ICT SECURITY DISCOURSE
Ceramah Kesedaran
CYBER SECURITY AWARENESS TALK
CyberQuest
CyberSAFE@ CyberQuest EXPLORACE
POSTERS, INFOGRAPHICS DAN WEBINAR
Kajian dan Garis Panduan

DEVELOP CYBERSECURITY PROFESSIONALS

CyberGuru

Cyber Security Capacity Development Collaboration

CyberSecurity Malaysia bundles its training programs into selected local and international training programs and work closely with industry collaborators to further enhance, deliver and market these services effectively and efficiently.

Cyber Security Academic Collaboration

Universiti Kebangsaan Malaysia
The National University of Malaysia
UUM
Universiti Utara Malaysia
UTeM
Universiti Teknikal Malaysia Melaka
UTM
UMT
Universiti Sains Islam Malaysia
UTHM
UPM
Politeknik Malaysia Mersing
Universiti Tenaga Nasional
The Energy University
UTP
HELP University
university of achievers

BUILDING CYBER SECURITY MANAGERS, STRATEGISTS AND PROFESSIONALS

CyberSecurity MALAYSIA

GLOBAL ACE CERTIFICATION

Global ACE Certification was selected as the Winner of the Category 5: Building Confidence and Security in the Use of ICT at WSIS Prizes 2020

GOAL & OBJECTIVES

GOAL

To create world class competent work-force in cyber security and promote the development of cyber security professional programmes within the region

OBJECTIVES

1 To establish a professional certification programme that is recognized globally

2 To provide cyber security professionals with the right knowledge, skills, attitude (KSA) and experience

3 To promote the development of cyber security professional programmes globally

4 To ensure accredited personnel has been independently assessed and committed to a consistent and high-quality service level

GLOBAL ACE CERTIFICATION TRAINING PROGRAMMES

A. Currently running Global ACE Certification Programmes

1. Certified Digital Forensics First Responder
2. Certified Information Security Management System Auditor
3. Certified Penetration Tester
4. Certified Secured Applications Practitioner
5. Certified Information Security Awareness Manager
6. Certified MyCC Evaluator
7. Certified Data Security Analyst
8. Certified IoT Security Analyst
9. Certified Cybersecurity Awareness Educator
10. Certified Security Operations Centre Analyst
11. Certified Incident Handling and Network Security Analyst
12. Certified IP Associate
13. Certified IT Associate
14. Certified Cybersecurity Data Science Analyst
15. Certified Mobile Security Analyst
16. Certified Cyber Law Practitioner
17. Certified Cybersecurity Risk Manager

B. Ready by 2023/2024

1. Certified Industrial Control System Security Analyst
2. Certified Secure Web Application (PHP) Developer
3. Certified Smart Card Reader Analyst
4. Certified Cloud Security Auditor
5. Certified IoT Blockchain Practitioner
6. Certified Cyber Forensics Analyst
7. Certified Web Application Penetration Tester
8. Certified Data Privacy Officer
9. Certified Data Privacy Specialist
10. Certified Chief Data Privacy Officer
11. Certified Cryptocurrency Seizing Officer

PROCESS

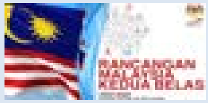
CSM's Role in **Supporting National** Cybersecurity Related Policies & Strategic Plans

National Technical Cybersecurity Agency responsible to **advice & implement** cybersecurity related programs

Kerangka Strategik KKD

Strategic Thrust 2:
Driving the Digital Economy and IT Towards Developed Countries

Strategic Thrust 3:
Strengthen the regulation of a reliable and stable communications and multimedia ecosystem



Rancangan Malaysia Kedua Belas (RMK-12)

Pillar 1: Source of Growth

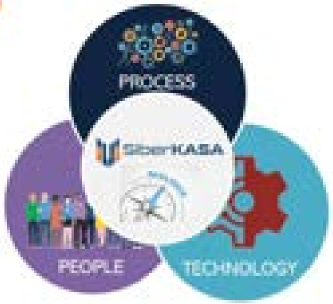
Pillar 4: Human Capital Transformation and Market Strengthening Labor:

Pillar 5: Inclusivity and People's Well being

Pillar 6: Institutional Reform

Pillar 7: Social Capital

SiberKASA



Malaysia Digital Economy Blueprint

Thrust 1: Drive digital transformation in the public sector

Thrust 4: Build agile and competent digital talent

Thrust 6: Build trusted, secure and ethical digital environment

Malaysia Cyber Security Strategy

Pillar 1: Effective Governance and Management

Pillar 2: Strengthening Legislative Framework and Enforcement

Pillar 3: Catalysing World Class Innovation, Technology, R&D and Industry

Pillar 4: Enhancing Capacity and Capability Building, Awareness and Education

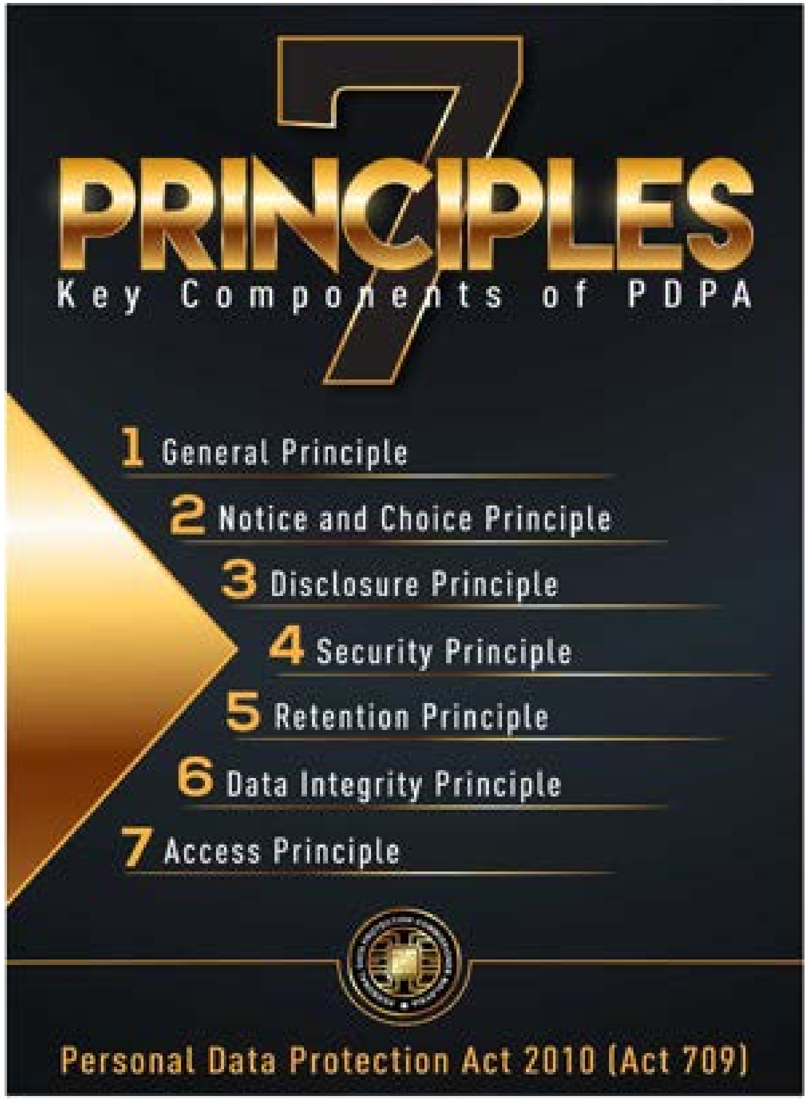
Pillar 5: Strengthening Global Collaboration

National 4th Industrial Revolution Policy (N4IR)

Thrust 1:
Equip the Rakyat with 4IR knowledge and skill sets

Thrust 3:
Future-proof regulations to be agile with technological changes

Personal Data Protection Act 2010 (PDPA)



7 PRINCIPLES

Key Components of PDPA

1 General Principle

2 Notice and Choice Principle

3 Disclosure Principle

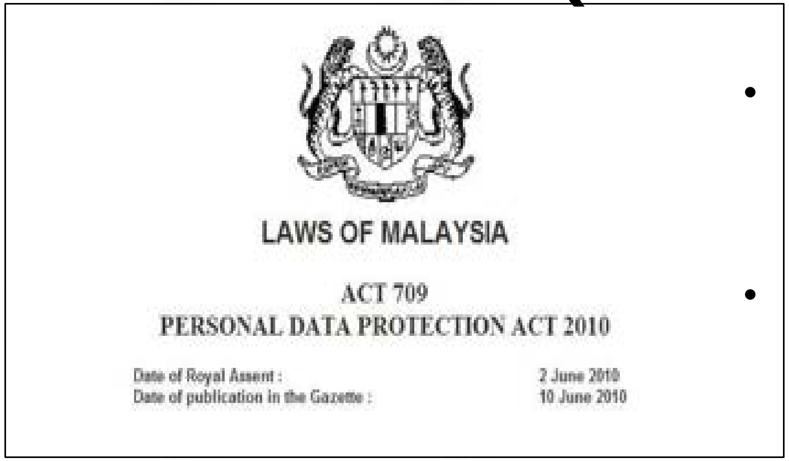
4 Security Principle

5 Retention Principle

6 Data Integrity Principle

7 Access Principle

Personal Data Protection Act 2010 (Act 709)



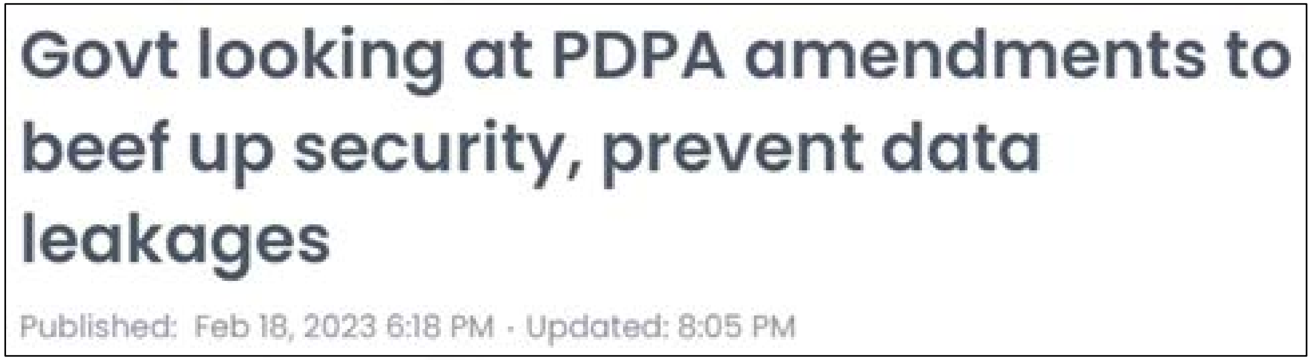
LAWS OF MALAYSIA

ACT 709

PERSONAL DATA PROTECTION ACT 2010

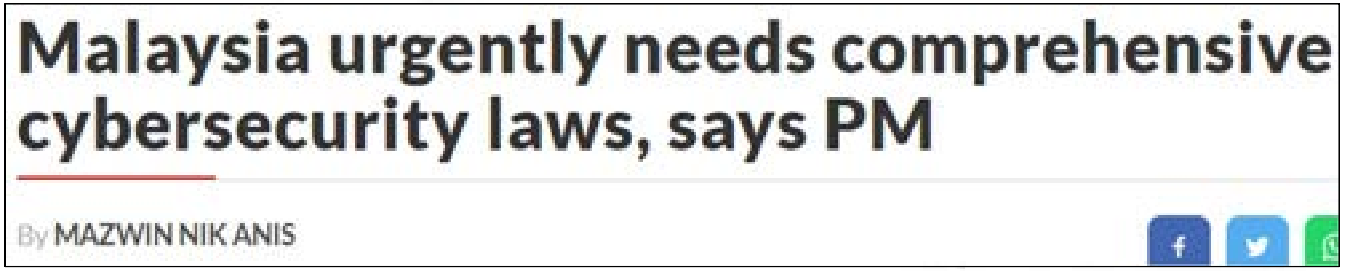
Date of Royal Assent :	2 June 2010
Date of publication in the Gazette :	10 June 2010

- Governs personally identifiable data collected via commercial transactions.
- Malaysia's PDPA is aligned with the EU's GDPR.



Govt looking at PDPA amendments to beef up security, prevent data leakages

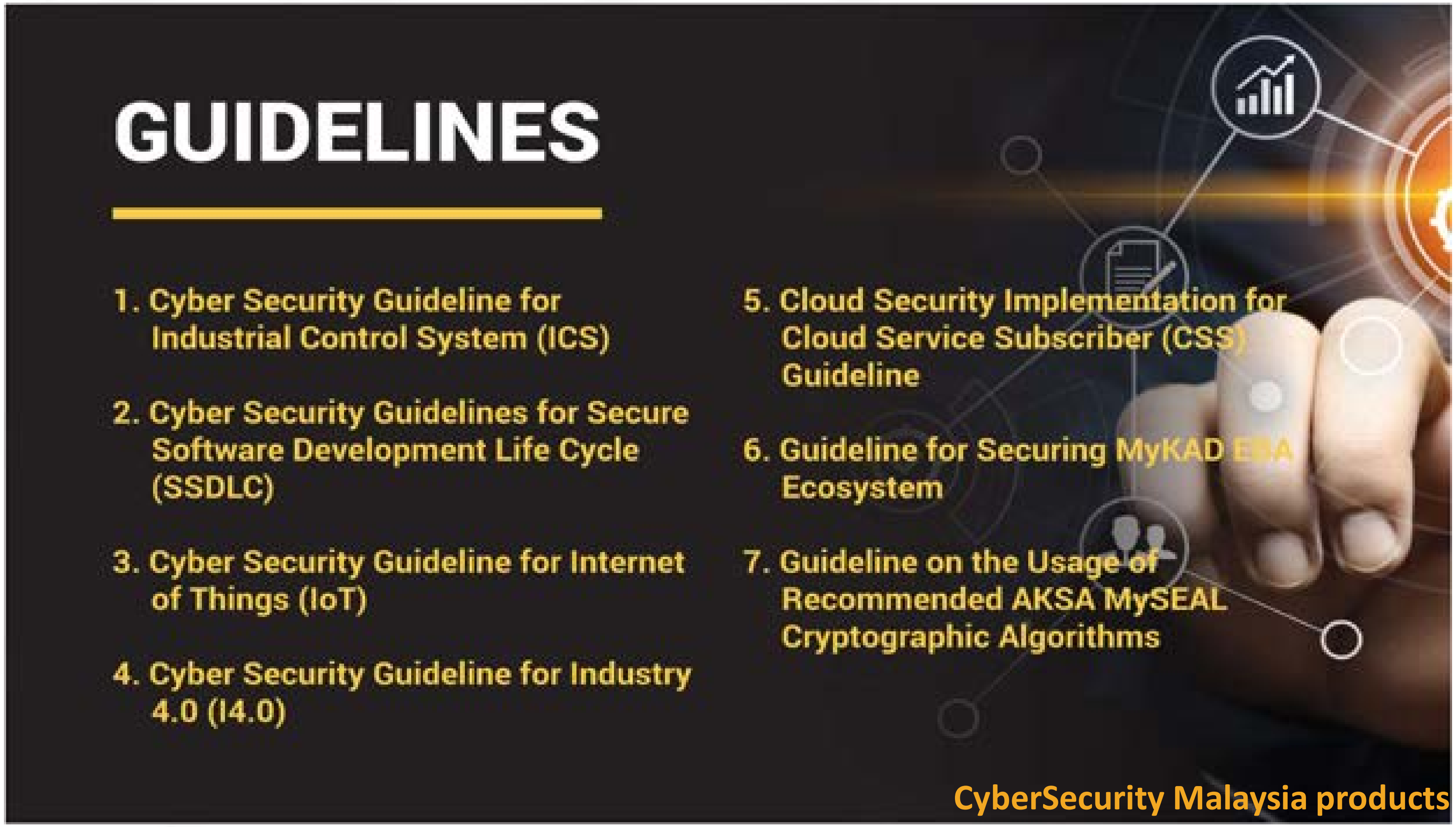
Published: Feb 18, 2023 6:18 PM · Updated: 8:05 PM



Malaysia urgently needs comprehensive cybersecurity laws, says PM

By MAZWIN NIK ANIS

ADDRESSING CYBERSECURITY ISSUES THROUGH GUIDELINES



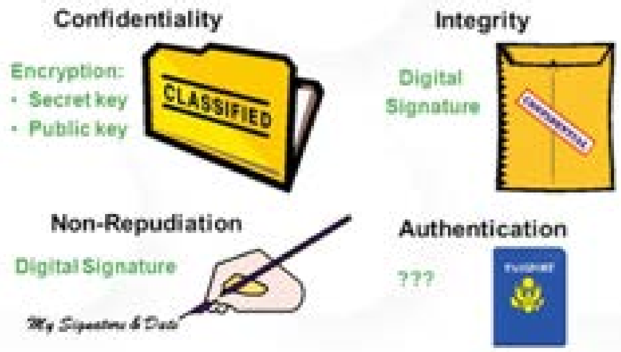
GUIDELINES

1. Cyber Security Guideline for Industrial Control System (ICS)
2. Cyber Security Guidelines for Secure Software Development Life Cycle (SSDLC)
3. Cyber Security Guideline for Internet of Things (IoT)
4. Cyber Security Guideline for Industry 4.0 (I4.0)
5. Cloud Security Implementation for Cloud Service Subscriber (CSS) Guideline
6. Guideline for Securing MyKAD EBA Ecosystem
7. Guideline on the Usage of Recommended AKSA MySEAL Cryptographic Algorithms

CyberSecurity Malaysia products

CyberSecurity Malaysia

ADDRESSING CYBERSECURITY THROUGH ENCRYPTION TECHNOLOGY



- **NATIONAL CRYPTOGRAPHY POLICY** approved by The Government In January 2013

- Comprehensive applications of cryptography in Government to Government (G2G), Government to Citizens (G2C), Government to Business (G2B) and Business to Business (B2B) activities towards ensuring a secure and trusted cyber environment.

- Cryptography also supports the National Digital Economy and the realization of the National Transformation Agenda to transform Malaysia into becoming an advanced and high-income nation

Proactive Services

Information Security Certification Body (ISCB)

Information Security Certification Body (ISCB) is a department within CyberSecurity Malaysia that **manages certification services focusing on the information security according to international standards and guidelines**. Among the services under ISCB:

- ❖ Information Security Management System (ISMS) Audit and Certification - CSM27001 Scheme
- ❖ Privacy Information Management System (PIMS)
- ❖ Business Continuity Management System (BCMS)
- ❖ MyTrustSEAL – web security validation
- ❖ Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme

MANAGEMENT SYSTEM CERTIFICATION

Process Certification

Continuous Audits conducted by Independent and Accredited Certification Body

ISO/IEC 27001
Information Security Management Systems

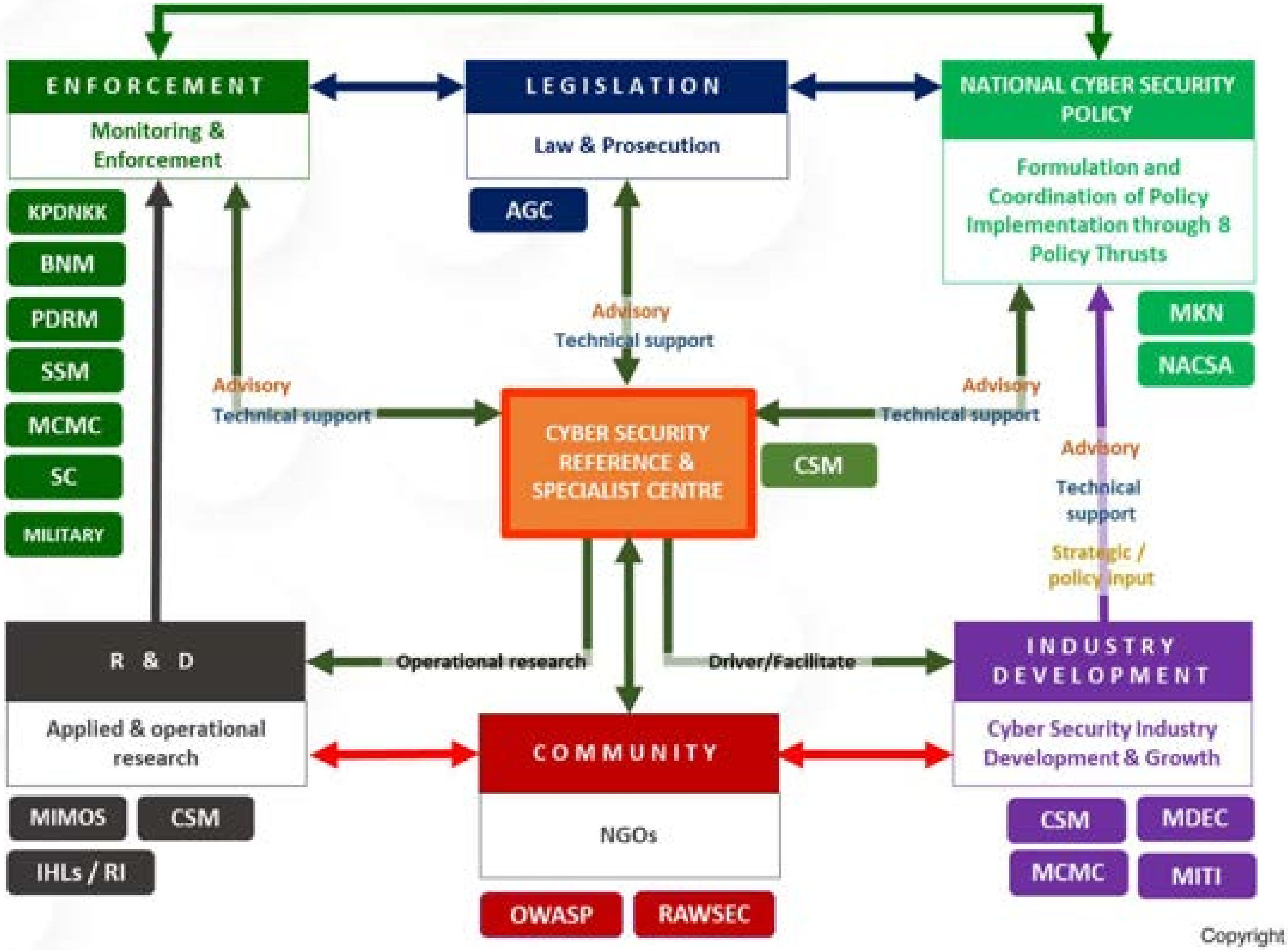
Specifies requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization which includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.

ISO 22301
Business Continuity Management Systems

Specifies requirements to plan, establish, implement, operate, monitor, review maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to and recover from disruptive incidents when they arise.

DOMESTIC COLLABORATION

CYBERSECURITY MALAYSIA ENGAGEMENT ECOSYSTEM



ENFORCEMENT

Monitoring & Enforcement

KPDNKK

BNM

PDRM

SSM

MCMC

SC

MILITARY

LEGISLATION

Law & Prosecution

AGC

NATIONAL CYBER SECURITY POLICY

Formulation and Coordination of Policy Implementation through 8 Policy Thrusts

MKN

NACSA

Advisory

Technical support

Advisory

Technical support

Advisory

Technical support

CYBER SECURITY REFERENCE & SPECIALIST CENTRE

CSM

Advisory

Technical support

Strategic / policy input

R & D

Applied & operational research

MIMOS

CSM

IHLs / RI

Operational research

Driver/Facilitate

INDUSTRY DEVELOPMENT

Cyber Security Industry Development & Growth

CSM

MDEC

MCMC

MITI

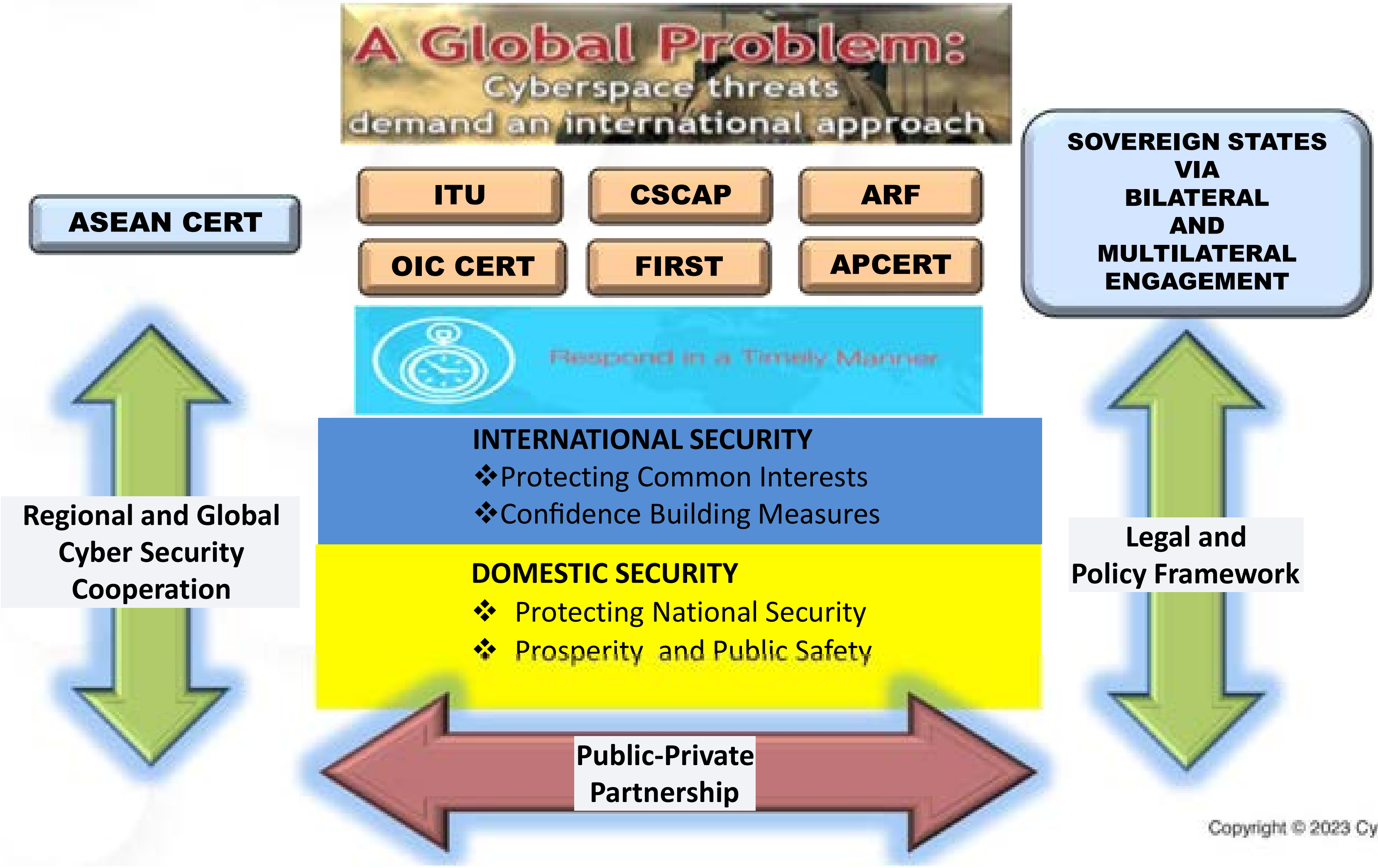
COMMUNITY

NGOs

OWASP

RAWSEC

INTERNATIONAL COLLABORATION
- Global Collaborative Efforts And Engagements



A Global Problem:
Cyberspace threats
demand an international approach

ASEAN CERT

ITU

CSCAP

ARF

OIC CERT

FIRST

APCERT

SOVEREIGN STATES VIA BILATERAL AND MULTILATERAL ENGAGEMENT

Respond in a Timely Manner

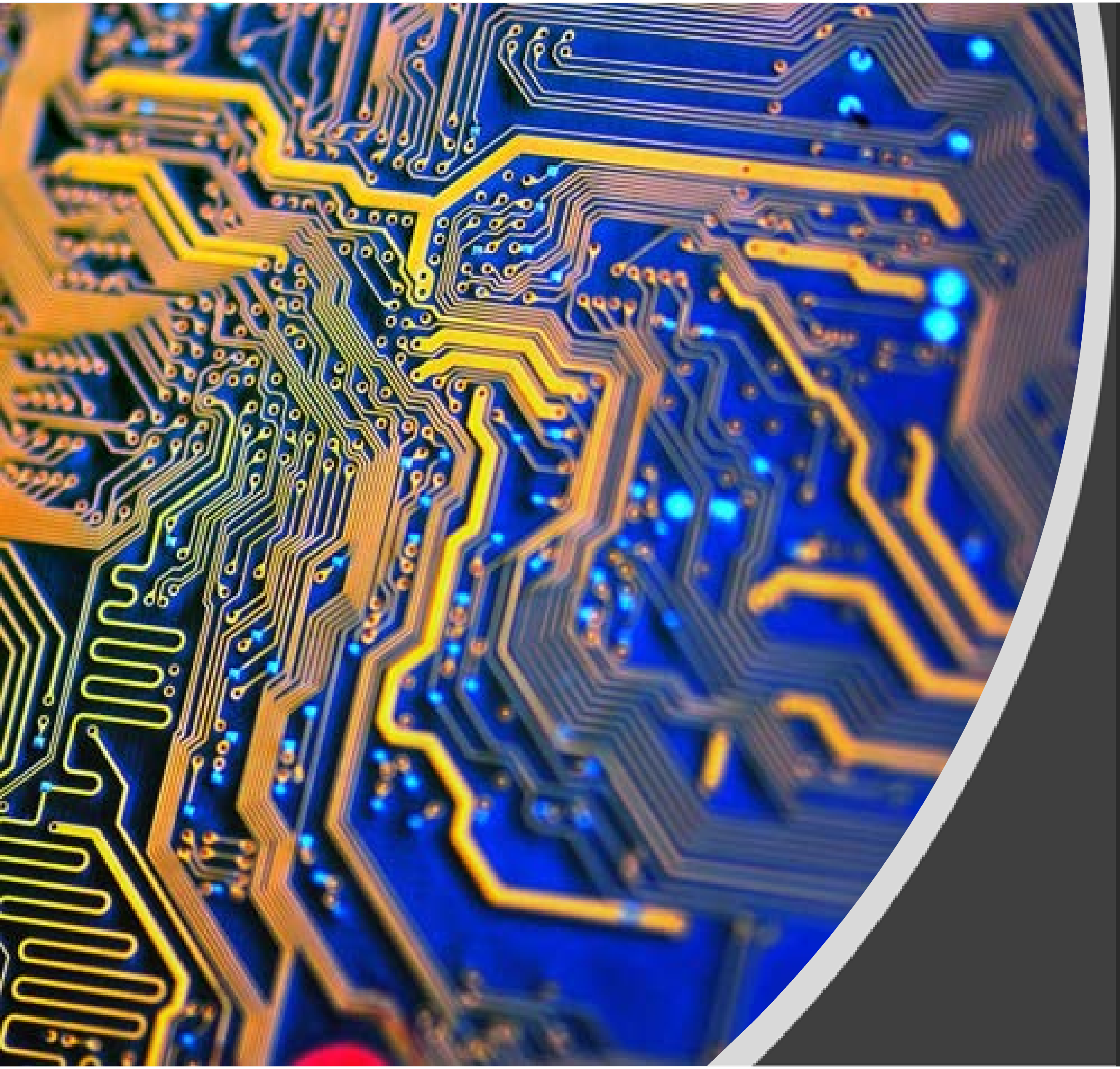
INTERNATIONAL SECURITY
❖Protecting Common Interests
❖Confidence Building Measures

DOMESTIC SECURITY
❖ Protecting National Security
❖ Prosperity and Public Safety

Regional and Global Cyber Security Cooperation

Legal and Policy Framework

Public-Private Partnership

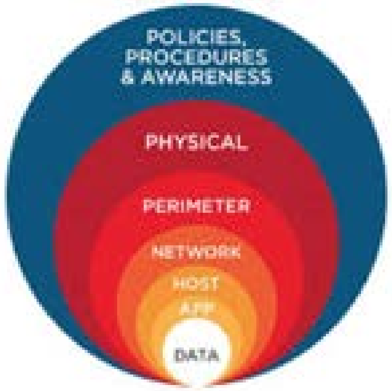


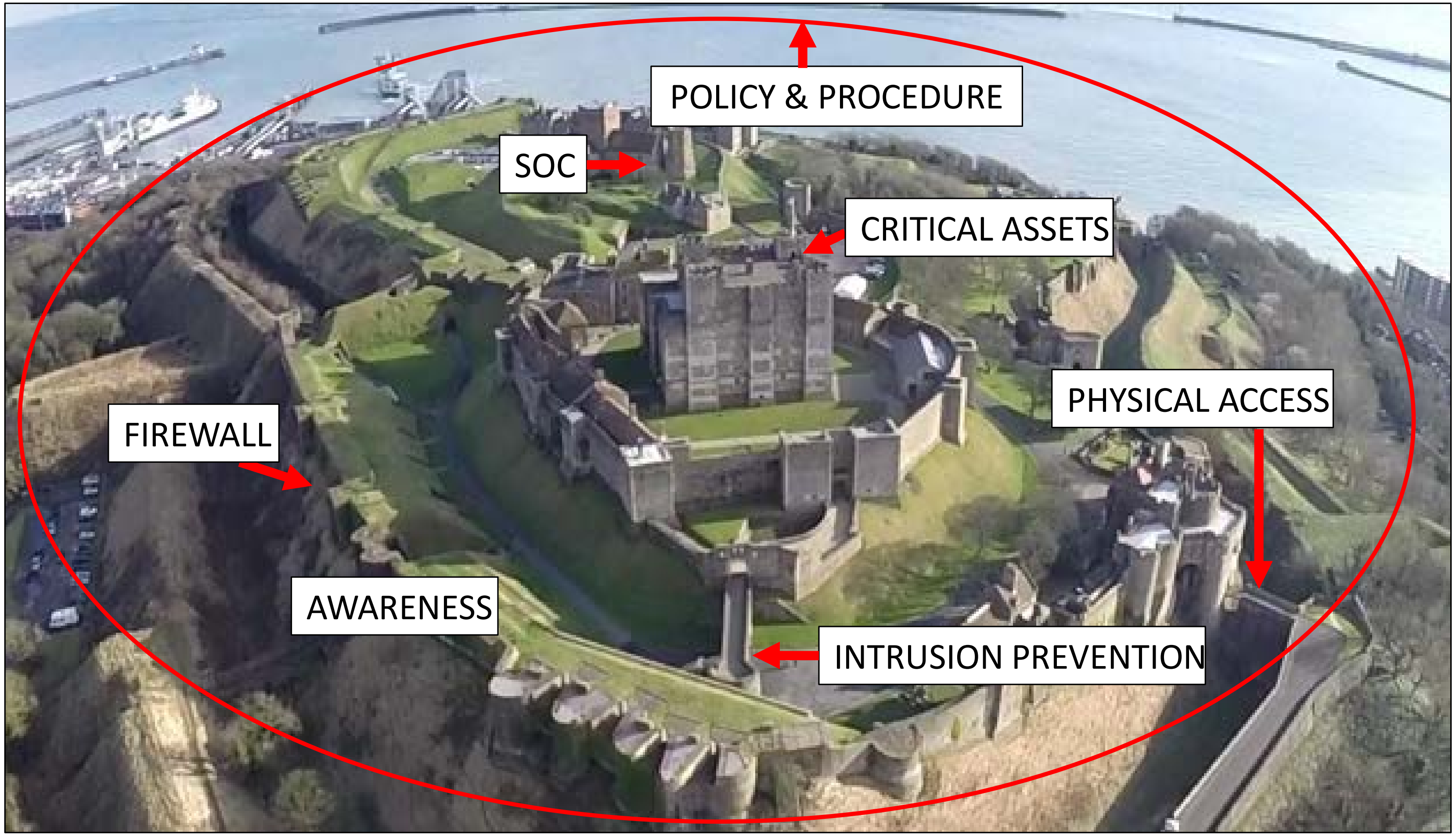
TECHNOLOGY

TRADITIONAL CYBERSECURITY APPROACH
- Not sufficient to deal with smart cyber threats

Protecting networks, data and devices in today's environment requires a multipronged approach that accounts for every possible vulnerability and entry point. We are way beyond firewalls and antivirus here.

DEFENSE IN DEPTH





POLICY & PROCEDURE

SOC

CRITICAL ASSETS

PHYSICAL ACCESS

FIREWALL

AWARENESS

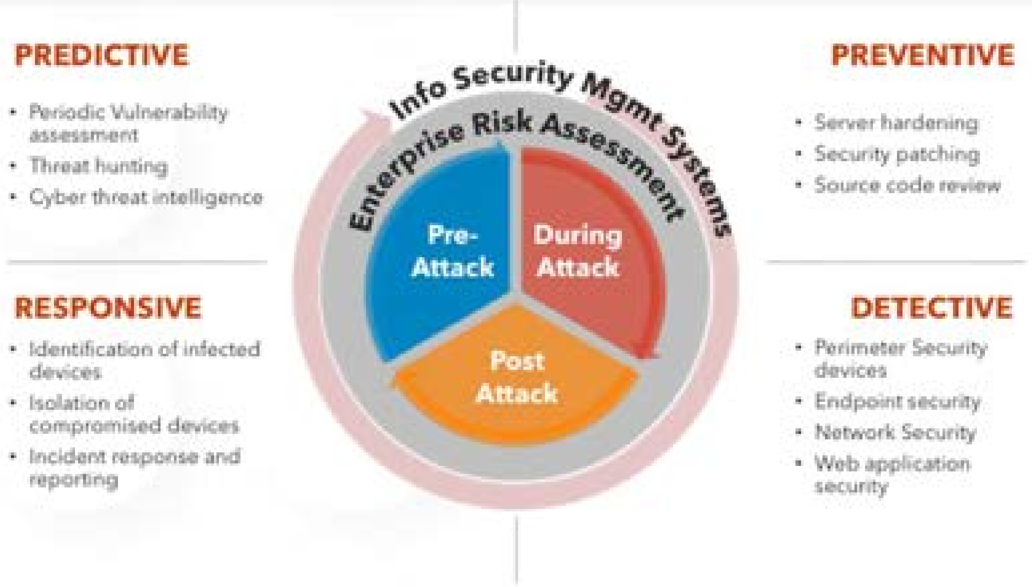
INTRUSION PREVENTION

This is an approach that relies on using a layered and redundant defensive mechanism to protect data and assets from cyber-attacks.

ADDRESSING CYBER RESILIENCY THROUGH ADAPTIVE SECURITY

To be more proactive, dynamic and integrated in cybersecurity approach

Adaptive Security is an approach to cybersecurity that analyzes behaviors and events to protect against and *adapt* to threats before they happen. With an Adaptive Security Architecture, an organization can continuously assess risk and automatically provide proportional enforcement that can be dialed up or down



PREDICTIVE

- Periodic Vulnerability assessment
- Threat hunting
- Cyber threat intelligence

PREVENTIVE

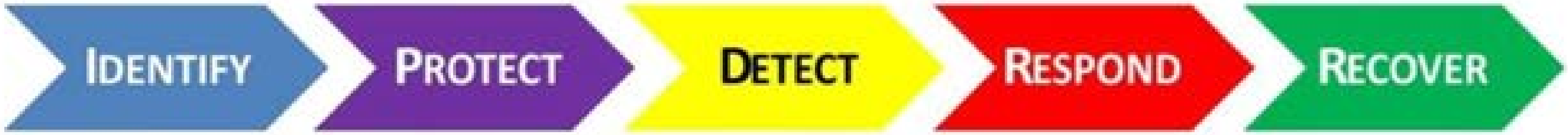
- Server hardening
- Security patching
- Source code review

RESPONSIVE

- Identification of infected devices
- Isolation of compromised devices
- Incident response and reporting

DETECTIVE

- Perimeter Security devices
- Endpoint security
- Network Security
- Web application security



The cost to organizations comes at each stage of the incident response lifecycle — **detection, notification, responses, post-incidents**, and the **cost of business losses**.

STRENGTHENING CYBERSECURITY THROUGH PREDICTIVE CYBER THREAT INTELLIGENCE (CTI)

AHMAD FAUZI (dua dari kanan) dan Amiruddin (dua dari kiri)

Makmal khas tangani serangan siber

Oleh AHMAD ISYAFIQ MAD DESA

JOHOR BAHRU – Universiti Teknologi Malaysia (UTM) menubuhkan makmal khas bertujuan melaksanakan kajian mengenai kaedah menangkis serangan siber yang semakin menular kini.

Timbalan Naib Canselor (Penyelidikan dan Inovasi) UTM, Prof. Dr. Ahmad Fauzi Ismail berkata, penubuhan UTM-CSM Cyber Security X Lab yang menelan kos sebanyak RM100,000 itu merupakan sebahagian daripada komitmen universiti mengekang je-

Beliau berkata, makmal yang ditempatkan di bawah Fakulti Pengkomputeran UTM menempatkan para penyelidik sepenuh masa.

"Fakulti berkenaan mempunyai 170 pensyarah dalam pelbagai bidang berkaitan teknologi siber. Sebanyak 15 penyelidik di UTM-CSM Cyber Security X Lab akan bertindak menangani jumlah serangan siber dan teknik penggodaman yang semakin canggih kini," katanya.

Beliau berkata demikian pada sidang akhbar selepas Majlis Menandatangani Perjanjian (MoU) antara UTM dan CyberSecurity Malaysia di sini semalam.

Hadir sama Ketua Pengarah Eksekutif CSM, Dr. Amiruddin Abdul Wahab.

Berdasarkan statistik terkini, kadar jenayah siber sedang meningkat di negara ini dengan purata 10,000 kes dilaporkan setiap tahun.

Ahmad Fauzi menambah, sebagai permulaan, UTM menerima peruntukan sebanyak RM360,000 daripada CSM untuk disalurkan kepada pembangunan projek yang dirancang.

"Pada peringkat awal, kerjasama kita menumpukan tiga bidang iaitu Malware Analitik, risikan ancaman siber dan ancaman berterusan

CyberSecurity MALAYSIA

ADDRESSING CYBERSECURITY THROUGH RESPONSIVE TECHNOLOGY & SERVICES

DIGITAL FORENSIC (DF)

CyberCSI

crime scene investigation

CyberDEF

Uncovering Future Threats

Cyber Detect, Eradicate and Forensics (CyberDEF)

Evidence Preservation Facility

CyberDiscovery

Digital Forensic Lab

X-Forensics Tools

PenDua

Kloner

Expert Development Lab

Data Recovery Lab

CamMuka V2.0

MyCERT

Malaysia Computer Emergency Response Team

CMERP

Detection | Eradication | Remediation

Coordinated Malware Eradication & Remediation Project (CMERP)

LebahNET.MY

Cybersecurity Honeynet Project

Lebahnet (Honeynet Project)

MyCERT

MASSA

Cyber Early Warning

Technical Coordination Centre

Cyber Threat Research Centre (CTRC)

Computer Security Incident Response Team (CSIRT) Consultancy

CyberSecurity Malaysia

malware research centre

Malware Research Center

Cyber999

Cyber999 Help Centre

STRENGTHENING CYBER SECURITY PREVENTION THROUGH TECHNOLOGY VULNERABILITY ASSESSMENT

Secure Software Development Lifecycle (SSDLC) Lab & Services

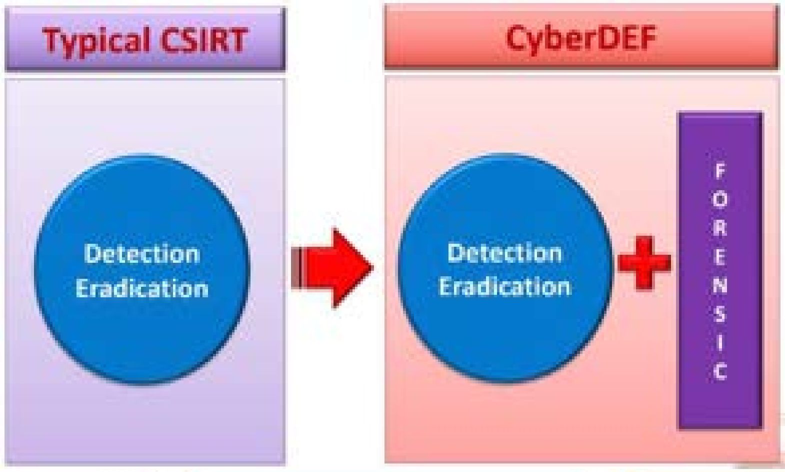
Internet of Things (IOT) Lab

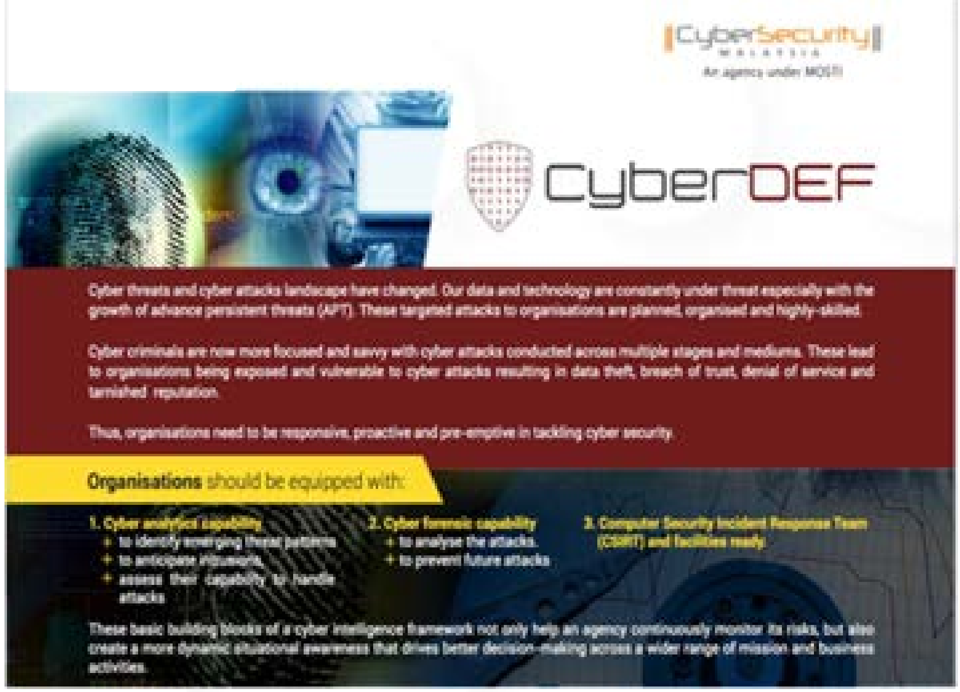
Robotic Lab (4th Industry Revolution)

ADDRESSING CYBERSECURITY THROUGH STRENGTHENING DETECTION TECHNOLOGY

CyberD.E.F

- Detection
- Eradication
- Forensic




CyberSecurity MALAYSIA
An agency under MOSTI
CyberDEF

Cyber threats and cyber attacks landscape have changed. Our data and technology are constantly under threat especially with the growth of advance persistent threats (APT). These targeted attacks to organisations are planned, organised and highly-skilled.

Cyber criminals are now more focused and savvy with cyber attacks conducted across multiple stages and mediums. These lead to organisations being exposed and vulnerable to cyber attacks resulting in data theft, breach of trust, denial of service and tarnished reputation.

Thus, organisations need to be responsive, proactive and pre-emptive in tackling cyber security.

Organisations should be equipped with:

1. Cyber analytical capability
   - to identify emerging threat patterns
   - to anticipate situations
   - assess their capability to handle attacks
2. Cyber forensic capability
   - to analyse the attacks.
   - to prevent future attacks
3. Computer Security Incident Response Team (CSIRT) and facilities ready

These basic building blocks of a cyber intelligence framework not only help an agency continuously monitor its risks, but also create a more dynamic situational awareness that drives better decision-making across a wider range of mission and business activities.

Detection

Identify any loopholes, vulnerabilities and existing threats

1. Sensors
2. Sandbox
3. Analytics
4. Visualization

Eradication

Close loopholes, patch vulnerabilities and neutralize existing threats

Perform cyber threats exercise or drill to test the feasibility and resiliency of the new defense / prevention system

Forensics

1. E-Discovery
2. Root cause analysis
3. Investigation
4. Forensics readiness
5. Forensic compliance

CONCLUSION AND WAY FORWARD

- There is no such thing as 100% security. There is still much room for improvement. We need to increase and strengthen our cybersecurity manpower and professional skills.

- This involves an ongoing process of identifying security risks and implementing plans to address them. Risk is determined by considering the likelihood that known threats will exploit vulnerabilities and the impact they may have on valuable assets.

- Furthermore, there is a need to ensure a secure, resilient, and trusted cyber environment to sustain progress and prosperity. In this regard, a more innovative and proactive adaptive security approach is required to address such situations. Adaptive cybersecurity encompasses predictive, detective, responsive, and corrective capabilities.

- Additionally, our approach also needs to be adaptive, dynamic, and innovative, covering people, processes, and technology.

MINISTRY OF
COMMUNICATIONS AND DIGITAL

CyberSecurity
MALAYSIA

THANK YOU

CyberSecurity Malaysia
Level 7, Tower 1, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya
Selangor Darul Ehsan, Malaysia

T +603 8800 7999 | **F** +603 8008 7000 | **H** +61 300 88 2999

www.cybersecurity.my | info@cybersecurity.my

f CyberSecurityMalaysia   cybersecuritymy   cybersecuritymy   in CyberSecurity Malaysia   cybersecurity_my

JUBLI PERAK

SIBER MALAYSIA MADANI

AiSP

Association of
Information Security Professionals

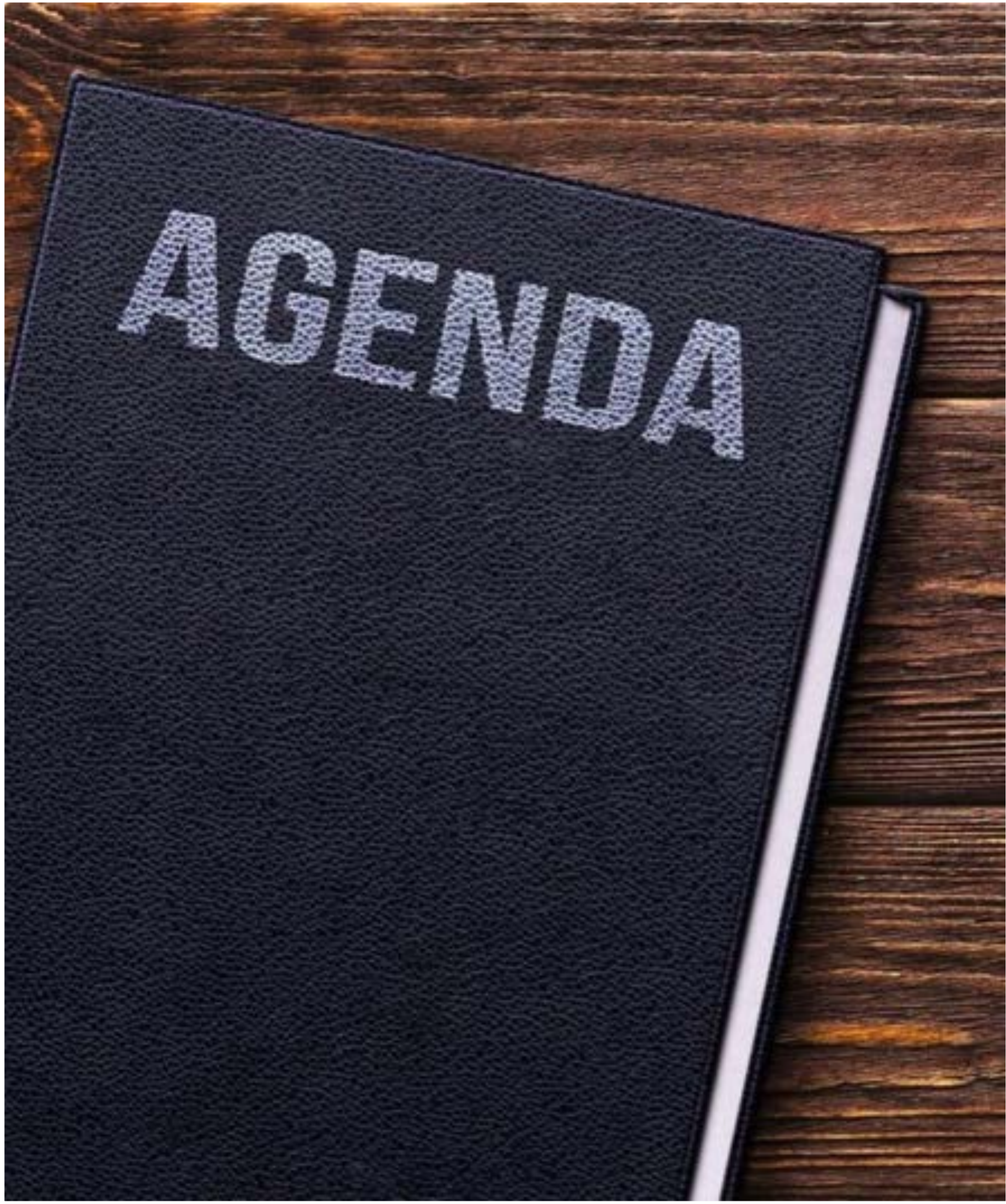
Challenges in building ASEAN Cyber Resilience

Tony Low, AiSP VP

Royalty-free image for Microsoft O365 subscribers.

Today’s Agenda

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



[Unknown]
Inflation & Recession

Not Skilled

Journey is rough

My Business

Treacherous Digital + Business Environment

Source: Movie Scene from Dunkirk 2017

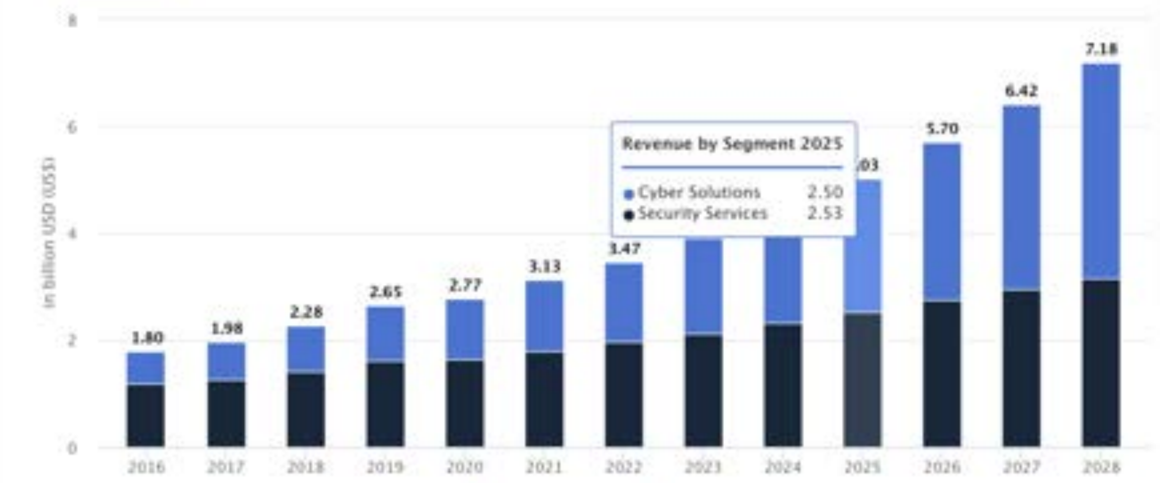
State of Digital and Cyber Security of ASEAN

Huge opportunity within Asean Post Pandemic and Beyond

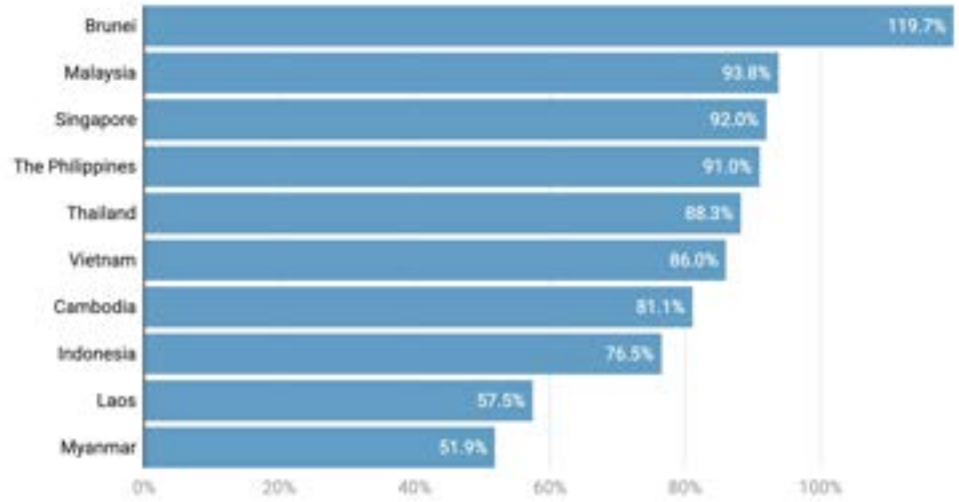
- **Foreign businesses** expect sales in the region to grow by 23.2% in 2023
- ASEAN is on track to become the world's **largest** market by 2030.
- Celebrated young and dynamic population with **34%** of ASEAN's population consists of young people, aged between **15 and 34 years old**
- In 2023, **86%**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

AiSP

REVENUE BY SEGMENT



Internet penetration rate in ASEAN



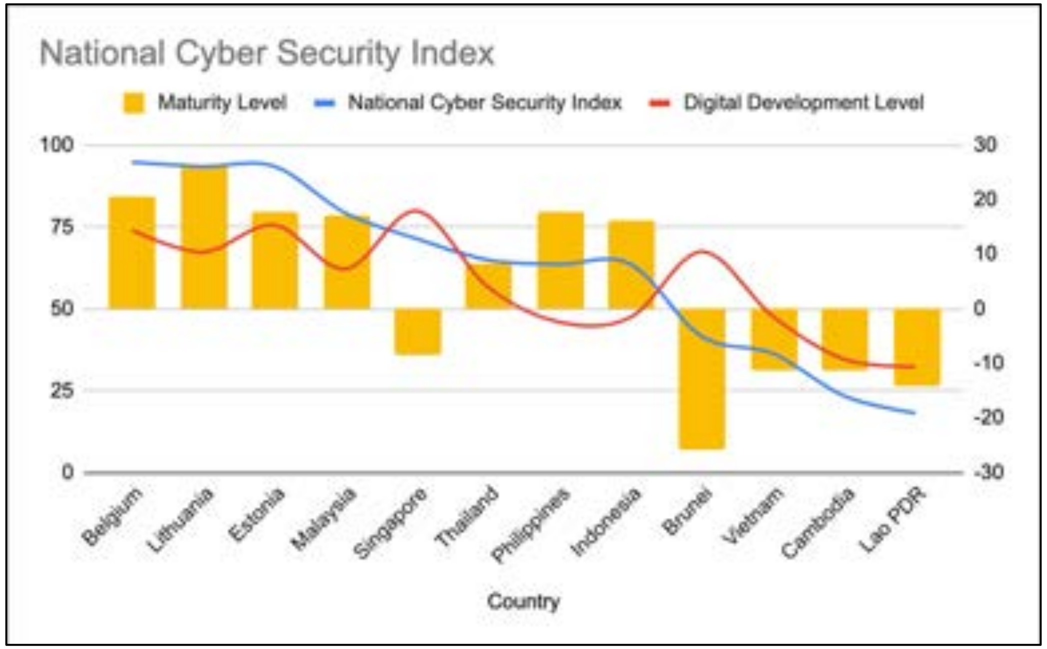
Data as of July 2022

Source: Statista • Get the data • Created with Datawrapper

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

Some Examples:

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



Source: NCSI ,**Survey by:** NCSI
Release date
July 2023

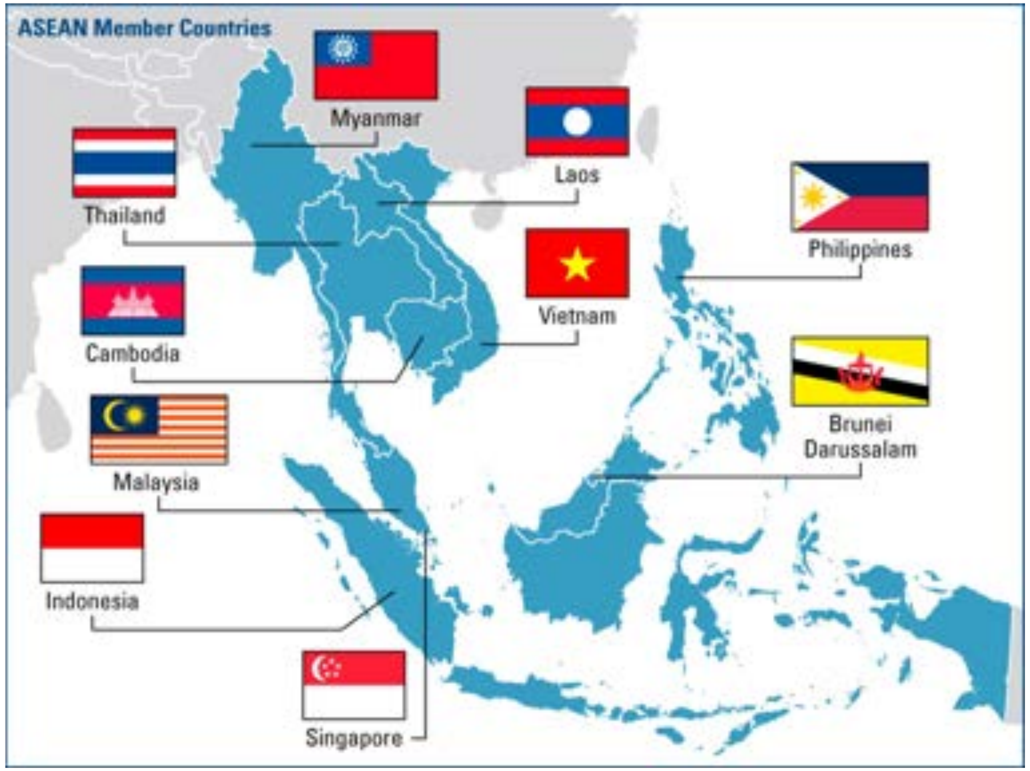
ASEAN countries can emerged as launchpads for cyberattacks

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

What are the countries in ASEAN facing today in Cybersecurity?

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

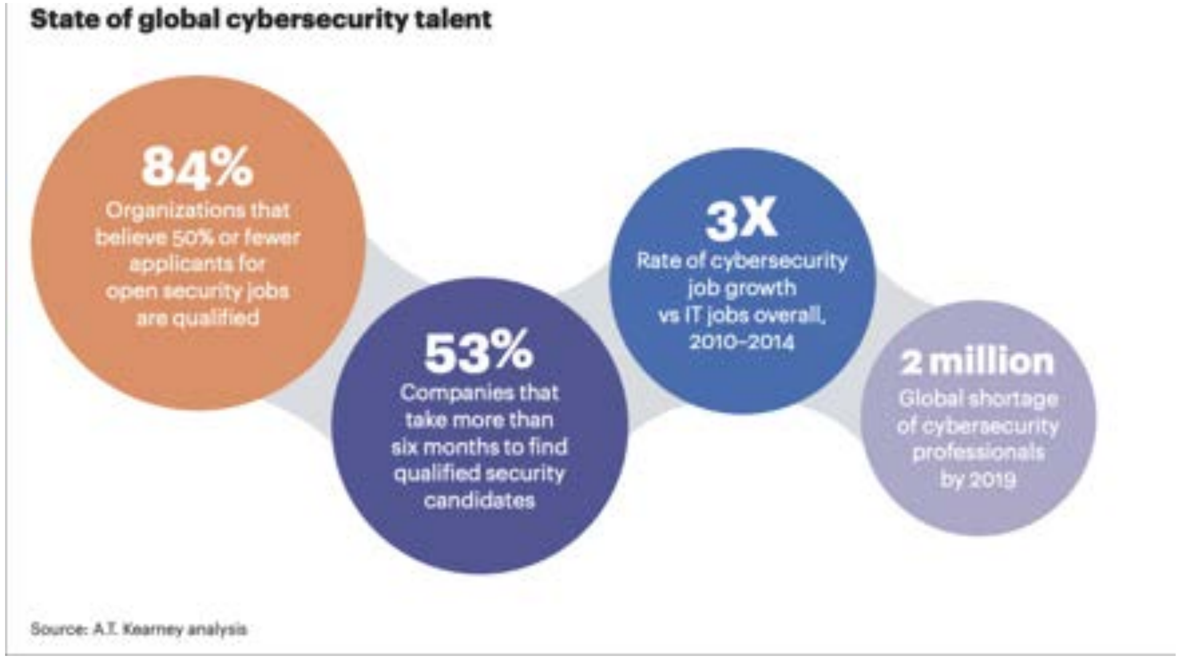
- **Limited resources**: Needed more resources to invest in cybersecurity, implementing necessary security measures and developing a skilled cybersecurity workforce
- **Lack of awareness**: General population must be fully aware of the cybersecurity risks they face, understand careless behavior makes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



Limited Resources - Talent, Budget & Capabilities

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

State of global cybersecurity talent



84% Organizations that believe 50% or fewer applicants for open security jobs are qualified

53% Companies that take more than six months to find qualified security candidates

3X Rate of cybersecurity job growth vs IT jobs overall, 2010–2014

2 million Global shortage of cybersecurity professionals by 2019

Source: A.T. Kearney analysis

Varying Maturity and approach towards Cybersecurity

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

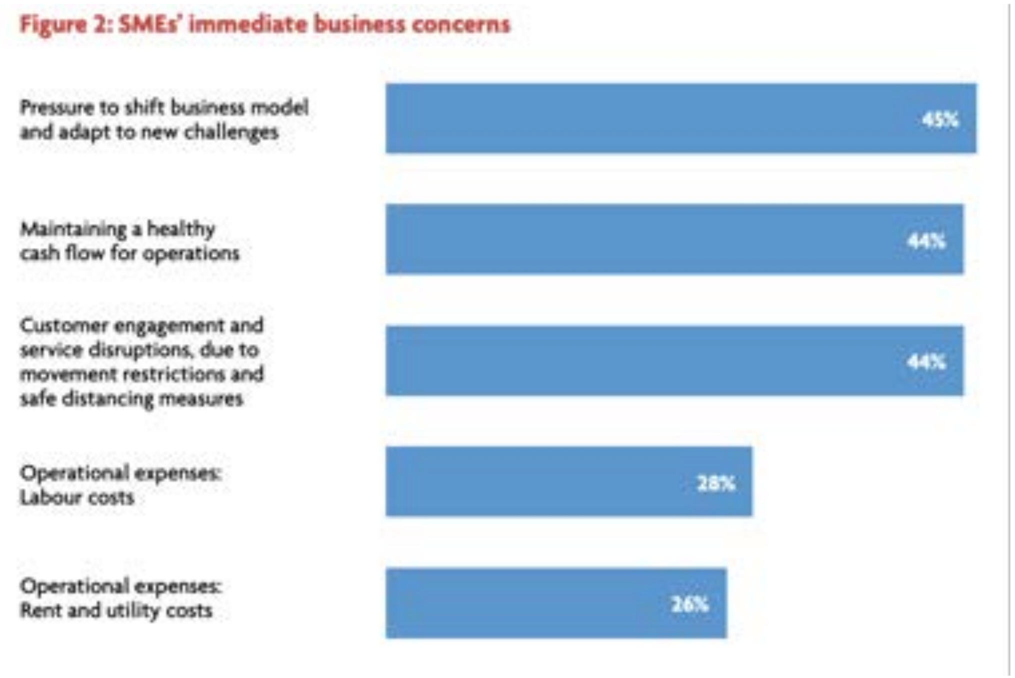
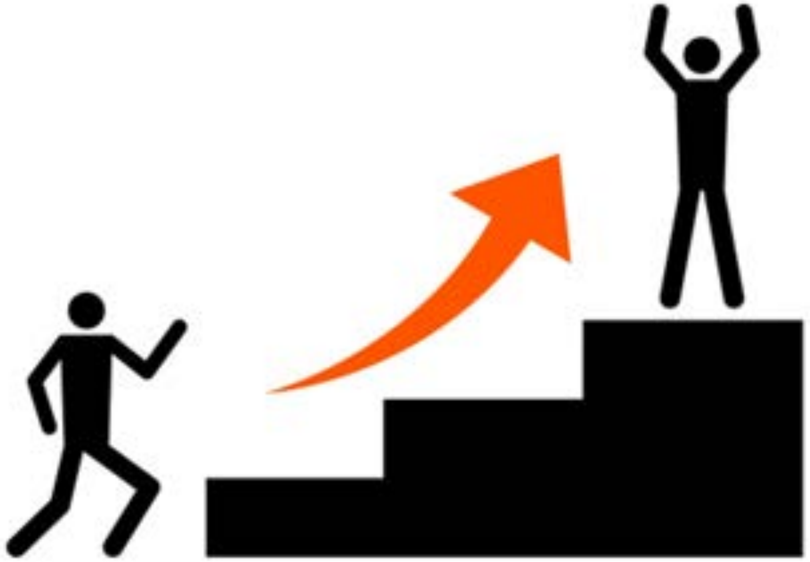


Figure 2: SMEs' immediate business concerns

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

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

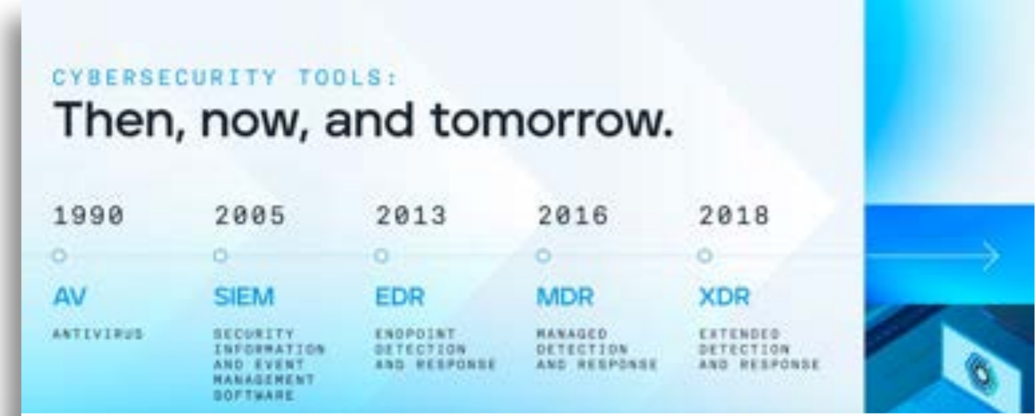


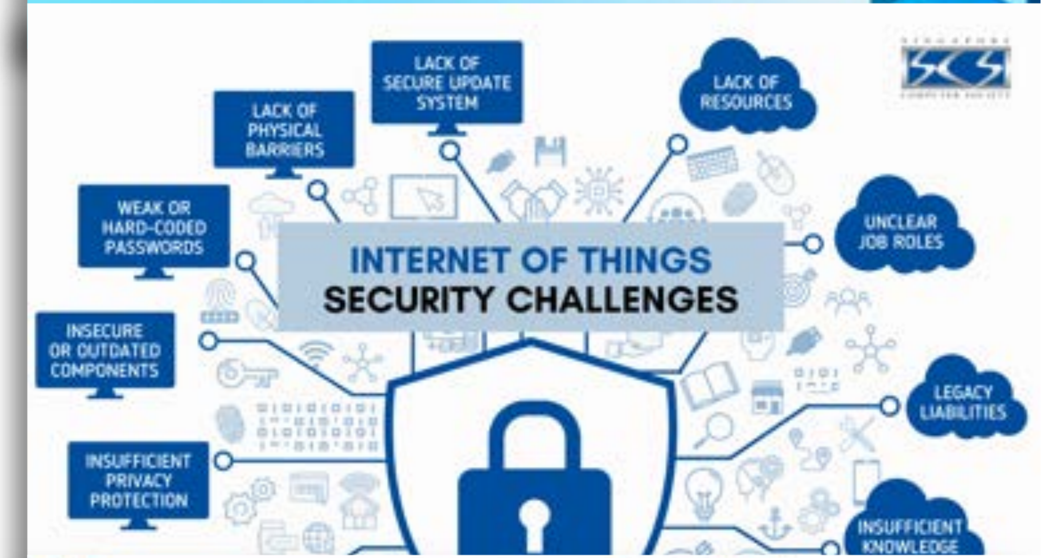
AiSP

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

Growing sophistication of cyber attacks

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


CYBERSECURITY TOOLS:
Then, now, and tomorrow.
1990
AV
ANTIVIRUS
2005
SIEM
SECURITY INFORMATION AND EVENT MANAGEMENT SOFTWARE
2013
EDR
ENDPOINT DETECTION AND RESPONSE
2016
MDR
MANAGED DETECTION AND RESPONSE
2018
XDR
EXTENDED DETECTION AND RESPONSE


INTERNET OF THINGS
SECURITY CHALLENGES
LACK OF PHYSICAL BARRIERS
LACK OF SECURE UPDATE SYSTEM
LACK OF RESOURCES
WEAK OR HARD-CODED PASSWORDS
UNCLEAR JOB ROLES
INSECURE OR OUTDATED COMPONENTS
LEGACY LIABILITIES
INSUFFICIENT PRIVACY PROTECTION
INSUFFICIENT KNOWLEDGE

WiFi
- Don't allow your device to auto-join unfamiliar networks.
- Always turn off WiFi when you aren't using it or don't need it.
- Never send sensitive information over WiFi unless you're absolutely sure it's a secure network.

Apps
- Only use apps available in your device's official store - NEVER download from a browser.
- Be wary of apps from unknown developers or those with limited/bad reviews.
- Keep them updated to ensure they have the latest security.
- If they're no longer supported by your store, just delete!
- Don't grant administrator, or excessive privileges to apps unless you truly trust them.

Browser
- Watch out for ads, giveaways and contests that seem too good to be true. Often these lead to

Bluetooth
- Disable automatic Bluetooth pairing.
- Always turn it off when you don't need it.

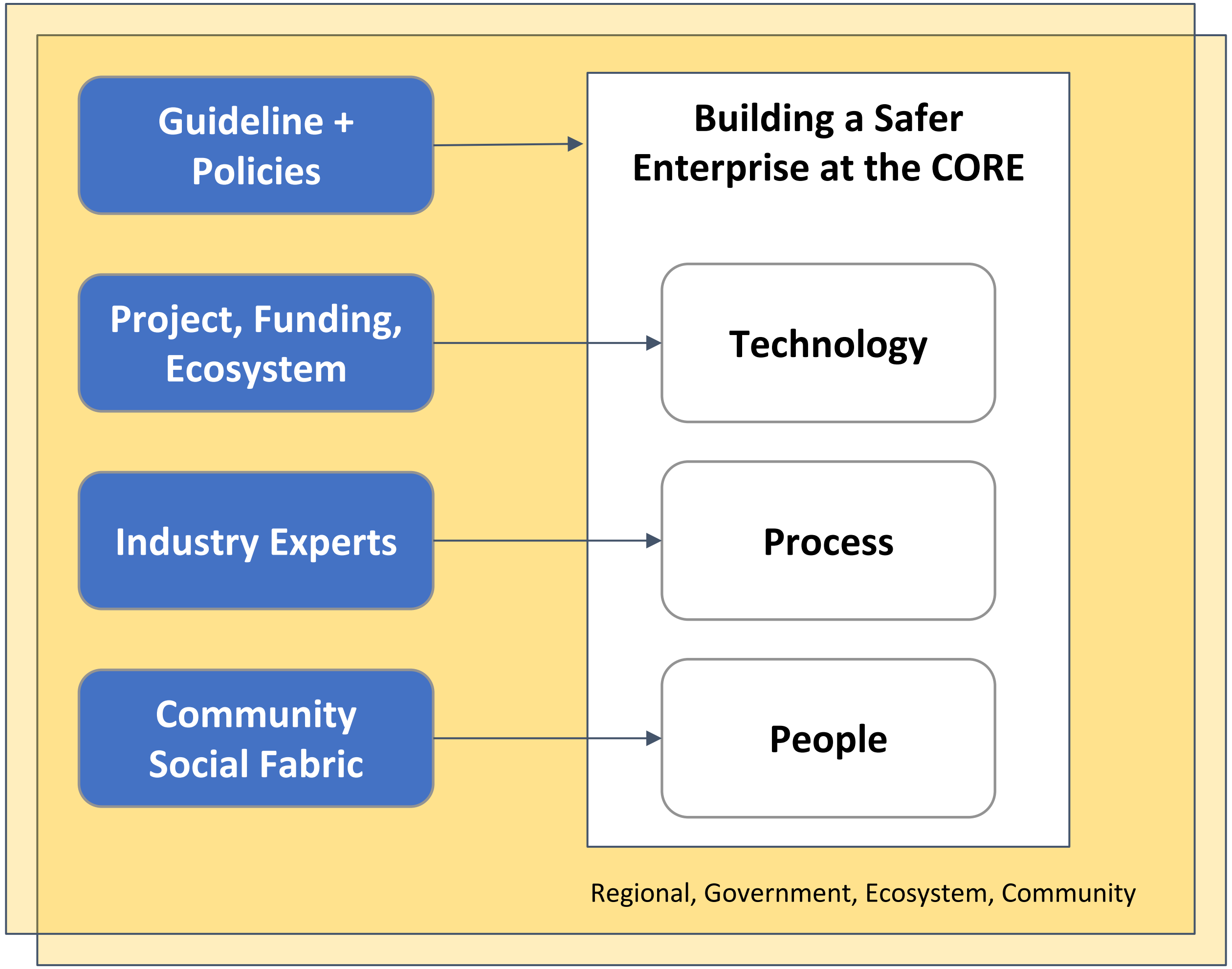
Smishing (phishing via SMS)
- Don't trust messages that attempt to get you to reveal any personal information
- Beware of similar tactics in platforms like What's App, Facebook Messenger Instagram, etc.
- Treat messages the same way you would treat email, always think before you click!

Vishing (voice phishing)
- Do not respond to telephone or email requests for personal financial information. If you are concerned, call the financial institution directly, using the phone number that appears on the back of your credit card or on your monthly statement.
- Never click on a link in an unsolicited commercial email.
- Speak only with live people when providing account information, and **only** when you initiate

Looking at a collective community Effort

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

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

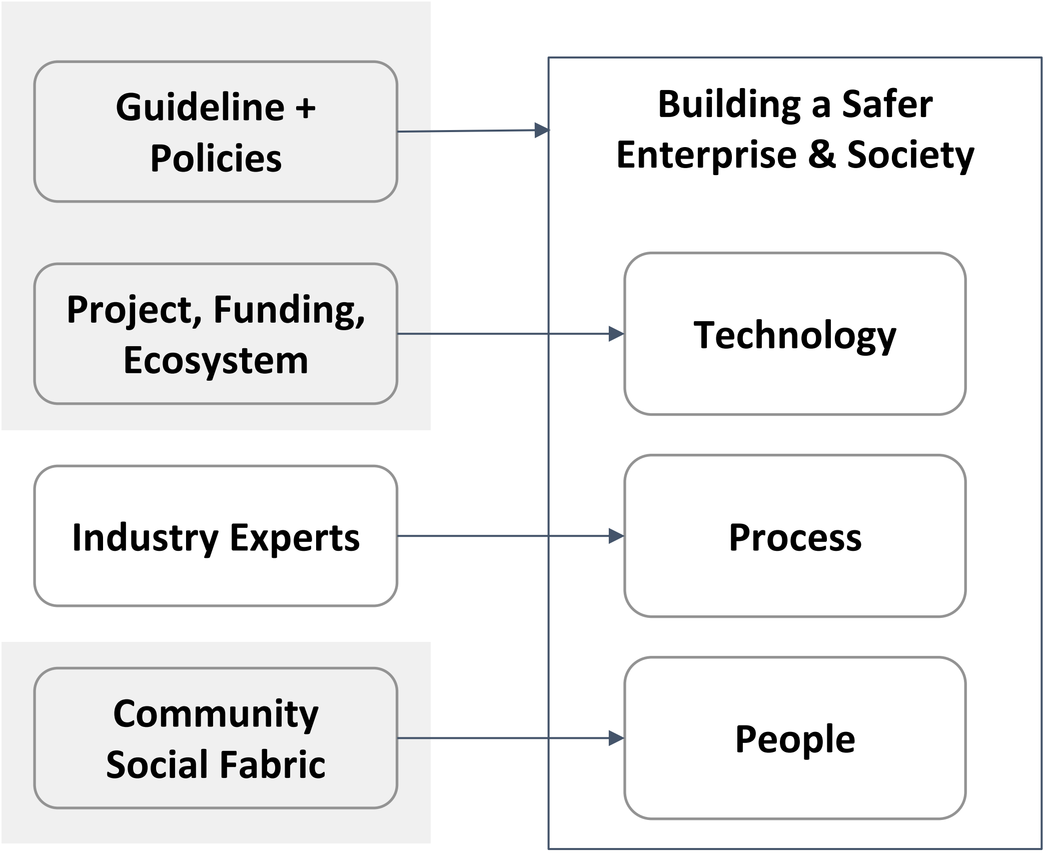

Guideline + Policies
Project, Funding, Ecosystem
Industry Experts
Community Social Fabric
Building a Safer Enterprise at the CORE
Technology
Process
People
Regional, Government, Ecosystem, Community

AiSP

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

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

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



Guideline + Policies

Project, Funding, Ecosystem

Industry Experts

Community Social Fabric

Building a Safer Enterprise & Society

Technology

Process

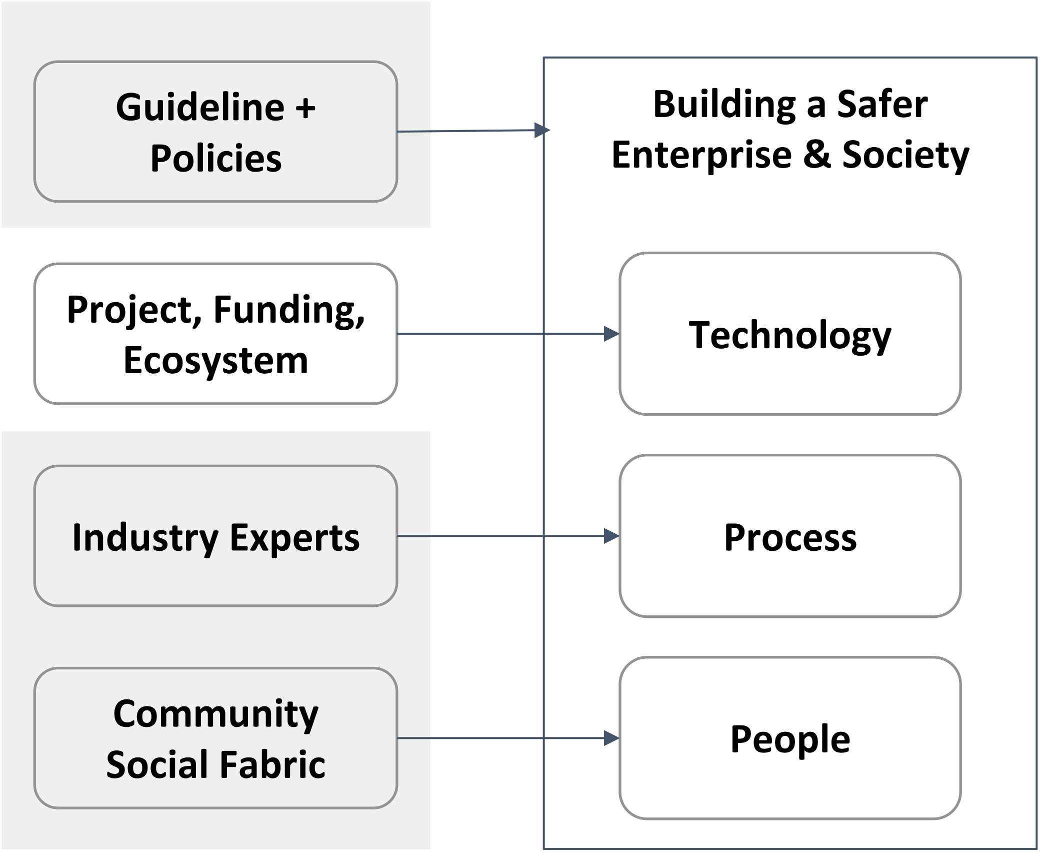
People

AiSP

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

Create a more supportive and innovative ecosystem for cybersecurity.

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

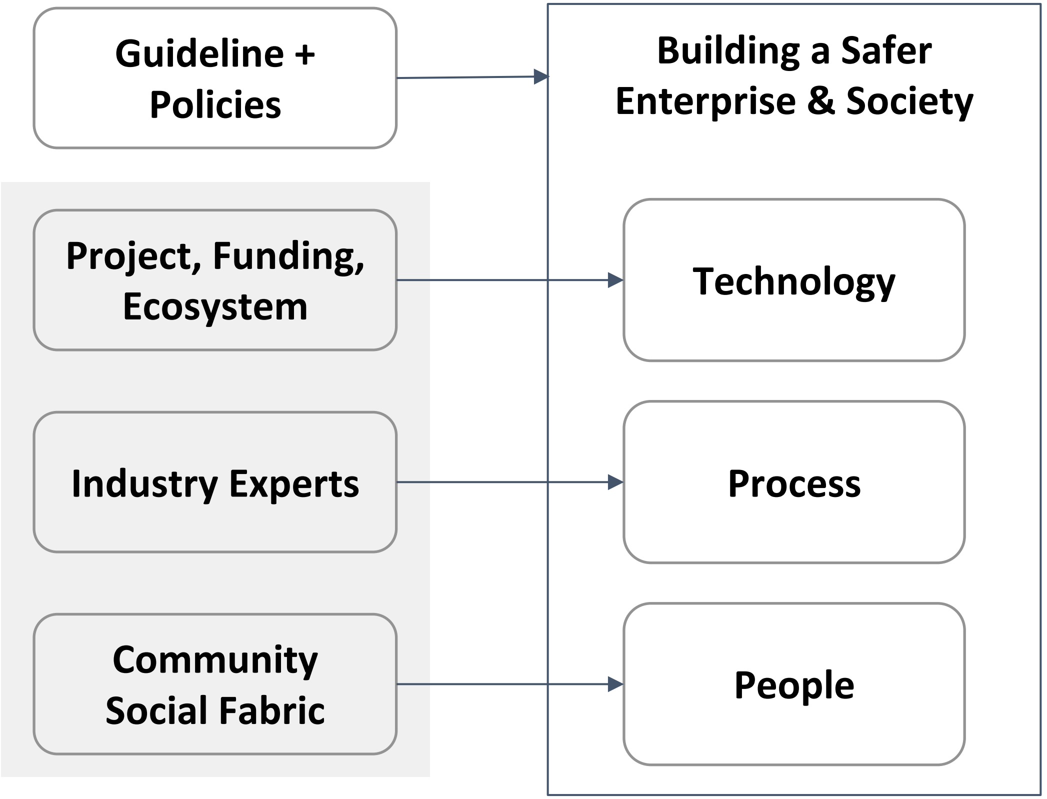


AiSP

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

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

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



Guideline + Policies

Project, Funding, Ecosystem

Industry Experts

Community Social Fabric

Building a Safer Enterprise & Society

Technology

Process

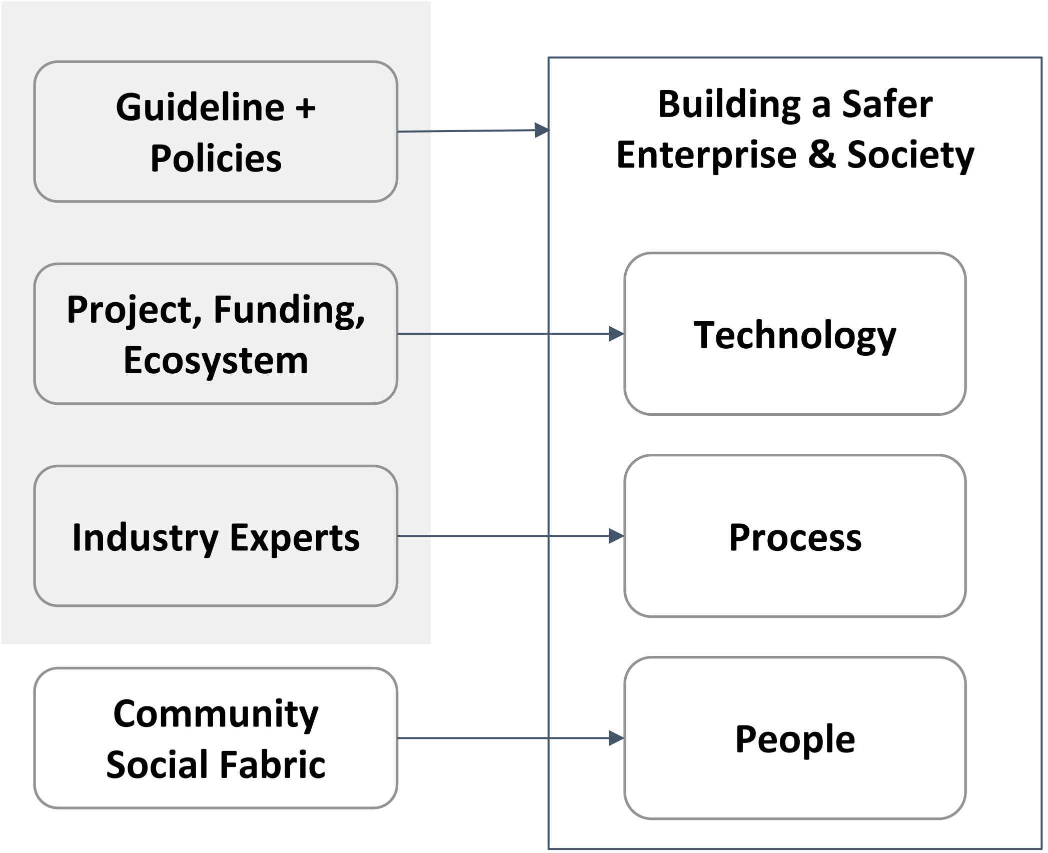
People

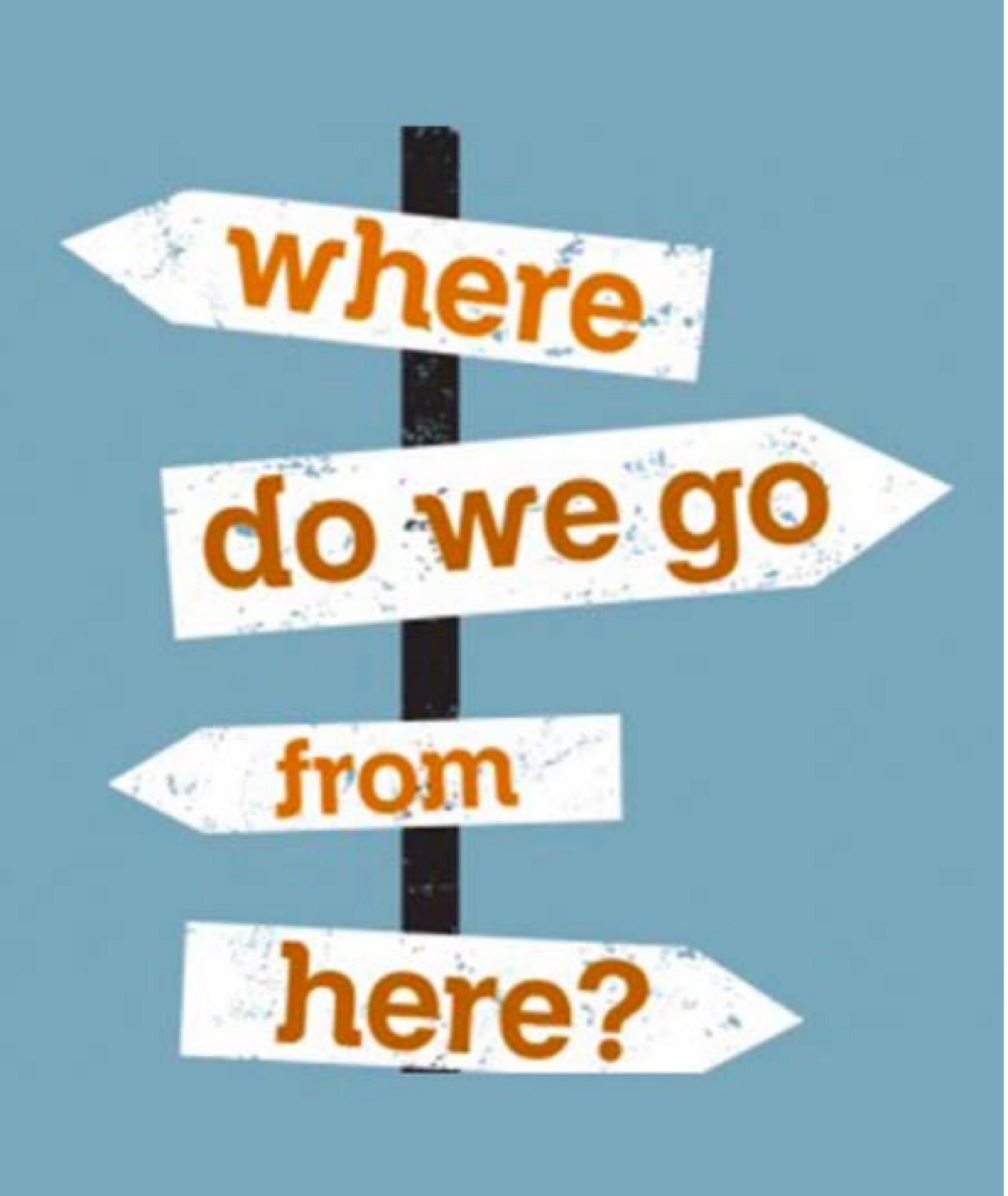
AiSP

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

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

1. **Training programs, workshops:**
   a. **Educate** people about cybersecurity risks and best practices.
   b. **Public awareness campaigns**, cybersecurity training for employees, and integrating cybersecurity into school curricula.
2. **Develop a cybersecurity awareness plan**:
   a. Identify the **key cybersecurity risks.**
   b. Best practices for **mitigating** these risks.
   c. **Communication Plan** for educating your employees and customers about cybersecurity risks.





Where are we today?

Collaboration and working across ASEAN Agencies

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

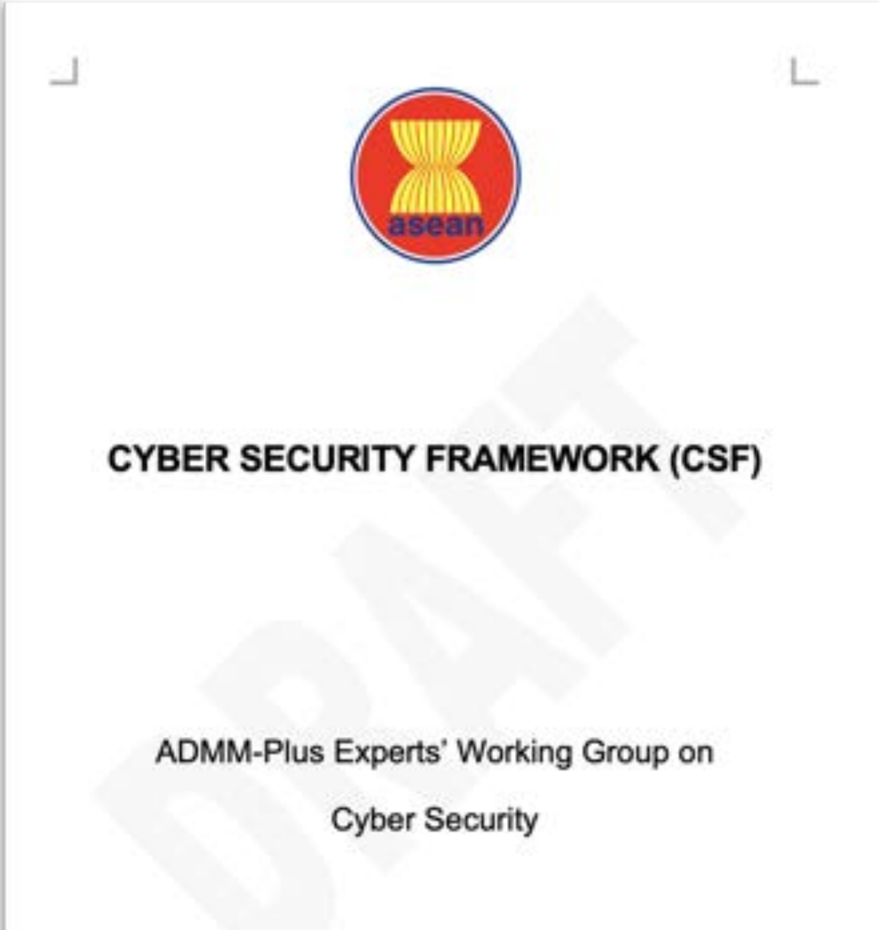
Full statements: https://asean.org/wp-content/uploads/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf

First ASEAN Strategy Paper (2017-2020)

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

ASEAN CYBERSECURITY COOPERATION STRATEGY

(2021 – 2025)



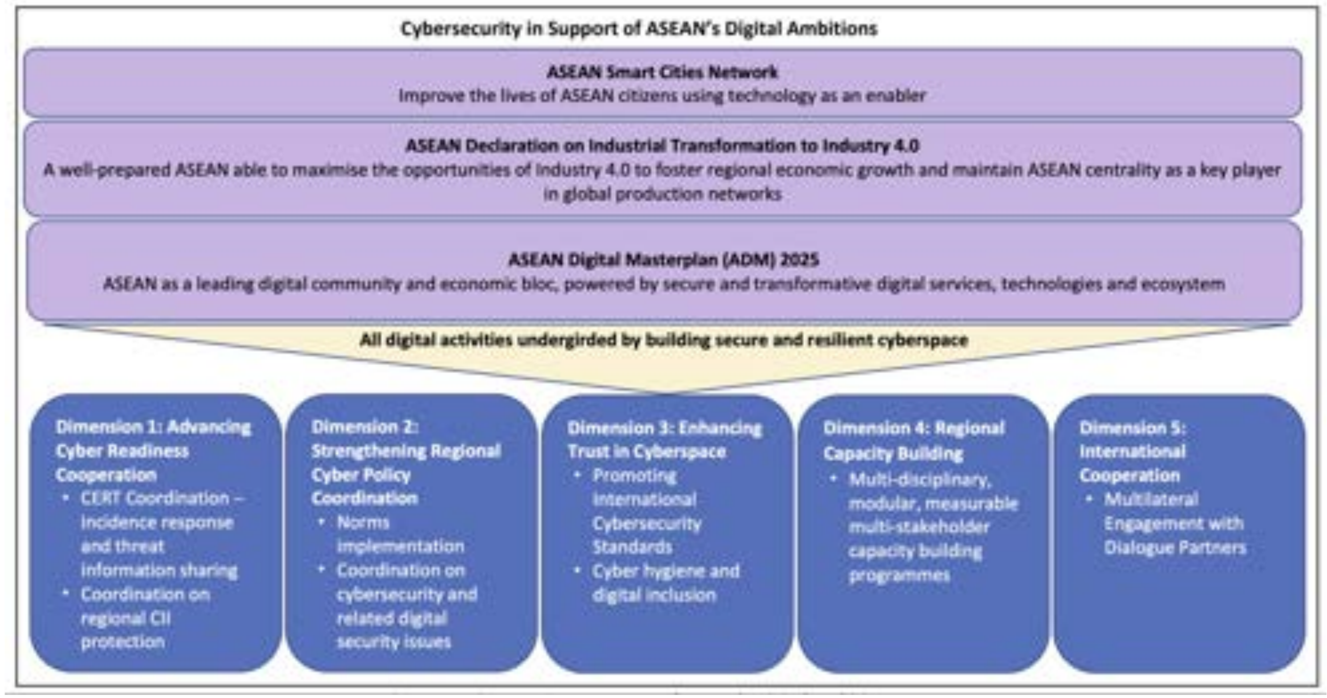
CYBER SECURITY FRAMEWORK (CSF)

ADMM-Plus Experts' Working Group on

Cyber Security

Looking Ahead - OBJECTIVE OF 2021-2025 STRATEGY

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



Cybersecurity in Support of ASEAN's Digital Ambitions

ASEAN Smart Cities Network
Improve the lives of ASEAN citizens using technology as an enabler

ASEAN Declaration on Industrial Transformation to Industry 4.0
A well-prepared ASEAN able to maximise the opportunities of Industry 4.0 to foster regional economic growth and maintain ASEAN centrality as a key player in global production networks

ASEAN Digital Masterplan (ADM) 2025
ASEAN as a leading digital community and economic bloc, powered by secure and transformative digital services, technologies and ecosystem

All digital activities undergirded by building secure and resilient cyberspace

Dimension 1: Advancing Cyber Readiness Cooperation
- CERT Coordination – incidence response and threat information sharing
- Coordination on regional CII protection

Dimension 2: Strengthening Regional Cyber Policy Coordination
- Norms implementation
- Coordination on cybersecurity and related digital security issues

Dimension 3: Enhancing Trust in Cyberspace
- Promoting International Cybersecurity Standards
- Cyber hygiene and digital inclusion

Dimension 4: Regional Capacity Building
- Multi-disciplinary, modular, measurable multi-stakeholder capacity building programmes

Dimension 5: International Cooperation
- Multilateral Engagement with Dialogue Partners

Source: ASEAN CYBERSECURITY COOPERATION STRATEGY (2021 – 2025), figure 1, page 8

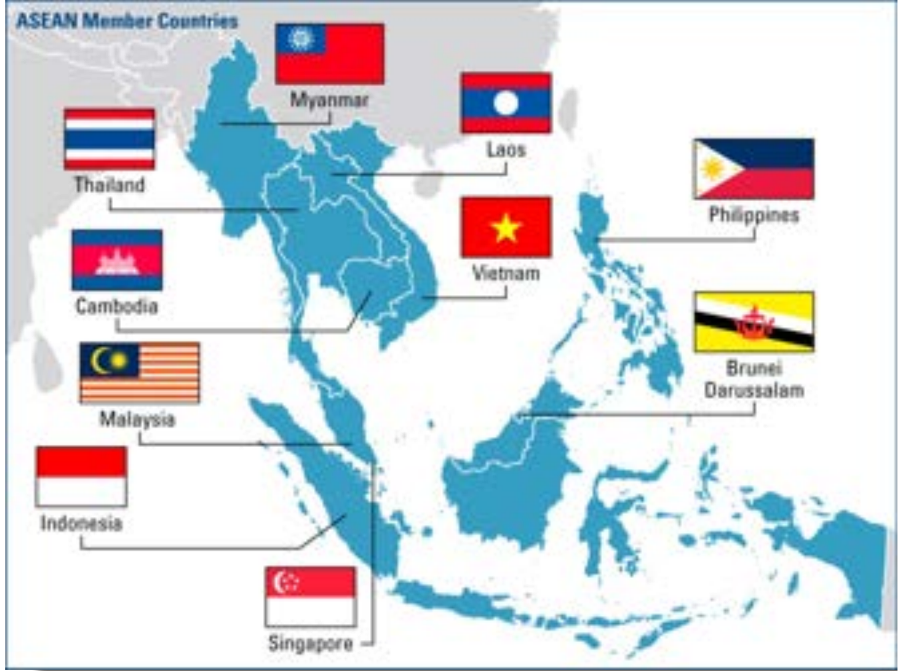
AiSP - Leading the formation of Southeast Asia Cybersecurity Consortium (SEACC)

MOU PARTNERSHIP with key overseas organisations to foster cooperation and collaboration

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

Objective:

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



Cybersecurity Awareness & Advisory Programme (CAAP)

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

Enhance security awareness and training

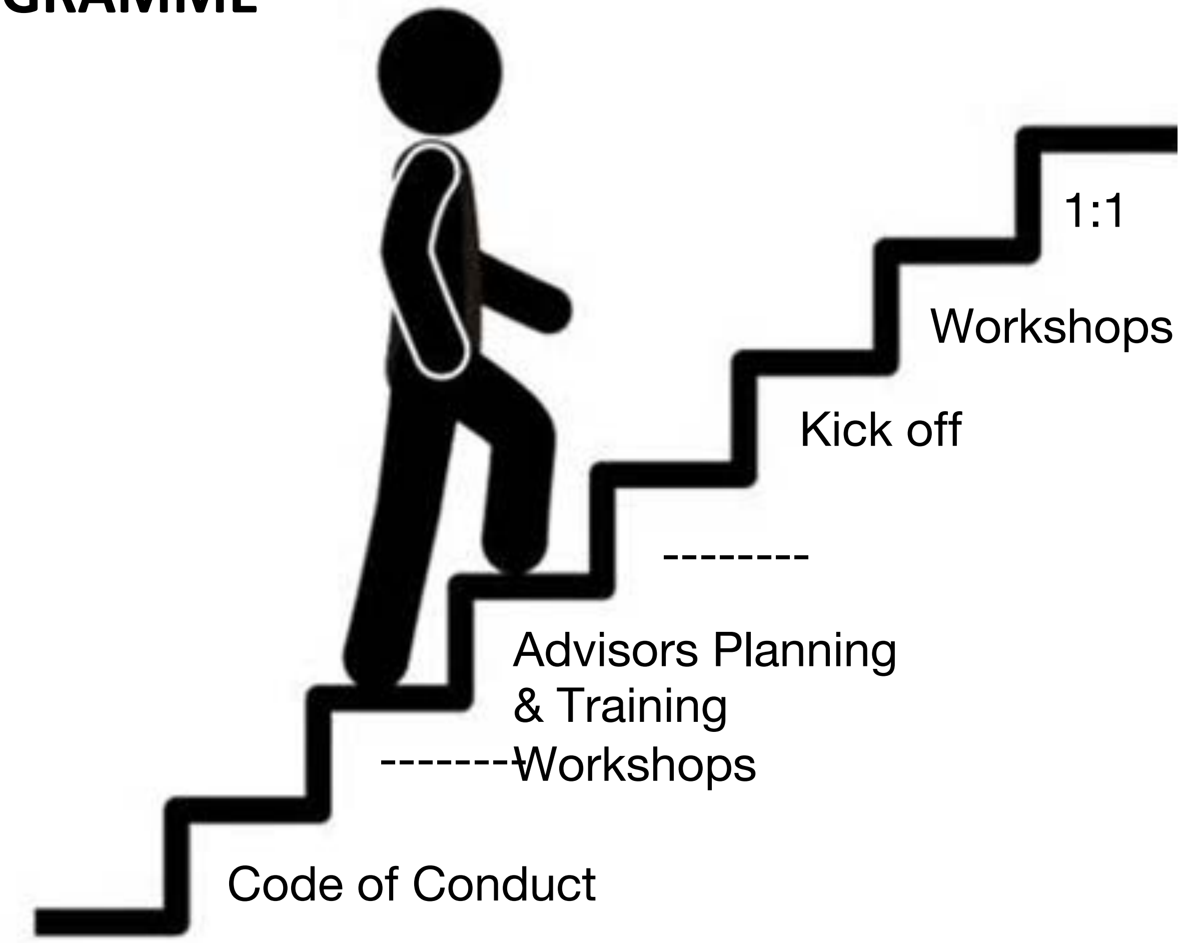
Create cohesive security knowledge resources

Offer security solutions and services support

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

CYBERSECURITY AWARENESS & ADVISORY PROGRAMME

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

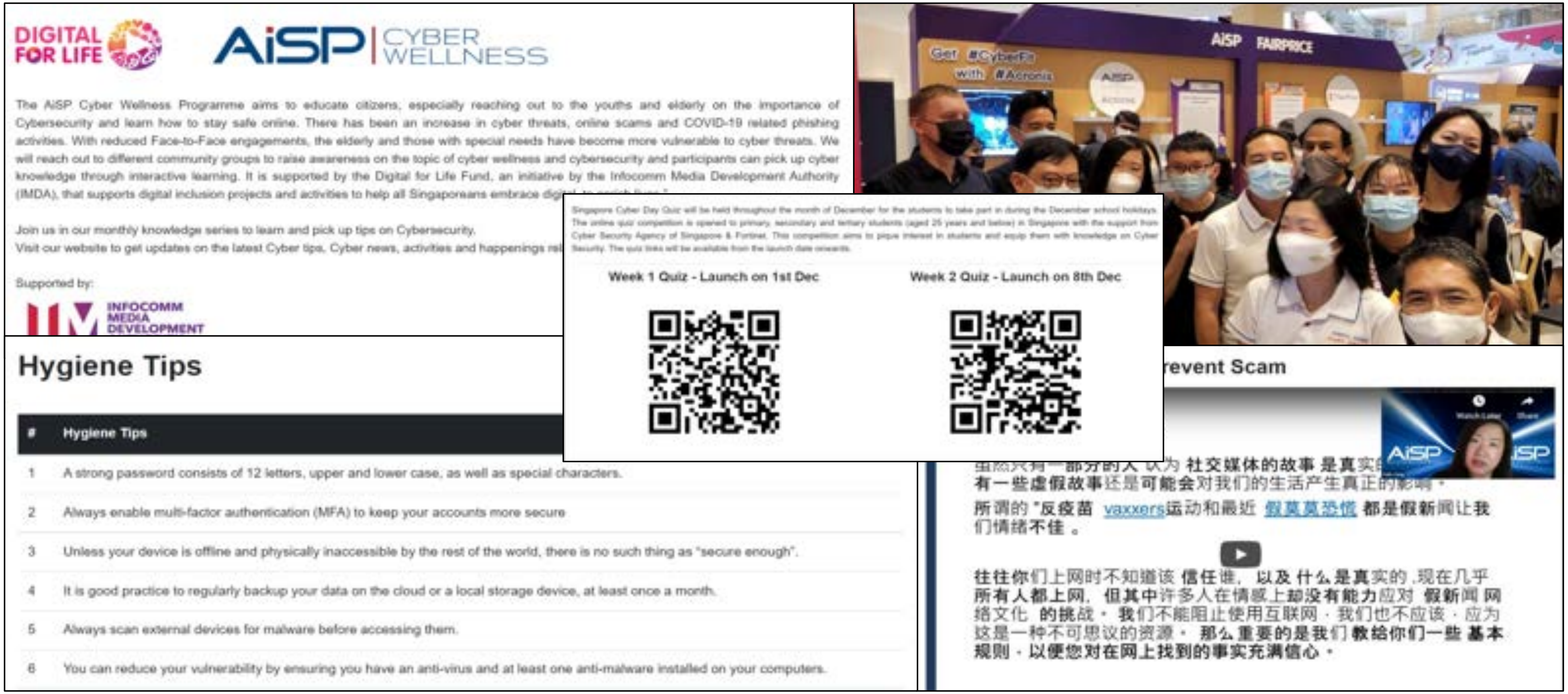


Next Steps: Awareness ⇨ Advisory

AiSP

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

Career Advice, Hygiene Tips, Game & Quiz



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

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

Supported by:

INFOCOMM MEDIA DEVELOPMENT

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

Week 1 Quiz - Launch on 1st Dec

Week 2 Quiz - Launch on 8th Dec

Hygiene Tips

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

revent Scam

虽然只有一部分的人 认为 社交媒体的故事 是真实
有一些虚假故事还是可能会对我们的生活产生真正的影响。

所谓的 "反疫苗 vaxxers运动和最近 假莫莫恐慌 都是假新闻让我们情绪不佳 。

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

Annual AiSP SME Conference - Bringing the community together

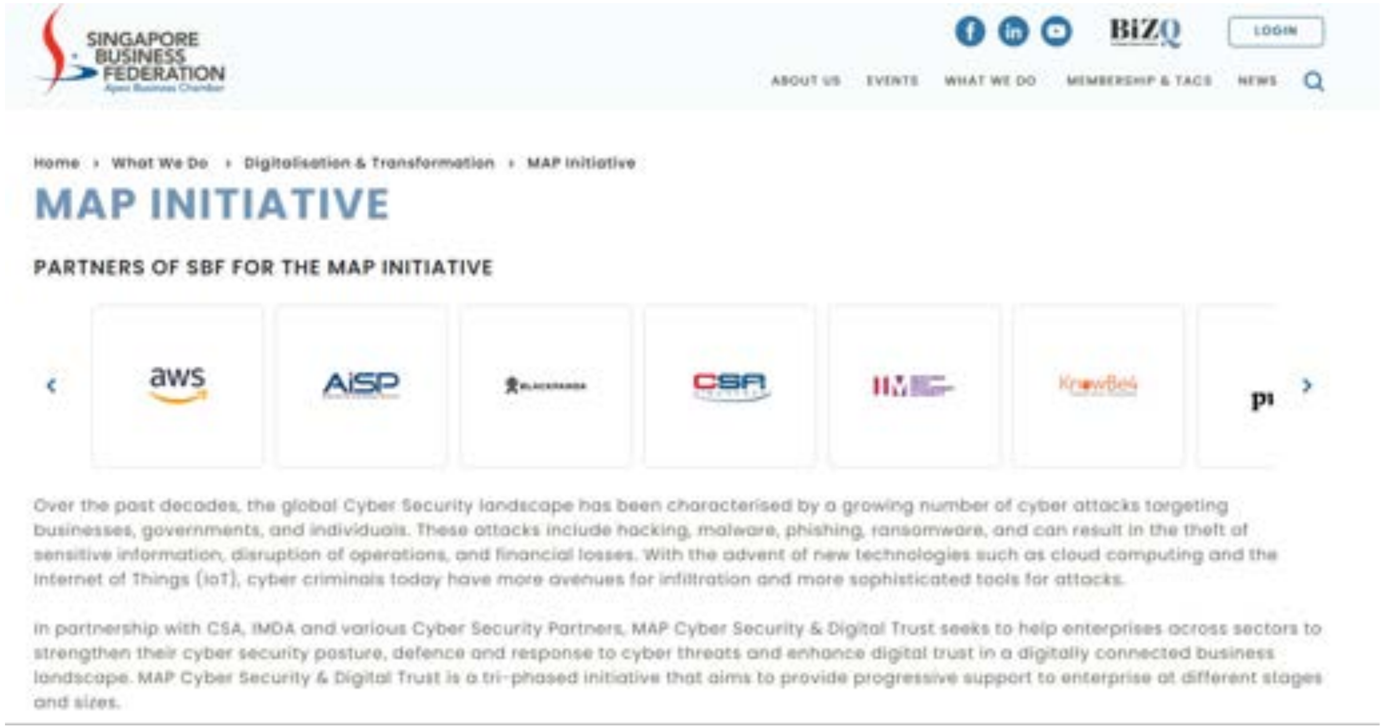
Supported by:

ASME CSCIS CREST CSA cloud security alliance CzechTrade Div0 HTCIA IASA

ISACA Singapore Chapter SINGAPORE ntuc SINGAPORE BUSINESS FEDERATION SCS COMPUTER SOCIETY SFA AHK

AiSP SGTECH SiAA TTAB Tech Talent AssemBly sme CSA SINGAPORE

Partnering with Agencies - Singapore Business Federation



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

MAP INITIATIVE

PARTNERS OF SBF FOR THE MAP INITIATIVE

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

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

AiSP
SHAPING CYBERSECURITY COMPETENCIES TO BUILD FUTURE-PROOF ECONOMIES
AiSP

Official Venue Partner:

Lifelong Learning Institute

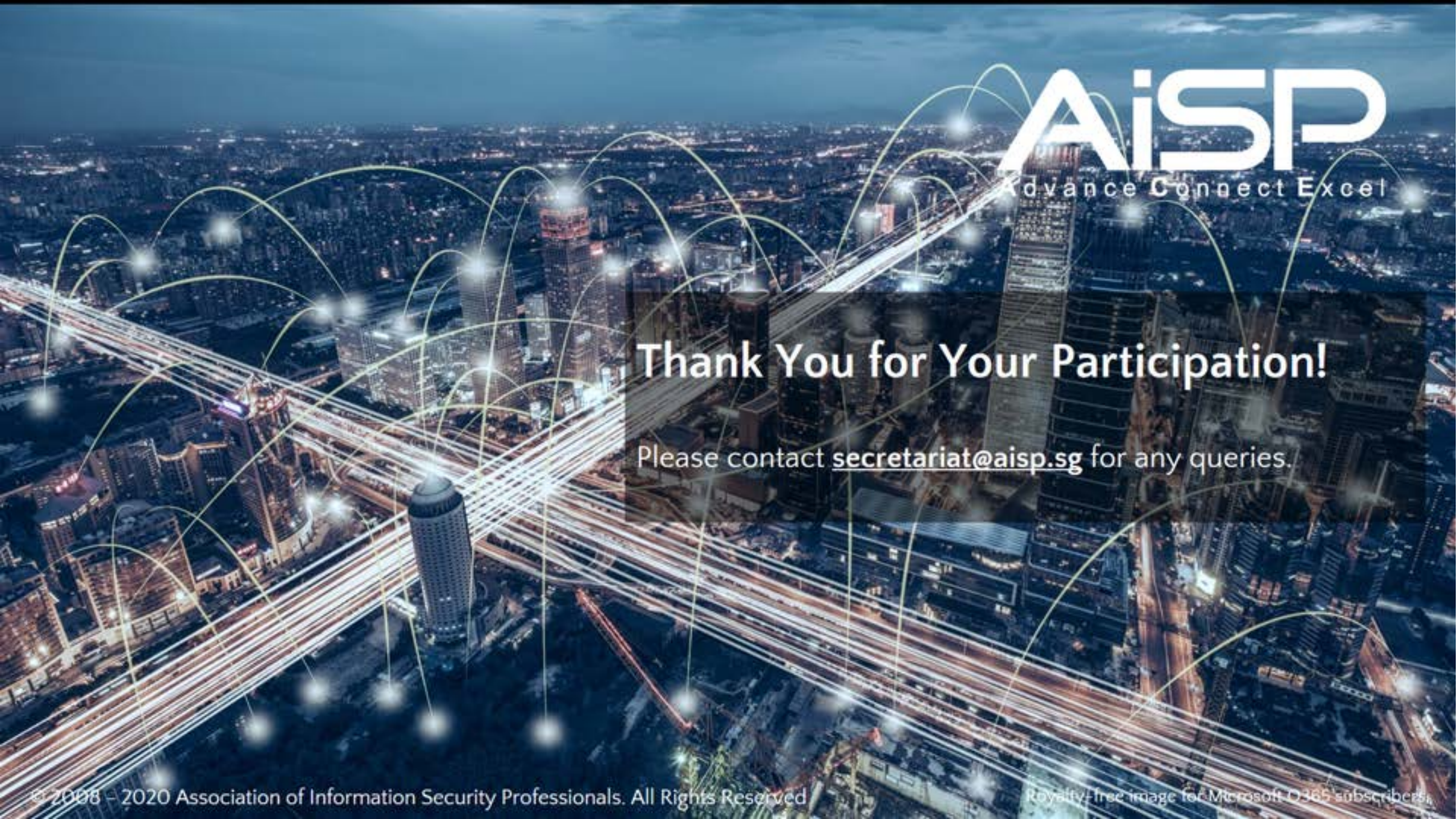
SKILLSfuture SG

MAP Cyber Security & Digital Trust is Supported By:

aws
AiSP
BLACKPANDA
CSA SINGAPORE
IM INFOCOMM MEDIA DEVELOPMENT AUTHORITY
KnowBe4
pwc
SGTECH
Singtel
sptel
Stone Forest IT

Summary - Call to Action

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



AiSP

Advance Connect Excel

Thank You for Your Participation!

Please contact **secretariat@aisp.sg** for any queries.

Royalty-free image for Microsoft O365 subscribers.

https://www.ptsecurity.com/ww-en/analytics/asia-cybersecurity-threatscape-2022-2023/#:~:text=Asia%2DPacific%20(APAC)%20was,vulnerable%20as%20digital%20transformation%20continues.

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

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

https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/06/asean-cyber-security-cooperation.pdf https://www.rsis.edu.sg/rsis-publication/idss/asean-moves-to-strengthen-digital-defence-cooperation/

CO23101 | ASEAN MOVES TO STRENGTHEN DIGITAL DEFENCE COOPERATION

Empowering ASEAN Cyber Resilience

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

Enterprise level

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

Cybersecurity is still challenging for ASEAN businesses

What the world can learn from ASEAN’s cyber cooperation

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

CYBERSECURITY CROSS-BORDER INNOVATION RESILIENCE

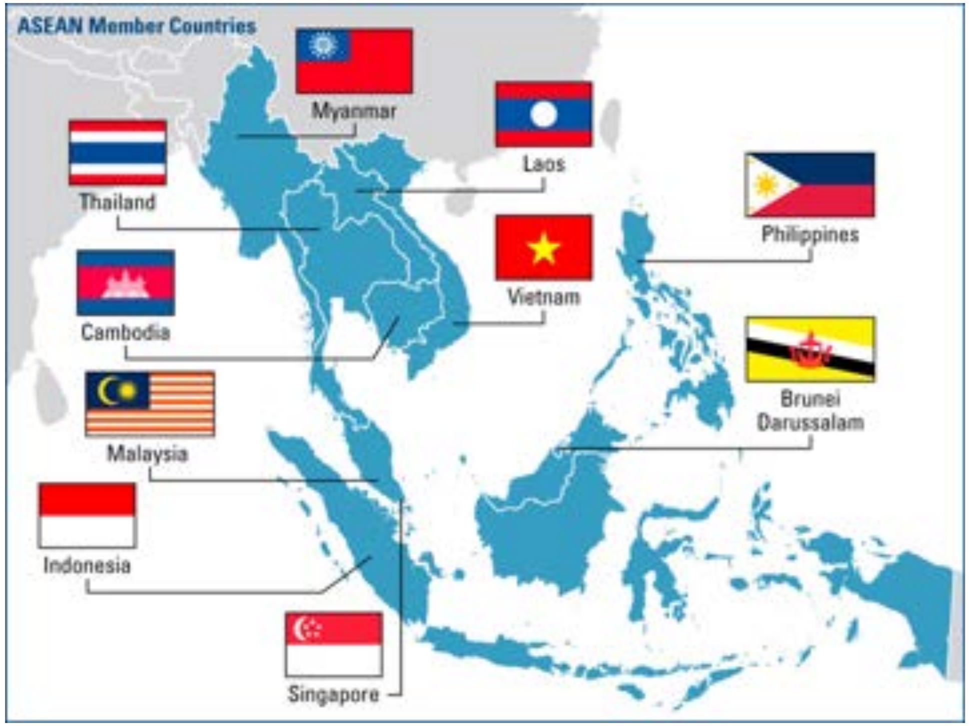
What the world can learn from ASEAN’s cyber cooperation

By Amit Roy Choudhury Nov 15, 2021

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

AiSP - Actively driving collaboration across ASEAN

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



South East Asia Cybersecurity Consortium (SEACC)

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

International Conference on ASEAN-JAPAN Cybersecurity Community

Trust Design for distributed Energy Resource Aggregation System on Cyber and Physical Security Framework”

October 2023

Project Leader, Systems Committee on Smart Energy, IEC

Keio University, Japan

Masaki Umejima, Ph.D

Director, National Advanced IPv6 Center (NAv6)

Universiti Sains Malaysia

Selvakumar Manickam, Ph.D

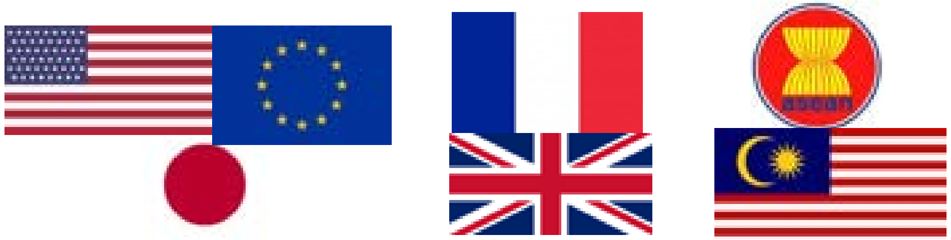
IEC System Committee Smart Energy

- The International Electrotechnical Commission（IEC）is a global non-profit organization that provides 10,000+ international standards, gathering 20,000 experts in more than 170 countries.
  - System Committee Smart Energy（SyC SE）in IEC provides systems-level standardization for smart energy and smart grids.

Cyber Civilization Research Center（CCRC）, Keio University

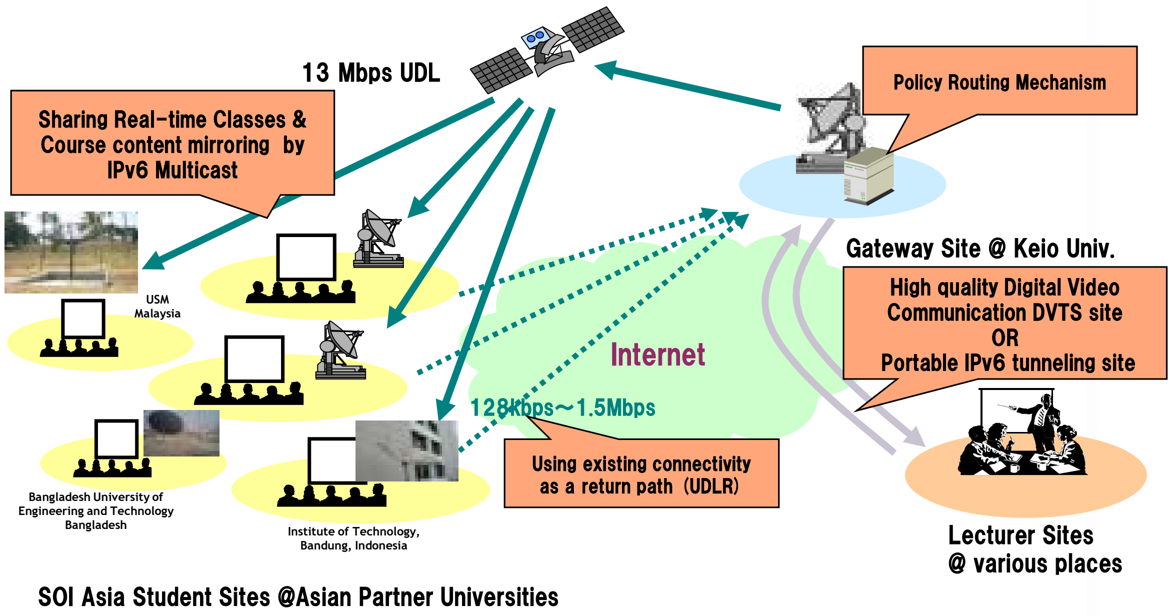
Dr. David Farber:Left
the **Internet** Hall of Fame
Fellow, the American Association for the Advancement of Science 〔AAAS〕
Dr. Jun Murai:Right
the **Internet** Hall of Fame
Special Advisor to the Cabinet

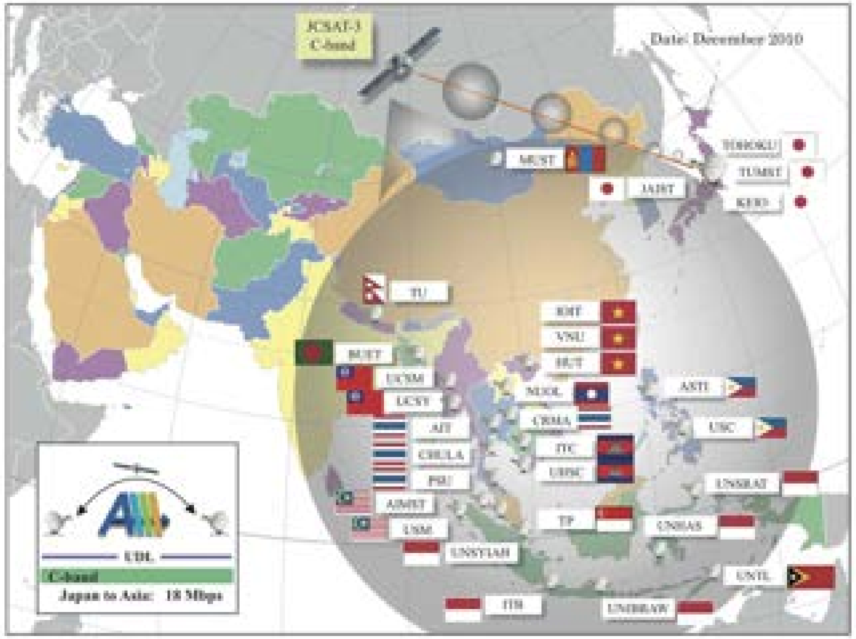
- *CCRC is addressing the security design of cyber and physical space with the leadership by the Internet giants in U.S. and Japan.*
- *Trust design of Cyber-Physical system like Energy Resource Aggregation Business system is our research interest. So, CCRC has done its related research, partnering with the institutions in U.S., EU, and ASEAN,*



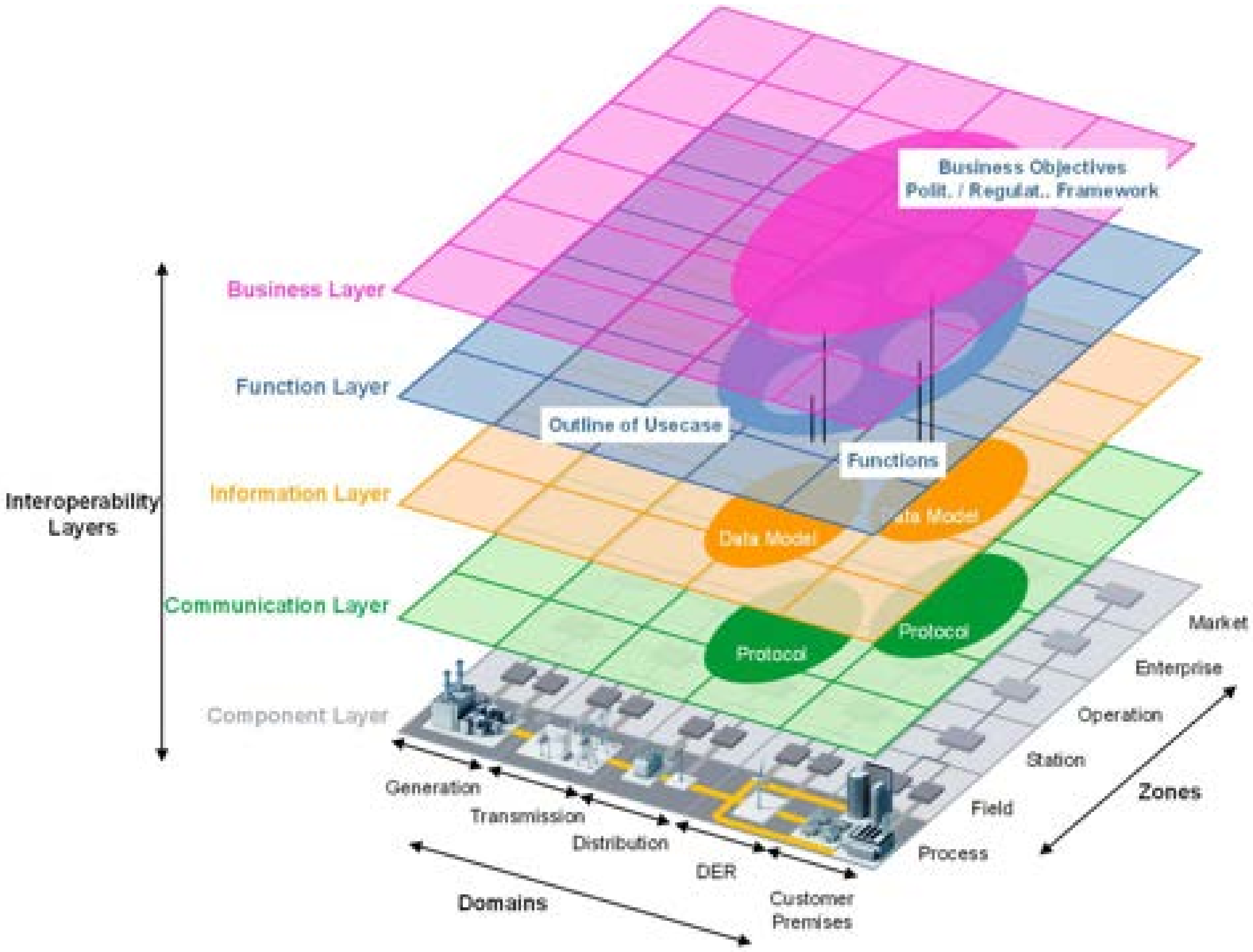
SOI Asia platform

- SOI Asia is the university alliance, connecting leading Asian-wide universities by the high-speed network configuring satellite communication and the internet.
    - Dr. Jun Murai, the father of the internet, has addressed SOI Asia in 1996 that is one year after when the internet was commercialized.


13 Mbps UDL
Sharing Real-time Classes & Course content mirroring by IPv6 Multicast
Policy Routing Mechanism
USM
Malaysia
Internet
Gateway Site @ Keio Univ.
High quality Digital Video Communication DVTS site
OR
Portable IPv6 tunneling site
128kbps～1.5Mbps
Using existing connectivity as a return path（UDLR)
Bangladesh University of Engineering and Technology
Bangladesh
Institute of Technology, Bandung, Indonesia
Lecturer Sites
@ various places
SOI Asia Student Sites @Asian Partner Universities



SGAM Plane by ”SMART GRID STANDARDIZATION ROADMAP” by SRD63097 in IEC SyC



ERAB enables the new relation between People and Energy

- Energy Resource Aggregation Business (ERAB) is a new business framework controlling distributed energy resources at a demand side like EV, a station battery, a fuel cell, and an air conditioner.

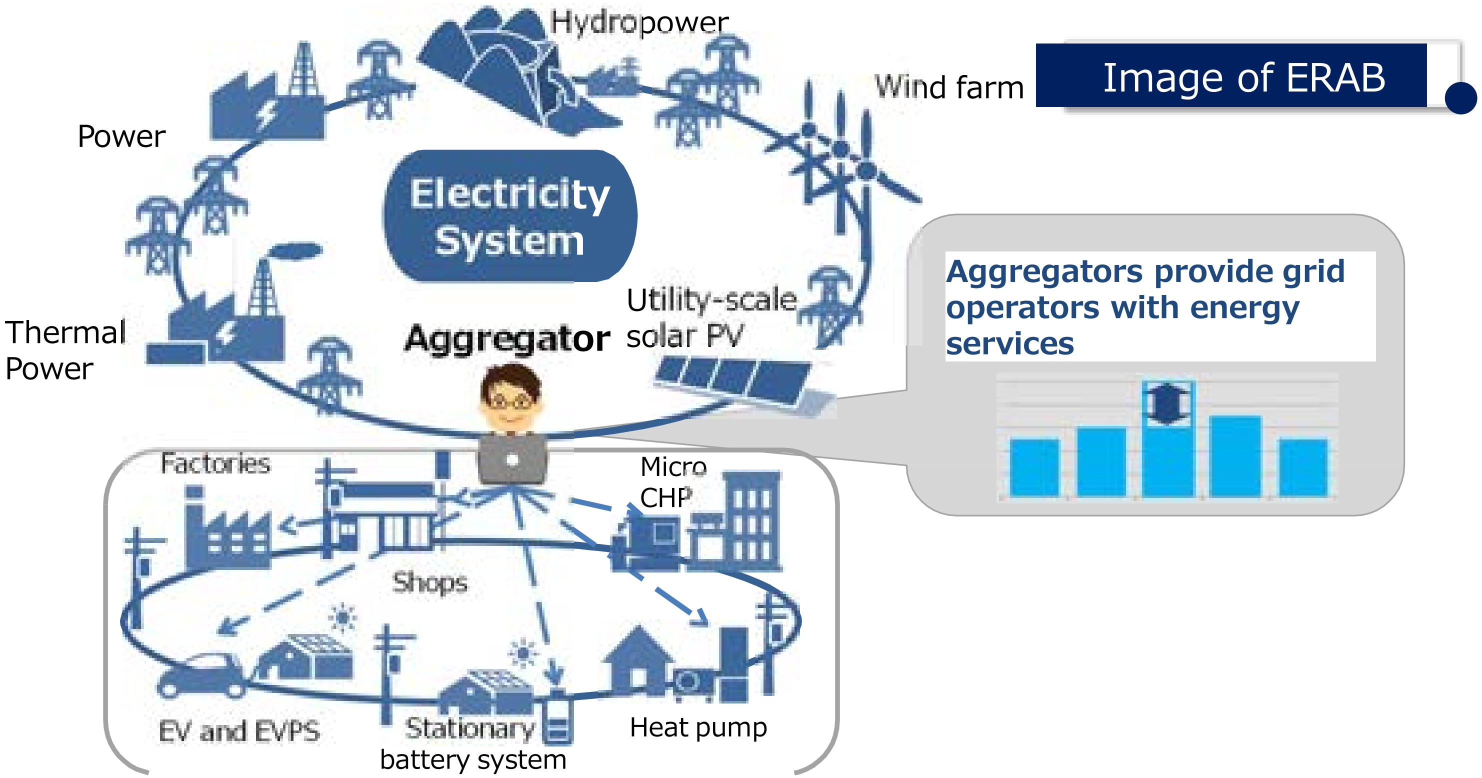
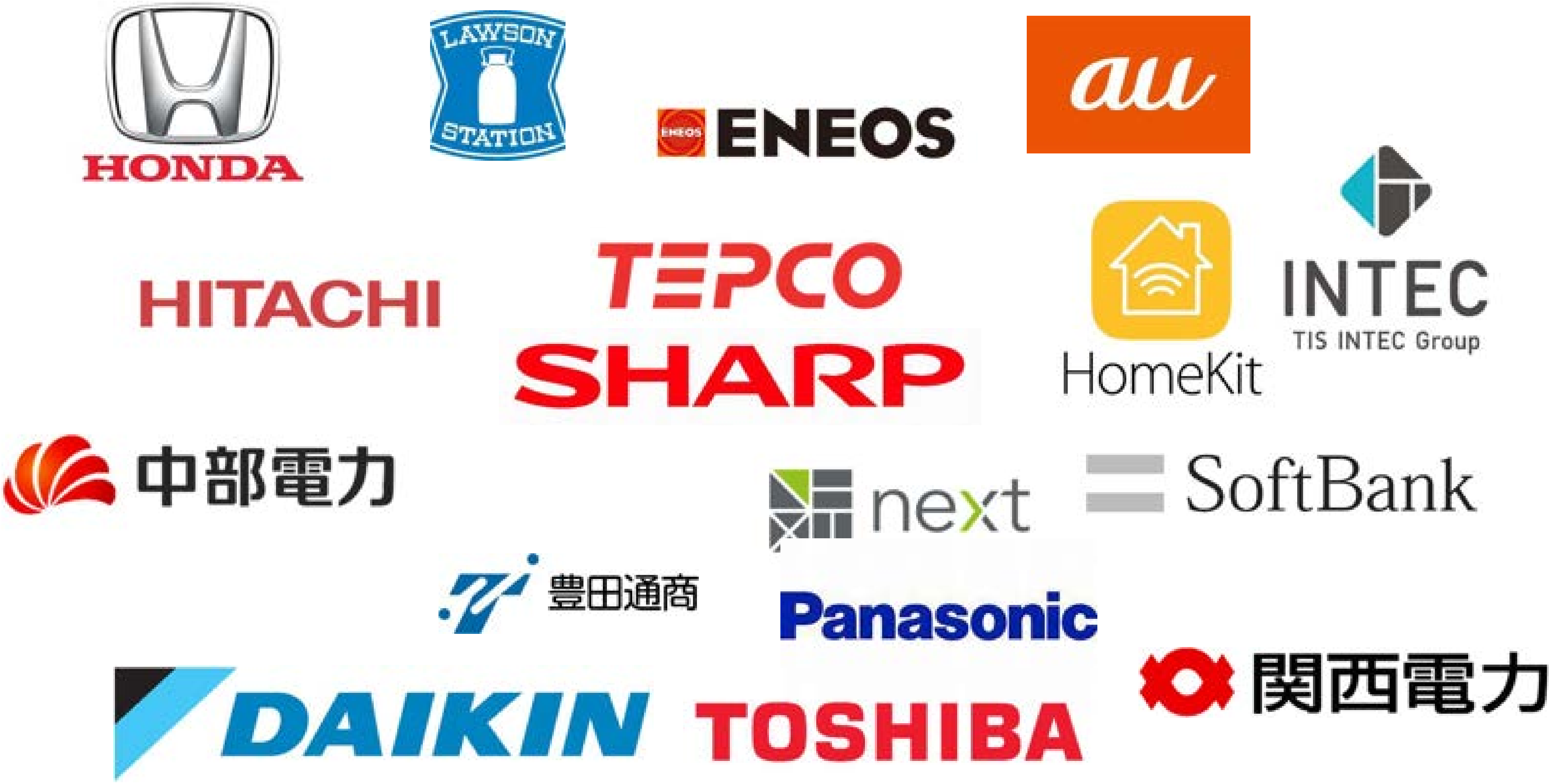


Image of ERAB

Aggregators provide grid operators with energy services

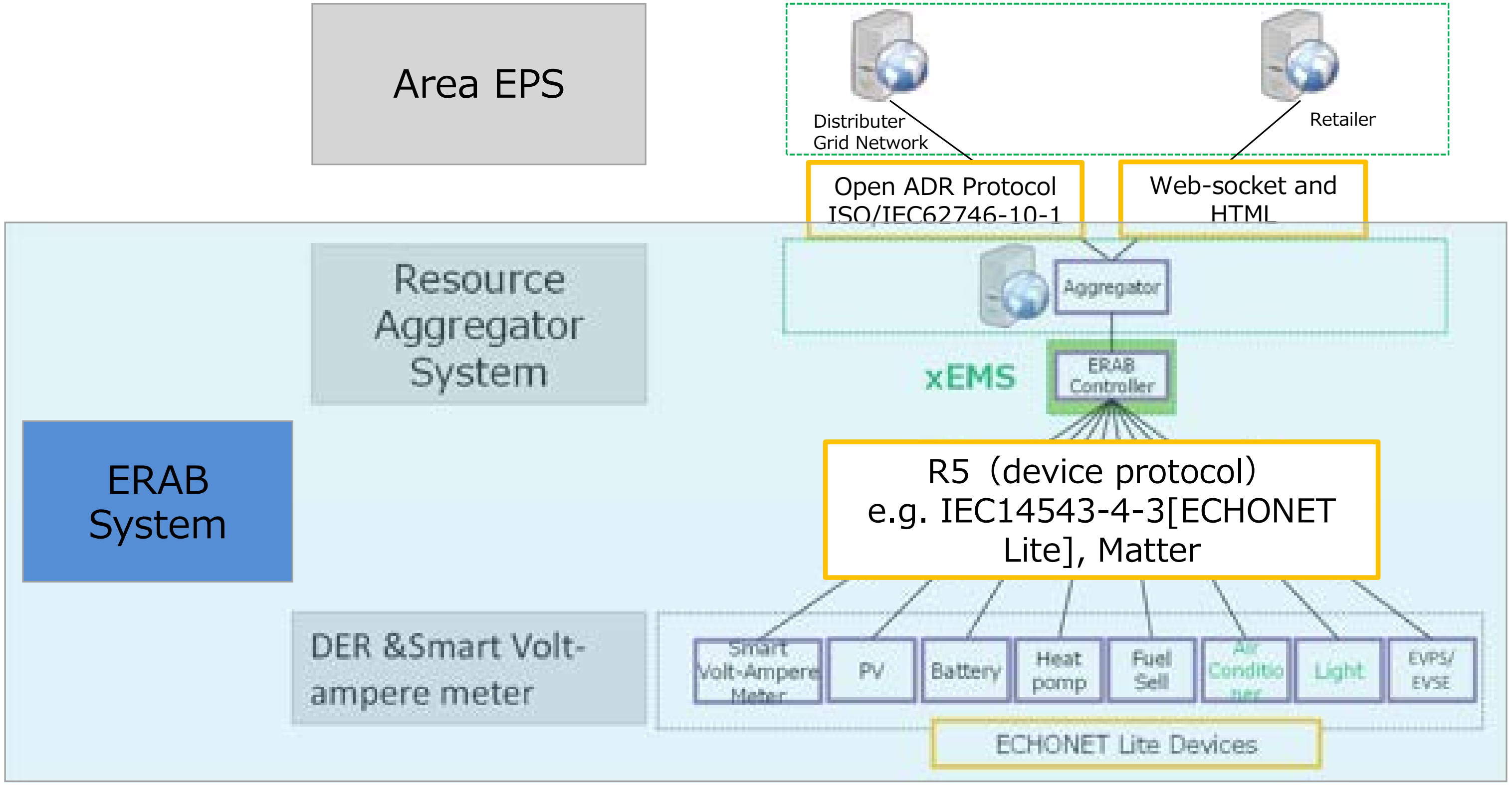
- The system is to **restrain or elevate the demand according to the request by retailers and a grid distributor** and to **provide the electricity traded in a supply and a demand adjustment market.**

Companies that have entered or shown interests in ERAB in Japan



Sample of ERAB system: remotely control DERs at a customer premise

- DER is a small-scale power generation source, located close to where electricity is used (e.g., homes or businesses), have the potential to provide an alternative to the traditional electric power grid.



Area EPS

Distributer Grid Network

Retailer

Open ADR Protocol ISO/IEC62746-10-1

Web-socket and HTML

Resource Aggregator System

Aggregator

xEMS

ERAB Controller

ERAB System

R5（device protocol) e.g. IEC14543-4-3[ECHONET Lite], Matter

DER &Smart Volt-ampere meter

Smart Volt-Ampere Meter

PV

Battery

Heat pomp

Fuel Sell

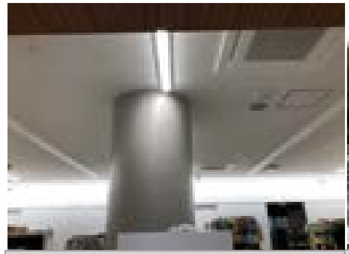
Air Conditioner

Light

EVPS/ EVSE

ECHONET Lite Devices

IoT-Gateway [EMS Controller]



Light & Air conditioning

PV

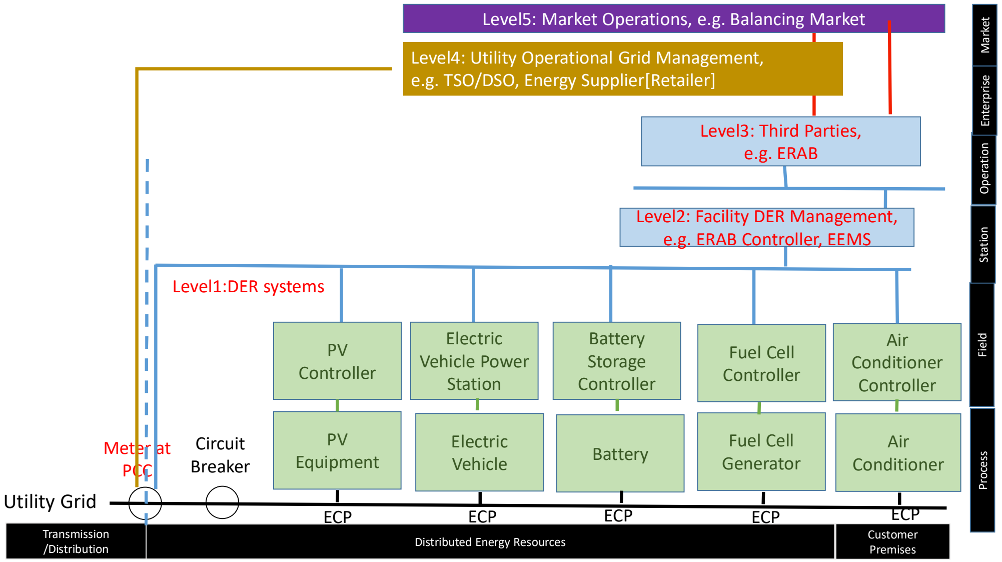
Activity towards SRD 63443: in SyC-SE

Title : Distributed Energy Resource Aggregation Business System: Architecture and Service scenario

The decentralized generation of electrical power as well as spread of energy storage and controllable loads becomes more and more important. The management of these Distributed Energy Resources ［DERs］ and Controllable Loads ［CLs］ at the customer premise near to the final customer offers economic and ecological benefits. In addition, information of Advanced Metering Infrastructure ［AMI］ provides a customer with the method measuring the value of aggregating these resources.

This activity aims to describe a distributed Energy Resource Aggregation Business（ERAB）in spotlighting a business & function layer on SGAM in SRD63097. Currently, we defined ERAB as:

Energy Resource Aggregation Business ［ERAB］ restrain or elevate power generations of DERs and demands of CLs in accordance to the performance measurement by the information of AMI and the requests by TSO/DSO, Electricity Supplier, and Energy Exchange.

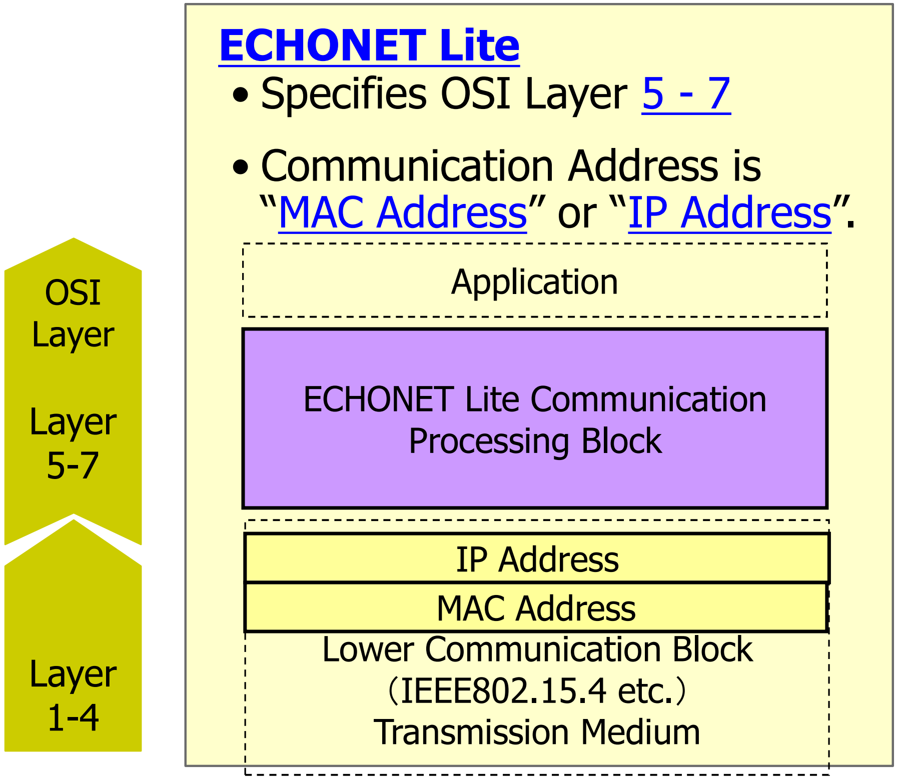

Level5: Market Operations, e.g. Balancing Market
Level4: Utility Operational Grid Management, e.g. TSO/DSO, Energy Supplier[Retailer]
Level3: Third Parties, e.g. ERAB
Level2: Facility DER Management, e.g. ERAB Controller, EEMS
Level1:DER systems
PV Controller
Electric Vehicle Power Station
Battery Storage Controller
Fuel Cell Controller
Air Conditioner Controller
PV Equipment
Electric Vehicle
Battery
Fuel Cell Generator
Air Conditioner
Meter at PCC
Circuit Breaker
Utility Grid
ECP
ECP
ECP
ECP
ECP
Transmission /Distribution
Distributed Energy Resources
Customer Premises
Market
Enterprise
Operation
Station
Field
Process

ERAB case is compatible with BUCs shown at IEC TR 63097:2017 SMART GRID STANDARDIZATION ROADMAP

Project Leader: JP
With experts from France, Canada, U.S. India, Korea, Australia

Standardization giving to DER interface at a customer premise
It reduces the cost of configuring multiple DERs

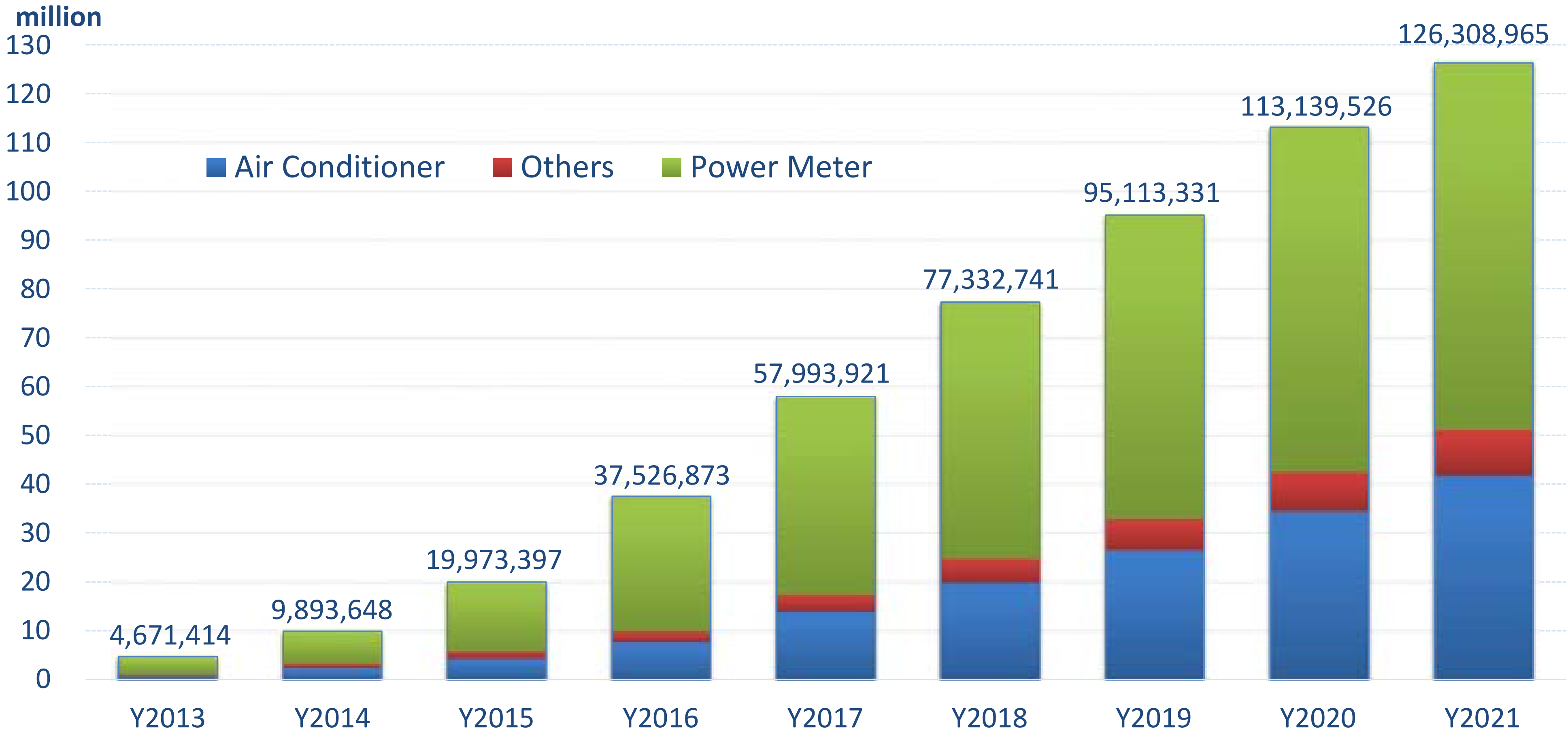
A current condition in Japan surrounding ERAB system is that DERs speak a single language called ECHONET Lite. Japanese Government and Industry liaison has proposed ISO/IEC14543-4-3, to be the enabler of the demand side management, around HEMS. Internet of Things over this international standard, ECHONET Lite in Japan, has provided a common language for 100s of devices: home appliances, power meter, EV, and PV



ECHONET Lite

- Specifies OSI Layer 5 - 7
- Communication Address is "MAC Address" or "IP Address".

ECHONET Lite devices: Approx. 138 millions in 2022



Lineup of DERs with ECHONET Lite

- In general, 30-40 Kw electricity is necessary for running a grocery store.
  - Lawson at SFC has the 12Kw solar power generation on the roof and the 5.6 Kw EV battery charger outside, connecting with EV which carries over 50Kwh battery.

※DER=Distributed Energy Resources

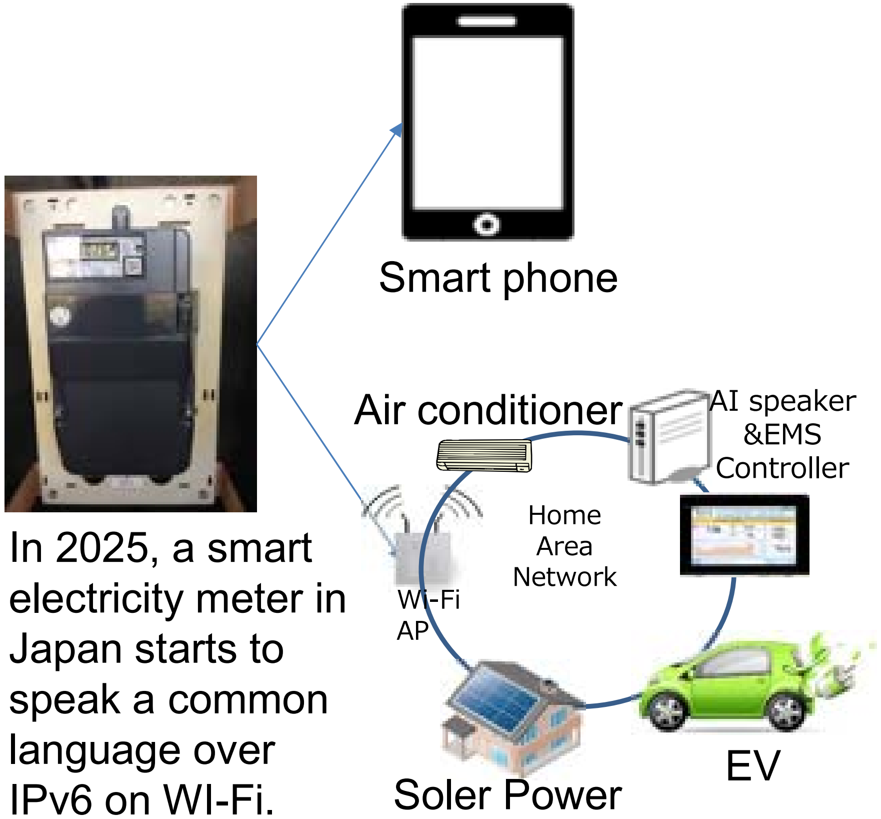
5.6 kw for storage

12 kw for generation

30-40 kw for usage
such as Air Conditioning

Next-gen power meter released in 2025

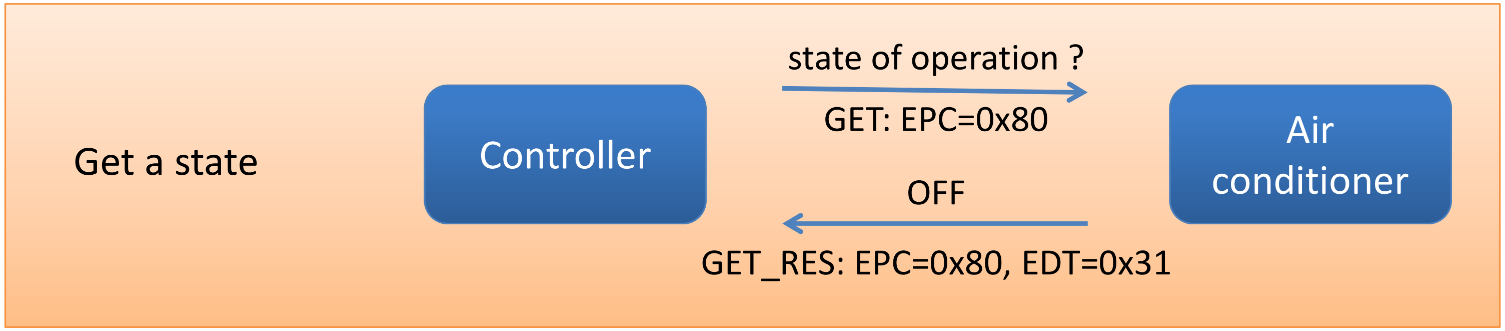
- Everyone’s Mob App can access the electricity usage data: The ambitious nationwide project starting in 2025 in Japan



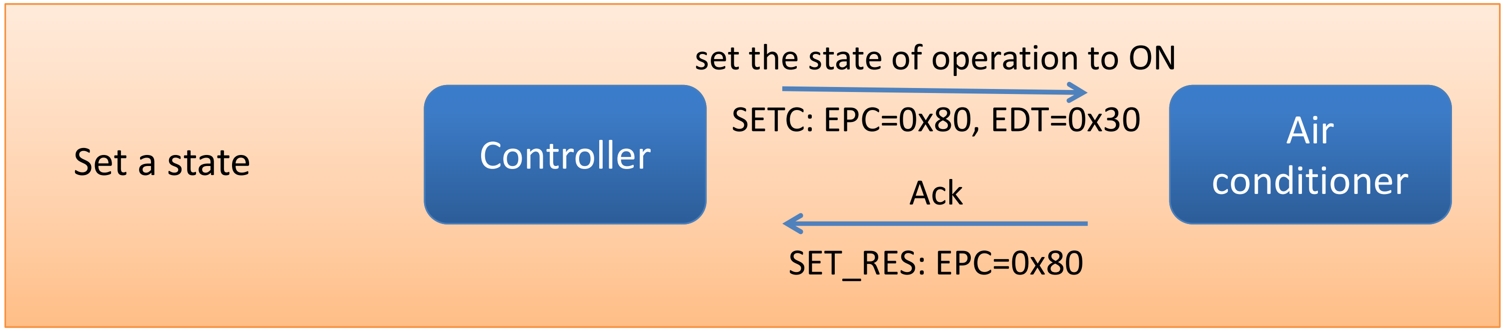
In 2025, a smart electricity meter in Japan starts to speak a common language over IPv6 on WI-Fi.

- The Japanese smart meter has two interfaces; B-root connects the meter with a user-owned device, complying with ECHONET Lite over an IPv6 single stack. A-root connects the meter with the utility company.
- New meter speaks a common language over IPv6 Link Local Address on Wi-Fi and Ethernet, covering nationwide users which is Approx. 90 millions

ECHONET Lite communication



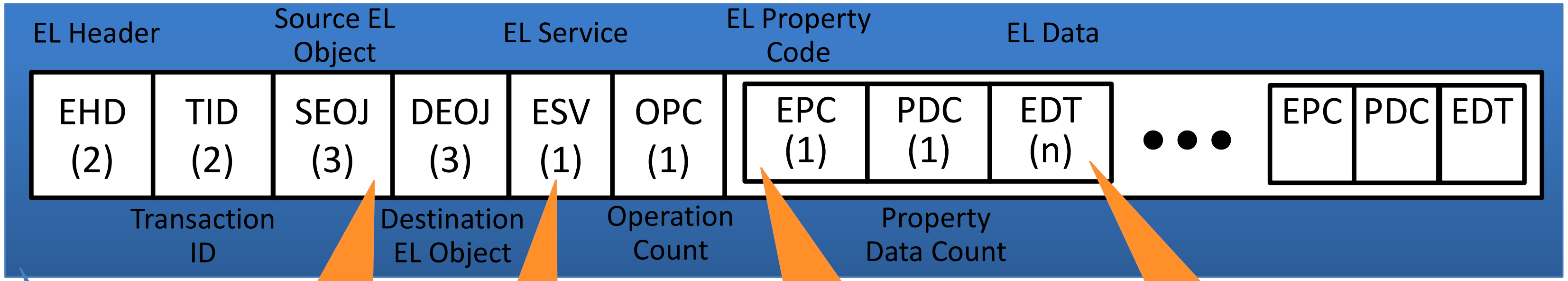
Get a state



Set a state

- UDP, Port 3610
  - Multicast address: 224.0.23.0
- Basic commands: GET, SET and INF
  - GET: Get property value
  - SET: Set property value
  - INF: Inform property value
- Every item is defined by binary data

ECHONET Lite Data Frame



EL Header, Source EL Object, EL Service, EL Property Code, EL Data

EHD	TID	SEOJ	DEOJ	ESV	OPC	EPC	PDC	EDT	•••	EPC	PDC	EDT
(2)	(2)	(3)	(3)	(1)	(1)	(1)	(1)	(n)				

Transaction ID, Destination EL Object, Operation Count, Property Data Count

EOJ: EL Object

0x013001: Air conditioner
0x029001: Lighting
0x05FF01: Controller
0x0EF001: Node profile

refer section 2 of the standard

ESV: EL Service

0x60: SETI
0x61: SETC
0x62: GET
0x71: SET_RES
0x72: GET_RES
0x73: INF

EPC: EL Property Code

EPCs of Air conditioer
0x80: Operation status
0xB0: Operating mode
0xB3: Target temperature

EPCs of Lighting
0x80: Operation status
0xB0: Brightness
0xB6: Lighting mode
0xC0: RGB value

EDT: EL Property Data

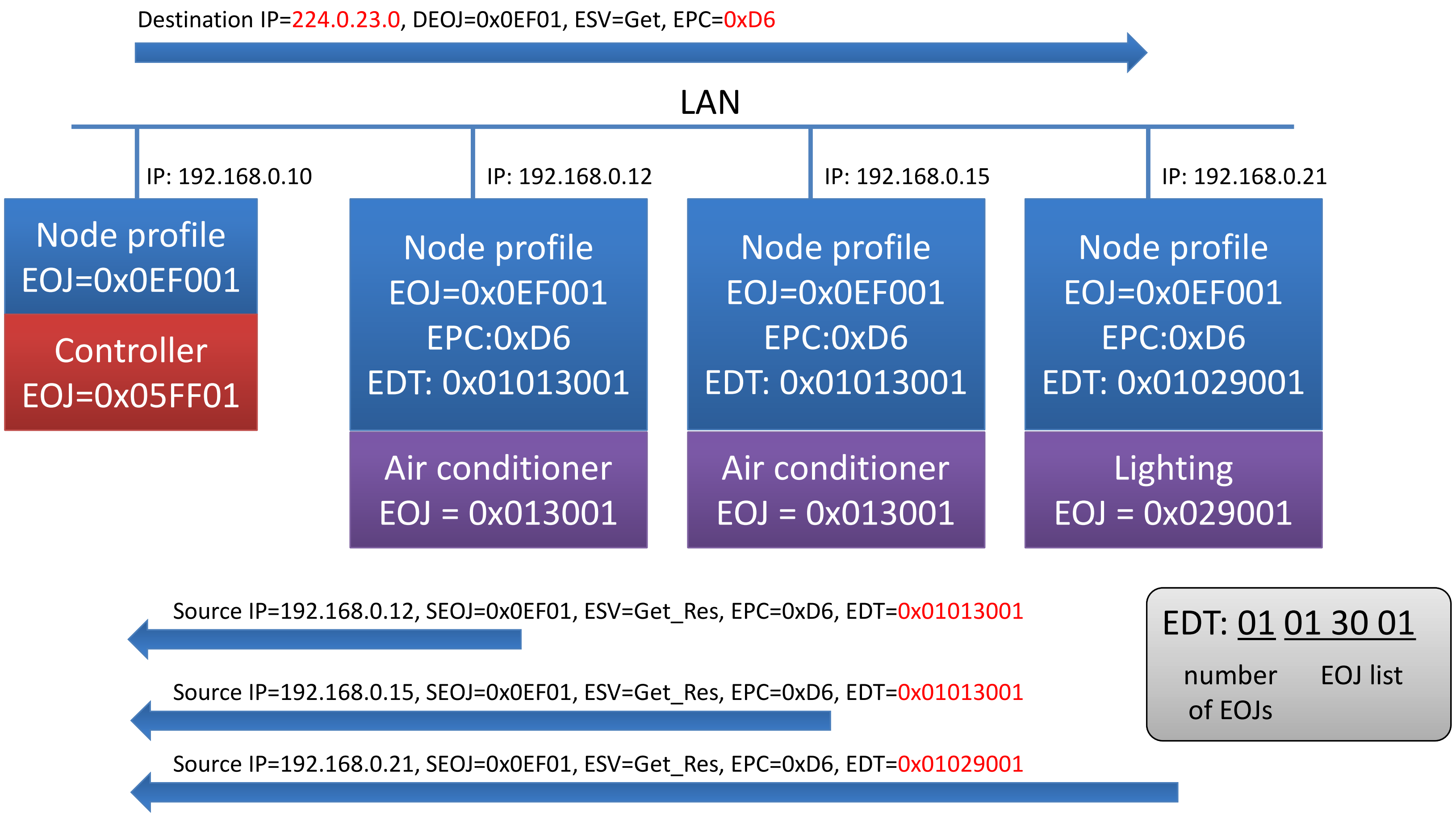
Ex： Air conditioner
EPC=0x80
EDT=0x30: ON
EDT=0x31: OFF

EPC=0xB0
EDT=0x41: Auto
EDT=0x42: Cooling

EPC=0xB3:
EDT=0x16: 22 Celsius

Device discovery on ECHONET Lite

A controller searches ECHONET Lite devices



Destination IP=224.0.23.0, DEOJ=0x0EF01, ESV=Get, EPC=0xD6

LAN

IP: 192.168.0.10

Node profile
EOJ=0x0EF001

Controller
EOJ=0x05FF01

IP: 192.168.0.12

Node profile
EOJ=0x0EF001
EPC:0xD6
EDT: 0x01013001

Air conditioner
EOJ = 0x013001

IP: 192.168.0.15

Node profile
EOJ=0x0EF001
EPC:0xD6
EDT: 0x01013001

Air conditioner
EOJ = 0x013001

IP: 192.168.0.21

Node profile
EOJ=0x0EF001
EPC:0xD6
EDT: 0x01029001

Lighting
EOJ = 0x029001

Source IP=192.168.0.12, SEOJ=0x0EF01, ESV=Get_Res, EPC=0xD6, EDT=0x01013001

Source IP=192.168.0.15, SEOJ=0x0EF01, ESV=Get_Res, EPC=0xD6, EDT=0x01013001

Source IP=192.168.0.21, SEOJ=0x0EF01, ESV=Get_Res, EPC=0xD6, EDT=0x01029001

EDT: 01 01 30 01

number of EOJs

EOJ list

Node profile EPC=0xD6: instance list S

Examples of communication protocols for Distributed Energy Resources

csa connectivity standards alliance

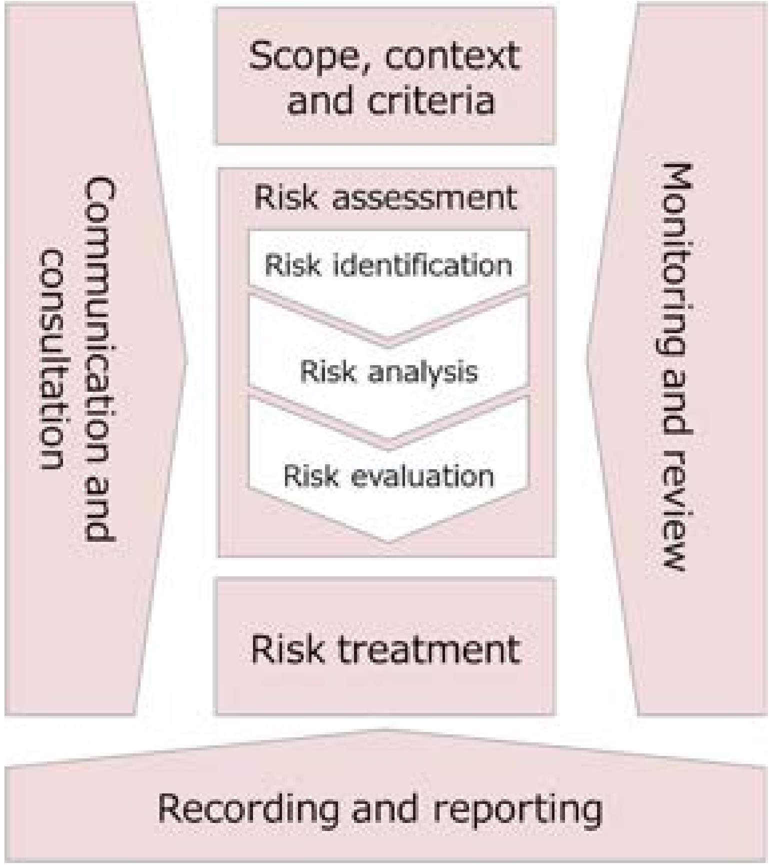
- Matter will enable communication across smart home devices, mobile app, and cloud services, and define a specific set of IP-based networking technologies for device certification.
- CSA in charge of Matter is the standard body for inter-connected devices created by the formerly Zigbee alliance. The membership has covered with: Amazon, Apple, COMCAST, Google, Huawei, IKEA, and so on

ECHONET

- Japanese Government and Industry liaison has proposed ISO/IEC14543-4-3, to be the enabler of the demand side management, around HEMS. Internet of Things over this international standard, ECHONET Lite in Japan, has provided a common language for 100s of devices: home appliances, power meter, EV, and PV.

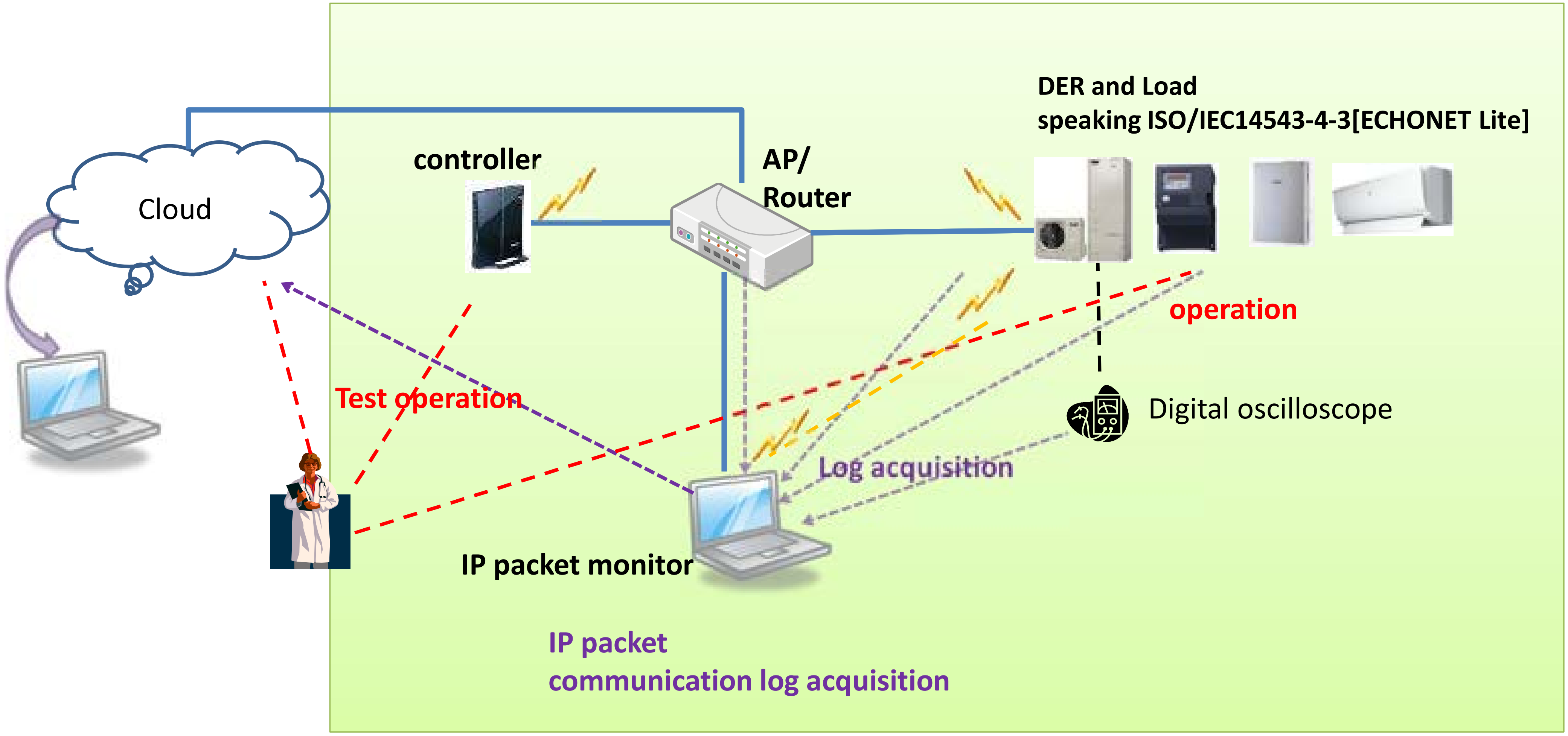
Proceed with risk management

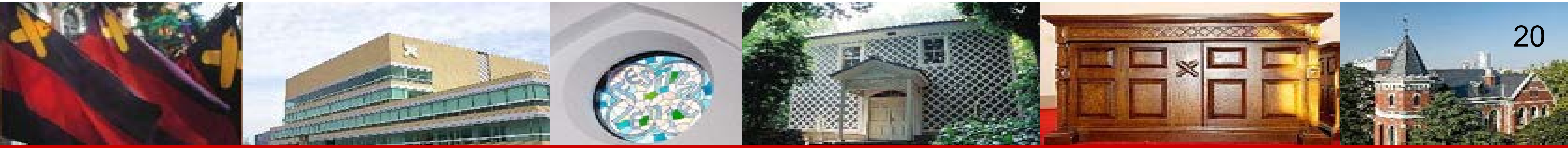
- Ppoceed with risk management that considers three-layer model and six elements in CPSF, citing ISO 31000:2018 and ISO/IEC 27001:2013.



Source: The Ministry of Economy, Trade and Industry、Japan(2019)Cyber/Physical Security Framework

A penetration test-bed on the common network design at a customer premise





National Advanced IPv6 Centre

Universiti Sains Malaysia

A Brief Introduction

Background

NETWORK
RESEARCH GROUP
NAv6
National Advanced IPv6
Centre of Excellence
USM
UNIVERSITI SAINS MALAYSIA

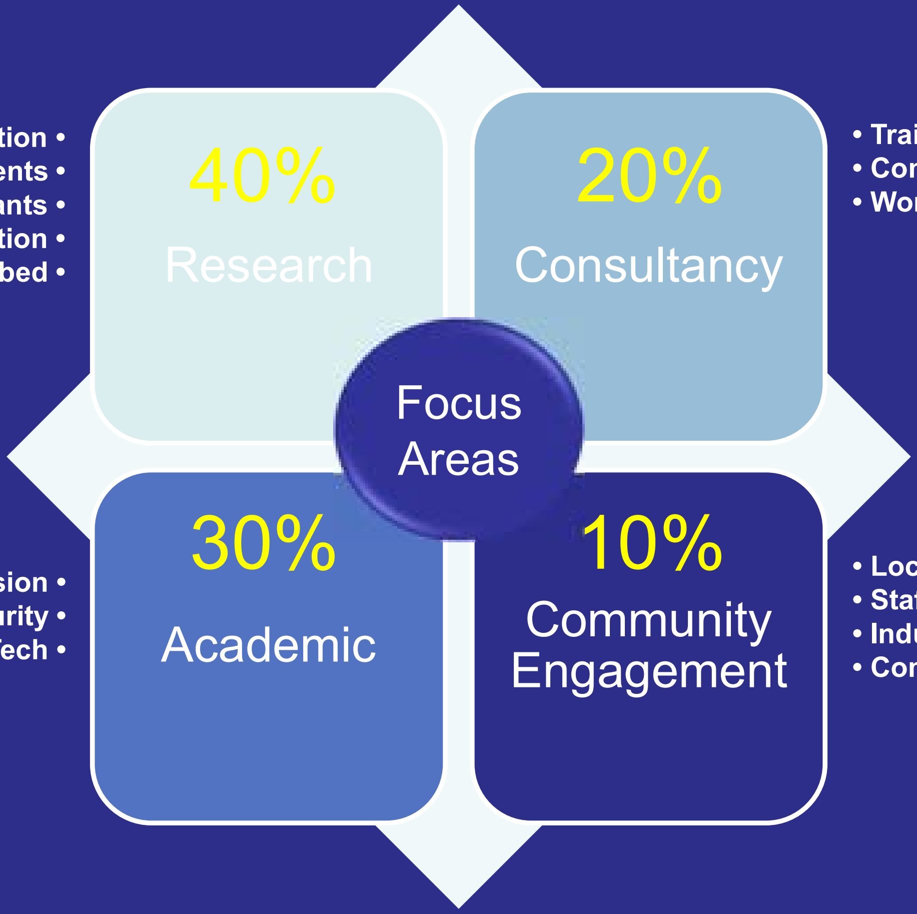
1992 - Network Research Group (NRG)

2005 - National Advanced IPv6 Centre of Excellence (NAv6) in Malaysia to implement IPv6 agenda

2008 – National Advanced IPv6 Centre (NAv6) as a center of excellence under the Senate USM.

R&D Areas

- High Impact Publication
- Cutting Edge Experiments
- Local & International Grants
- Local & International Collaboration
- Experimental Campus Testbed



- Training/certification Programs
- Contract-out Services
- Work with commercialization arm

- MSc and PhD Supervision
- MSc Cybersecurity
- Short Courses on Emerging Tech

- Local & International Internship
- Staff Exchange Program
- Industrial Collaboration
- Community Outreach Programs

Focus Areas

Augmented Reality

Cloud Computing

Wireless Communication

Machine Learning

Internet Protocol

Software Defined Network

IPv6

Virtual Reality

Fog Computing

Industry 4.0

Data Science

Artificial Intelligence

M2M and V2V

Internet Governance

Embedded System

Cyber Security

Smart Objects

Web Technologies

Drone

Cyber-Physical System

Sensor Network

Robotic Process Automation

5G

Data Analytics

Blockchain

Internet of Things

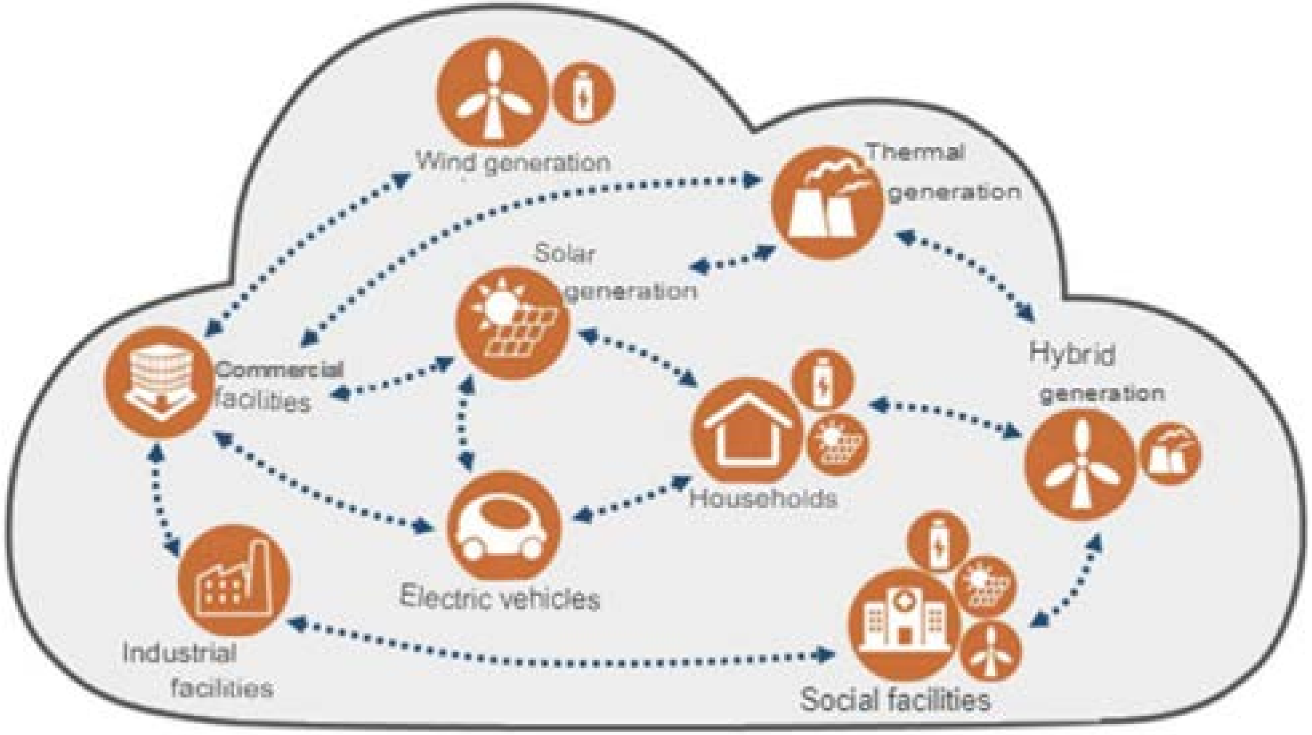
Mobile Communication

Edge Computing

Mobile Application

Satellite Communication

Digitalization of DER Ecosystem

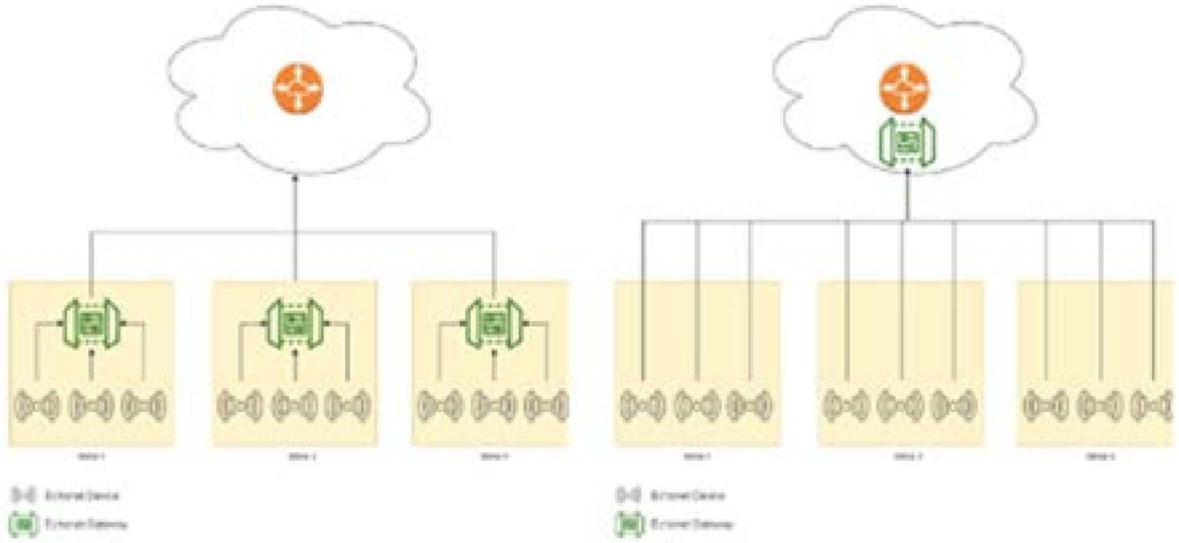


Digitalization of DER Ecosystem

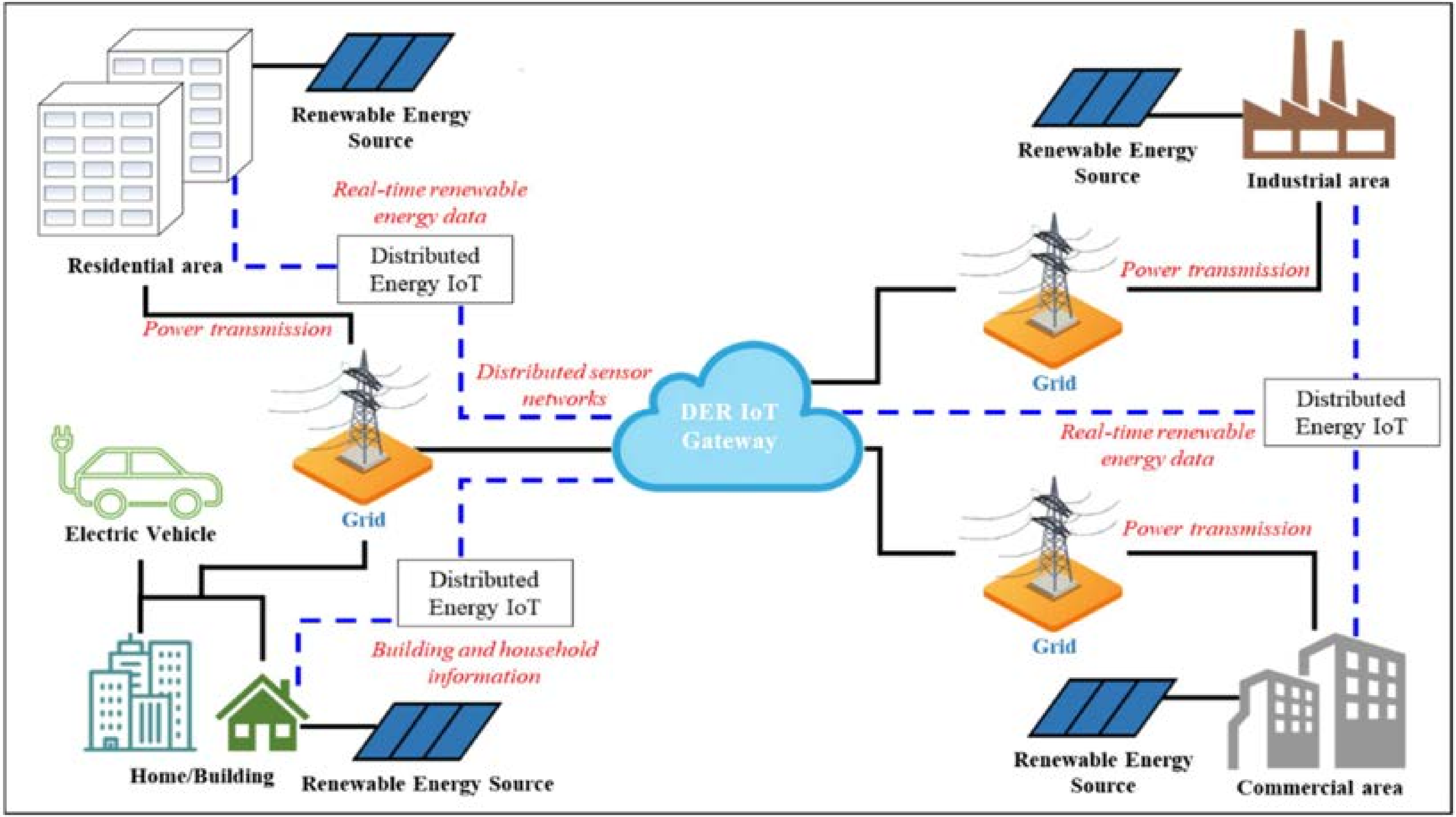
- **Increased Visibility and Control**: Digitalization offers real-time visibility, aiding DER owners in better asset management and optimization.
- **Improved Efficiency**: Digital tools automate tasks like scheduling and maintenance, enhancing operational efficiency for DER owners.
- **New Revenue Opportunities**: Digitalization opens avenues for generating revenue through grid services like frequency regulation and voltage support using DERs.
- **Reduced Costs**: Digital tools optimize energy consumption and cut waste, leading to cost reductions for DER owners.
- **Enhanced Customer Experience**: Digitalization allows for more customer interaction, offering real-time insights into energy usage and personalized energy management services.

IOT Gateway: a controller to facilitate DERs

- A DER gateway system, like an IoT gateway, collects and aggregates data from various DERs.
- The gateway bridges communication between DERs, IoT devices, sensors, other equipment and the cloud. By systematically connecting the field and the cloud, the gateway offers local processing and storage capabilities as well as the ability to autonomously control DERs based on data sensor input.



a Physical IoT GW (left), b Cloud-based IoT GW (right)


Renewable Energy Source
Residential area
Real-time renewable energy data
Distributed Energy IoT
Power transmission
Distributed sensor networks
Grid
DER IoT Gateway
Electric Vehicle
Distributed Energy IoT
Building and household information
Home/Building
Renewable Energy Source
Renewable Energy Source
Industrial area
Power transmission
Grid
Distributed Energy IoT
Real-time renewable energy data
Power transmission
Grid
Renewable Energy Source
Commercial area

Physical On-Premise Gateway

Advantages

- **Low latency**: **Data processed locally, reducing latency for critical applications.**
- **Privacy and data control**: **Data stays within organization's infrastructure, providing greater control and compliance.**
- **Reliability**: **Can continue to function without Internet or cloud service disruption.**
- **Scalability**: **Can be scaled to meet specific needs without relying on cloud resources.**
- **Security**: **Additional layer of security as data doesn't travel over public Internet.**
- **Cost-effectiveness**: **Cost-effective for large-scale deployments as reduces data transmission costs.**

Disadvantages

- Limited processing power: May not be able to handle complex analytics.
- Maintenance overhead: Organizations responsible for maintaining and updating hardware and software.
- Initial setup: More complex than cloud-based solutions.
- Scaling challenges: Can be difficult to scale as IoT ecosystem grows.
- Single point of failure: If gateway fails, entire IoT system may be disrupted.
- Limited remote access: Access to data and control may be restricted.
- Cost of ownership: Higher initial hardware and ongoing maintenance costs than cloud-based alternatives.

Security Advantages

1. **Centralized Security Management**: DER gateways centralize security management, simplifying policy implementation and enforcement.
2. **Enhanced Visibility**: They offer improved visibility into the DER system, enabling faster detection and response to security incidents.
3. **Comprehensive Security Features**: DER gateways include authentication, authorization, encryption, and intrusion detection, fortifying the DER system against unauthorized access and cyberattacks.

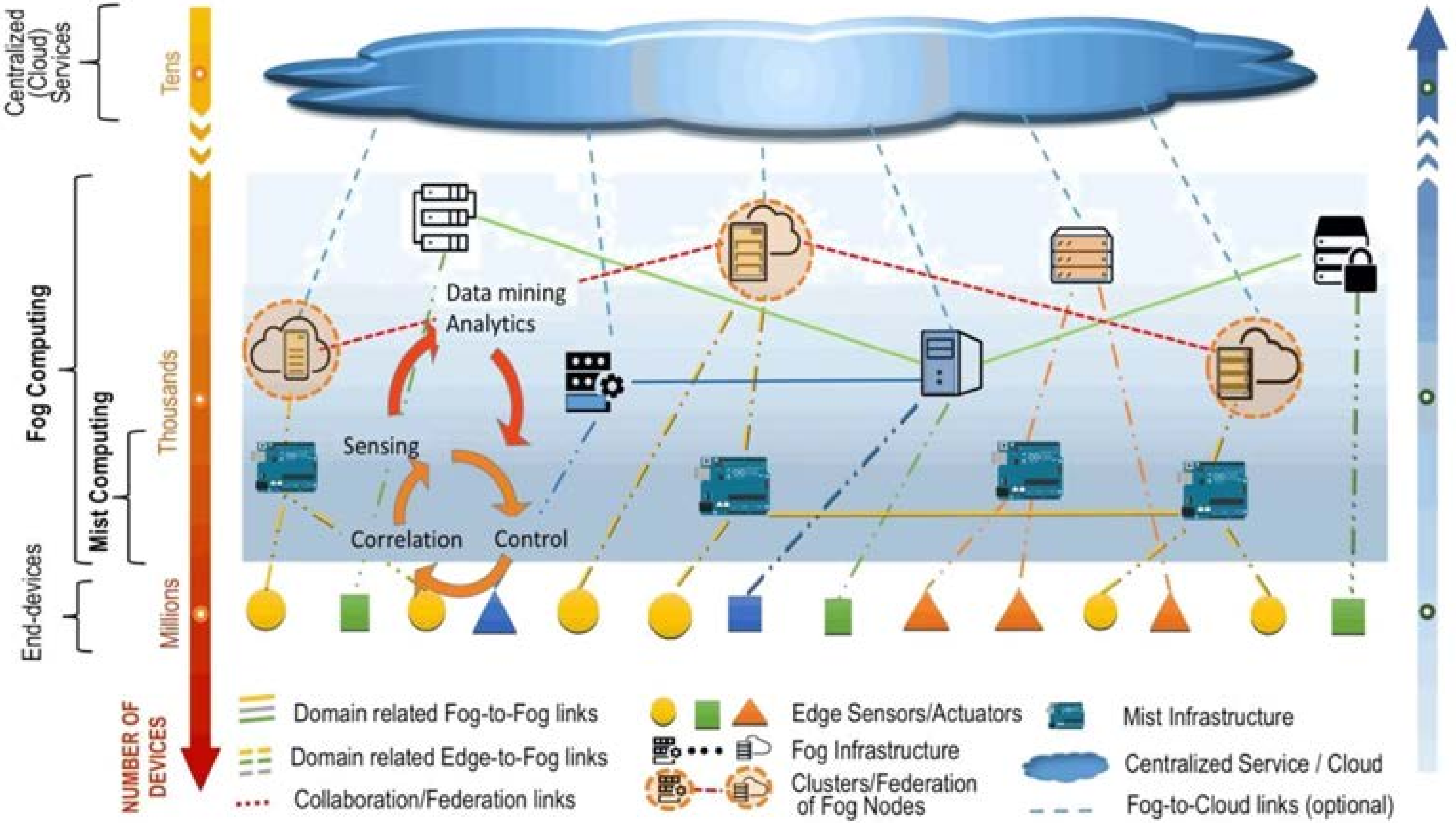
Security Issues

- Biggest security risks associated with DER gateway systems is that they are a single point of failure.
- Attacker could use the gateway
  - to inject malicious code into the DER system.
  - to disrupt the communication between the DER system and the grid.
- Vulnerable to a number of common cyberattacks, such as malware attacks, denial-of-service attacks, and phishing attacks.

- **Auth & Auth Weaknesses**: DER gateways must authenticate and authorize users/devices. Failure here can lead to unauthorized access.
- **Encryption Weaknesses**: Proper encryption is vital to protect data in transit/at rest. Inadequate implementation risks data theft.
- **Software Weaknesses**: Software-based DER gateways need regular patching. Neglect can lead to exploits and gateway control.
- **Physical Security**: Often remote, physical security lapses can grant attackers access, compromising the gateway.

Cloud-based Gateway

- Cloud-based: **Entire controller function in the cloud.**
- Edge and fog integration: **Edge processes data at the source, fog distributes across edge, fog, and cloud based on criticality.**
- Edge computing: **Decentralized data processing at the edge, minimizes network traffic, enables near real-time analysis.**
- Fog computing: **Supports latency-sensitive apps with scalable, multi-tiered systems.**
- Complex deployment: **Integrating edge, fog, and cloud adds complexity, requires careful consideration of data processing locations.**


Centralized (Cloud) Services
Fog Computing
Mist Computing
End-devices
Tens
Thousands
Millions
NUMBER OF DEVICES
LATENCY
Data mining
Analytics
Sensing
Correlation
Control
Domain related Fog-to-Fog links
Domain related Edge-to-Fog links
Collaboration/Federation links
Edge Sensors/Actuators
Fog Infrastructure
Clusters/Federation of Fog Nodes
Mist Infrastructure
Centralized Service / Cloud
Fog-to-Cloud links (optional)

Cloud-based Gateway

Advantages

- **Scalability:** Easily scale to accommodate large-scale deployments.
- **Cost-efficiency:** Lower upfront costs, pay for cloud resources used.
- **Flexibility:** Adapt to changing requirements and updates seamlessly.
- **Easy deployment:** Faster than deploying physical hardware.
- **High availability:** Built-in failover mechanisms and data replication.
- **Advanced analytics:** Take advantage of cloud-based analytics and machine learning.
- **Advanced security:** Advanced analytics and up-to-date threat intelligence can prevent future threats.

Disadvantages

- Latency: May introduce latency for real-time applications.
- Data privacy concerns: Storing sensitive data in the cloud may raise privacy and compliance issues.
- Data transmission costs: Sending large volumes of data to the cloud can be costly.
- Connectivity dependency: Relies on Internet connectivity, which can be a problem in remote environments.
- Security risks: Data transmitted to the cloud may be at risk of security breaches.
- Vendor lock-in: Organizations may become dependent on a specific cloud provider.
- Regulatory compliance: Meeting regulatory compliance requirements can be complex.

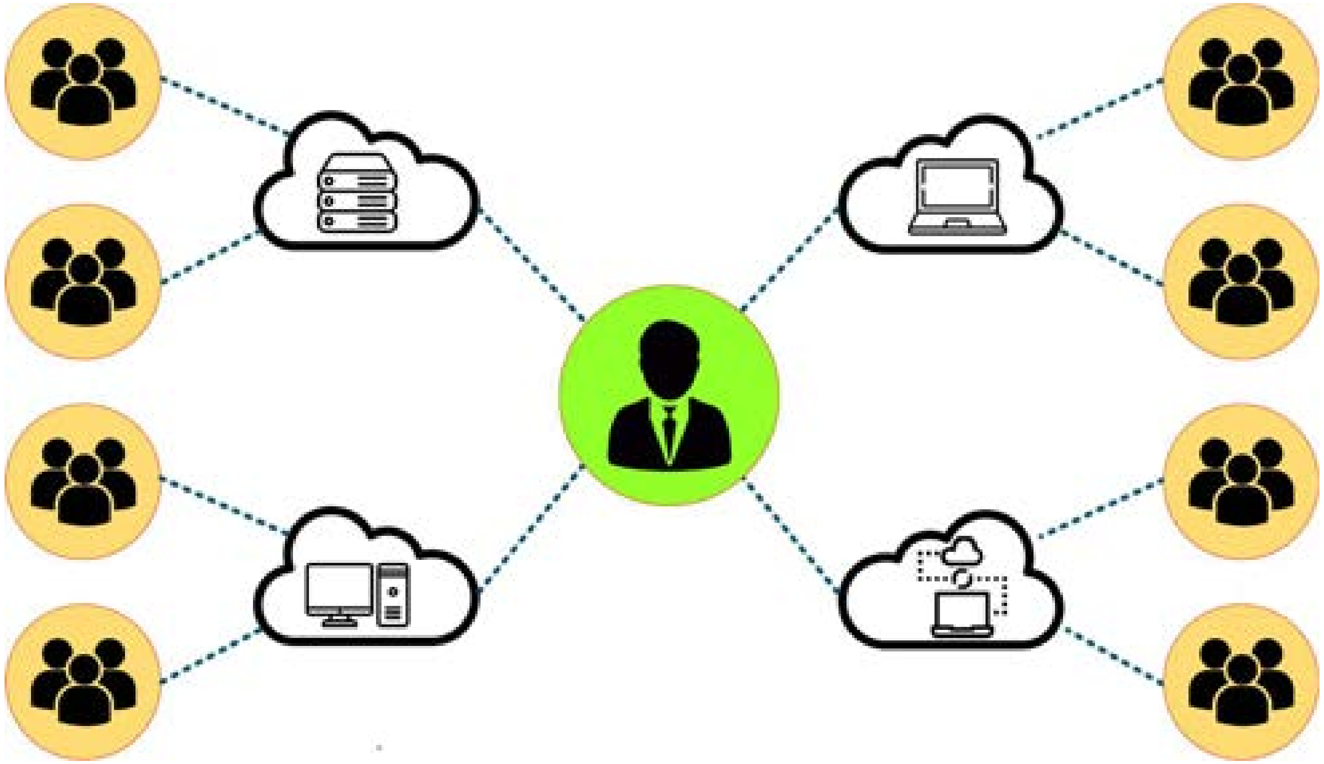
Security Advantages

- **Strong security from cloud providers**: Cloud providers invest in security infrastructure and tools to protect against cyber threats.
- **Automatic security updates**: Cloud providers automatically update their infrastructure and software, reducing security risks.
- **High availability and redundancy**: Cloud platforms have multiple data centers and redundancy features to ensure continuous service.
- **Advanced security monitoring and analytics**: Cloud providers offer tools to detect and respond to security threats in real time.
- **Secure user and device access**: Cloud platforms provide tools to control and manage user and device access.
- **Data encryption**: Data transmitted to and from the cloud-based IoT gateway is encrypted using strong encryption protocols.

Security Issues

- **Data privacy:** Storing sensitive data in the cloud can raise privacy and compliance risks.
- **Latency:** Data transmission to and from the cloud can introduce latency, which can be a problem for real-time apps.
- **Data transmission security:** Securing data transmission is crucial. Vulnerabilities can be exploited by attackers.
- **Vendor lock-in:** Organizations may become dependent on a specific cloud provider.
- **Access control:** Strong access control and authentication are essential to prevent unauthorized access.
- **Compliance:** Organizations must comply with industry standards and regulations when deploying cloud-based IoT solutions.
- **DDoS attacks:** Cloud services are susceptible to DDoS attacks. Mitigation strategies and controls are essential.

Fragmented Landscape



Hybrid Gateway

Hybrid gateways combine on-premises and cloud-based benefits, processing sensitive data locally and non-sensitive data in the cloud.

The choice between on-premises, cloud-based, or hybrid IoT gateways depends on specific needs. On-premises prioritizes security and compliance, cloud-based focuses on cost and ease, while hybrid offers a balance.

According to a recent PTC survey, 45% of organizations use on-premises IoT gateways, 35% opt for cloud-based, and 20% favor hybrid gateways, indicating a preference for on-premises with growing interest in cloud-based solutions.

The adoption of hybrid gateways is expected to increase as organizations seek a balanced approach, aiming to combine the strengths of both on-premises and cloud-based solutions.

Hybrid Gateway

- Integration: **Combines on-prem and cloud processing for flexibility.**
- Latency: **Reduces latency for real-time apps, sends non-time-sensitive data to cloud.**
- Privacy: **Keeps sensitive data on-prem for privacy and compliance.**
- Scalability: **Handles growing number of devices, cost-effective.**
- Complexity: **Implementing and managing can be complex, requires expertise.**

Hybrid Gateway

Advantages

- **Low latency:** Processes data locally for real-time response.
- **Privacy:** Sensitive data processed on-prem for compliance and control.
- **Scalability:** Handles growing number of devices, cost-effective.
- **High availability:** Local processing ensures continued functionality.
- **Security:** Data transmitted within organization's network, reducing threats.

Disadvantages

- Complexity: Requires expertise, more complex than on-prem or cloud-based solutions.
- Initial setup: Learning curve, may require additional integration.
- Maintenance overhead: Increased maintenance workload for both on-prem and cloud components.
- Hybrid integration challenges: Seamless integration can be challenging, requires careful design and monitoring.
- Resource management: Complex to manage resources between on-prem and cloud environments.
- Data routing: Complex decision-making process to determine data direction.

Security Advantages

- **Enhanced Security:** Hybrid gateways offer robust security by processing sensitive data on-premise and less sensitive data in the cloud, reducing the attack surface.
- **Improved Data Protection:** They enhance data protection through a mix of on-premises and cloud-based security measures, including encryption and restricted access.
- **Advanced Visibility and Control:** Hybrid gateways boost visibility and control over IoT data and traffic, enabling quicker threat detection and response.
- **Streamlined Compliance:** They aid in compliance with data privacy and security regulations by enabling on-premise storage and processing of sensitive data.

Security Issues

- **Complexity:** Hybrid gateways are more complex to configure and manage than standalone options, posing challenges for effective security implementation.
- **Security Vulnerabilities**: They may face security vulnerabilities in both on-premise and cloud components, increasing the risk to the gateway and processed data.
- **Security Gaps:** Poor integration between on-premise and cloud components can create exploitable security gaps.
- **Data Leakage:** Inadequate data protection at both levels can lead to potential data leakage risks.

Why Hybrid Approach?

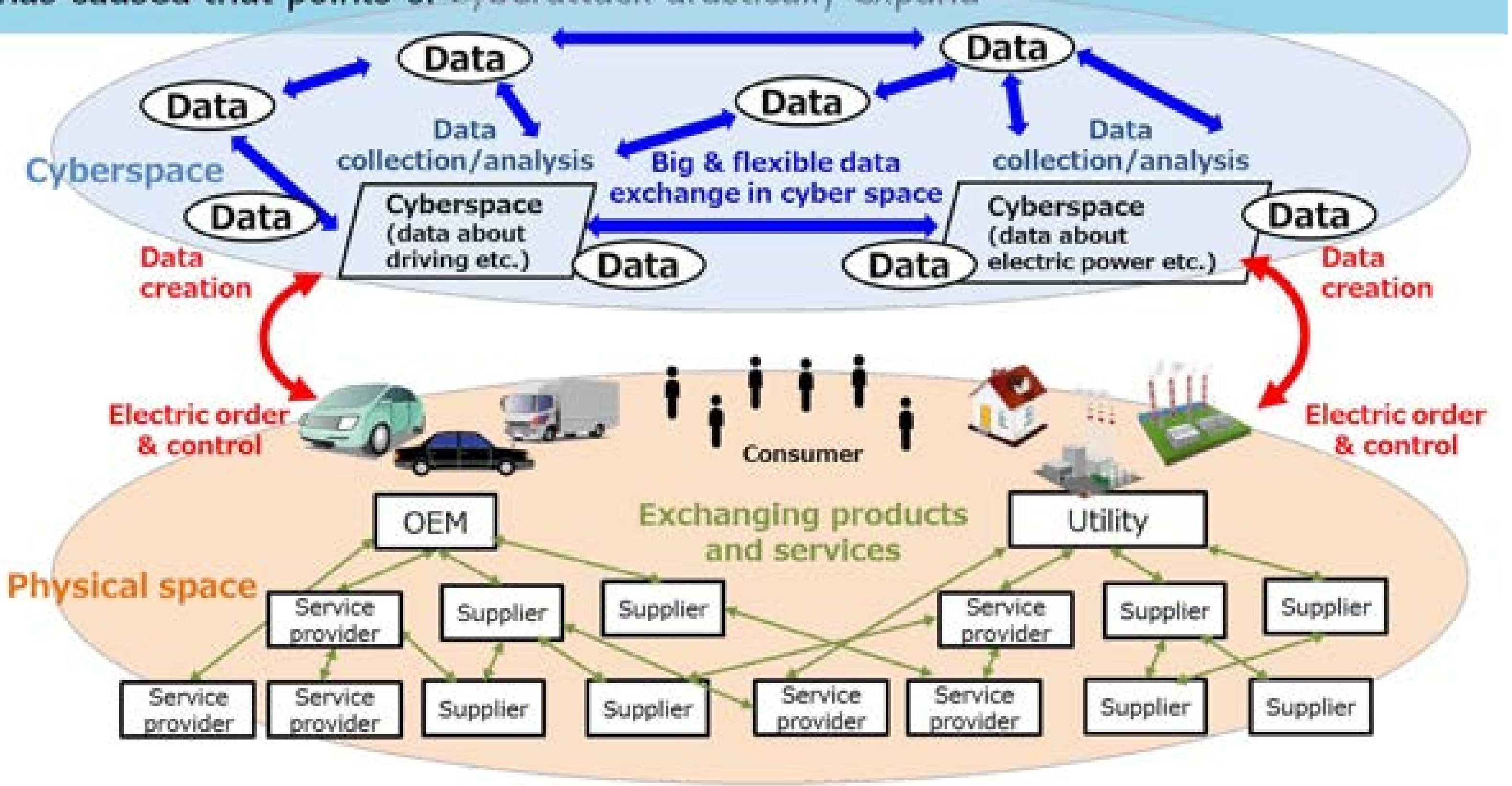
- Performance: Processes data locally for real-time response, critical for low-latency applications.
- Privacy: Sensitive data kept on-premise for control and compliance.
- Scalability: Leverages cloud resources for non-time-sensitive tasks, cost-effective.
- Resilience: Local processing ensures high availability, even with internet outages.
- Security: Minimal attack surface by processing sensitive data on-premise.
- Customization: Organizations can tailor the model to their needs.
- Compliance: Meets data sovereignty laws by keeping data within geographical boundaries.
- Traffic optimization: Reduces network congestion by sending only relevant data to the cloud.

Moving Forward..

- **Leverage Hybrid Controllers**: Use a hybrid controller approach to combine on-premises and cloud-based controllers for benefits like IoT communication using physical controllers and cloud-based virtual controllers.
- **Address Security Risks**: Mitigate security risks associated with hybrid controllers through strong encryption and access control measures.
- **Consider Specific Needs**: When designing your hybrid controller architecture, consider data types, latency requirements, and budget to tailor it to your needs.
- **Choose Reputable Vendors**: Select a secure, scalable, and manageable hybrid controller solution from a reputable vendor.
- **Simplify Integration**: Opt for a single cloud platform for your hybrid controller to simplify integration and management.
- **Utilize Managed Service Providers**: Consider using managed service providers (MSPs) for implementing and managing your hybrid controller solution, especially if you lack in-house expertise.
- **Regularly Review Architecture**: Periodically review your hybrid controller architecture to ensure it meets evolving needs, keeping up with technology trends and best practices.

Cyber Physical System

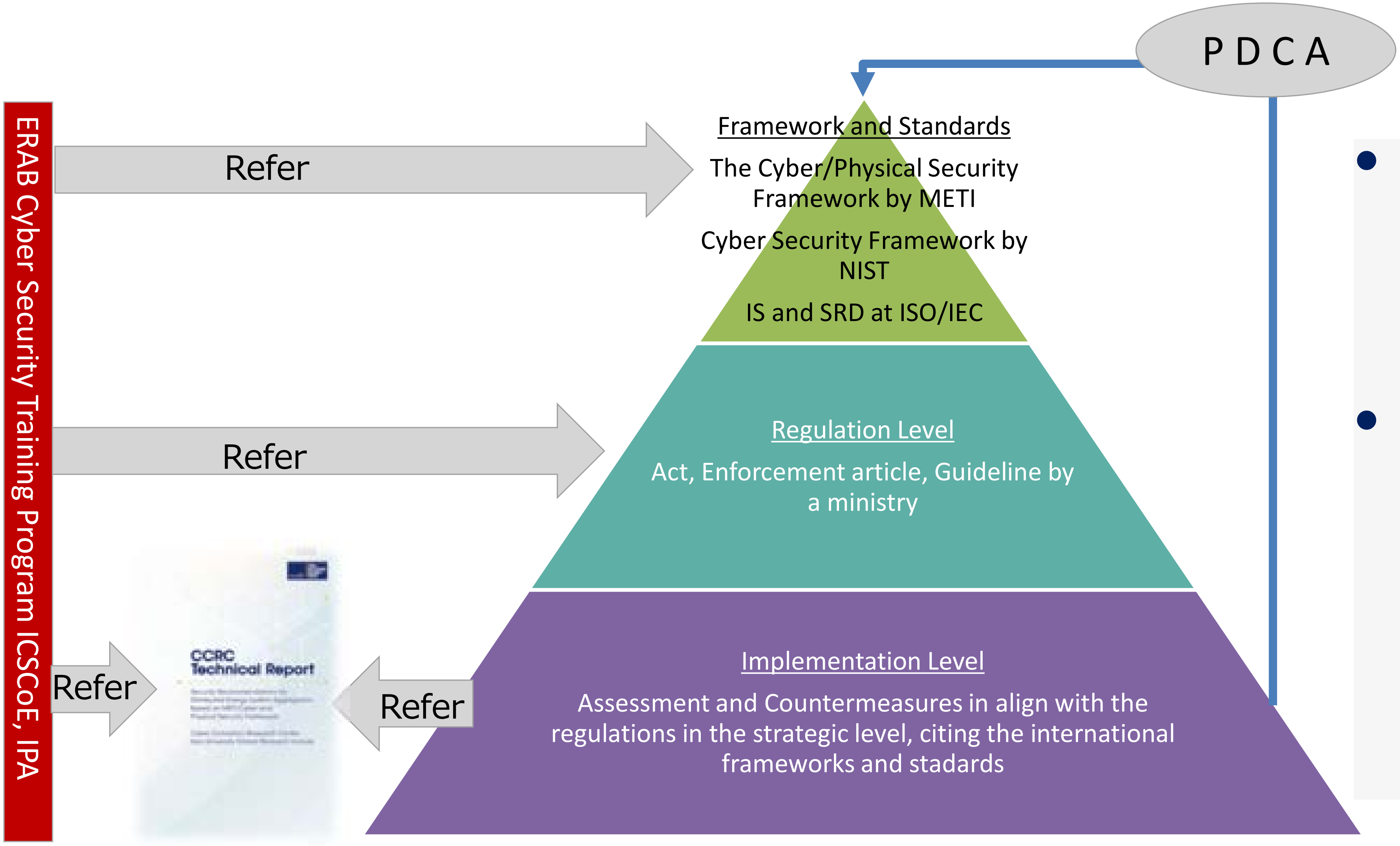
- Cyberspace and Physical space will be highly integrated
  - Two spaces interacting with each other increase the impact of the damages on physical space.
  - It has caused that points of cyberattack drastically expand



Source: The Ministry of Economy, Trade and Industry、Japan(2019)Cyber/Physical Security Framework

Security implementation example
ERAB case in Japan
Y2023

The security triangle of Energy Resource Aggregation Business



ERAB Cyber Security Training Program ICSCoE, IPA

Refer

Refer

Refer

Refer

CCRC Technical Report

PDCA

Framework and Standards

The Cyber/Physical Security Framework by METI

Cyber Security Framework by NIST

IS and SRD at ISO/IEC

Regulation Level

Act, Enforcement article, Guideline by a ministry

Implementation Level

Assessment and Countermeasures in align with the regulations in the strategic level, citing the international frameworks and stadards

- Japanese aggregators develop security countermeasures ,referring CCRC Technical Report.
- In Japan, a good coordinated triangle exists from implementation to the high-level framework.

The Cyber/Physical Security Framework [CPSF] by METI, Japanese Government

- In "Society 5.0" which is realized by IoT and AI, supply chain is transforming from traditional linear style to non-linear style where various kinds of connections exist. The Cyber/Physical Security Framework grasps the industrial society where value is created as Three Layers composed of Six Elements.

The Third Layer (Data circulation)

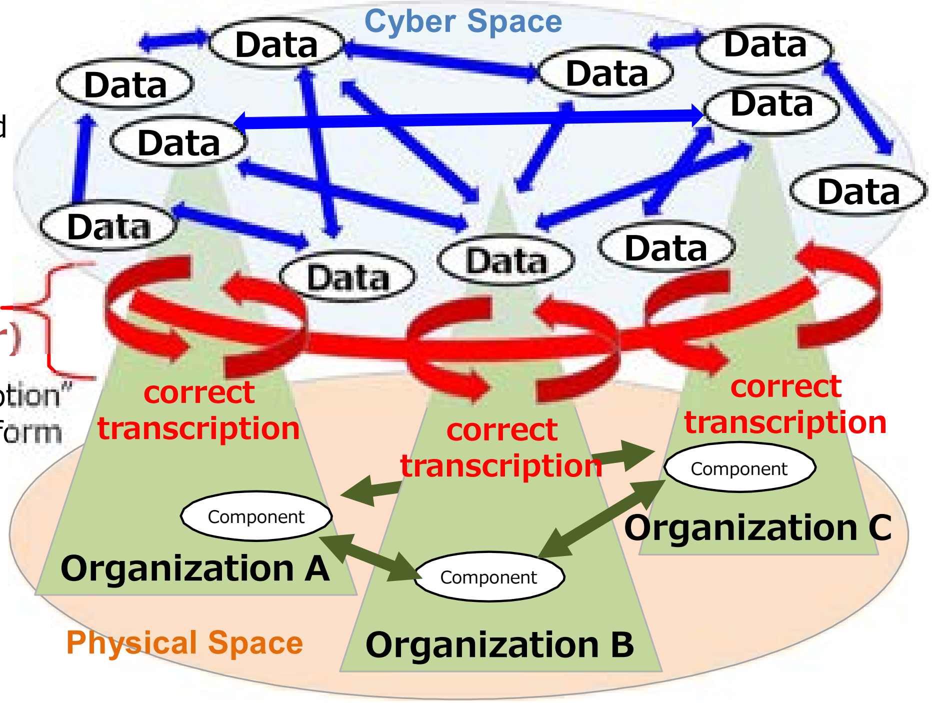
- Trustworthiness of data that freely circulate and are processed or created to produce services

The Second Layer (Cyber to physical/Physical to cyber)

- Trustworthiness of function for "correct transcription" from cyber to physical / from physical to cyber form

The First Layer (Relationship among Organizations)

- Trustworthiness of each organization based on appropriate management

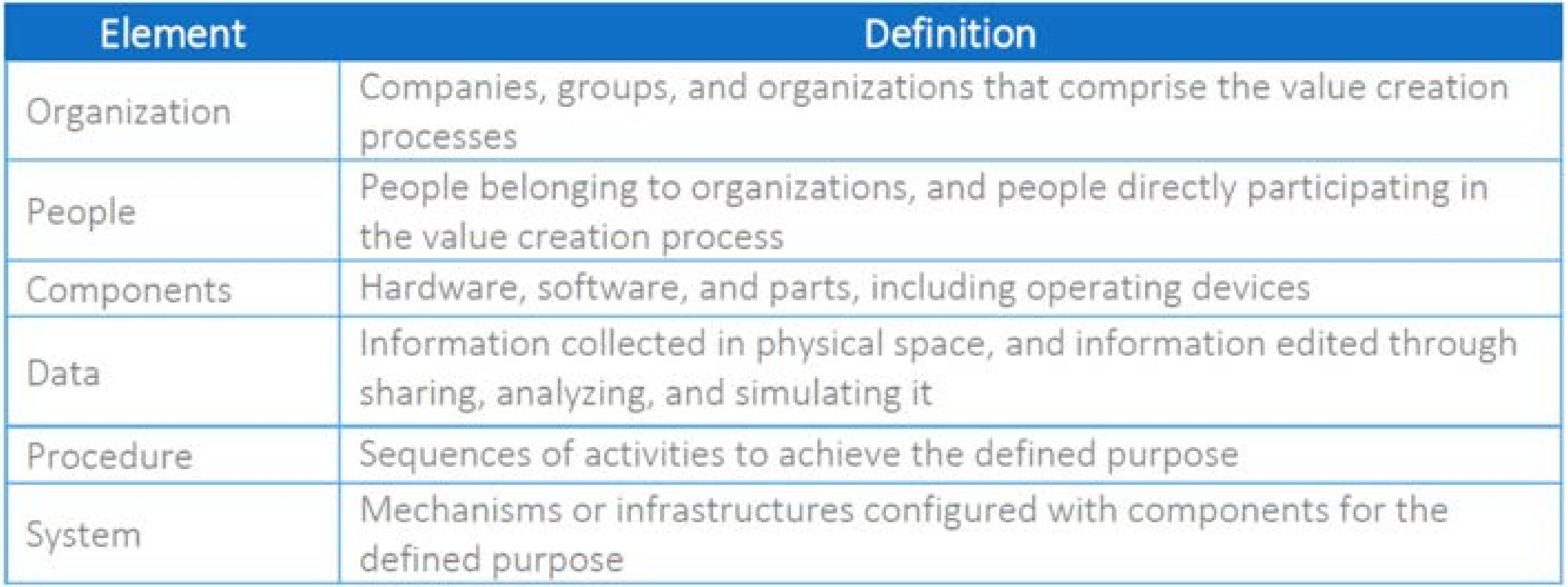


◆Six Elements: **Organization, people, component, data, procedure, system**

Source: The Ministry of Economy, Trade and Industry、Japan(2019)Cyber/Physical Security Framework

Six elements in CPSF

- It is necessary to grasp fixed business assets. In the CPSF, the elements are shown by 6 elements: the organization, the people, the components, the data, the procedure, and the system



Element	Definition
Organization	Companies, groups, and organizations that comprise the value creation processes
People	People belonging to organizations, and people directly participating in the value creation process
Components	Hardware, software, and parts, including operating devices
Data	Information collected in physical space, and information edited through sharing, analyzing, and simulating it
Procedure	Sequences of activities to achieve the defined purpose
System	Mechanisms or infrastructures configured with components for the defined purpose

Source: The Ministry of Economy, Trade and Industry、Japan(2019)Cyber/Physical Security Framework

Compatibility between CPSF in JP and CSF in U.S

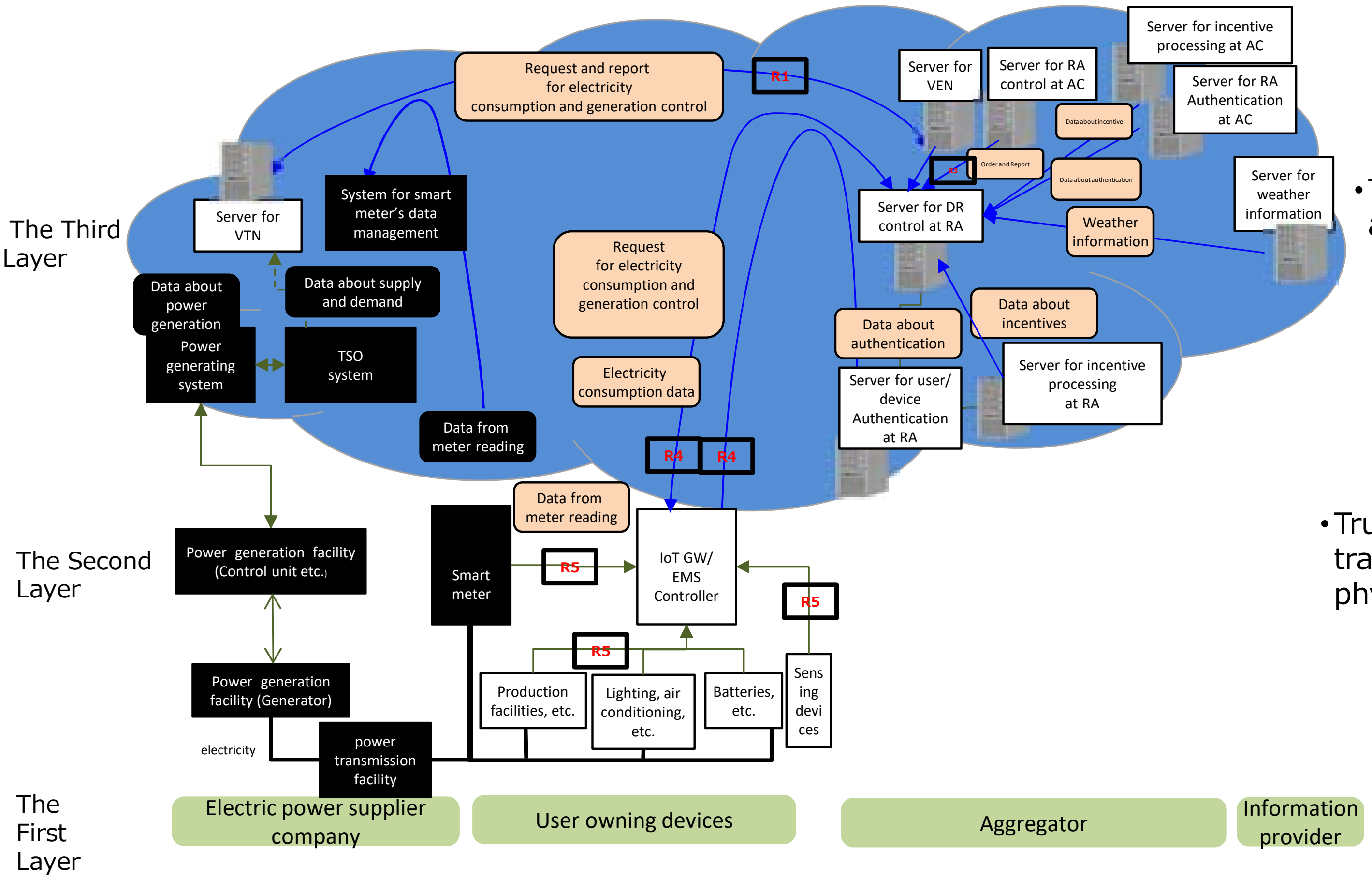
- Cyber/Physical Security Framework in J.P
  - The Cyber/Physical Security Framework (meti.go.jp)
- Cybersecurity Framework Version 1.1 in U.S.
  - https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Category names in CPSF	Acronym	Related category names in CSF
Asset Management	CPSF.AM	ID.AM (Asset Management)
Business Environment	CPSF.BE	ID.BE (Business Environment)
Governance	CPSF.GV	ID.GV (Governance)
Risk Assessment	CPSF.RA	ID.RA (Risk Assessment)
Risk Management Strategy	CPSF.RM	ID.RM (Risk Management Strategy)
Supply Chain Risk Management	CPSF.SC	ID.SC (Supply Chain Risk Management)
Identity Management, Authentication, and Access Control	CPSF.AC	PR.AC (Identity Management and Access Control)
Awareness and Training	CPSF.AT	PR.AT (Awareness and Training)
Data Security	CPSF.DS	PR.DS (Data Security)
Information Protection Processes and Procedures	CPSF.IP	PR.IP (Information Protection Processes and Procedures)
Maintenance	CPSF.MA	PR.MA (Maintenance)
Protective Technology	CPSF.PT	PR.PT (Protective Technology)
Anomalies and Events	CPSF.AE	DE.AE (Anomalies and Events)
Security Continuous Monitoring	CPSF.CM	DE.CM (Security Continuous Monitoring)
Detection Processes	CPSF.DP	DE.DP (Detection Processes)
Response Planning	CPSF.RP	RS.RP (Response Planning) RC.RP (Recovery Planning)
Communications	CPSF.CO	RS.CO (Communications) RC.CO (Communications)
Analysis	CPSF.AN	RS.AN (Analysis)
Mitigation	CPSF.MI	RS.MI (Mitigation)
Improvements	CPSF.IM	RS.IM (Improvements) RC.IM (Improvements)

Source: The Ministry of Economy, Trade and Industry、Japan(2019)Cyber/Physical Security Framework

Mapping Energy Resource Aggregation Business [ERAB] System on CPSF

◆**Six Elements: Organization, people, component, data, procedure, system**



Request and report for electricity consumption and generation control

R1

Server for VEN

Server for RA control at AC

Server for incentive processing at AC

Server for RA Authentication at AC

Data about incentive

Order and Report

R3

Data about authentication

Server for DR control at RA

Weather information

Server for weather information

The Third Layer

Server for VTN

System for smart meter's data management

Request for electricity consumption and generation control

Data about power generation

Data about supply and demand

Power generating system

TSO system

Electricity consumption data

Data from meter reading

Data about authentication

Data about incentives

Server for user/ device Authentication at RA

Server for incentive processing at RA

R4

R4

The Second Layer

Power generation facility (Control unit etc.)

Data from meter reading

Smart meter

R5

IoT GW/ EMS Controller

R5

R5

Power generation facility (Generator)

Production facilities, etc.

Lighting, air conditioning, etc.

Batteries, etc.

Sens ing devi ces

electricity

power transmission facility

The First Layer

Electric power supplier company

User owning devices

Aggregator

Information provider

The Third Layer (Data circulation)

- Trustworthiness of data that freely circulate and are processed or created to produce services

The Second Layer (Cyber to physical/Physical to cyber)

- Trustworthiness of function for "correct transcription" from cyber to physical / from physical to cyber form

The First Layer (Relationship among Organizations)

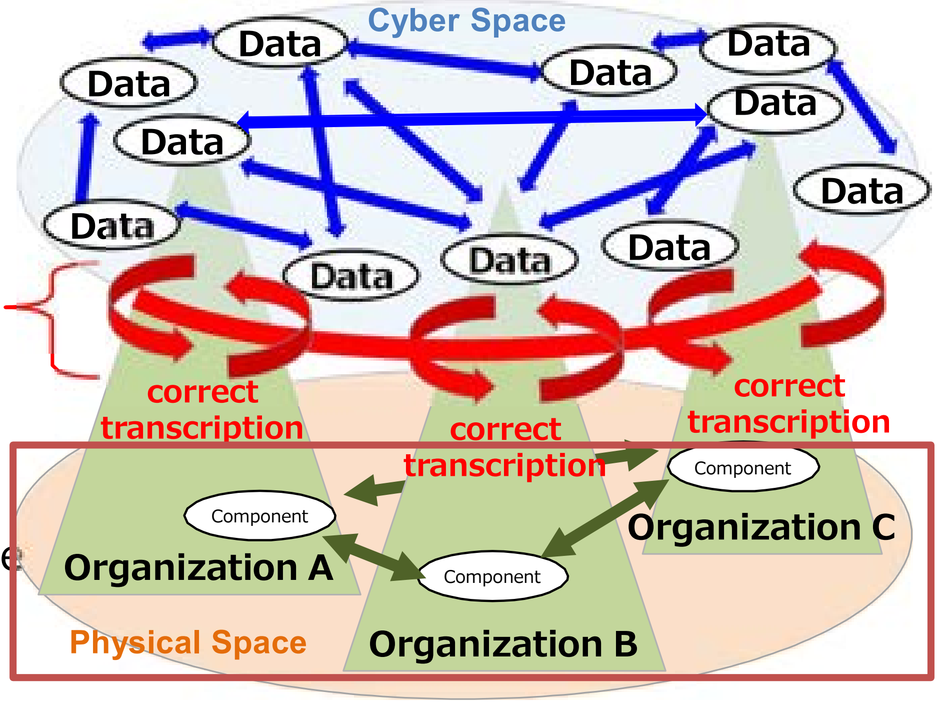
- Trustworthiness of each organization based on appropriate management

Source: The Ministry of Economy, Trade and Industry、Japan(2019)Cyber/Physical Security Framework

First Layer in CPSF

- The First Layer (Relationship among Organizations)
  - The first layer aims to ensure trust in the management of an organization. It has been adopted to achieve security across supply chains.

- Certification programs such as ISMS (based on ISO/IEC 27001) focus on confirming trust in company management
- The first layer in CPSF aims to achieve shared and certified security policies as a basis for promoting trust.
- In Cyber-Physical system, where cyber and physical space are integrated, it is impossible to ensure trust throughout the entire value creation process only by security implementation in the first layer.

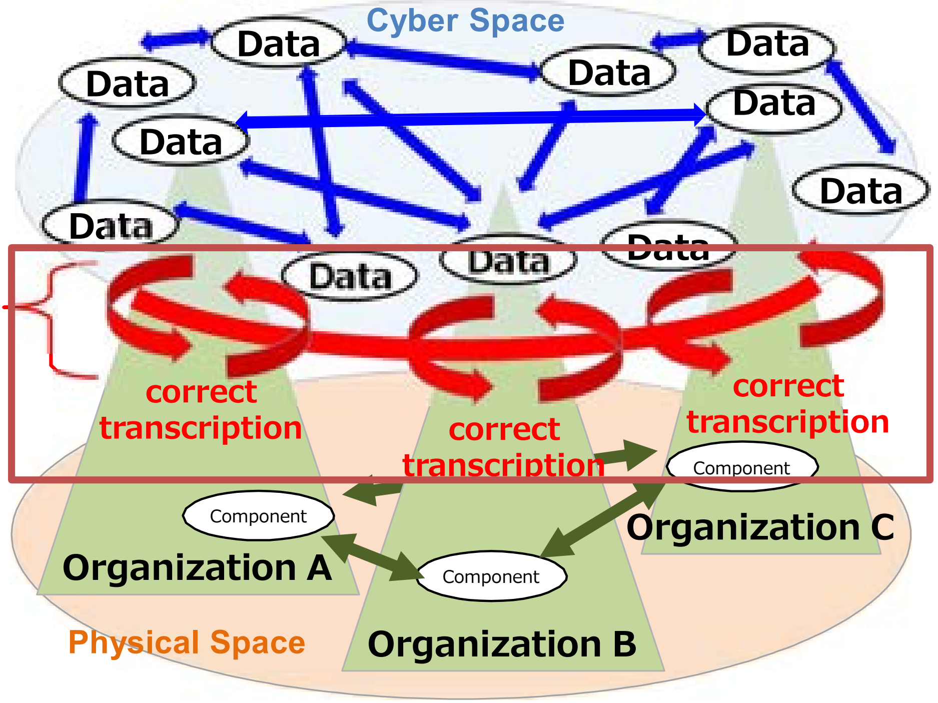


Source: The Ministry of Economy, Trade and Industry、Japan(2019)Cyber/Physical Security Framework

Second Layer in CPSF

- The Second Layer (connections between cyberspace and physical space)
  - Unreliable interactions between cyberspace and physical space could cause uncertainty throughout industrial society.

- The second layer is based on the accuracy and trustworthiness of data transcription and transfer (including accurate translation) between cyberspace and physical space.
- Certification programs such as ISO/IEC 27036 focus on confirming trustworthiness in transcription
- It is impossible to ensure trust throughout the entire value creation process only by ISO/IEC 27036.

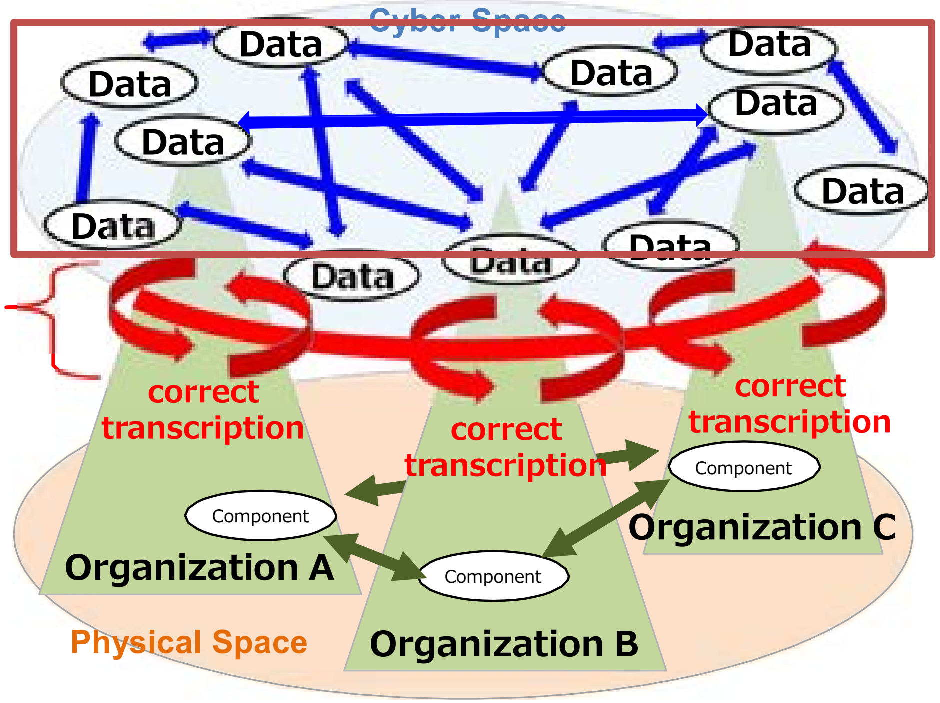


Source: The Ministry of Economy, Trade and Industry、Japan(2019)Cyber/Physical Security Framework

Third Layer in CPSF

- The Third Layer (connections in cyberspace)
  - security measures need to be implemented in the third layer for data distribution and storage and appropriate editing and processing

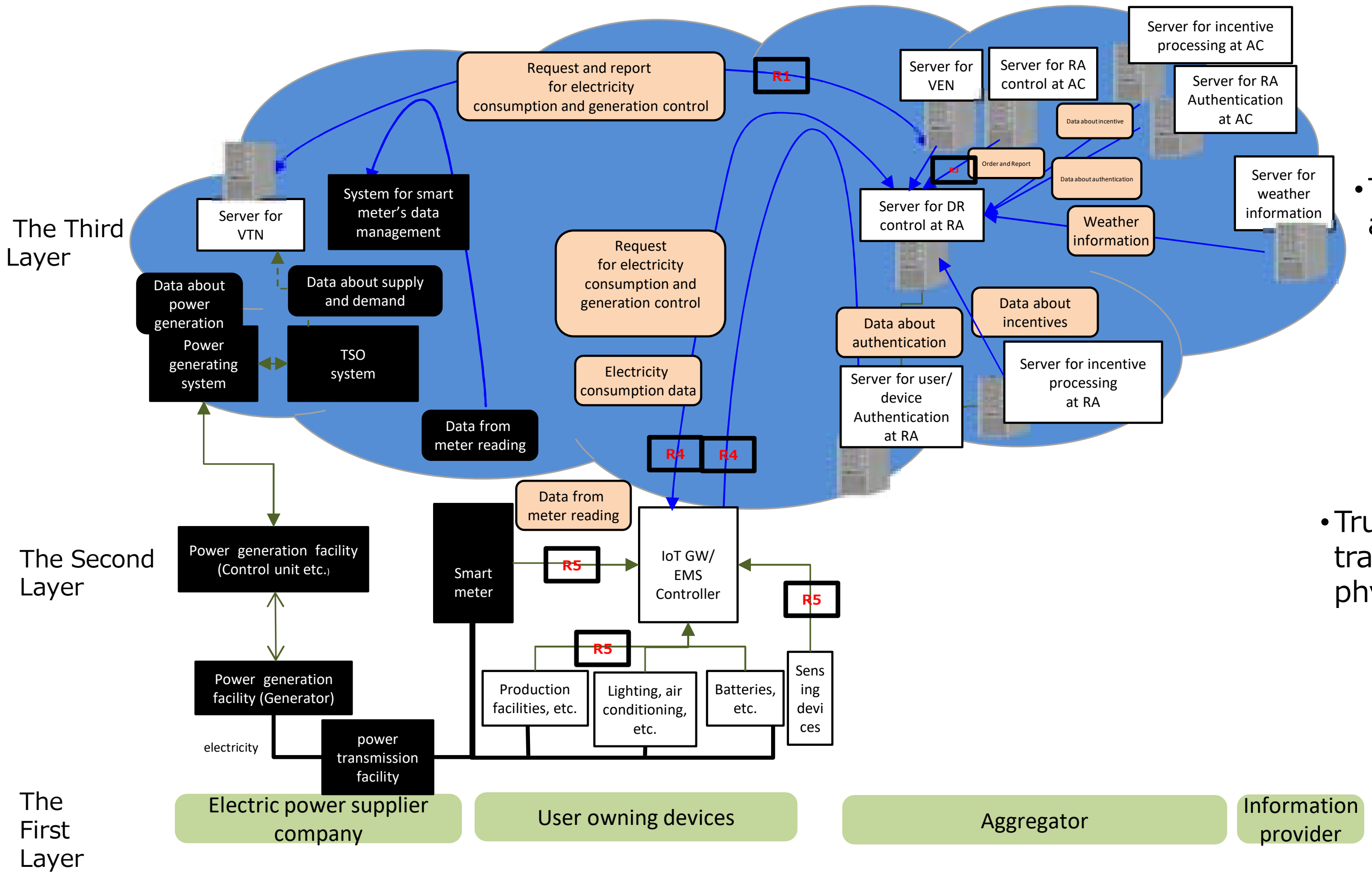
- Certification programs such as ISO/IEC 27017 focus on confirming trustworthiness in cloud data storage
- It is impossible to ensure trust throughout the entire value creation process only by ISO/IEC 27017.



Source: The Ministry of Economy, Trade and Industry、Japan(2019)Cyber/Physical Security Framework

Mapping Energy Resource Aggregation Business [ERAB] System on CPSF

◆**Six Elements:** **Organization, people, component, data, procedure, system**


The Third Layer
The Second Layer
The First Layer
Request and report for electricity consumption and generation control
R1
Server for VEN
Server for RA control at AC
Server for incentive processing at AC
Server for RA Authentication at AC
Data about incentive
Order and Report
R3
Data about authentication
Server for VTN
System for smart meter's data management
Server for DR control at RA
Weather information
Server for weather information
Data about power generation
Data about supply and demand
Request for electricity consumption and generation control
Data about authentication
Data about incentives
Power generating system
TSO system
Electricity consumption data
Server for user/ device Authentication at RA
Server for incentive processing at RA
Data from meter reading
R4
R4
Data from meter reading
Power generation facility (Control unit etc.)
Smart meter
R5
IoT GW/ EMS Controller
R5
R5
Power generation facility (Generator)
Production facilities, etc.
Lighting, air conditioning, etc.
Batteries, etc.
Sensing devices
electricity
power transmission facility
Electric power supplier company
User owning devices
Aggregator
Information provider

The Third Layer (Data circulation)

- Trustworthiness of data that freely circulate and are processed or created to produce services

The Second Layer (Cyber to physical/Physical to cyber)

- Trustworthiness of function for "correct transcription" from cyber to physical / from physical to cyber form

The First Layer (Relationship among Organizations)

- Trustworthiness of each organization based on appropriate management

Source: The Ministry of Economy, Trade and Industry、Japan(2019)Cyber/Physical Security Framework

Cybersecurity Guideline for Energy Resource Aggregation Business ver.2.0

- Agency for Natural Resources and Energy and Information-technology Promotion Agency [IPA] provide the guideline showing the cybersecurity measures that businesses participants in ERAB should take.

エネルギー・リソース・アグリゲーション・
ビジネスに関するサイバーセキュリティ
ガイドライン Ver2.0

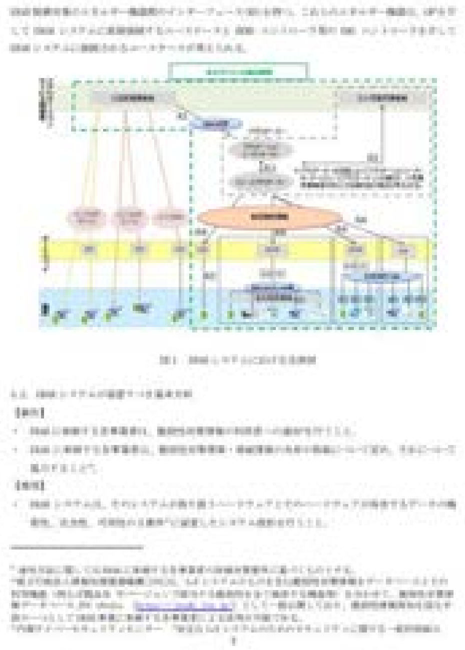
策定　平成29年　4月26日

改定　平成29年11月29日

改定　令和元年　12月　27日

資源エネルギー庁
独立行政法人情報処理推進機構[IPA]

1



- Japanese original version is available at:
  - https://www.meti.go.jp/english/press/2019/1227_005.html
- English translation with a research purpose is available at:
  - https://www.enecho.meti.go.jp/en/category/vpp_dr/data/cybersecurity_guidelines_for_erab.pdf

Japan case: Cybersecurity Guideline for Energy Resource Aggregation Business Ver. 2.0

- Article 3.6 defines the design on cybersecurity measures for ERAB system

Process	Content
Step1	Clarify the overall system configuration and responsibility demarcation point of intended IoT product or service.
Step2	Clarify the information, function and assets for protection in the system
Strep3	Clarify the possible threat for the information, function and assets for protection
Step4	Clarify countermeasures (best practice) against threat
Step5	Select measures to implement considering threat level, damage level, cost, etc.
Step6	Verify the implementation of countermeasures that the mandatory items are prioritized through third-party audits (including certification), educational programs.
Step7	Design, operate and train the way to respond to accidents

Source: Agency for Natural Resources and Energy Information-technology Promotion Agency(2019) Cybersecurity Guideline for Energy Resource Aggregation Business Ver. 2.0

CCRC CONTRIBUTES TO DESIGN ERAB SYSTEM SECURITY

- **In 2021, CCRC published the technical report on "Security Recommendations for Distributed Energy System Aggregators, Based on METI Cyber and Physical Security Framework", showing 51 recommendations to be countermeasures to the major vulnerabilities of ERAB system.**
  - The report is backed by 5 years experience of running a prototype system
  - The full report is available at
    - https://www.ccrc.keio.ac.jp/ccrc-technical-report-202109/

CCRC
Technical Report

Security Recommendations for
Distributed Energy System Aggregat
Based on METI Cyber and
Physical Security Framework

Cyber Civilization Research Center,
Keio University Global Research Insti

ERAB Cyber Security Training Program ICSCoE, IPA

- Industrial Cyber Security Center of Excellence in IPA (ICSCoE) has provided a training program to help aggregators have an appropriate security design about an electricity aggregation system.
- The program has complied with “Cybersecurity Guideline for Energy Resource Aggregation Business Ver. 2.0” published in Agency for Natural Resources and Energy in Japanese Government and IPA, referring “The Cyber/Physical Security Framework” in METI and CCRC Technical Report “Distributed Energy System Aggregators, Based on METI Cyber and Physical Security Framework” published in Keio University

The training program has the three components:

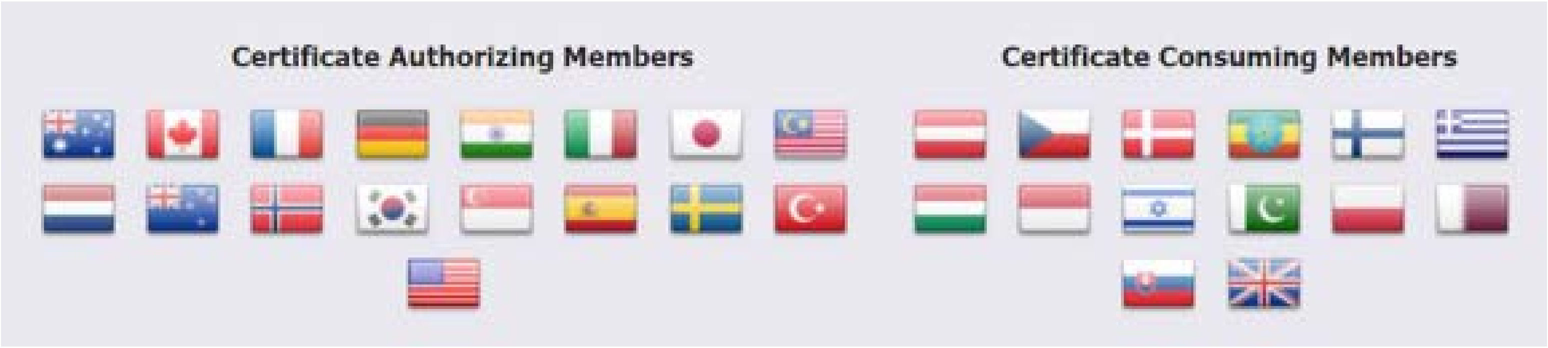
● Learn the related regulations and bibliographies

● Exercise a risk assessment

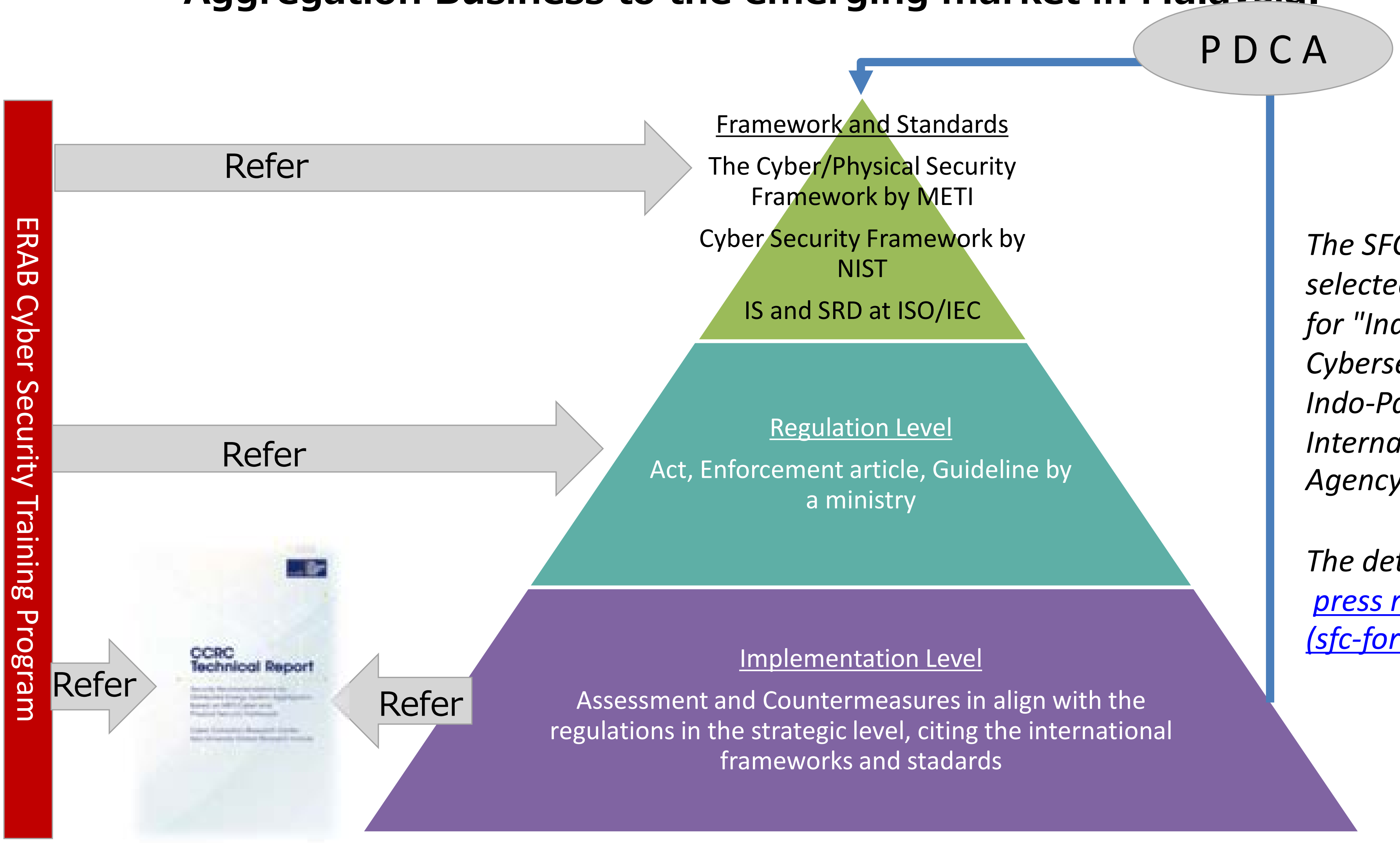
● Experience multiple hazards on a demo system

Common Criteria: ISO/IEC 15408 is the standard to ensure IT product security at a customer premise

- ISO/IEC 15408 as it were Common Criteria (CC) is the standard dealing with product safety.
  - The basis for evaluation of security properties of IT products.
  - Globally recognized certification.
  - Malaysia and Japan have partnered as the Certificate Authorizing Member


Certificate Authorizing Members
Certificate Consuming Members

As per CPSF, Japanese and Malaysian security experts have launched empirical study applying the security triangle of Energy Resource Aggregation Business to the emerging market in Malaysia.



Framework and Standards

The Cyber/Physical Security Framework by METI

Cyber Security Framework by NIST

IS and SRD at ISO/IEC

Regulation Level

Act, Enforcement article, Guideline by a ministry

Implementation Level

Assessment and Countermeasures in align with the regulations in the strategic level, citing the international frameworks and stadards

The SFC Forum has been selected to conduct the survey for "Industrial Control Systems Cybersecurity Training for Indo-Pacific Region" for Japan International Cooperation Agency （JICA）

The details is at:
press release_en＿20230900 (sfc-forum.or.jp)

State of the Art of *Secure Internet of Things (S-IoT):*
The Development of New Cryptographic Key Updating Schemes to Improve the Security of Long-Range Wide Area Network (LoRaWAN) Protocol

Kalamullah Ramli and Nur Hayati

Co-Founder, Indonesia Cyber Awareness and Resilience (id-CARE) Institute

Professor, Electrical Engineering Department

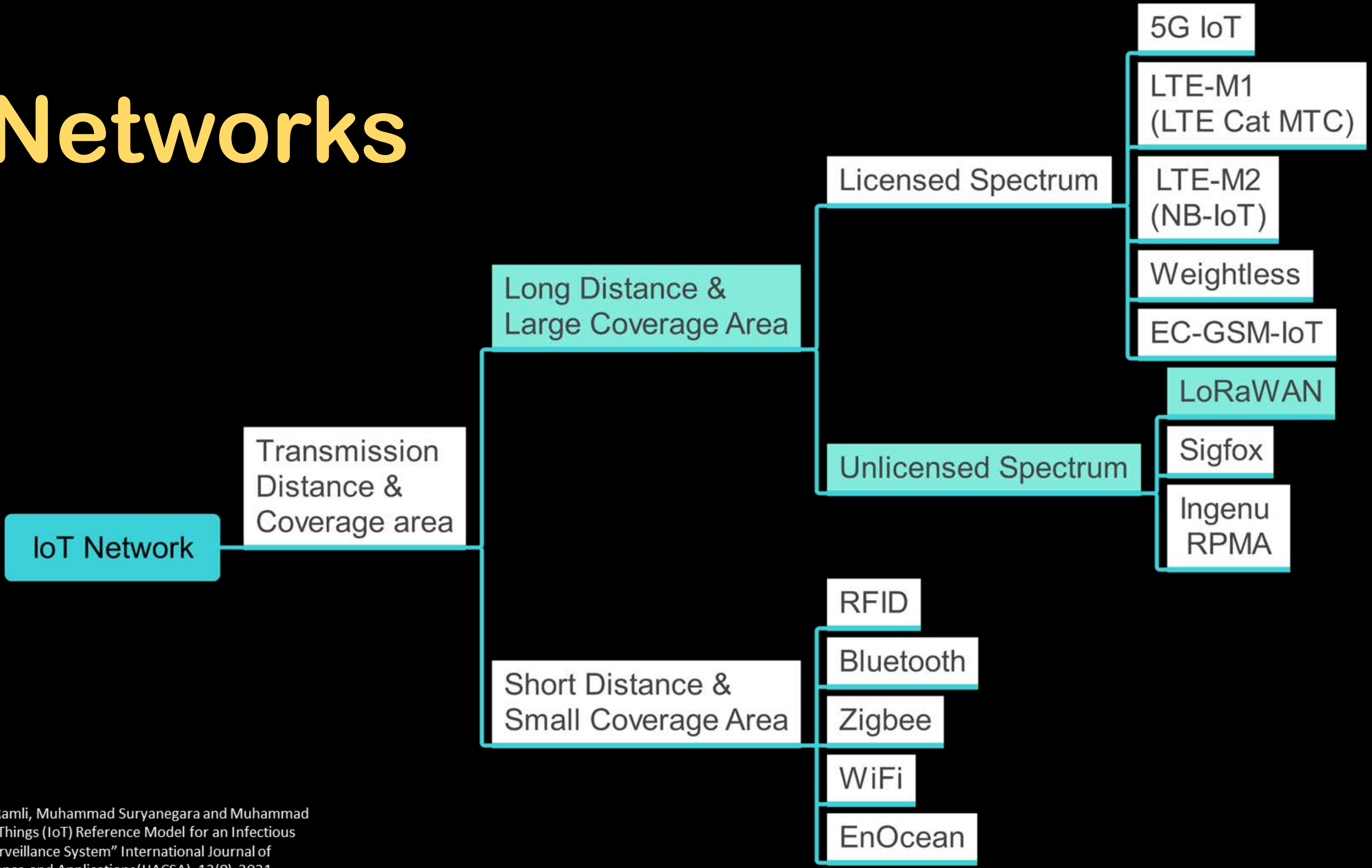
Universitas Indonesia

50th Year of
ASEAN-Japan
Friendship and Cooperation

OUTLINE

- **Introduction:** IoT Use Case and IoT Security Threats
- **LoRaWAN Security**
- **LoRaWan Security Issues**
- **Proposed Solutions:**
  - **Root Key Update Scheme**
  - **Session Key Update Scheme**
- **Conclusions**

IoT Networks



- IoT Network
  - Transmission Distance & Coverage area
    - Long Distance & Large Coverage Area
      - Licensed Spectrum
        - 5G IoT
        - LTE-M1 (LTE Cat MTC)
        - LTE-M2 (NB-IoT)
        - Weightless
        - EC-GSM-IoT
      - Unlicensed Spectrum
        - LoRaWAN
        - Sigfox
        - Ingenu RPMA
    - Short Distance & Small Coverage Area
      - RFID
      - Bluetooth
      - Zigbee
      - WiFi
      - EnOcean

Nur Hayati, Kalamullah Ramli, Muhammad Suryanegara and Muhammad Salman, “An Internet of Things (IoT) Reference Model for an Infectious Disease Active Digital Surveillance System” International Journal of Advanced Computer Science and Applications(IJACSA), 12(9), 2021. http://dx.doi.org/10.14569/IJACSA.2021.0120956

IoT Security Threats

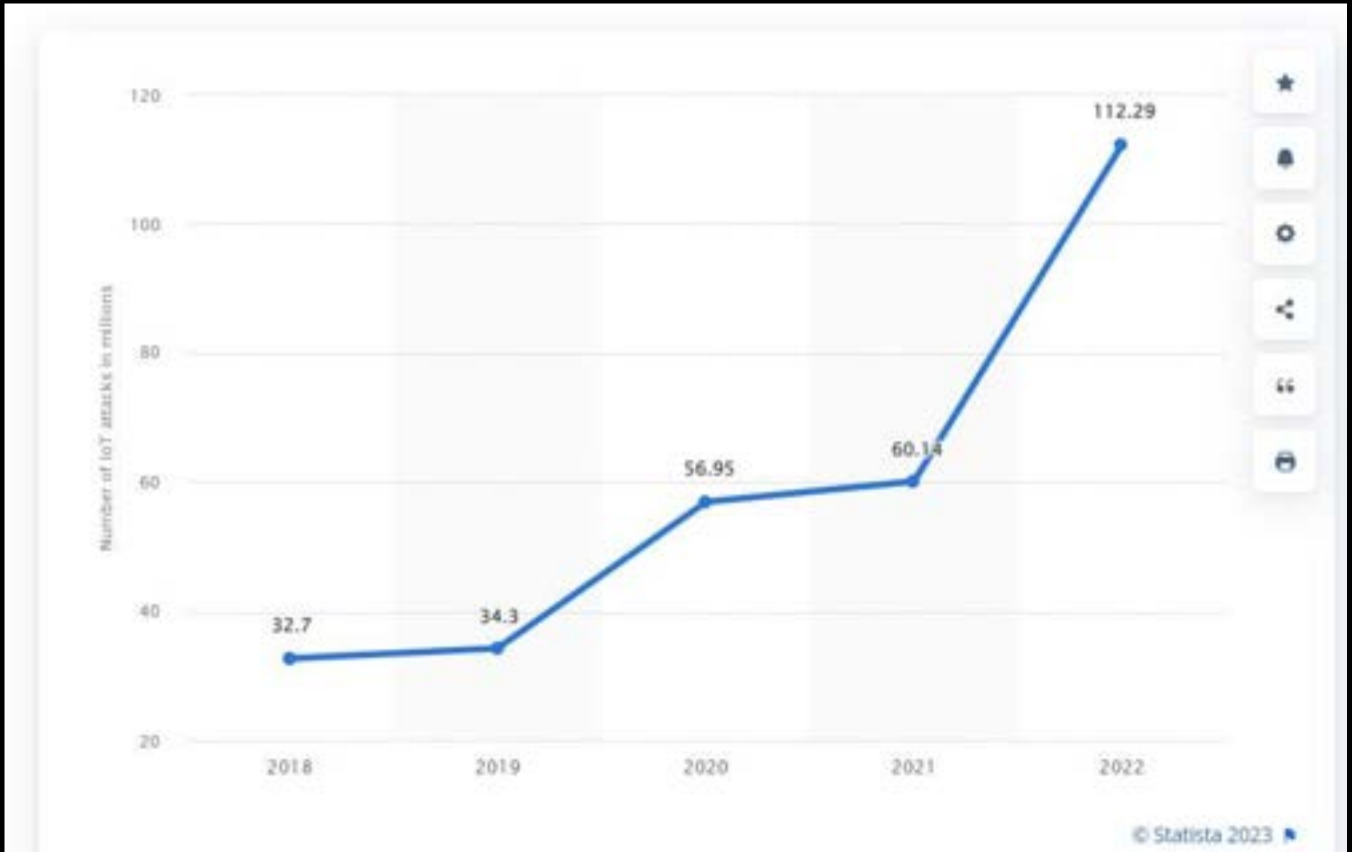
- An IoT attack is a malicious attempt to exploit vulnerabilities in Internet-connected devices such as smart office devices, industrial control system, and critical infrastructure key components
- Attackers may seize control of the device, steal sensitive data, or use the device as a part of a botnet for other malicious purposes
- With limited resources and processing power, IoT devices may lack security features to protect against attacks, making them more vulnerable to attacks than other IT equipment

IoT Security Threat
(in numbers)

The number of Internet of Things (IoT) cyber attacks worldwide amounted to over 112 million in 2022. Over the recent years, this figure has increased significantly from around 32 million detected cases in 2018. In the latest measured year, the year-over-year increase in the number of Internet of Things (IoT) malware incidents was 87 percent

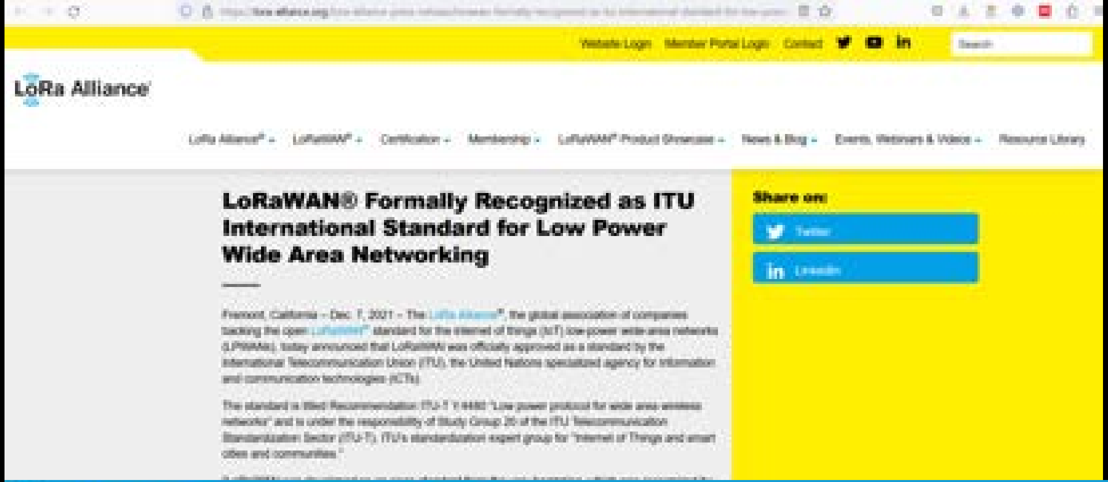
Source: Statista, Feb 2023

https://www.statista.com/statistics/1377569/worldwide-annual-internet-of-things-attacks/



Why LoRaWAN ?

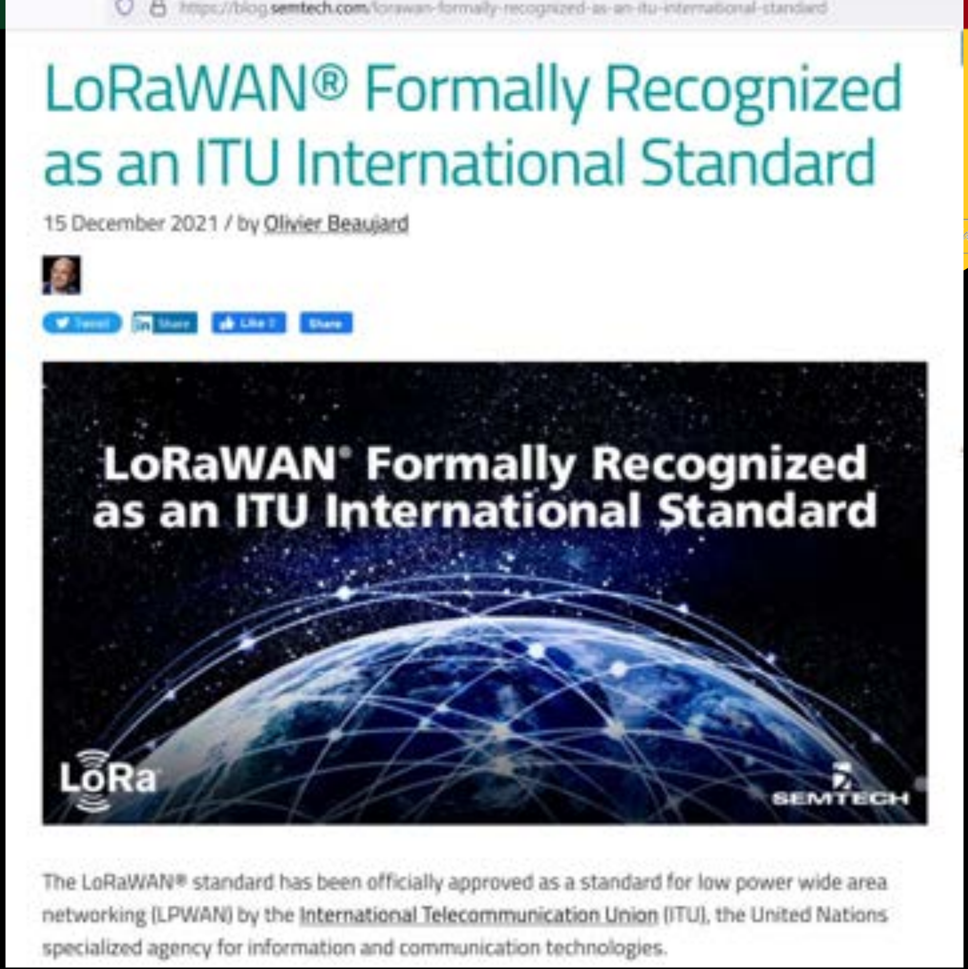
- LoRaWAN become the standard of Internet of Things (IoT) Low Power Wide Area Network (LPWAN) through **ITU-TY.4480 recommendation** (Des, 2021)



LoRaWAN® Formally Recognized as ITU International Standard for Low Power Wide Area Networking

Fremont, California – Dec. 7, 2021 – The LoRa Alliance®, the global association of companies backing the open LoRaWAN® standard for the internet of things (IoT) low-power wide-area networks (LPWANs), today announced that LoRaWAN was officially approved as a standard by the International Telecommunication Union (ITU), the United Nations specialized agency for information and communication technologies (ICTs).

The standard is titled Recommendation ITU-T Y.4480 "Low power protocol for wide area wireless networks" and is under the responsibility of Study Group 20 of the ITU Telecommunication Standardization Sector (ITU-T), ITU's standardization expert group for "Internet of Things and smart cities and communities."

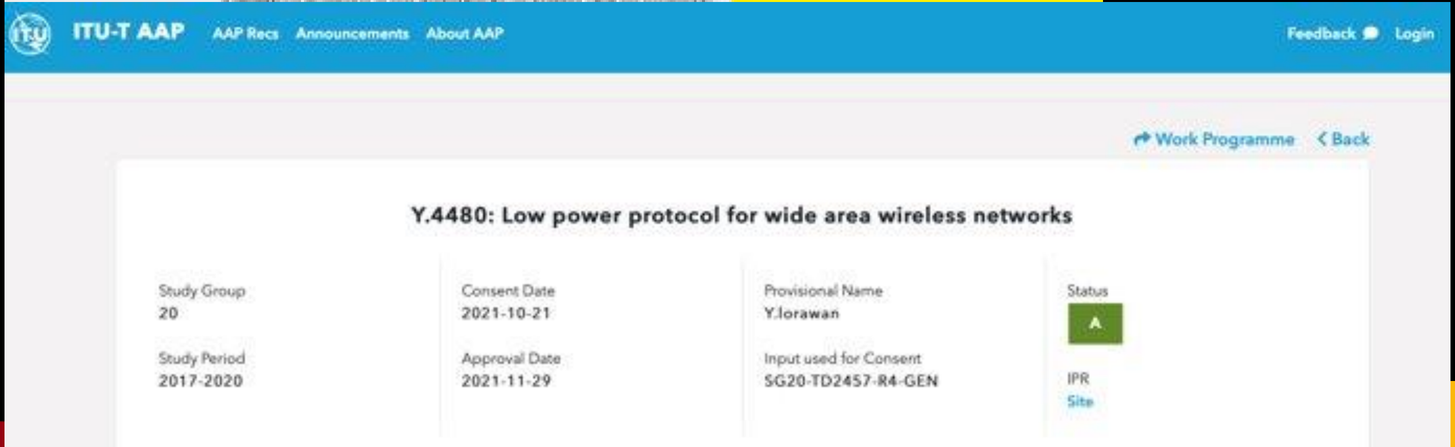


https://blog.semtech.com/lorawan-formally-recognized-as-an-itu-international-standard
Tweet
Share
Like
Share
LoRaWAN® Formally Recognized as an ITU International Standard
LoRa
SEMTECH

LoRaWAN® Formally Recognized as an ITU International Standard

15 December 2021 / by Olivier Beaujard

The LoRaWAN® standard has been officially approved as a standard for low power wide area networking (LPWAN) by the International Telecommunication Union (ITU), the United Nations specialized agency for information and communication technologies.



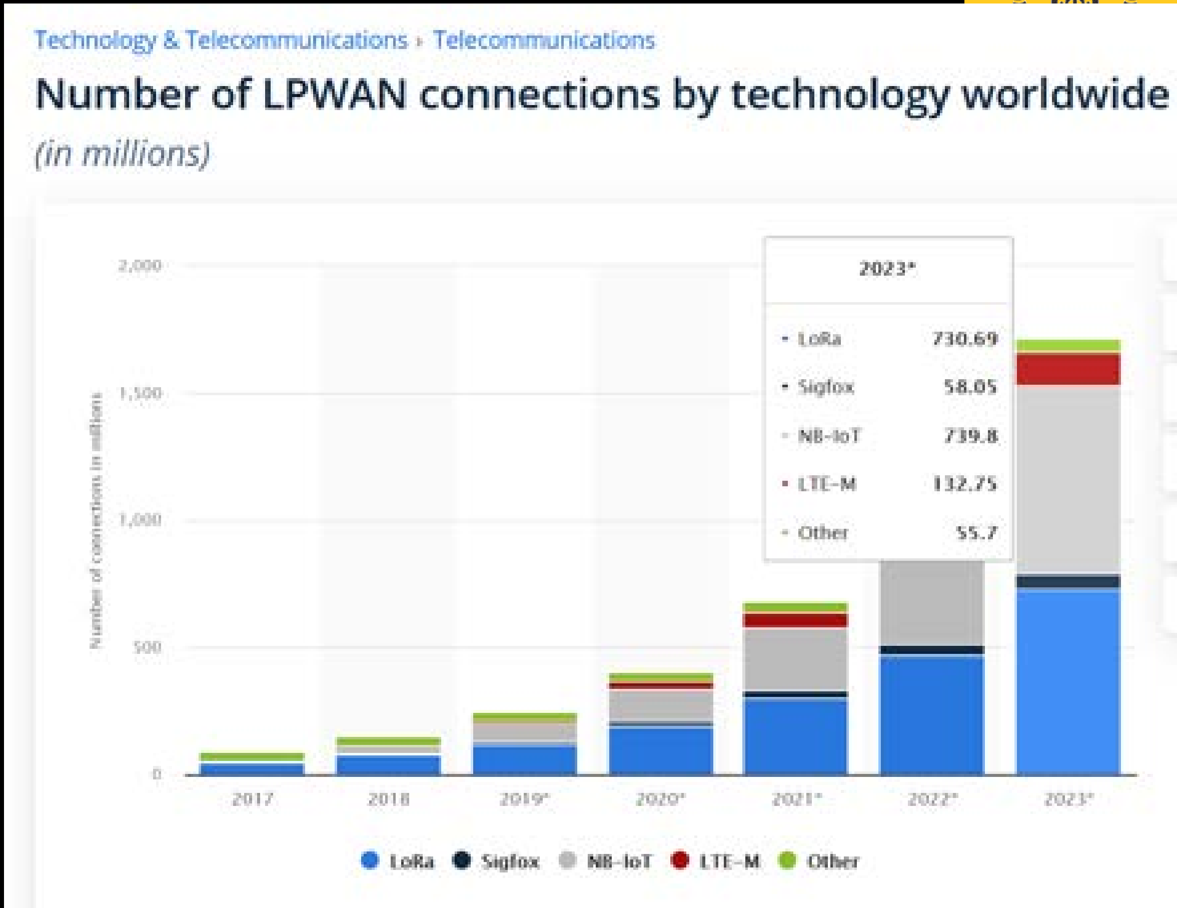
Y.4480: Low power protocol for wide area wireless networks

Study Group 20	Consent Date 2021-10-21	Provisional Name Y.lorawan	Status A
Study Period 2017-2020	Approval Date 2021-11-29	Input used for Consent SG20-TD2457-R4-GEN	IPR Site

- https://www.itu.int/rec/T-REC-Y.4480/en
- https://lora-alliance.org/lora-alliance-press-release/lorawan-formally-recognized-as-itu-international-standard-for-low-power-wide-area-networking/
- https://blog.semtech.com/lorawan-formally-recognized-as-an-itu-international-standard

Why LoRaWAN ?

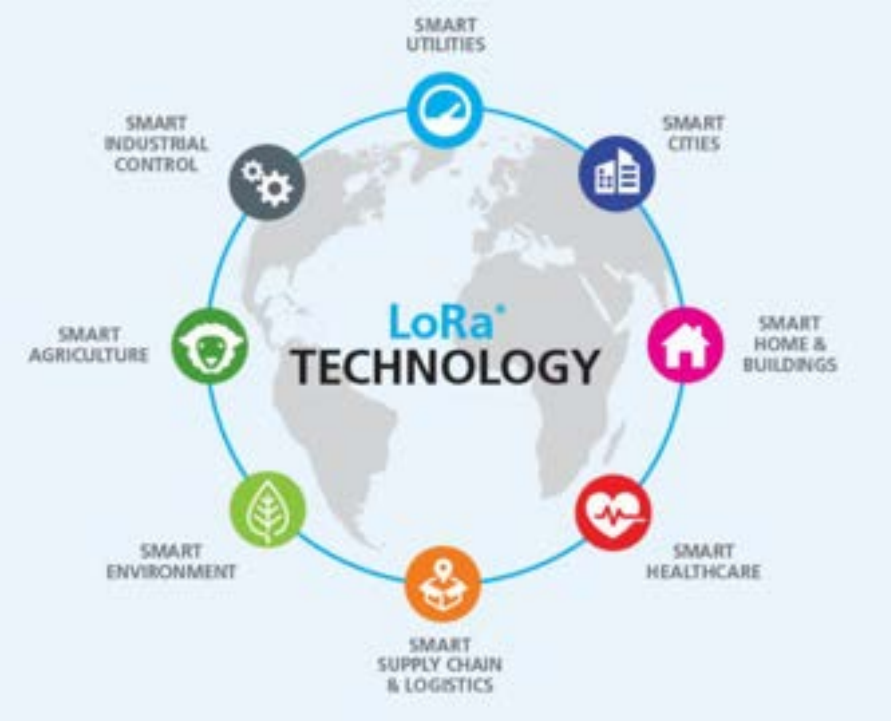
- The Number of IoT Connections in 2023 is 1,716.99 Million. LoRa connections reach ± 42.55% of the total or as many as 730.69 million (Source: Statista, July 2023)
- There are 5.9 million LoRa gateways, 300 million end devices/nodes, and 181 public network operators. LoRa technology has been applied to various sectors (Source: Semtech, August 2023)

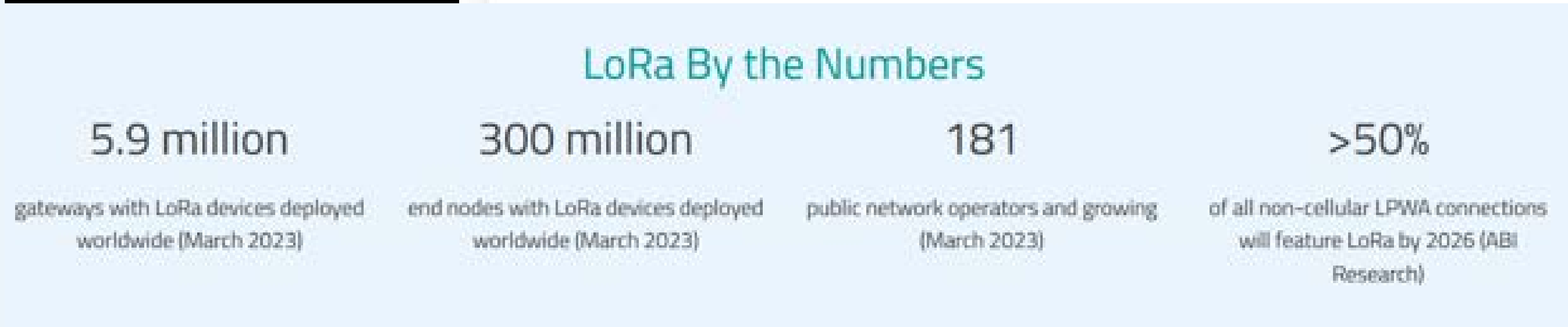

Technology & Telecommunications › Telecommunications

Number of LPWAN connections by technology worldwide

(in millions)

2023*	
LoRa	730.69
Sigfox	58.05
NB-IoT	739.8
LTE-M	132.75
Other	55.7




LoRa By the Numbers

5.9 million

gateways with LoRa devices deployed worldwide (March 2023)

300 million

end nodes with LoRa devices deployed worldwide (March 2023)

181

public network operators and growing (March 2023)

>50%

of all non-cellular LPWA connections will feature LoRa by 2026 (ABI Research)

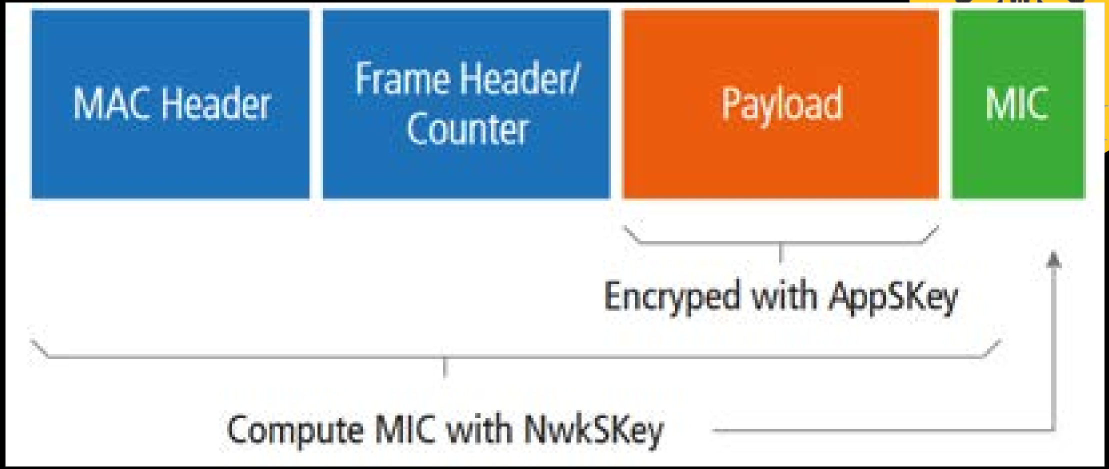
https://www.statista.com/statistics/880822/lpwan-ic-market-share-by-technology/
https://www.semtech.com/lora

LoRaWAN Security

1. **Mutual authentication**
2. **Data Integrity**
3. **Data Confidentiality**

AES
128 bit

LoRaWAN security mechanisms rely on the AES cryptographic algorithms



MIC: Message Integrity Code

- **Mutual authentication** is established between a LoRaWAN end-device and the LoRaWAN network as part of the network join procedure through Over-the-Air-Activation (OTAA). The OTAA Join Procedure proves that both the end device and the network have the knowledge of the **root key**, specifically AppKey.

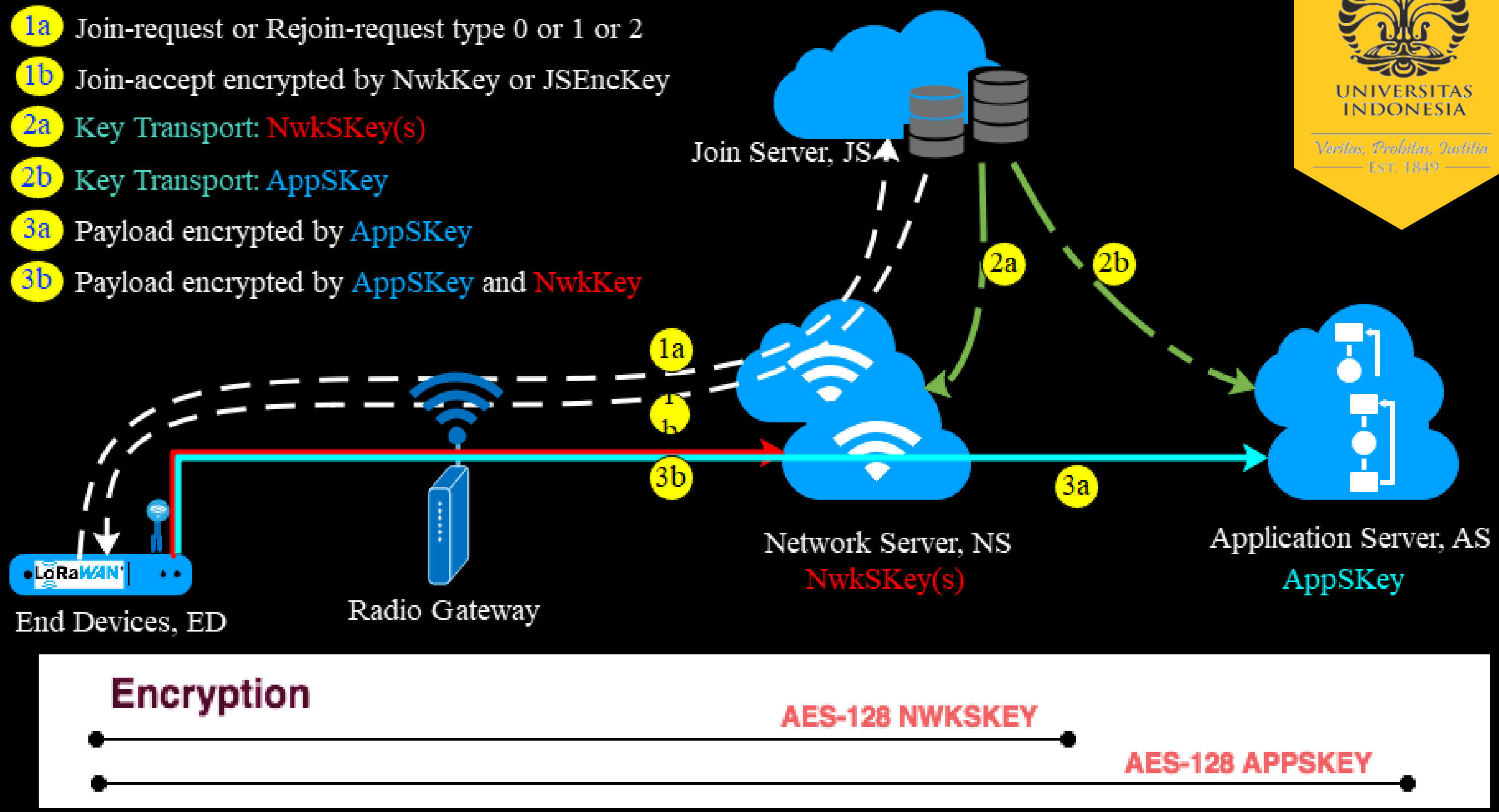
- **Data Integrity and Confidentiality Protection:** All LoRaWAN traffic is protected using the **two session keys**. Each payload is encrypted by AES-CTR and carries a frame counter (to avoid packet replay) and a Message Integrity Code (MIC) computed with AES-CMAC (to avoid packet tampering).

Gemalto, Actility, and Semtech, “"LoRaWAN™ Security A White Paper.” Accessed: Dec. 03, 2021. [Online]. Available: https://lora-alliance.org /sites/lorawan_security_whitepaper.pdf

LoRaWAN Security

- LoRaWAN security uses the AES cryptographic algorithm for integrity protection and encryption.

- Each LoRaWAN device is personalized with a unique 128 bit AES key (**called root key**)
  - Root key LoRaWAN consist of NwkKey & AppKey



1a Join-request or Rejoin-request type 0 or 1 or 2
1b Join-accept encrypted by NwkKey or JSEncKey
2a Key Transport: NwkSKey(s)
2b Key Transport: AppSKey
3a Payload encrypted by AppSKey
3b Payload encrypted by AppSKey and NwkKey

- LoRaWAN **session keys** are then derived, one for providing integrity protection and encryption of the LoRaWAN MAC commands and application payload (the NwkSKey), and one for end-to-end encryption of application payload (the AppSKey).
  - The NwkSKey is distributed to the LoRaWAN network in order to prove/verify the packets authenticity & integrity.
  - The AppSKey is distributed to the application server in order to encrypt/decrypt the application payload.

N. Hayati, K. Ramli, S. Windarta and M. Suryanegara, "A Novel Secure Root Key Updating Scheme for LoRaWANs Based on CTR_AES DRBG 128," in *IEEE Access*, vol. 10, pp. 18807-18819, 2022, doi: 10.1109/ACCESS.2022.3150281.

LoRaWAN Security Issues

Root Key

- Root Key is LoRaWAN Master key
- Root Key is the LoRaWAN principal key used to derive all other cryptographic keys
- **Root Key issues :** The root key value **remains the same** throughout the device's lifespan, implying that its crypto period exceeds the recommended value

Session Key

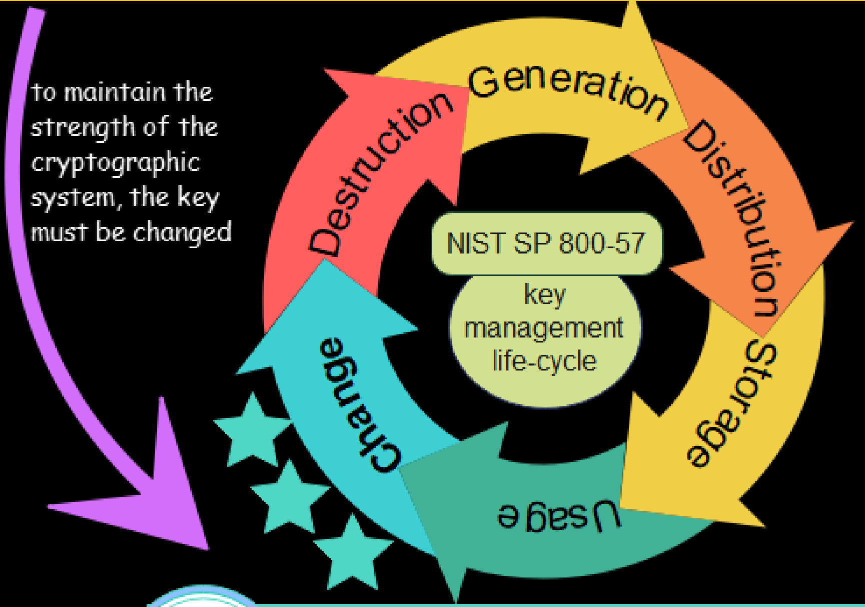
- Session Key is a derivation key used to secure communication and payload transmission.
- **Session Key issue**: LoRaWAN apply the **same session** key to secure **multiple communication sessions** – Key repetition leads to data leakage when it is compromised.

The Problem of LoRaWAN Cryptographic Keys

Root Key: Static
The Value is never change during device's lifespan

Session Keys: Dynamic
Used to Secure ≥ 1x Communication Session

Endanger LoRaWAN Security Protocol: potential for key compromises.



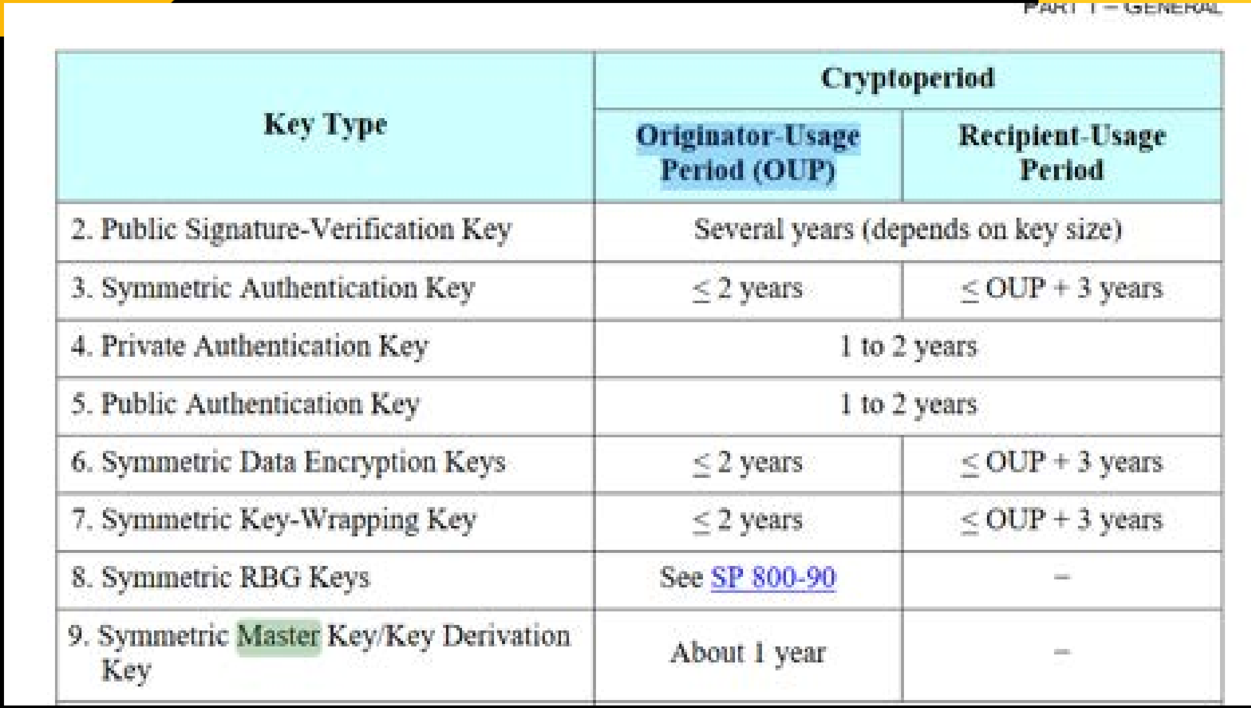
to maintain the strength of the cryptographic system, the key must be changed

Potential Solution:
Key Change/Update

LoRaWAN Security Issues

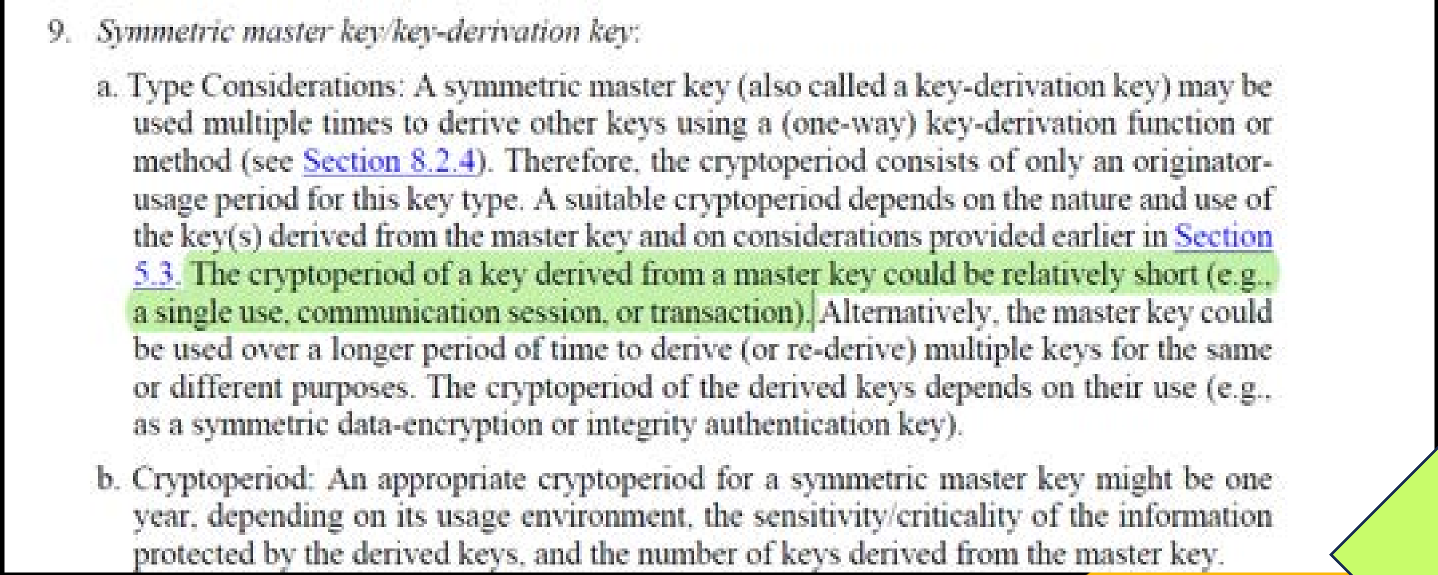
- Cryptoperiod of **Root Key** →It must be changed **at least once** a year (NIST Special Publication 800-57 Part 1 Rev. 5)
- Root Key = LoRaWAN's Master key

NIST SP 800-57



PART 1 – GENERAL

Key Type	Cryptoperiod	
	Originator-Usage Period (OUP)	Recipient-Usage Period
2. Public Signature-Verification Key	Several years (depends on key size)	
3. Symmetric Authentication Key	≤ 2 years	≤ OUP + 3 years
4. Private Authentication Key	1 to 2 years	
5. Public Authentication Key	1 to 2 years	
6. Symmetric Data Encryption Keys	≤ 2 years	≤ OUP + 3 years
7. Symmetric Key-Wrapping Key	≤ 2 years	≤ OUP + 3 years
8. Symmetric RBG Keys	See SP 800-90	–
9. Symmetric Master Key/Key Derivation Key	About 1 year	–



9. *Symmetric master key/key-derivation key:*

a. Type Considerations: A symmetric master key (also called a key-derivation key) may be used multiple times to derive other keys using a (one-way) key-derivation function or method (see Section 8.2.4). Therefore, the cryptoperiod consists of only an originator-usage period for this key type. A suitable cryptoperiod depends on the nature and use of the key(s) derived from the master key and on considerations provided earlier in Section 5.3. The cryptoperiod of a key derived from a master key could be relatively short (e.g., a single use, communication session, or transaction). Alternatively, the master key could be used over a longer period of time to derive (or re-derive) multiple keys for the same or different purposes. The cryptoperiod of the derived keys depends on their use (e.g., as a symmetric data-encryption or integrity authentication key).

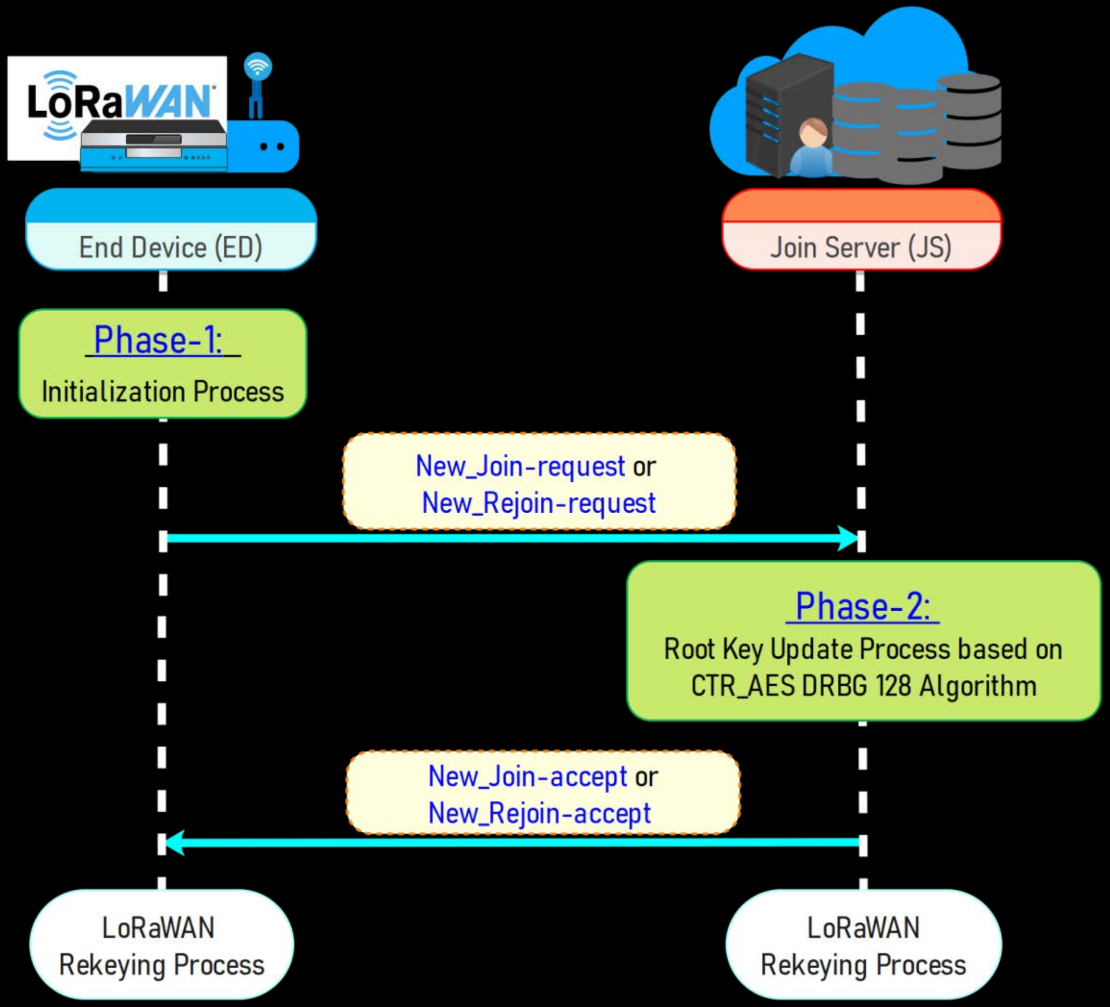
b. Cryptoperiod: An appropriate cryptoperiod for a symmetric master key might be one year, depending on its usage environment, the sensitivity/criticality of the information protected by the derived keys, and the number of keys derived from the master key.

- Cryptoperiod of **Session Key** → NIST recommends that the session key should be applied **only once** in every communication or should be **unique to each session** (NIST Special Publication 800-57 Part 3 Rev. 1)

NIST SP 800-57

A Novel Secure Root Key Updating Scheme Based on CTR_AES DRBG 128

Novel Secure Root Key Updating Scheme for LoRaWANs Based on CTR_AES DRBG 128



Pict 3.1 General Architecture of LoRaWAN's root key update

- The involved Entities
  1. ED
  2. JS

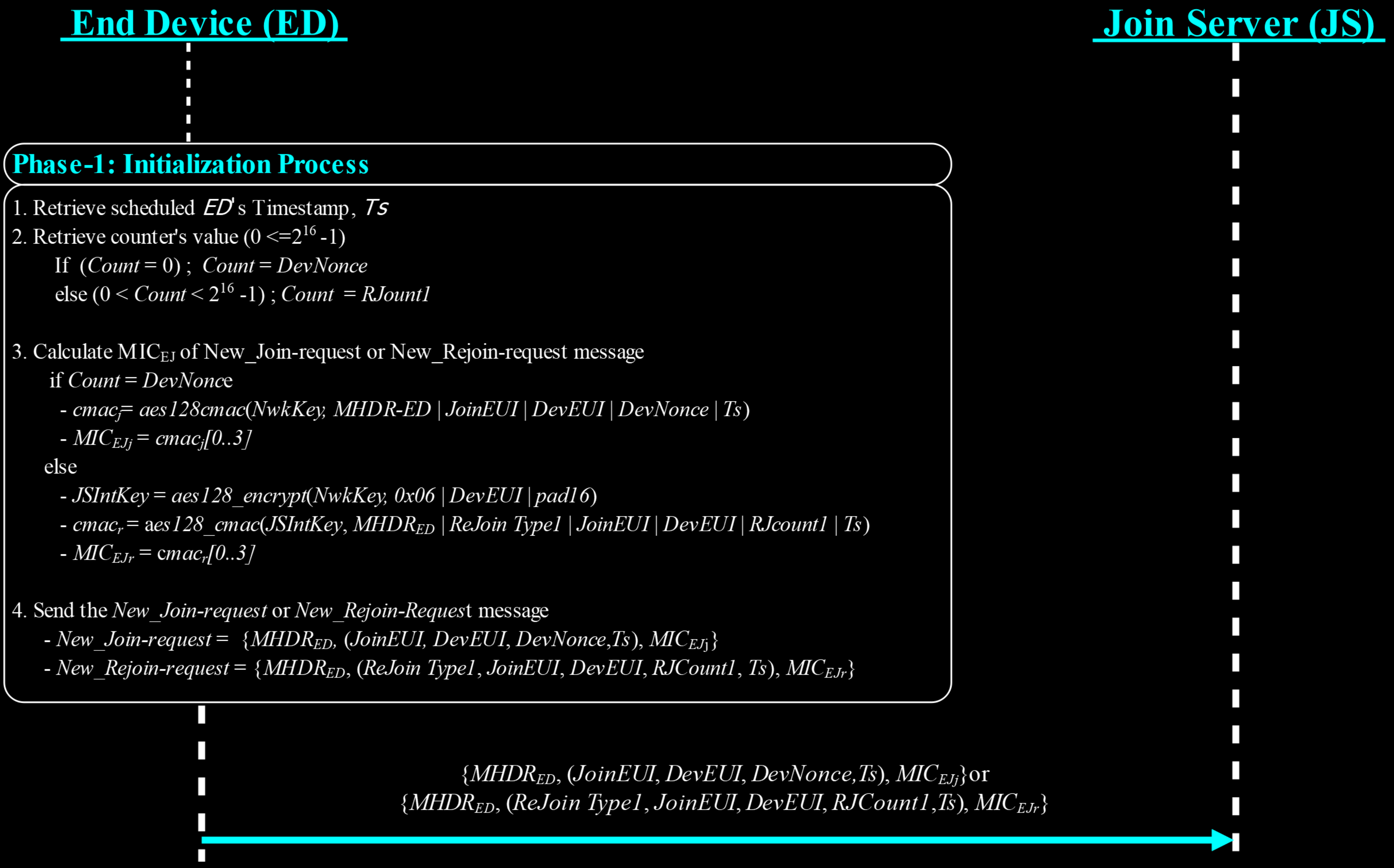
- Scheme
  - ❖ *Time-driven: Periodic Update*

- Phases
  - ❖ Phase-1: Initialization at ED
  - ❖ Phase-2: Root Key update process at JS

- Communication Protocol
  - ❖ *New_Join-request & New_Rejoin-request*
  - ❖ *New_Join-accept & New_Rejoin-accept*

- Root Key Update Algorithm
  - ❖ CTR_AES DRBG 128 bit
  - ❖ *Input: Key + Counter* generated by RBG module complied to FIPS 140 standard
  - ❖ *Output: New Root Key*

Phase 1: Initialization Process of *Root key Update*



End Device (ED)

Join Server (JS)

Phase-1: Initialization Process

```
1. Retrieve scheduled ED's Timestamp, Ts
2. Retrieve counter's value ($0 <= 2^{16} - 1$)
      If ($Count = 0$) ; $Count = DevNonce$
      else ($0 < Count < 2^{16} - 1$) ; $Count = RJount1$

3. Calculate $MIC_{EJ}$ of New_Join-request or New_Rejoin-request message
      if $Count = DevNonce$
        - $cmac_j = aes128cmac(NwkKey, MHDR\text{-}ED \mid JoinEUI \mid DevEUI \mid DevNonce \mid Ts)$
        - $MIC_{EJj} = cmac_j[0..3]$
      else
        - $JSIntKey = aes128\_encrypt(NwkKey, 0x06 \mid DevEUI \mid pad16)$
        - $cmac_r = aes128\_cmac(JSIntKey, MHDR_{ED} \mid ReJoin\ Type1 \mid JoinEUI \mid DevEUI \mid RJcount1 \mid Ts)$
        - $MIC_{EJr} = cmac_r[0..3]$

4. Send the New_Join-request or New_Rejoin-Request message
      - $New\_Join\text{-}request = \{MHDR_{ED}, (JoinEUI, DevEUI, DevNonce, Ts), MIC_{EJj}\}$
      - $New\_Rejoin\text{-}request = \{MHDR_{ED}, (ReJoin\ Type1, JoinEUI, DevEUI, RJCount1, Ts), MIC_{EJr}\}$
```

$\{MHDR_{ED}, (JoinEUI, DevEUI, DevNonce, Ts), MIC_{EJj}\}$ or

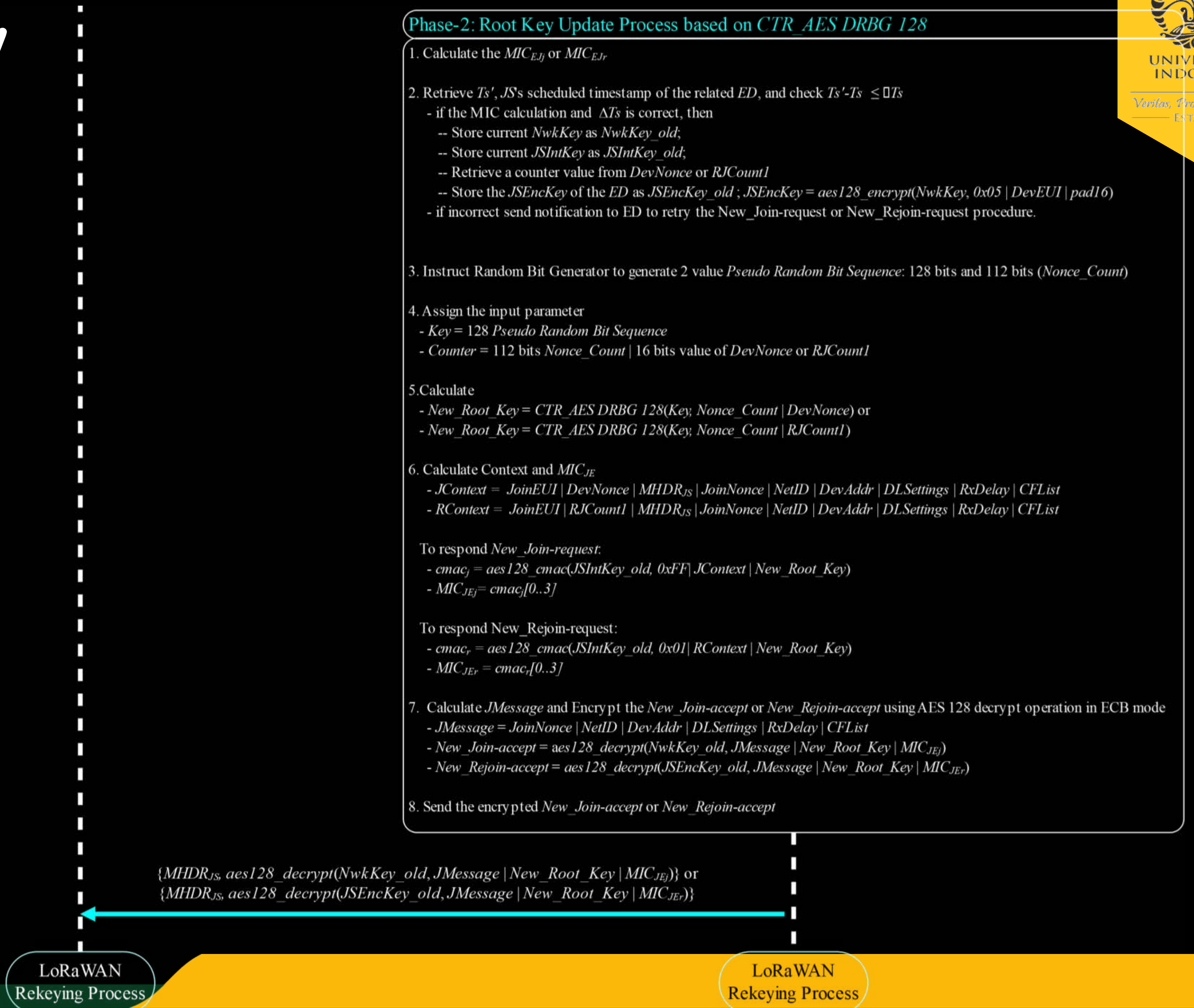
$\{MHDR_{ED}, (ReJoin\ Type1, JoinEUI, DevEUI, RJCount1, Ts), MIC_{EJr}\}$

Phase 2: Root key Update Process

- *New_Root_Key=CTR_AES DRBG_128bits (Key, Nonce_Count|DevNonce)*

<u>or</u>

- *New_Root_Key=CTR_AES DRBG_128bits(Key, Nonce_Count|RJCount1)*



Phase-2: Root Key Update Process based on *CTR_AES DRBG 128*

1. Calculate the MIC_{EJj} or MIC_{EJr}

2. Retrieve *Ts'*, *JS*'s scheduled timestamp of the related *ED*, and check *Ts'-Ts* ≤ □*Ts*
   - if the MIC calculation and Δ*Ts* is correct, then
     -- Store current *NwkKey* as *NwkKey_old*;
     -- Store current *JSIntKey* as *JSIntKey_old*;
     -- Retrieve a counter value from *DevNonce* or *RJCount1*
     -- Store the *JSEncKey* of the *ED* as *JSEncKey_old* ; *JSEncKey = aes128_encrypt(NwkKey, 0x05 | DevEUI | pad16)*
   - if incorrect send notification to ED to retry the New_Join-request or New_Rejoin-request procedure.

3. Instruct Random Bit Generator to generate 2 value *Pseudo Random Bit Sequence*: 128 bits and 112 bits (*Nonce_Count*)

4. Assign the input parameter
   - *Key* = 128 *Pseudo Random Bit Sequence*
   - *Counter* = 112 bits *Nonce_Count* | 16 bits value of *DevNonce* or *RJCount1*

5.Calculate
   - *New_Root_Key = CTR_AES DRBG 128(Key, Nonce_Count | DevNonce)* or
   - *New_Root_Key = CTR_AES DRBG 128(Key, Nonce_Count | RJCount1)*

6. Calculate Context and MIC_{JE}
   - *JContext = JoinEUI | DevNonce |* $MHDR_{JS}$ *| JoinNonce | NetID | DevAddr | DLSettings | RxDelay | CFList*
   - *RContext = JoinEUI | RJCount1 |* $MHDR_{JS}$ *| JoinNonce | NetID | DevAddr | DLSettings | RxDelay | CFList*

   To respond *New_Join-request*:
   - $cmac_j$ *= aes128_cmac(JSIntKey_old, 0xFF| JContext | New_Root_Key)*
   - MIC_{JEj}*= $cmac_j$[0..3]*

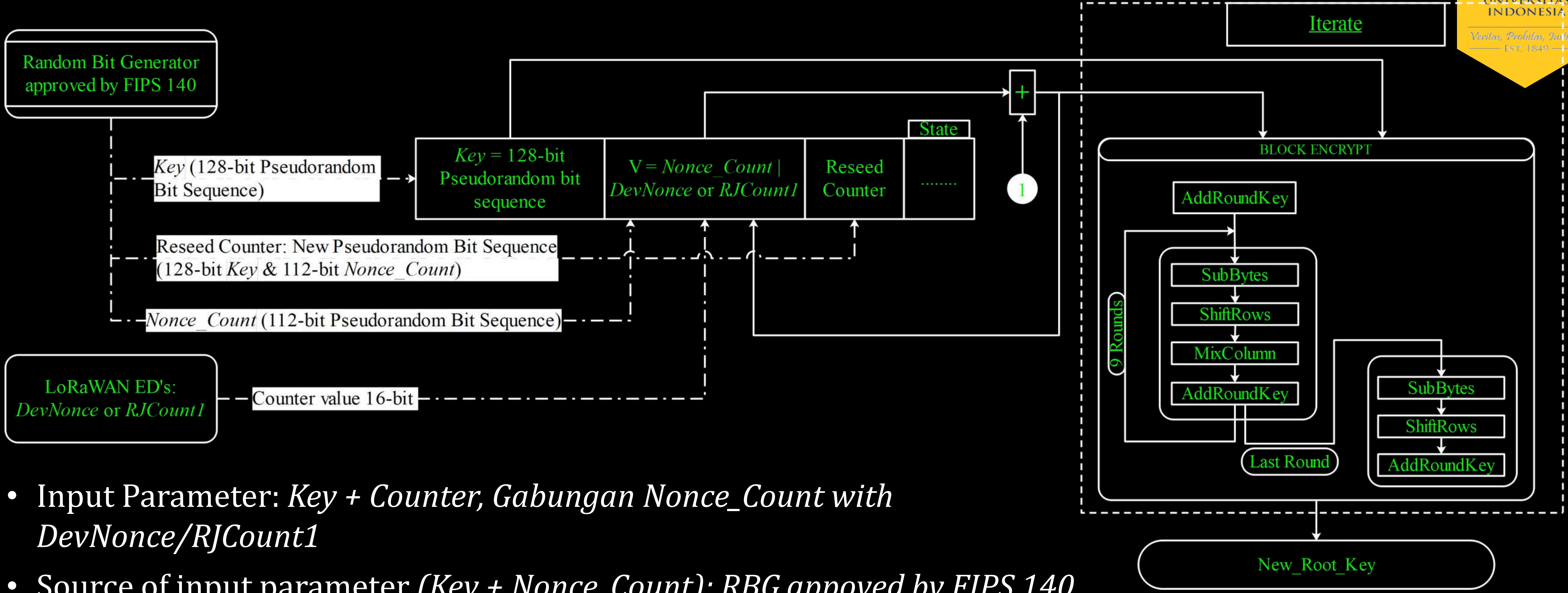
   To respond New_Rejoin-request:
   - $cmac_r$ *= aes128_cmac(JSIntKey_old, 0x01| RContext | New_Root_Key)*
   - MIC_{JEr} *=* $cmac_r$*[0..3]*

7. Calculate *JMessage* and Encrypt the *New_Join-accept* or *New_Rejoin-accept* using AES 128 decrypt operation in ECB mode
   - *JMessage = JoinNonce | NetID | DevAddr | DLSettings | RxDelay | CFList*
   - *New_Join-accept* = aes128_*decrypt(NwkKey_old, JMessage | New_Root_Key |* MIC_{JEj}*)*
   - *New_Rejoin-accept = aes128_decrypt(JSEncKey_old, JMessage | New_Root_Key |* MIC_{JEr}*)*

8. Send the encrypted *New_Join-accept* or *New_Rejoin-accept*

{$MHDR_{JS}$, *aes128_decrypt(NwkKey_old, JMessage | New_Root_Key |* MIC_{JEj}*)*} or
{$MHDR_{JS}$, *aes128_decrypt(JSEncKey_old, JMessage | New_Root_Key |* MIC_{JEr}*)*}

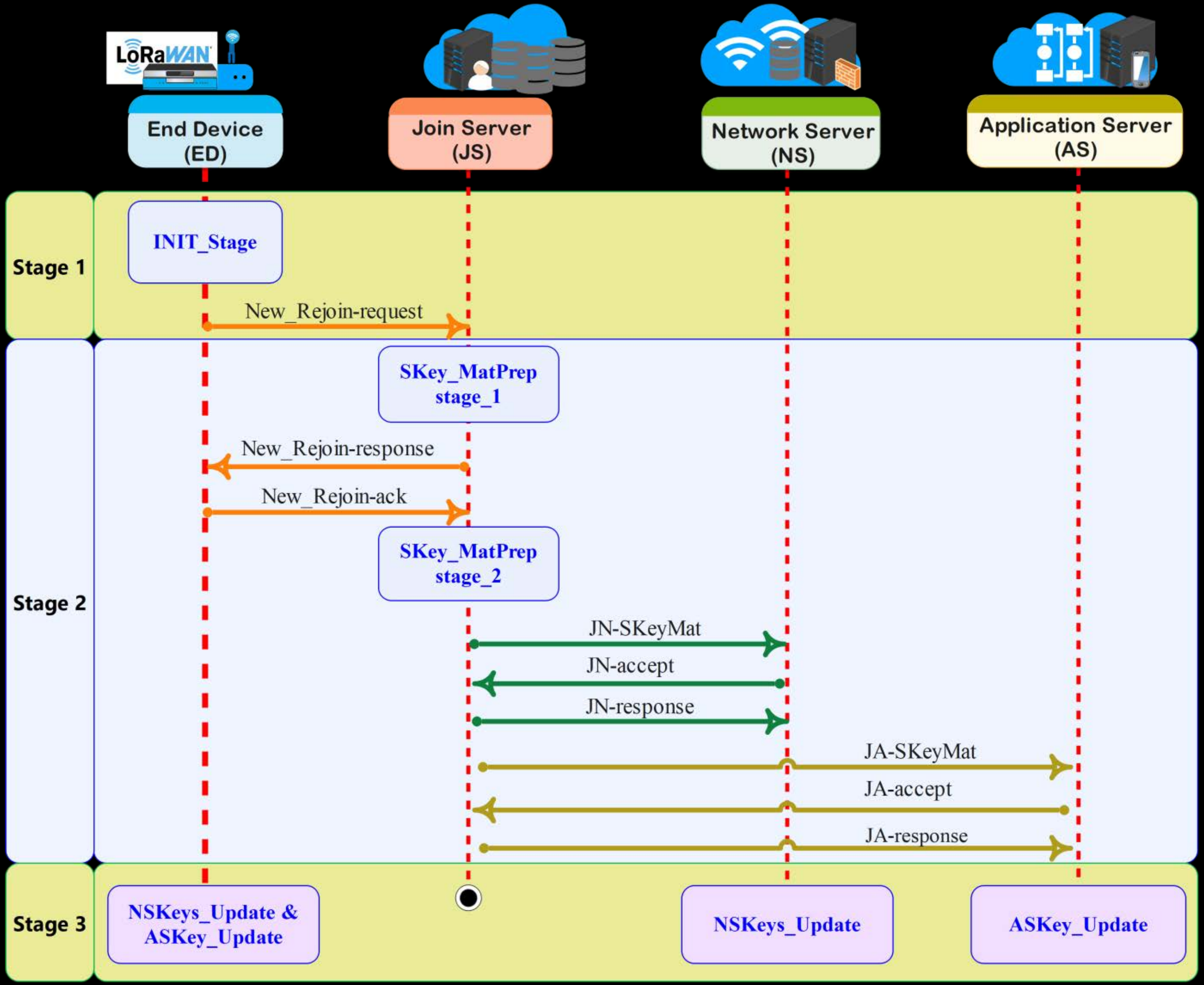
Algorithm Design of The CTR_AES DRBG 128-bits


Iterate
Random Bit Generator approved by FIPS 140
Key (128-bit Pseudorandom Bit Sequence)
State
Key = 128-bit Pseudorandom bit sequence
V = Nonce_Count | DevNonce or RJCount1
Reseed Counter
....
+
1
Reseed Counter: New Pseudorandom Bit Sequence (128-bit Key & 112-bit Nonce_Count)
Nonce_Count (112-bit Pseudorandom Bit Sequence)
LoRaWAN ED's: DevNonce or RJCount1
Counter value 16-bit
BLOCK ENCRYPT
AddRoundKey
9 Rounds
SubBytes
ShiftRows
MixColumn
AddRoundKey
Last Round
SubBytes
ShiftRows
AddRoundKey
New_Root_Key

- Input Parameter: *Key + Counter, Gabungan Nonce_Count with DevNonce/RJCount1*
- Source of input parameter *(Key + Nonce_Count): RBG appoved by FIPS 140*
- Reseed counter dijalankan setiap 2^16 – 1
- *Internal state (block encrypt) : CTR_AES 128-bits*
- *Algorithm output*: *New_Root_Key*

A Novel Session Key Update Scheme Based on Truncated Photon-256

General Architecture: Session Key Update Scheme based on Truncated Photon-256



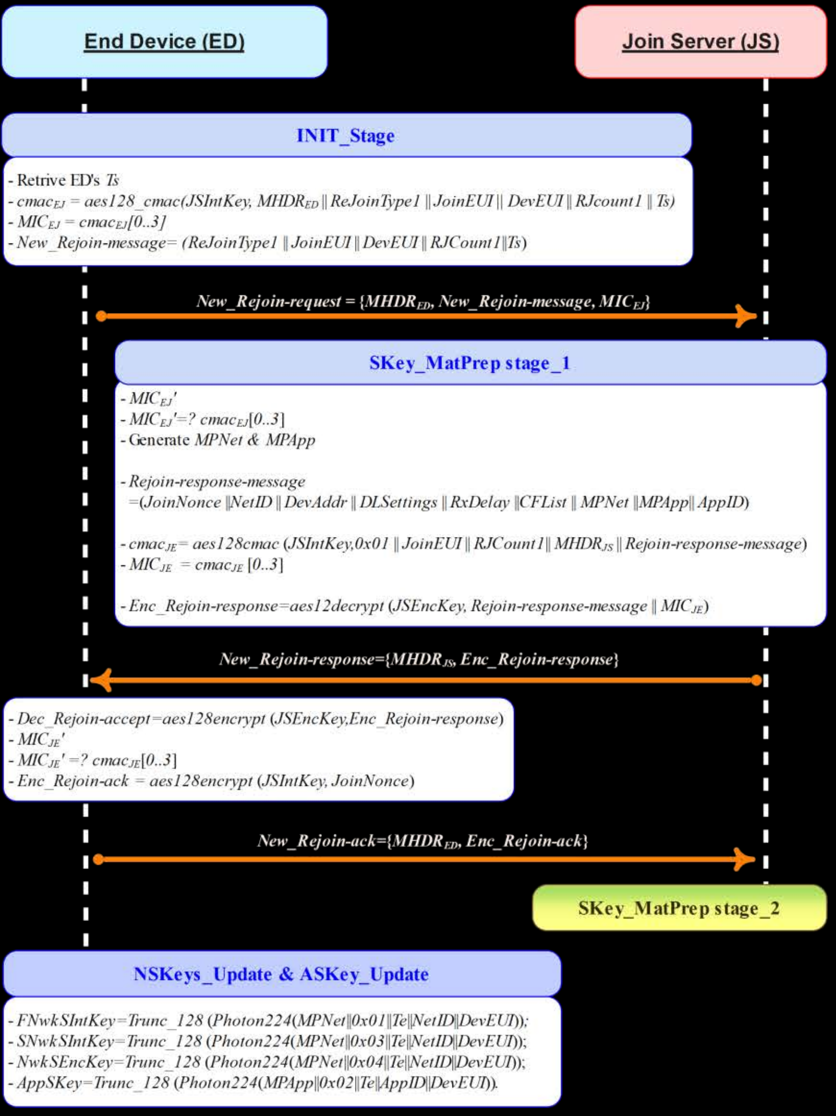
- Proposed Approach
  - ❖ *Time-driven: Periodic Update*
- Entities involved in the scheme:
  - ❖ End Device (ED), Join Server (JS), Network Server (NS), Application Server (AS)
- The scheme consists of three stages

1. *INIT_Stage* occurs at ED
2. *SKey_MatPrep* occurs at JS
3. *NSKey_Update & AS_KeyUpdate* occur at ED, NS, AS

- Communication Protocol between ED-JS
  - ❖ *New_Rejoin-request*
  - ❖ *New_ReJoin-response*
  - ❖ *New_Rejoin-ack*
- Communication Protocol between JS-NS & JS-AS
  - ❖ *JN-SKeyMat & JA-SKeyMat*
  - ❖ *JN-accept & JA-accept*
  - ❖ *JN-response & JA-response*

Communication Session between ED-JS, JS-NS & JS-AS

Section 2.2



INIT_Stage

- Retrive ED's *Ts*
- $cmac_{EJ}$ = *aes128_cmac(JSIntKey,* $MHDR_{ED}$ *‖ ReJoinType1 ‖ JoinEUI ‖ DevEUI ‖ RJcount1 ‖ Ts)*
- MIC_{EJ} = $cmac_{EJ}$*[0..3]*
- *New_Rejoin-message= (ReJoinType1 ‖ JoinEUI ‖ DevEUI ‖ RJCount1‖Ts)*

New_Rejoin-request = {$MHDR_{ED}$, *New_Rejoin-message,* MIC_{EJ}}

SKey_MatPrep stage_1

- MIC_{EJ}'
- MIC_{EJ}'=? $cmac_{EJ}$[0..3]
- Generate *MPNet & MPApp*

- *Rejoin-response-message*
  =(JoinNonce ‖NetID ‖ DevAddr ‖ DLSettings ‖ RxDelay ‖CFList ‖ MPNet ‖MPApp‖ AppID)

- $cmac_{JE}$= *aes128cmac (JSIntKey,0x01 ‖ JoinEUI ‖ RJCount1‖* $MHDR_{JS}$ *‖ Rejoin-response-message)*
- MIC_{JE} = $cmac_{JE}$ [0..3]

- *Enc_Rejoin-response=aes12decrypt (JSEncKey, Rejoin-response-message ‖* MIC_{JE})

New_Rejoin-response={$MHDR_{JS}$, *Enc_Rejoin-response*}

- *Dec_Rejoin-accept=aes128encrypt (JSEncKey,Enc_Rejoin-response)*
- MIC_{JE}'
- MIC_{JE}' =? $cmac_{JE}$[0..3]
- *Enc_Rejoin-ack = aes128encrypt (JSIntKey, JoinNonce)*

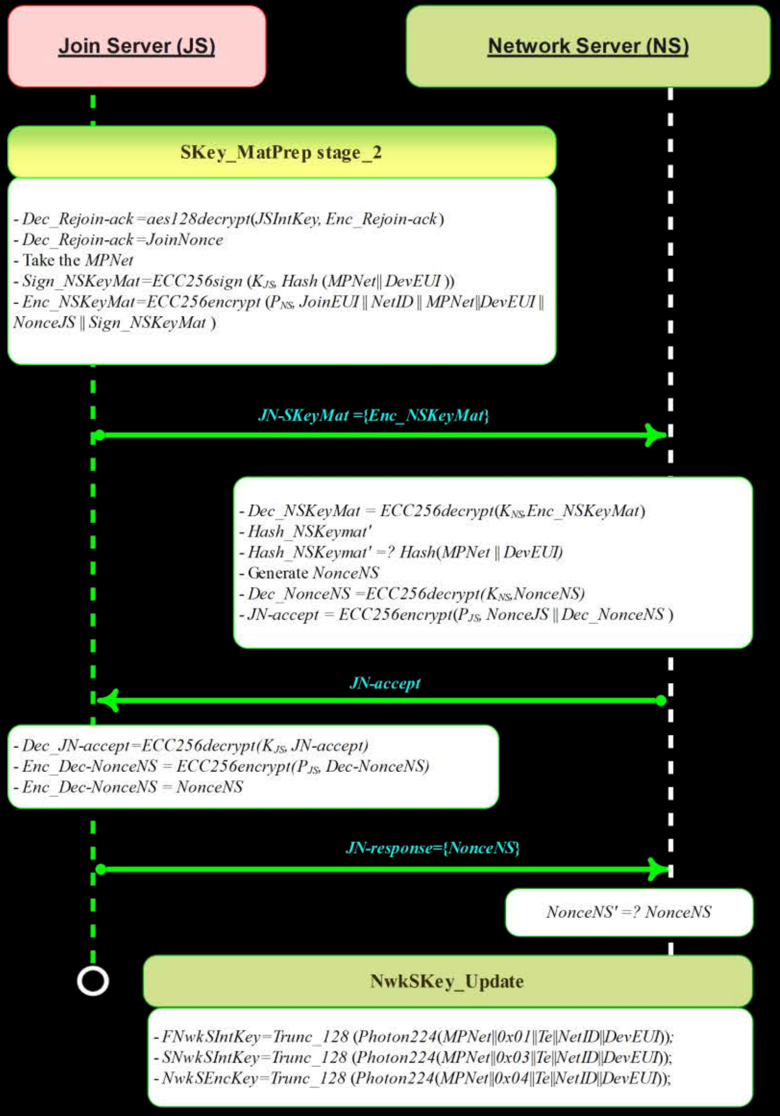
New_Rejoin-ack={$MHDR_{ED}$, *Enc_Rejoin-ack*}

SKey_MatPrep stage_2

NSKeys_Update & ASKey_Update

- *FNwkSIntKey=Trunc_128 (Photon224(MPNet‖0x01‖Te‖NetID‖DevEUI));*
- *SNwkSIntKey=Trunc_128 (Photon224(MPNet‖0x03‖Te‖NetID‖DevEUI));*
- *NwkSEncKey=Trunc_128 (Photon224(MPNet‖0x04‖Te‖NetID‖DevEUI));*
- *AppSKey=Trunc_128 (Photon224(MPApp‖0x02‖Te‖AppID‖DevEUI)).*

Between ED-JS



SKey_MatPrep stage_2

- *Dec_Rejoin-ack=aes128decrypt(JSIntKey, Enc_Rejoin-ack)*
- *Dec_Rejoin-ack=JoinNonce*
- Take the *MPNet*
- *Sign_NSKeyMat=ECC256sign (*K_{JS}, *Hash (MPNet‖ DevEUI))*
- *Enc_NSKeyMat=ECC256encrypt (*P_{NS}, *JoinEUI ‖ NetID ‖ MPNet‖DevEUI ‖ NonceJS ‖ Sign_NSKeyMat)*

JN-SKeyMat ={Enc_NSKeyMat}

- *Dec_NSKeyMat = ECC256decrypt(*K_{NS},*Enc_NSKeyMat)*
- *Hash_NSKeymat'*
- *Hash_NSKeymat' =? Hash(MPNet ‖ DevEUI)*
- Generate *NonceNS*
- *Dec_NonceNS =ECC256decrypt(*K_{NS},*NonceNS)*
- *JN-accept = ECC256encrypt(*P_{JS}, *NonceJS ‖ Dec_NonceNS)*

JN-accept

- *Dec_JN-accept=ECC256decrypt(*K_{JS}, *JN-accept)*
- *Enc_Dec-NonceNS = ECC256encrypt(*P_{JS}, *Dec-NonceNS)*
- *Enc_Dec-NonceNS = NonceNS*

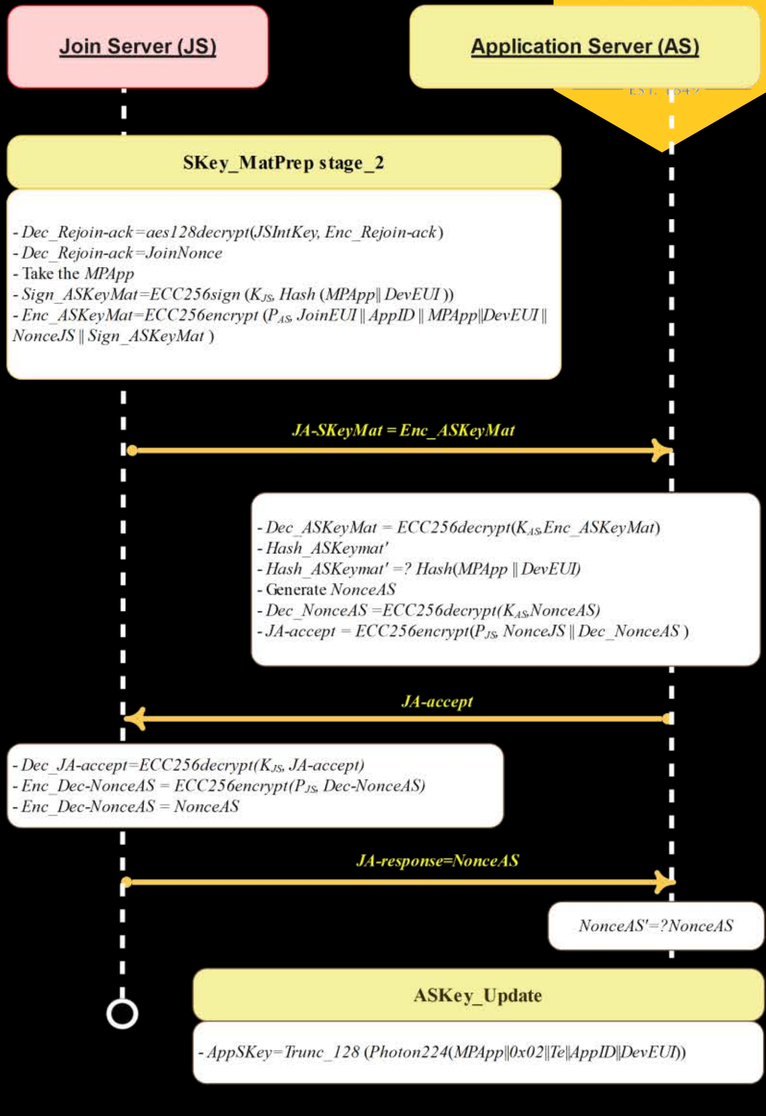
JN-response={NonceNS}

NonceNS' =? NonceNS

NwkSKey_Update

- *FNwkSIntKey=Trunc_128 (Photon224(MPNet‖0x01‖Te‖NetID‖DevEUI));*
- *SNwkSIntKey=Trunc_128 (Photon224(MPNet‖0x03‖Te‖NetID‖DevEUI));*
- *NwkSEncKey=Trunc_128 (Photon224(MPNet‖0x04‖Te‖NetID‖DevEUI));*

Between JS-NS



SKey_MatPrep stage_2

- *Dec_Rejoin-ack=aes128decrypt(JSIntKey, Enc_Rejoin-ack)*
- *Dec_Rejoin-ack=JoinNonce*
- Take the *MPApp*
- *Sign_ASKeyMat=ECC256sign (*K_{JS}, *Hash (MPApp‖ DevEUI))*
- *Enc_ASKeyMat=ECC256encrypt (*P_{AS}, *JoinEUI ‖ AppID ‖ MPApp‖DevEUI ‖ NonceJS ‖ Sign_ASKeyMat)*

JA-SKeyMat = Enc_ASKeyMat

- *Dec_ASKeyMat = ECC256decrypt(*K_{AS},*Enc_ASKeyMat)*
- *Hash_ASKeymat'*
- *Hash_ASKeymat' =? Hash(MPApp ‖ DevEUI)*
- Generate *NonceAS*
- *Dec_NonceAS =ECC256decrypt(*K_{AS},*NonceAS)*
- *JA-accept = ECC256encrypt(*P_{JS}, *NonceJS ‖ Dec_NonceAS)*

JA-accept

- *Dec_JA-accept=ECC256decrypt(*K_{JS}, *JA-accept)*
- *Enc_Dec-NonceAS = ECC256encrypt(*P_{JS}, *Dec-NonceAS)*
- *Enc_Dec-NonceAS = NonceAS*

JA-response=NonceAS

NonceAS'=?NonceAS

ASKey_Update

- *AppSKey=Trunc_128 (Photon224(MPApp‖0x02‖Te‖AppID‖DevEUI))*

Between JS-AS

Truncated Photon-256 Algorithm of NSKey_Update & ASKey_Update

➢NSKey_Update

- *FNwkSIntKey=Trunc_128 (Photon-256 (MPNet||0x01||Te||NetID||DevEUI));*
- *SNwkSIntKey=Trunc_128 (Photon- 256 (MPNet||0x03||Te||NetID||DevEUI));*
- *NwkSEncKey=Trunc_128 (Photon-256 (MPNet||0x04||Te||NetID||DevEUI));*

➢ASKey_Update

- *AppSKey=Trunc_128 (Photon- 256 (MPApp||0x02||Te||AppID||DevEUI)).*

Research overview and Conclusions

UNIVERSITAS INDONESIA

Veritas, Probitas, Iustitia

EST. 1849

Problem Statements

Section 1

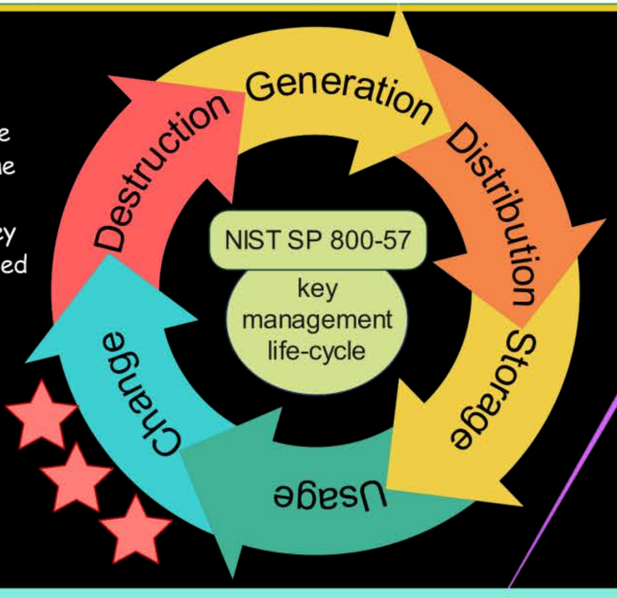
Manajemen kunci kriptografi LoRaWAN

Root Key: Static
The Value is never change during device's lifespan

Session Keys: Dynamic
Used to Secure ≥ 1x Communication Session

Endanger LoRaWAN Security Protocol: potential for key compromises.

to maintain the strength of the cryptographic system, the key must be changed



Potential Solution: Key Update

Proposed Solutions

Section 2.1

A Novel Secure Root Key Updating Scheme Based on CTR_AES DRBG 128

Section 5

Change the Root Key from Static to Dynamic

Section 2.2

A Novel Session Key Update Scheme Based on Truncated Photon-256

Section 5

Change Session Key from used ≥ 1x session to unique key for each communication session.

Result & Discussion

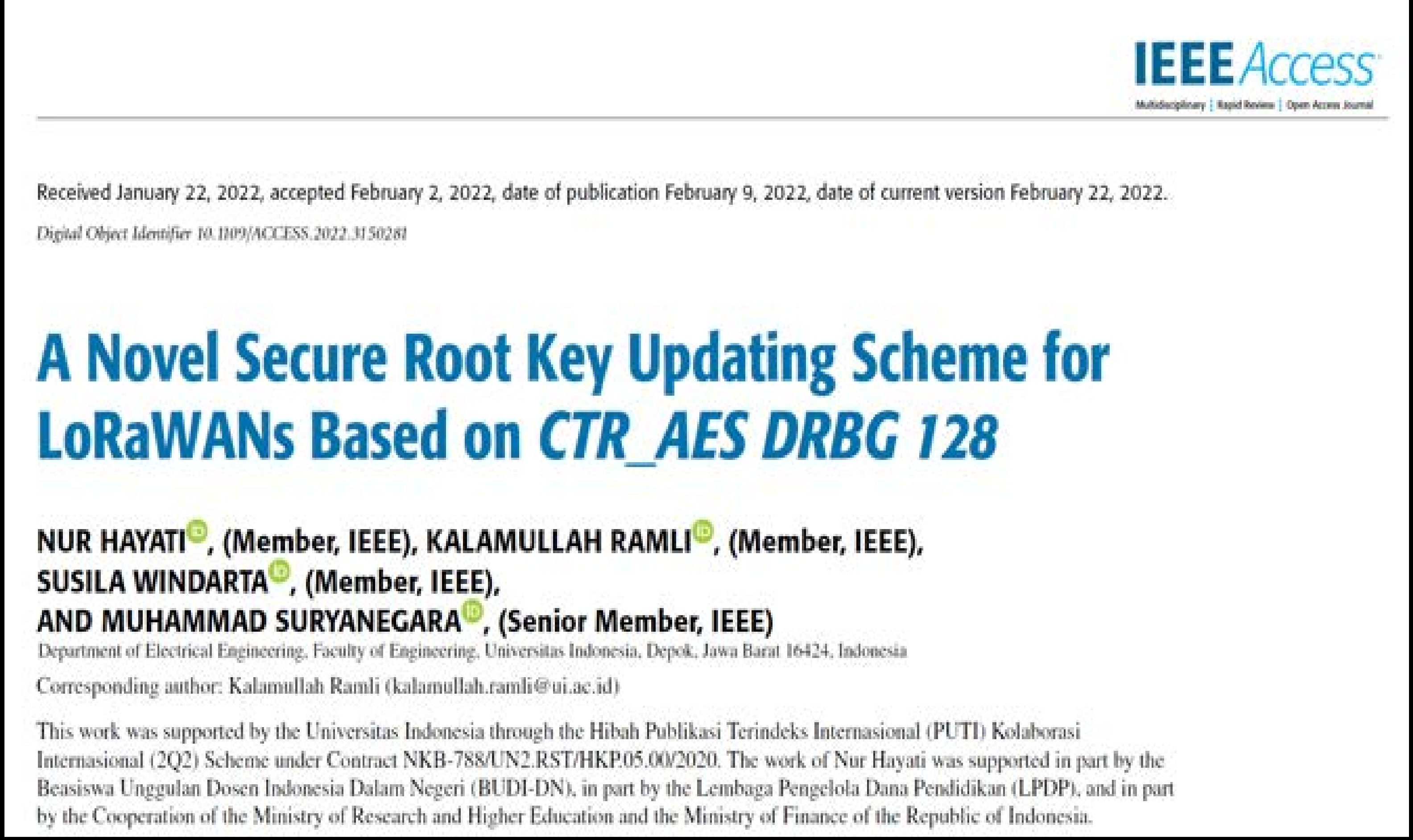
Section 3 & 4

The Analysis of Cryptographic Key Update

- Randomness test of Key bit sequences - NIST 802-22
- Security Communication Protocol Test - Scyther tools
- Formal Security Protocol Analysis - GNY Logic
- Informal Security Protocol (Integrity Protection, Replay attack resistance, Perfect forward secrecy, End-to-end data secrecy, Mutual authentication)
- Performance (Computation cost, Updating method, Implementation compatibility, Communication cost, Storage)

N. Hayati, K. Ramli, S. Windarta, M. Suryanegara, "A Novel Secure Root Key Updating Scheme for LoRaWANs Based on CTR_AES DRBG 128," IEEE Access, vol. 10, pp. 18807–18819, 2022,

Doi: 10.1109/ACCESS.2022.3150281.



IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 22, 2022, accepted February 2, 2022, date of publication February 9, 2022, date of current version February 22, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3150281

A Novel Secure Root Key Updating Scheme for LoRaWANs Based on *CTR_AES DRBG 128*

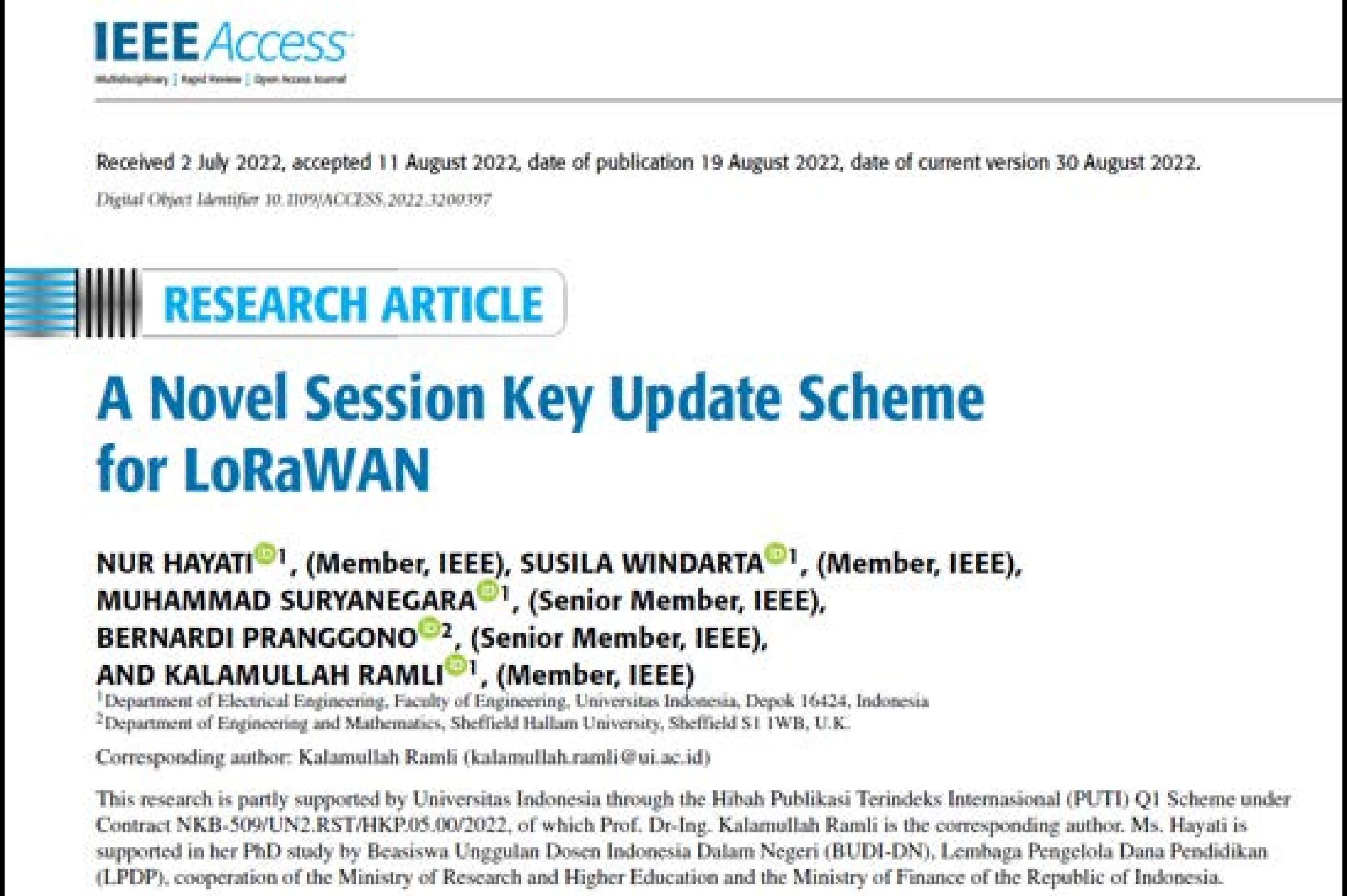
NUR HAYATI, (Member, IEEE), KALAMULLAH RAMLI, (Member, IEEE), SUSILA WINDARTA, (Member, IEEE), AND MUHAMMAD SURYANEGARA, (Senior Member, IEEE)
Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia, Depok, Jawa Barat 16424, Indonesia

Corresponding author: Kalamullah Ramli (kalamullah.ramli@ui.ac.id)

This work was supported by the Universitas Indonesia through the Hibah Publikasi Terindeks Internasional (PUTI) Kolaborasi Internasional (2Q2) Scheme under Contract NKB-788/UN2.RST/HKP.05.00/2020. The work of Nur Hayati was supported in part by the Beasiswa Unggulan Dosen Indonesia Dalam Negeri (BUDI-DN), in part by the Lembaga Pengelola Dana Pendidikan (LPDP), and in part by the Cooperation of the Ministry of Research and Higher Education and the Ministry of Finance of the Republic of Indonesia.

N. Hayati, S. Windarta, M. Suryanegara, B. Pranggono and K. Ramli, "A Novel Session Key Update Scheme for LoRaWAN," in IEEE Access, vol. 10, pp. 89696-89713, 2022,

Doi: 10.1109/ACCESS.2022.3200397



IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 2 July 2022, accepted 11 August 2022, date of publication 19 August 2022, date of current version 30 August 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3200397

RESEARCH ARTICLE

A Novel Session Key Update Scheme for LoRaWAN

NUR HAYATI[1], (Member, IEEE), SUSILA WINDARTA[1], (Member, IEEE), MUHAMMAD SURYANEGARA[1], (Senior Member, IEEE), BERNARDI PRANGGONO[2], (Senior Member, IEEE), AND KALAMULLAH RAMLI[1], (Member, IEEE)

[1]Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia, Depok 16424, Indonesia
[2]Department of Engineering and Mathematics, Sheffield Hallam University, Sheffield S1 1WB, U.K.

Corresponding author: Kalamullah Ramli (kalamullah.ramli@ui.ac.id)

This research is partly supported by Universitas Indonesia through the Hibah Publikasi Terindeks Internasional (PUTI) Q1 Scheme under Contract NKB-509/UN2.RST/HKP.05.00/2022, of which Prof. Dr-Ing. Kalamullah Ramli is the corresponding author. Ms. Hayati is supported in her PhD study by Beasiswa Unggulan Dosen Indonesia Dalam Negeri (BUDI-DN), Lembaga Pengelola Dana Pendidikan (LPDP), cooperation of the Ministry of Research and Higher Education and the Ministry of Finance of the Republic of Indonesia.

THANK YOU

50th Year of
ASEAN-Japan
Friendship and Cooperation

Role of Academe in Cybersecurity Human Resource

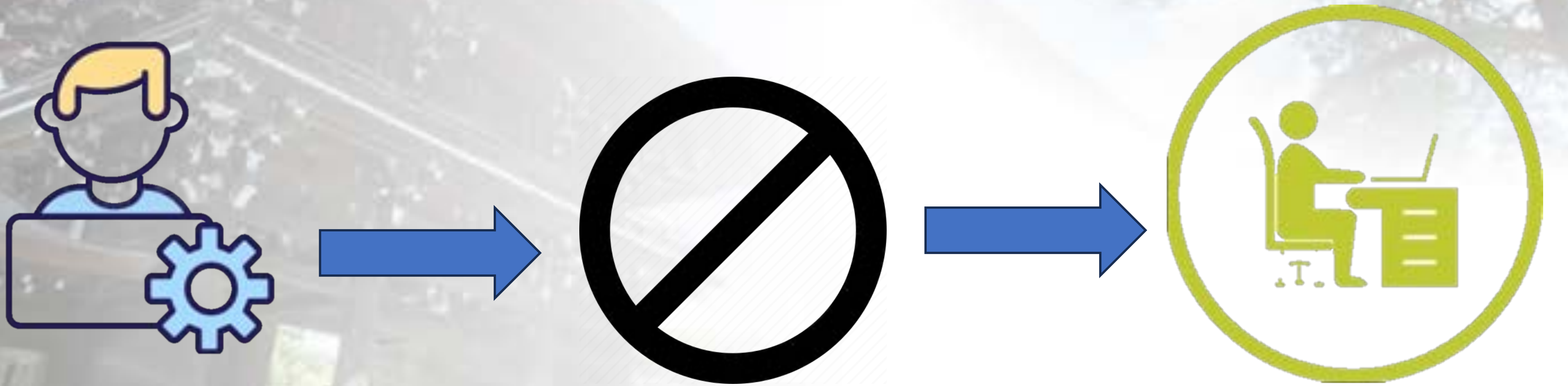
Dr. Marlon I. Tayag, CEH (P),eJPT,MCP,DIT

Dean, School of Computing

Holy Angel University

50th Year of ASEAN-Japan Friendship and Cooperation

Cyber Security Skills Gap



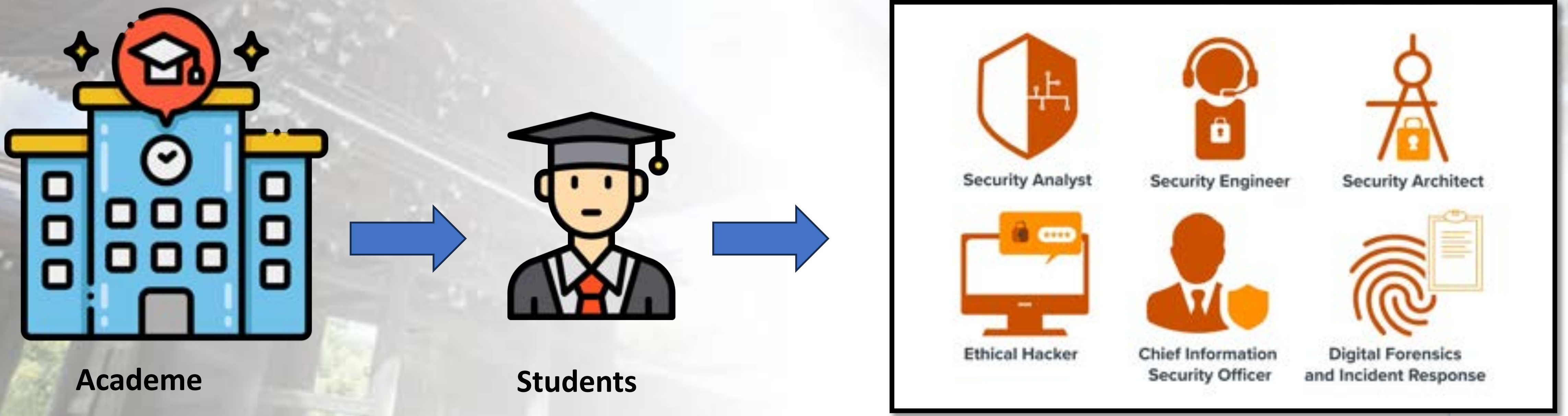
Professionals

Skills Gap

Industry Workforce

50th Year of
ASEAN-Japan
Friendship and Cooperation

Role of Academe in Filling the Gap in Cybersecurity Workforce



Academe

Students

Security Analyst
Security Engineer
Security Architect
Ethical Hacker
Chief Information Security Officer
Digital Forensics and Incident Response

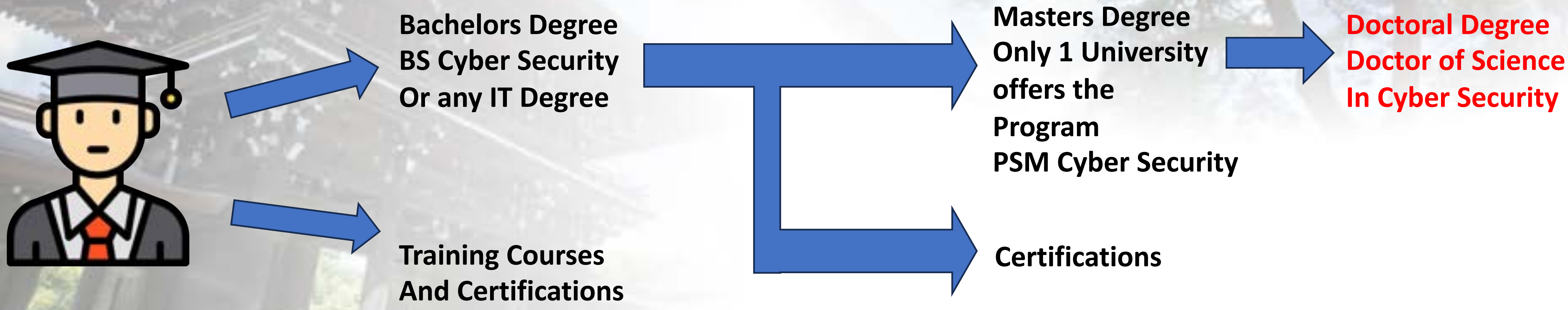
Professional Job

Philippines Settings

- Philippines, 4th most attack nation in the world
- Recorded cyber attacks (2020-2022) half government sites
- In the Philippines, few programs and educational institutions offer specialized cybersecurity training and education. As a result, there is a significant gap between the skills and knowledge required for the job and the skills and knowledge many candidates possess.
- 200,000 needed, 300 professional are working in cyber security (DICT source)

50th Year of ASEAN-Japan Friendship and Cooperation

Career Pathway



Bachelors Degree
BS Cyber Security
Or any IT Degree

Training Courses
And Certifications

Masters Degree
Only 1 University
offers the
Program
PSM Cyber Security

Certifications

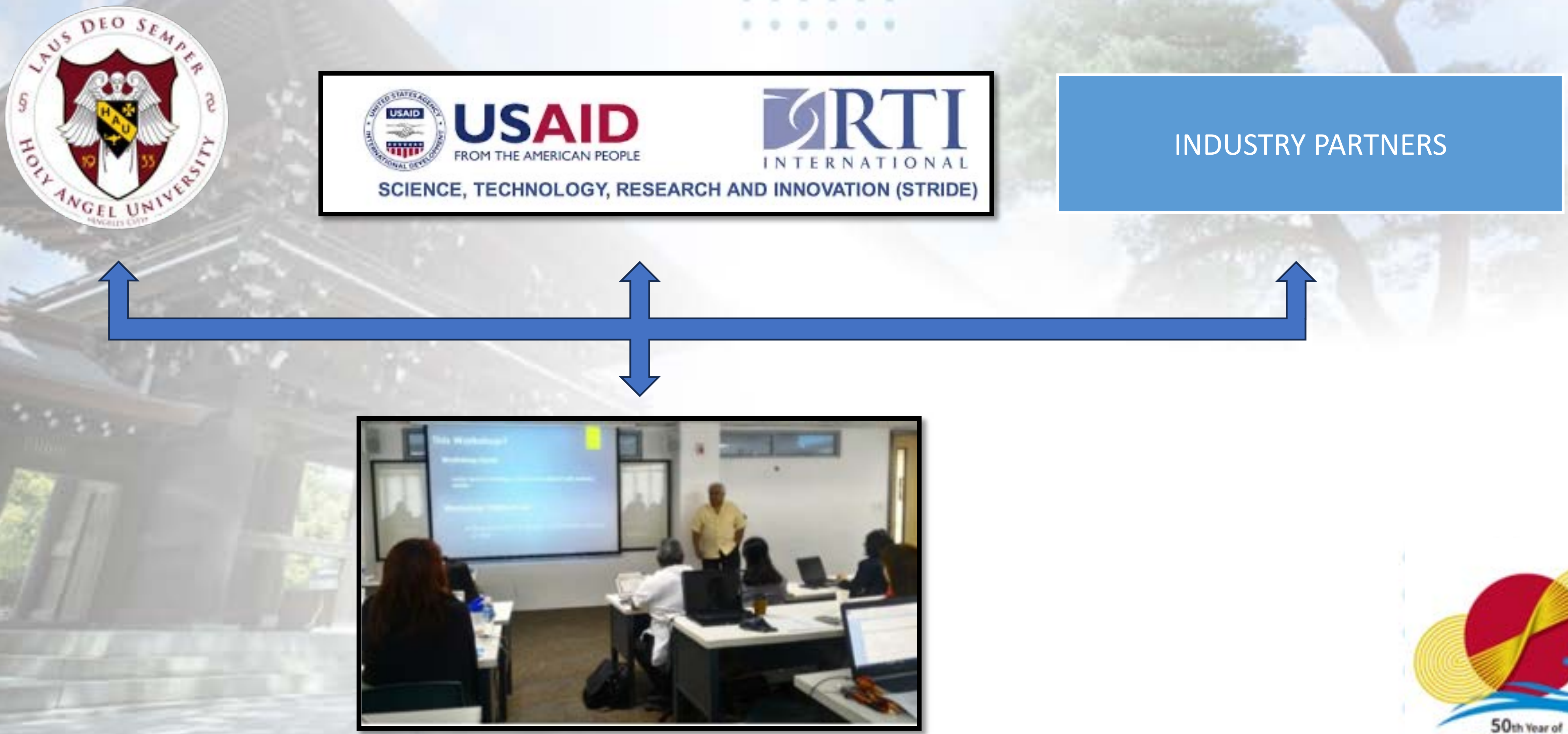
Doctoral Degree
Doctor of Science
In Cyber Security

50th Year of
ASEAN-Japan
Friendship and Cooperation

Holy Angel University Cyber Security Program

- Professional Science Master’s Cyber Security (PSM Cyber Security)
- Offered in 2018 and development under partnership with USAID STRIDE (Science, Technology, Research, and Innovation for Development) program.
- BS Cyber Security (4 yrs.), offered in 2020
- BS Cyber Security 3+2 (Bachelors → Masters) , offered in 2020

Developing the Curriculum



Training the Faculty

- Training the faculty in teaching cybersecurity is a crucial step in ensuring that students receive an education that is current, relevant, and effective.

50th Year of ASEAN-Japan Friendship and Cooperation

Cyber Security Curriculum

- The cybersecurity curricula using was develop using NICE Framework
- Creating a robust skill framework for a cybersecurity curriculum is essential to ensure that learners are equipped with the knowledge and competencies needed to excel in the field.

50th Year of ASEAN-Japan Friendship and Cooperation

Students Needs

- **Foundational Knowledge**
- **Core Cybersecurity Skills**
- **Threat Intelligence and Analysis**
- **Soft Skills**
- **Legal and Compliance**

Hands-On Experience

- **Simulated Environments:** Engaging in war rooms or cybersecurity labs to simulate real-world attacks.
- **Internships:** Gaining real-world experience in corporate or governmental cybersecurity roles.
- **Case Studies:** Analyzing past security breaches to learn and adapt.

50th Year of
ASEAN-Japan
Friendship and Cooperation

Cyber Range

Capture-the-flag

50th Year of ASEAN-Japan Friendship and Cooperation

Industry Partnership

Industry partnership in the realm of cybersecurity education and training is of paramount importance for several compelling reasons:

1. Relevance of Curriculum
2. Practical Exposure
3. Resource Sharing
4. Joint Research and Development
5. Faculty Development
6. Career Opportunities
7. Workshops and Seminars
8. Feedback Loop
9. Funding and Grants
10. Setting Standards

50th Year of
ASEAN-Japan
Friendship and Cooperation

Degree programs vs. certifications: Which is more effective?

- The effectiveness of degree programs versus certifications in the cybersecurity domain depends on specific goals, career stages, and individual needs

Nurturing Skilled and Capable Cybersecurity Professionals

- Regular Training & Workshops
- Certification Programs
- Simulated Cyber Attacks
- Mentorship Programs
- Scholarship & Education Sponsorships
- Continuing Education
- Collaboration & Networking
- Wellness & Mental Health
- Clear Career Pathways
- Competitive Compensation

Summary

- The cybersecurity skills gap is a pressing concern, leaving organizations vulnerable to threats and hindering technological progress. Central to addressing this gap is the academe.
- The academe is a beacon of hope, driving initiatives and programs that mold, inspire, and equip the next generation of cybersecurity professionals.
- An effective cybersecurity curriculum is pivotal in producing skilled students ready to face the evolving digital threats of our age and become a part of the cyber security human resources.

50th Year of
ASEAN-Japan
Friendship and Cooperation

International Conference on ASEAN-Japan Cybersecurity Community (IC-AJCC 2023) | Tokyo

CYBERSECURITY

IN FINANCIAL INSTITUTIONS

A Philippine Perspective (focus on FinTech)

By Sam Jacoba
PH-CERT President & NADPOP President
October 6, 2023

THREE POINTS

01 PH FINTECH ECOSYSTEM

02 CURRENT CHALLENGES

03 SOLUTIONS

01 Philippines at a Glance

The Philippines’ Flourishing Growth in Banking and Connectivity

PHILIPPINES IN NUMBERS

6.4%
GDP growth (1Q of 2023)

6%
GDP forecast (2023)

US3,623
GDP Per Capita (2022)

5.4%
Inflation forecast (2023)

115,559,009
Total population (2022)

47.9%
Urban Population

30M
Filipinos aged 10-24

6M
Number of micro-enterprise

93.2M (+9.2%)
Number of deposit accounts Q3 2022 (Growth from Q3 2021)

23,022 (+1.06%)
Number of ATMs 2022 Q2 (Growth from 2020 Q4)

28.3
Number of access points per 10,000 adults Q3 2022

55
Number of banks with digital onboarding capability 2022

84.9%
Smartphone penetration (2022)

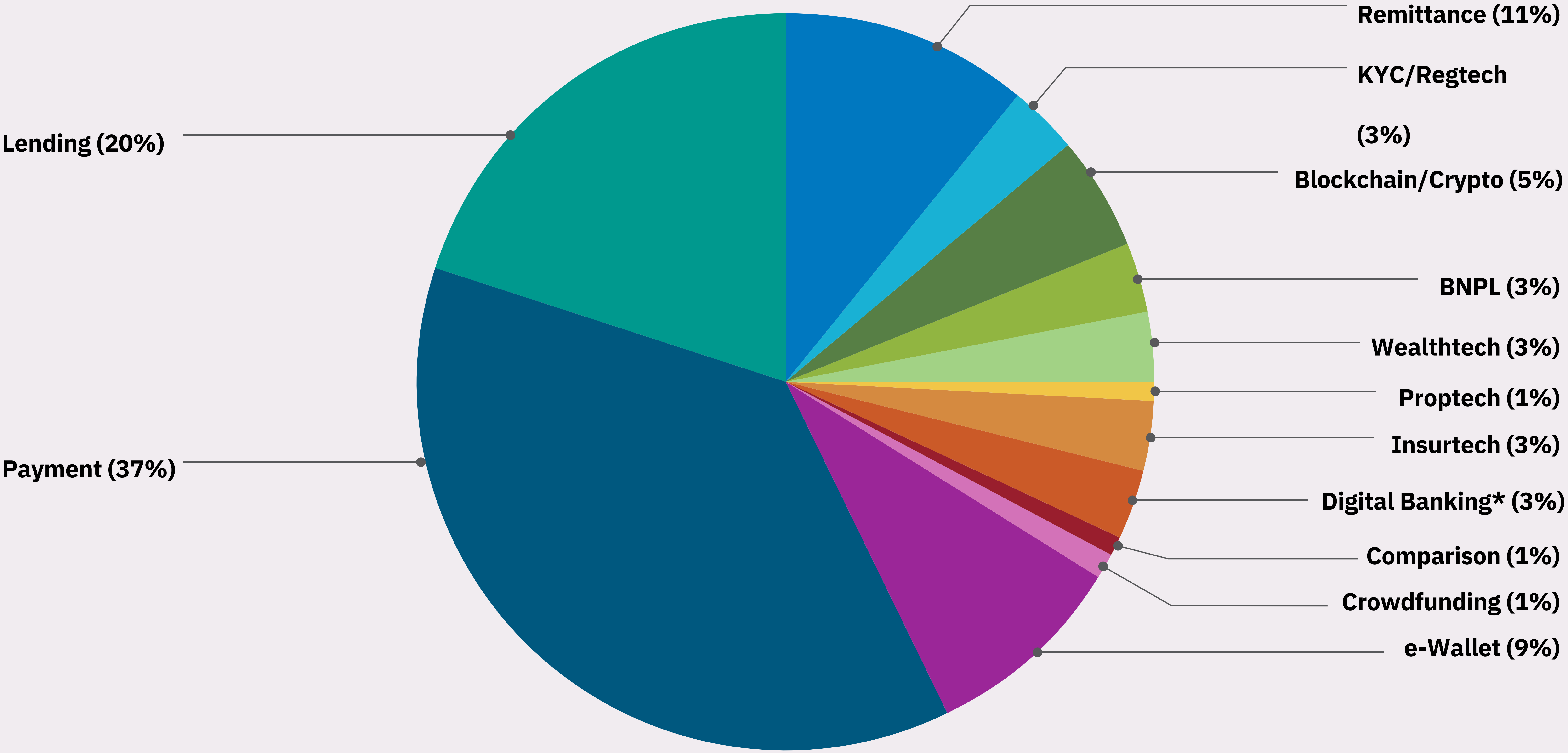
84.75M
Number of Internet users (2022)

97.5%
Mobile Broadband Connections (2022)

71.32M
Mobile internet user penetration

*Sources: BSP Monetary Policy Report - November 2022, latest Financial Inclusion Survey (2022 Q2), Statista, Philippine Statistics Authority (PSA) *Mobile broadband connections - number of sim cards that are 3G and above (as percentage of total population)*

Philippines Fintech Map 2023



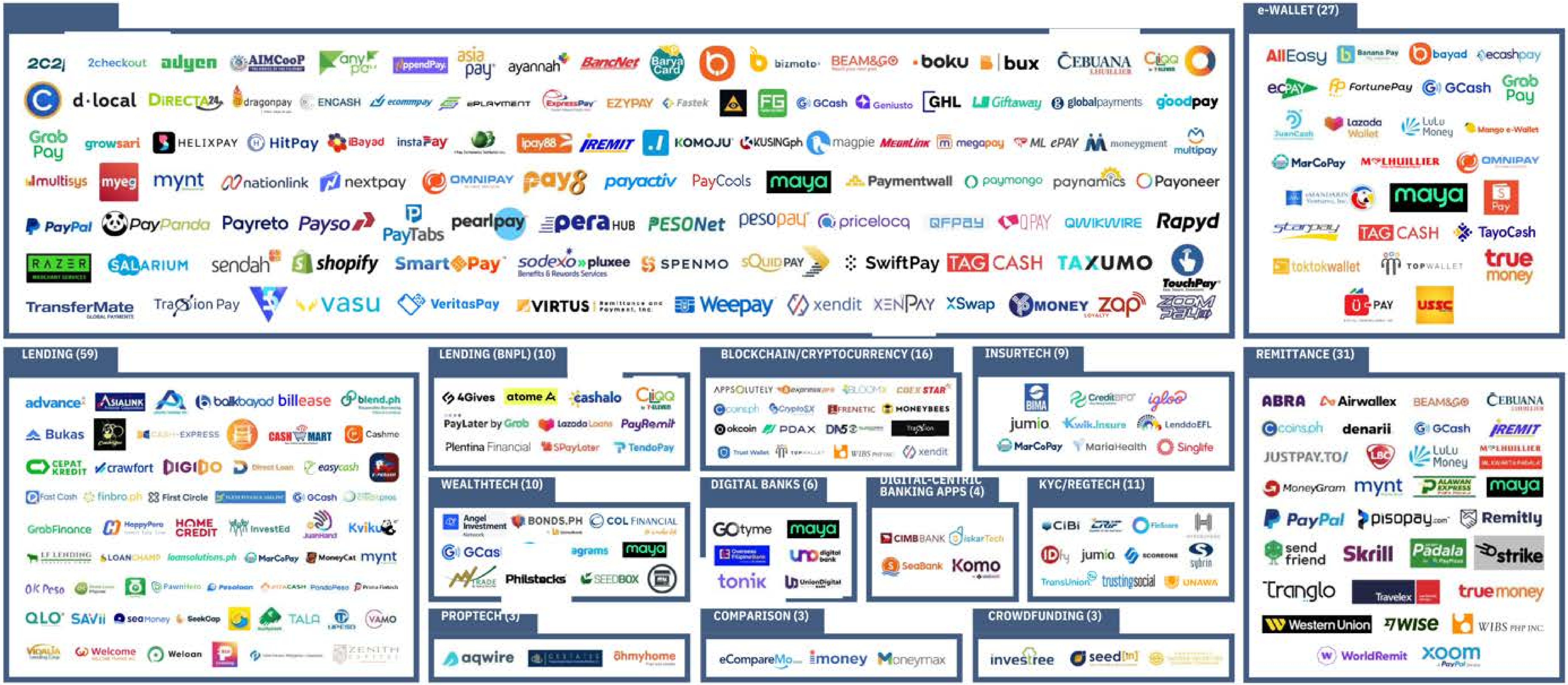
Source: Fintech News Philippines

**Digital Banking (Banks + Digital-centric apps combined)*

02 Philippines' Fintech Landscape

Philippines Fintech Map 2023 (Total: 285 Fintech Companies)

Alibaba Cloud FINTECH ALLIANCE.PH FINTECH PHILIPPINES fintechnews.ph



Note: Some companies appear in more than 1 category to better reflect the nature of their businesses, but they still count as one towards the total. Source: Fintech News Philippines

CURRENT CHALLENGES

UNSECURE ECOSYSTEM

UNSECURE CUSTOMERS

INSTITUTION RESILIENCE & MATURITY

SOLUTIONS

SE

Synchronize & harmonize the whole ecosystem

CU

Customer understanding (KYC) with ubiquitous protection

RE

Resiliency and maturity for everyone

THANK YOU!

sam@samjacoba.com

ASEAN JAPAN CYBERSECURITY
COMMUNITY ALLIANCE (AJCCA)

Public Private Partnership Community Report

- PATHUWMAN PRINCESS HOTEL –

- BANGKOK 7 FEBRUARY 2024 -

ASEAN JAPAN CYBERSECURITY COMMUNITY ALLIANCE (AJCCA)

Agenda

- About US
  - Establishment
  - Profile
- Public Private Partnership / Cooperation Community Report

ASEAN JAPAN CYBERSECURITY
COMMUNITY ALLIANCE (AJCCA)

Establishment

Understanding that community roles and collaboration is very important in emerging digital landscape nowadays,
Nine Cyber Security Communities in ASEAN and Japan signed MoU on 5 October 2023

↓

Establishment of AJCCA

Establishment

Brunei Cybersecurity Association

Information Sharing And Analytic Center in Cambodia

Indonesia Network Security Association

Japan Network Security Association

Malaysia CyberSecurity Community

Philippine Computer Emergency Response Team

Association of Information Security Professionals

Thailand Information Security Association

Vietnam Information Security Association

Community ? :

- They have their own community or member to serve
- They have routine activities that they conduct monthly or at least annually
- They are nonprofit and usually funded by them self or from sponsor
- They are independent from any intervention
- They may have already cooperation agreement with other international organization/communities
- They have the same understanding about the important of community role

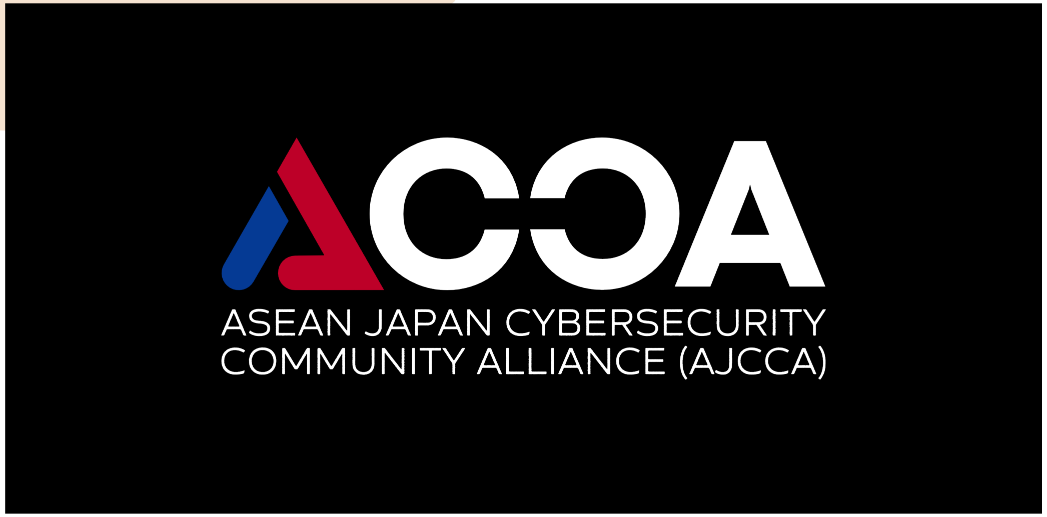
AJCCA Vision

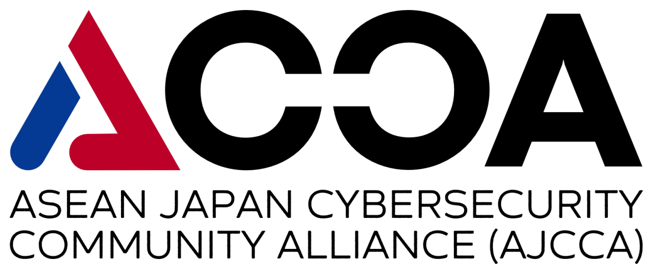
"A dynamic and resilient cybersecurity community in our region through trustworthy and respectful collaboration"

AJCCA Mission

- Facilitate Exchanges Among Organizations :
  - Recognizing the importance of diverse perspective and experiences in tackling cyber threats, the AJCCA aims to deepen mutual understanding , interactions and collaborations across member countries about cybersecurity governance and operations.
- 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.
- 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

AJCCA Logo and web site





website : https://ajcca.net

•**First 'A' for ASEAN and Japan:** This 'A' is likely 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 which could be referencing the colors found in many ASEAN nations' flags as well as the Japanese flag.

•**Second and Third 'C's:** These letters are stylized to represent a chain or a secure connection, which aligns with the cybersecurity focus of the alliance. The interconnected circles may symbolize unity, strength, and the interconnected nature of cybersecurity efforts across nations.

•**Color Scheme:** The use of red, blue, and black may have been chosen for 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 may be intended to convey a sense of dynamism and adaptability, important traits for cybersecurity.

AJCCA Article of Organization

- Articles of organization are part of a formal legal document used to establish a limited liability company (LLC) at the state level.
- The materials are also used to create the rights, powers, duties, liabilities, and other obligations between each member of an LLC and also between the LLC and its members. **" Organization Rules and Standard"**
- All articles of organization filings tend to require basic information :
    - Organization's business name and address,
    - The names and addresses of members,
    - The statement of the organization's purpose : Vision and Mission

ASEAN JAPAN CYBERSECURITY COMMUNITY ALLIANCE (AJCCA)

AJCCA Article of Organization

- 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

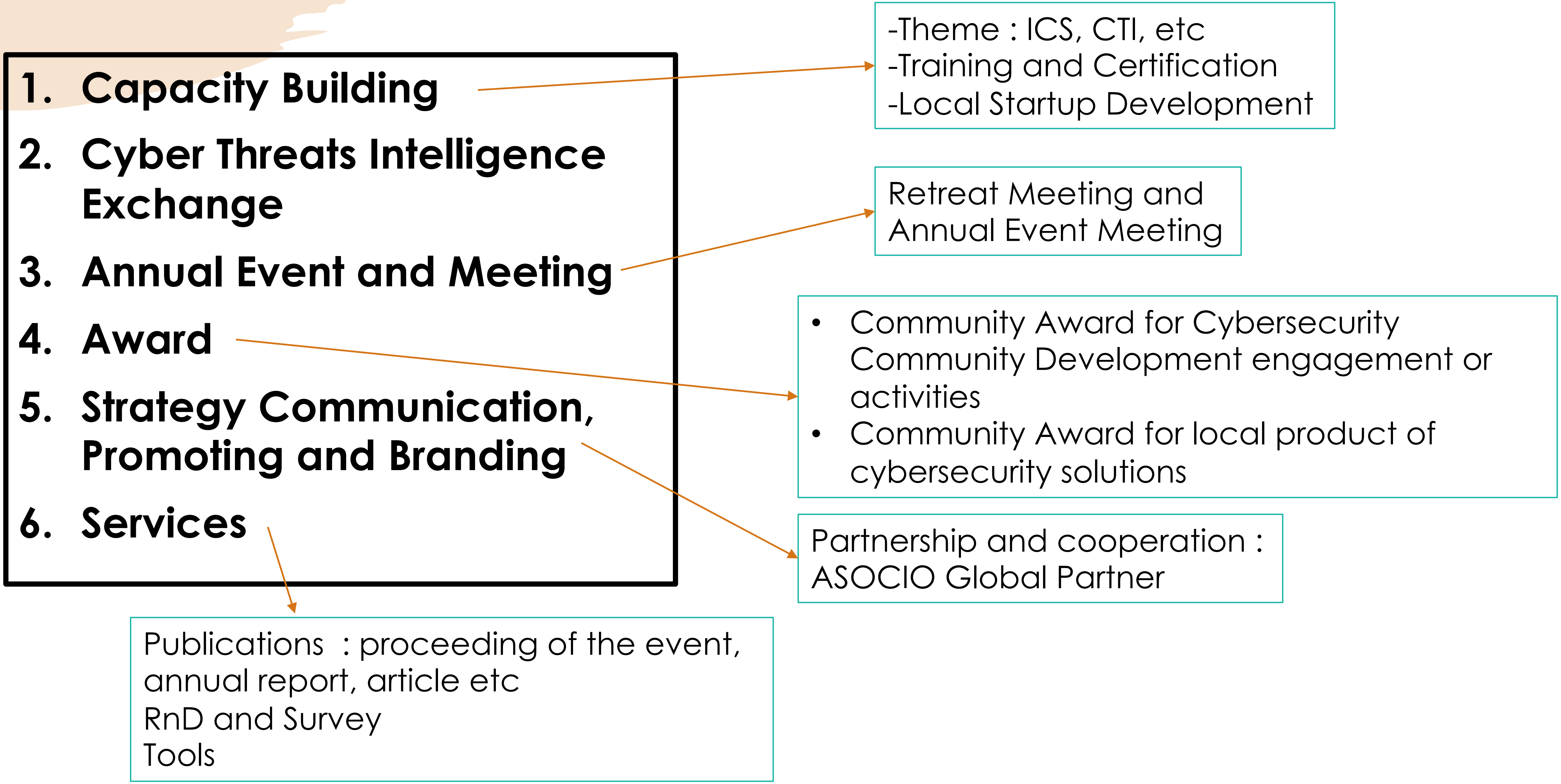
AJCCA Article of Organization

- **Article IV – Board of Trustees**
- **Section 1. Member of Trustees and Election.**
- The affairs of the AJCCA shall be directed by the Board of AJCCA (the "Board"), that is consisted by Board of Trustees (the "Trustees"). Every AJCCA member organization assigns one Trustee. The Chair of AJCCA (the "Chair") shall be elected in Annual Board Meeting (the "AGM") every two years.

Chairman : Rudi Lumanto (IdNSA)
Vice Chair (General Affairs) : Prof Esaki (JNSA)
Secretary : Mr Ito (JNSA)
Vice Chair (Annual Event) : Mr Johnny Kho (AiSP)

AJCCA Activities

ASEAN JAPAN CYBERSECURITY COMMUNITY ALLIANCE (AJCCA)



1. **Capacity Building**
2. **Cyber Threats Intelligence Exchange**
3. **Annual Event and Meeting**
4. **Award**
5. **Strategy Communication, Promoting and Branding**
6. **Services**

-Theme : ICS, CTI, etc
-Training and Certification
-Local Startup Development

Retreat Meeting and
Annual Event Meeting

- Community Award for Cybersecurity Community Development engagement or activities
- Community Award for local product of cybersecurity solutions

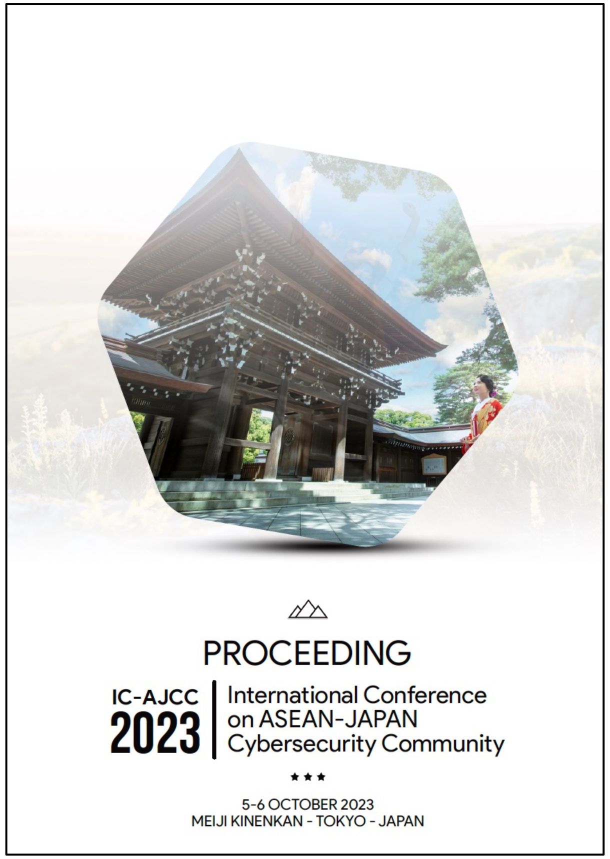
Partnership and cooperation :
ASOCIO Global Partner

Publications : proceeding of the event, annual report, article etc
RnD and Survey
Tools

AJCCA Activities

6. Services :

- Publications : proceeding of the event, annual report, article etc
- RnD and Survey
- Tools



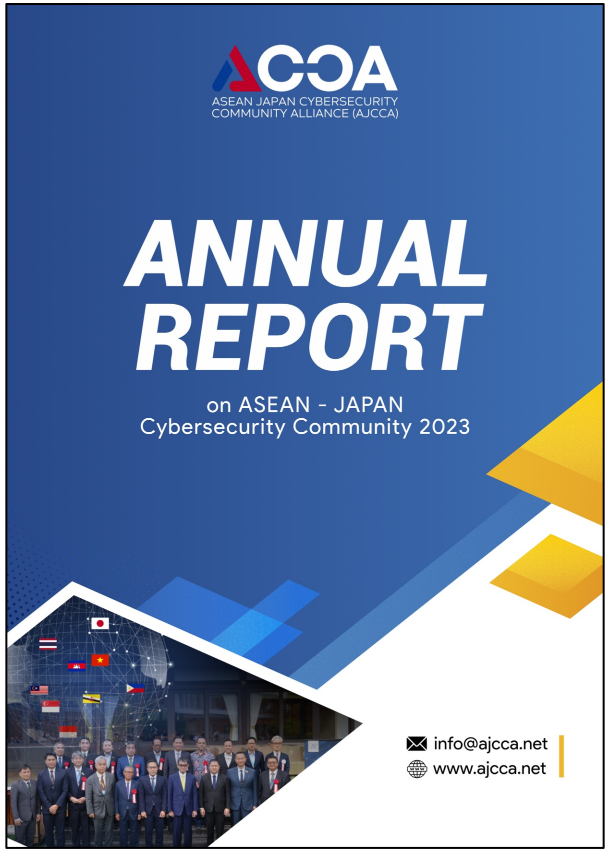
PROCEEDING

IC-AJCC 2023

International Conference on ASEAN-JAPAN Cybersecurity Community

★★★

5-6 OCTOBER 2023
MEIJI KINENKAN - TOKYO - JAPAN



ASEAN JAPAN CYBERSECURITY COMMUNITY ALLIANCE (AJCCA)

ANNUAL REPORT

on ASEAN - JAPAN
Cybersecurity Community 2023

info@ajcca.net
www.ajcca.net

AJCCA CALENDAR

- 20-21 May (AJCCA)

  Agenda : Strategic Comm, Annual event, etc

  Venue : Cambodia

- 3-4 October is AJCCA Annual General Meeting

  Agenda : AGM

  Venue : Singapore

ASEAN JAPAN CYBERSECURITY
COMMUNITY ALLIANCE (AJCCA)

Cybersecurity community view on Public Private Cooperation and Cybersecurity Ecosystem

AJCCA:
Cybersecurity community view on Public Private Cooperation and Cybersecurity Ecosystem

ASEAN JAPAN CYBERSECURITY
COMMUNITY ALLIANCE (AJCCA)

BACKGROUND

- Public Private Cooperation is very important due to emerging cyber threats landscape
- Good partnership between public and private create more cyber resilience environment

Reff:
1. Emerging Practices in Cybersecurity-Related Public-Private Partnerships and Collaboration in OSCE participating States, Organization for Security and Co-operation in Europe, 17 March 2023
2. The New "Cyber" Space Race: Integrating the Private Sector Into U.S. Cyber Strategy, May 4, 2023
3. Public–private partnerships in national cyber-security strategies, *International Affairs*, Volume 92, Issue 1, January 2016, Pages 43–62

AJCCA:
Cybersecurity community view on
Public Private Cooperation (PPC) and Cybersecurity Ecosystem

ASEAN JAPAN CYBERSECURITY
COMMUNITY ALLIANCE (AJCCA)

1. OBJECTIVES

1. Assess the level of current cooperation and level satisfaction
2. Identify areas of improvement,
3. Gather feedback on current initiatives

2. KEY AREA OF FOCUS (QUESTIONS CATEGORIES)

-PPC
1. Current State of Cooperation
2. Challenges and Barriers
3. Opportunities for Collaboration
4. Resource Allocation
5. Expectations and Suggestions

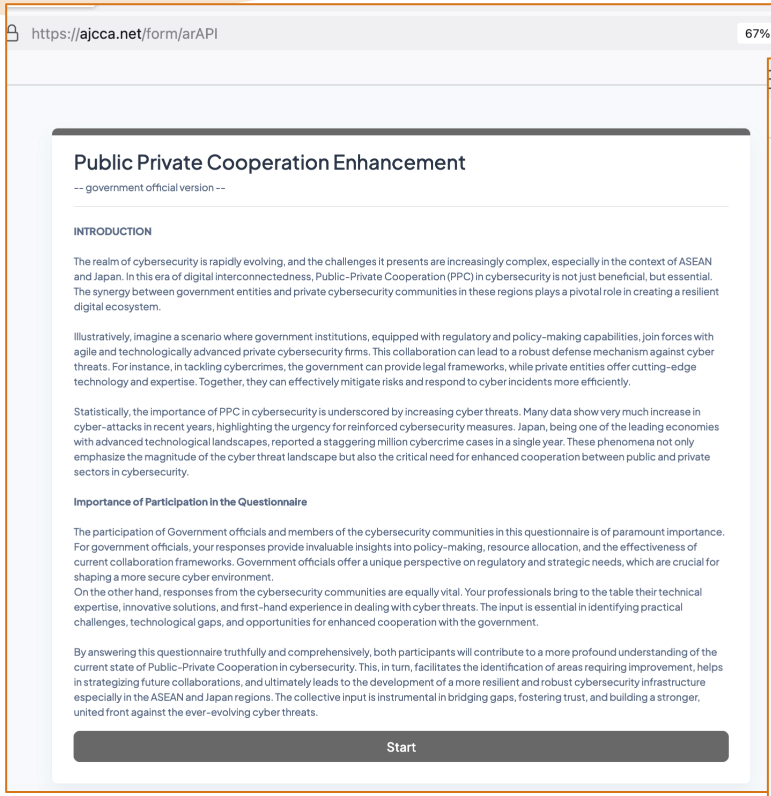
Cybersecurity Ecosystem
- impact of GCI 5 items

3. EXPECTED OUTPUT

Valuable insights, identify areas for improvement, and strengthen the cooperation between public and private entities in the realm of cybersecurity.

ASEAN JAPAN CYBERSECURITY COMMUNITY ALLIANCE (AJCCA)

Web Base Public Private Cooperation Survey



https://ajcca.net/form/arAPI

67%

Public Private Cooperation Enhancement

-- government official version --

INTRODUCTION

The realm of cybersecurity is rapidly evolving, and the challenges it presents are increasingly complex, especially in the context of ASEAN and Japan. In this era of digital interconnectedness, Public-Private Cooperation (PPC) in cybersecurity is not just beneficial, but essential. The synergy between government entities and private cybersecurity communities in these regions plays a pivotal role in creating a resilient digital ecosystem.

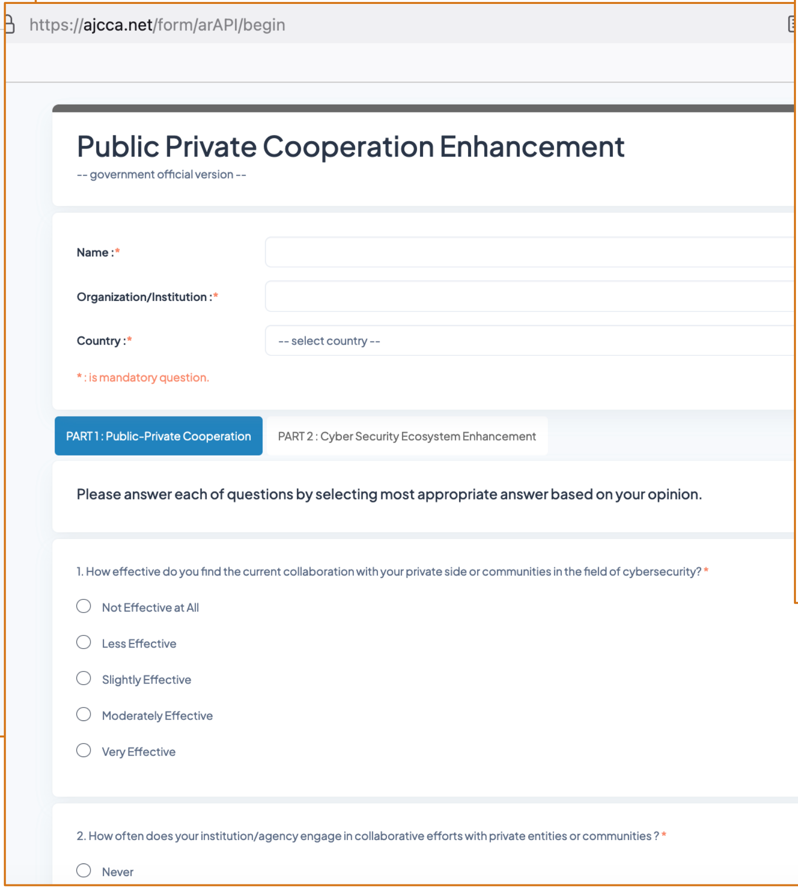
Illustratively, imagine a scenario where government institutions, equipped with regulatory and policy-making capabilities, join forces with agile and technologically advanced private cybersecurity firms. This collaboration can lead to a robust defense mechanism against cyber threats. For instance, in tackling cybercrimes, the government can provide legal frameworks, while private entities offer cutting-edge technology and expertise. Together, they can effectively mitigate risks and respond to cyber incidents more efficiently.

Statistically, the importance of PPC in cybersecurity is underscored by increasing cyber threats. Many data show very much increase in cyber-attacks in recent years, highlighting the urgency for reinforced cybersecurity measures. Japan, being one of the leading economies with advanced technological landscapes, reported a staggering million cybercrime cases in a single year. These phenomena not only emphasize the magnitude of the cyber threat landscape but also the critical need for enhanced cooperation between public and private sectors in cybersecurity.

Importance of Participation in the Questionnaire

The participation of Government officials and members of the cybersecurity communities in this questionnaire is of paramount importance. For government officials, your responses provide invaluable insights into policy-making, resource allocation, and the effectiveness of current collaboration frameworks. Government officials offer a unique perspective on regulatory and strategic needs, which are crucial for shaping a more secure cyber environment.
On the other hand, responses from the cybersecurity communities are equally vital. Your professionals bring to the table their technical expertise, innovative solutions, and first-hand experience in dealing with cyber threats. The input is essential in identifying practical challenges, technological gaps, and opportunities for enhanced cooperation with the government.

By answering this questionnaire truthfully and comprehensively, both participants will contribute to a more profound understanding of the current state of Public-Private Cooperation in cybersecurity. This, in turn, facilitates the identification of areas requiring improvement, helps in strategizing future collaborations, and ultimately leads to the development of a more resilient and robust cybersecurity infrastructure especially in the ASEAN and Japan regions. The collective input is instrumental in bridging gaps, fostering trust, and building a stronger, united front against the ever-evolving cyber threats.



https://ajcca.net/form/arAPI/begin

Public Private Cooperation Enhancement

-- government official version --

Name :*

Organization/Institution :*

Country :* -- select country --

* : is mandatory question.

PART 1 : Public-Private Cooperation
PART 2 : Cyber Security Ecosystem Enhancement

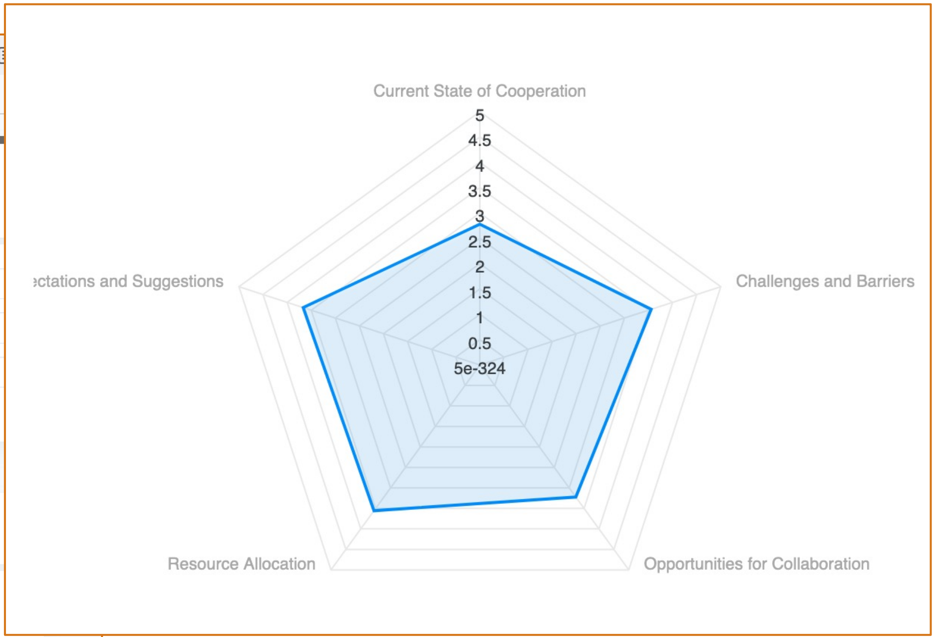
Please answer each of questions by selecting most appropriate answer based on your opinion.

1. How effective do you find the current collaboration with your private side or communities in the field of cybersecurity? *

○ Not Effective at All
○ Less Effective
○ Slightly Effective
○ Moderately Effective
○ Very Effective

2. How often does your institution/agency engage in collaborative efforts with private entities or communities ? *

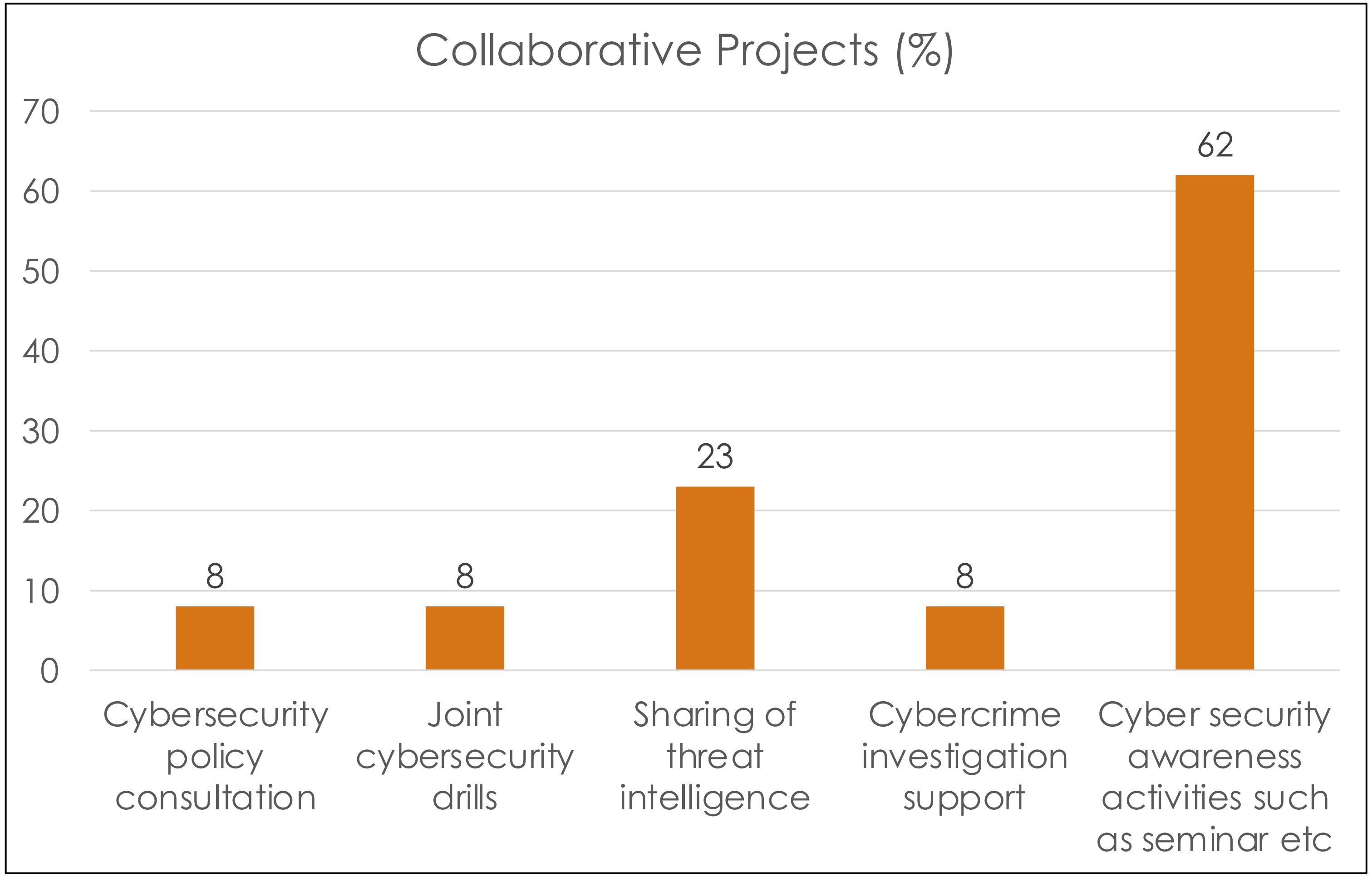
○ Never



AJCCA:
Cybersecurity community view on Public Private Cooperation and cybersecurity ecosystem

ASEAN JAPAN CYBERSECURITY COMMUNITY ALLIANCE (AJCCA)

1. What types of collaborative projects have you been most involved in with the government ?



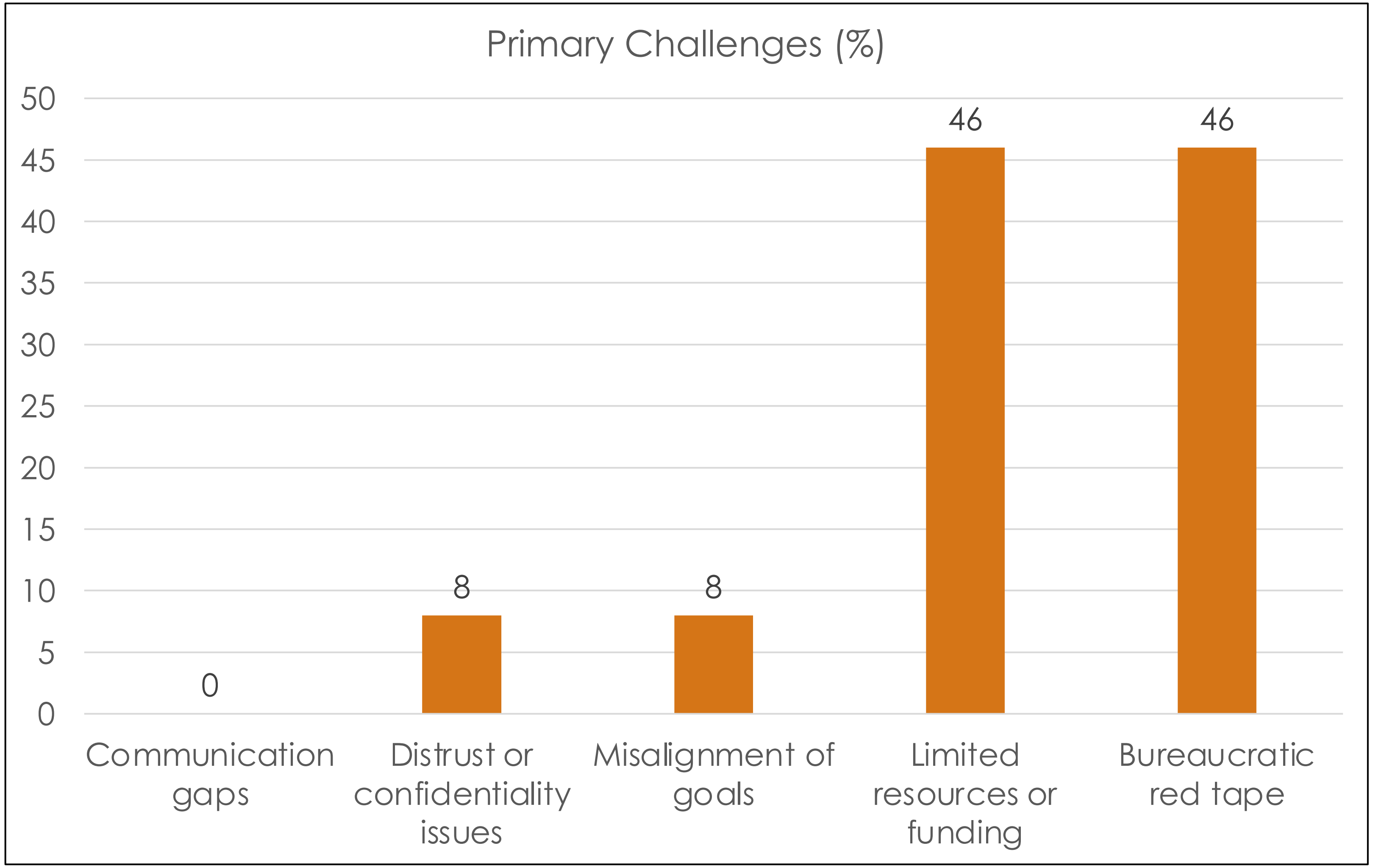
Purpose :
To identify the nature of past collaborative efforts.

AJCCA:
Cybersecurity community view on Public Private Cooperation and cybersecurity ecosystem

ASEAN JAPAN CYBERSECURITY COMMUNITY ALLIANCE (AJCCA)

2. What are the primary challenges you face when collaborating with government entities in cybersecurity ?

Purpose : To identify barriers from the community's perspective.

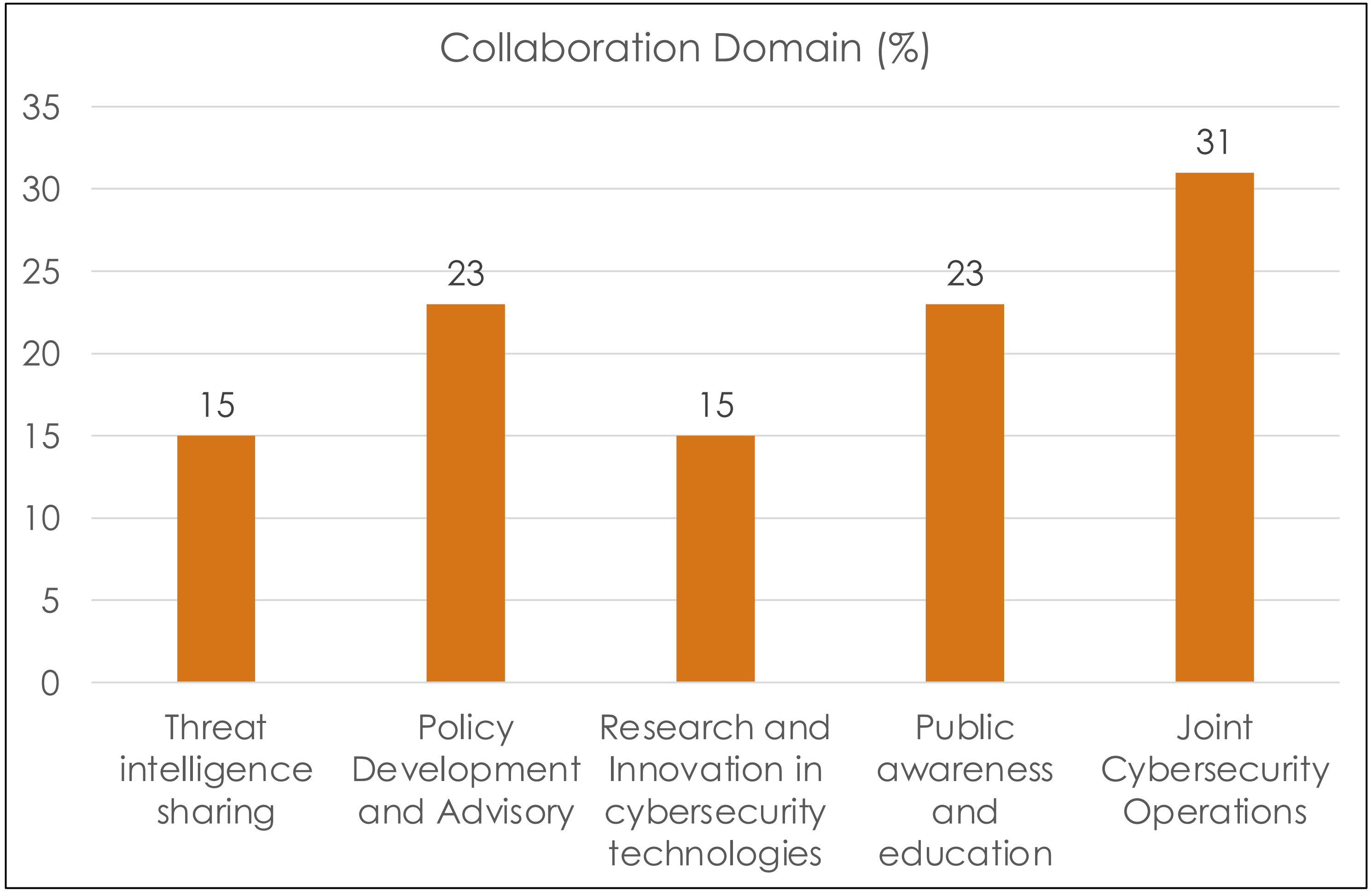


AJCCA: Cybersecurity community view on Public Private Cooperation and cybersecurity ecosystem

ASEAN JAPAN CYBERSECURITY COMMUNITY ALLIANCE (AJCCA)

3. Are there specific cybersecurity domains where you believe increased collaboration with the government is essential ?

Purpose : To pinpoint areas needing more focus for collaboration.

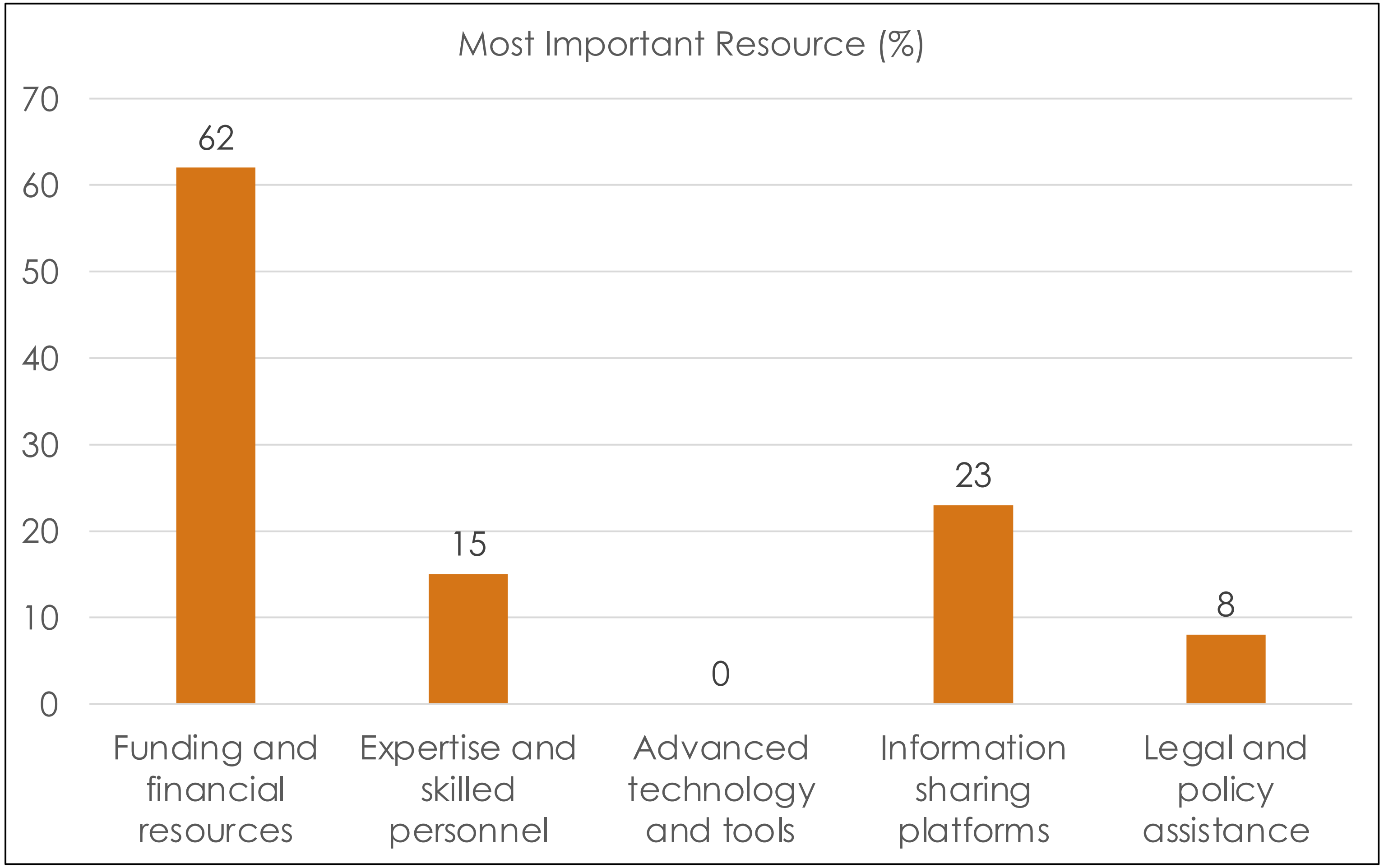


AJCCA:
Cybersecurity community view on Public Private Cooperation and cybersecurity ecosystem

ASEAN JAPAN CYBERSECURITY COMMUNITY ALLIANCE (AJCCA)

4. What types of resources are most critically needed to enhance public-private collaboration in cybersecurity ?

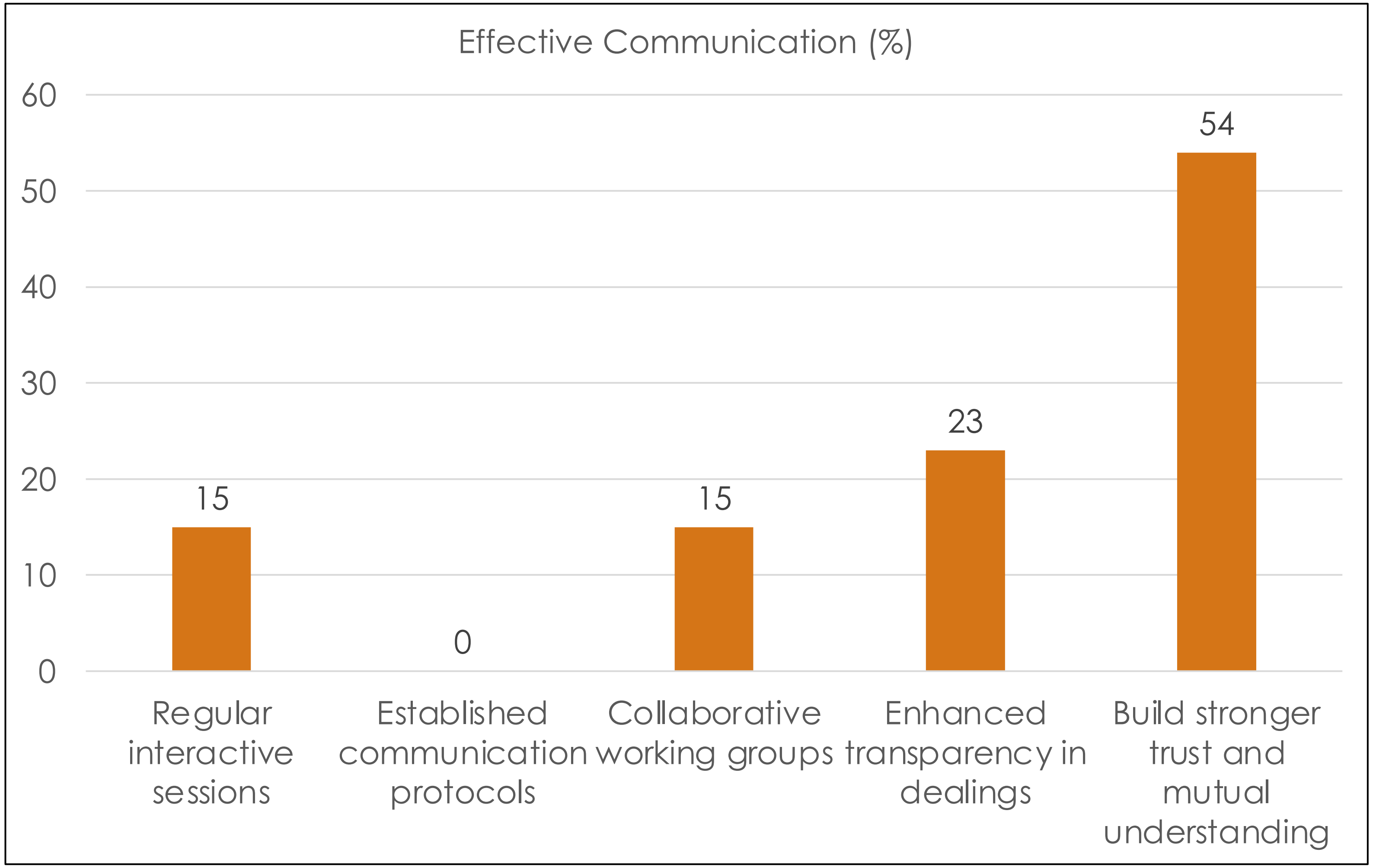
Purpose : To identify key resource needs.



AJCCA: Cybersecurity community view on Public Private Cooperation and cybersecurity ecosystem

5. How can communication between cybersecurity communities and the government you think be effectively improved?

Purpose : To solicit suggestions for better communication



AJCCA:
Cybersecurity community view on Public Private Cooperation and Cybersecurity ecosystem

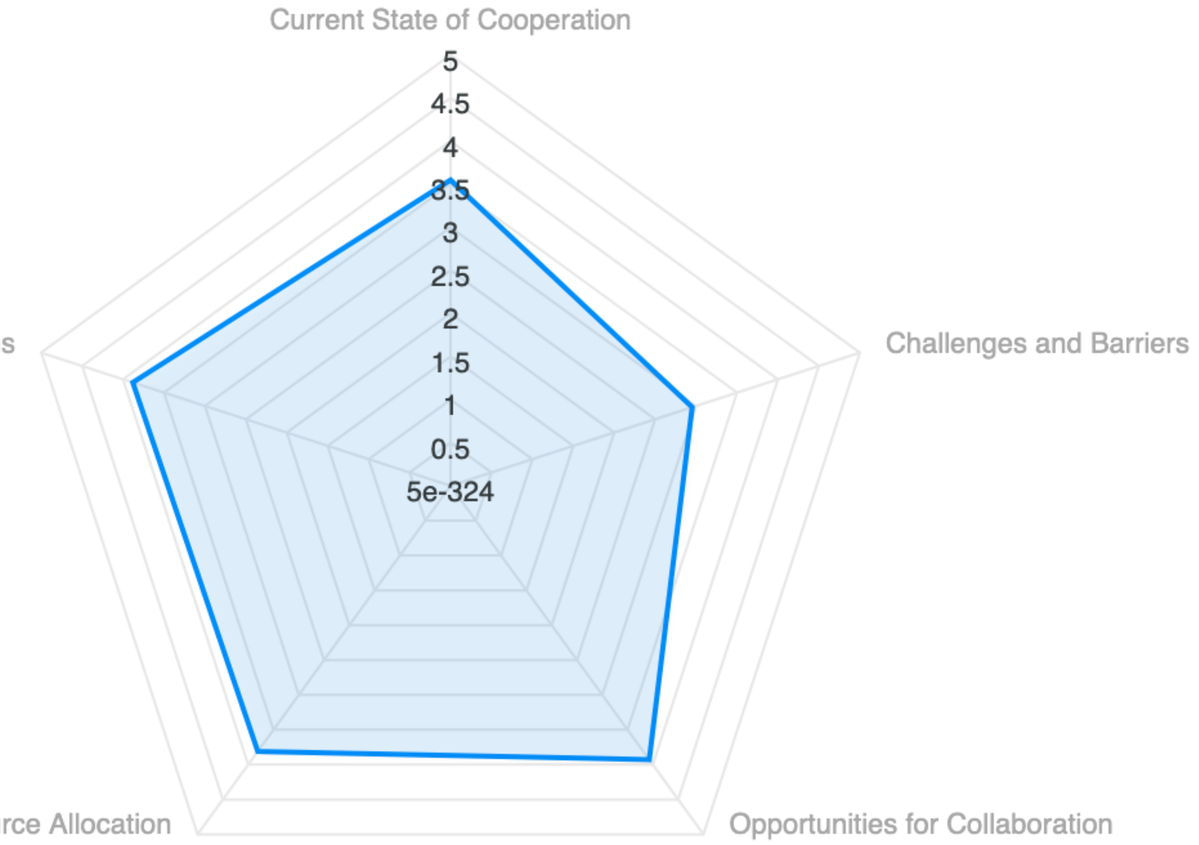
ASEAN JAPAN CYBERSECURITY COMMUNITY ALLIANCE (AJCCA)

KEY AREA OF FOCUS

1. Current State of Cooperation
2. Challenges and Barriers
3. Opportunities for Collaboration
4. Resource Allocation
5. Expectations and Suggestions

Community View on PPC

1. Current State of Cooperation :
Closed to Good
2. Challenges and Barriers :
Enough challenges but can be handle
3. Opportunities :
Good.
4. Resource Allocation:
Closed to Good
5. Expectation : Closed to Good

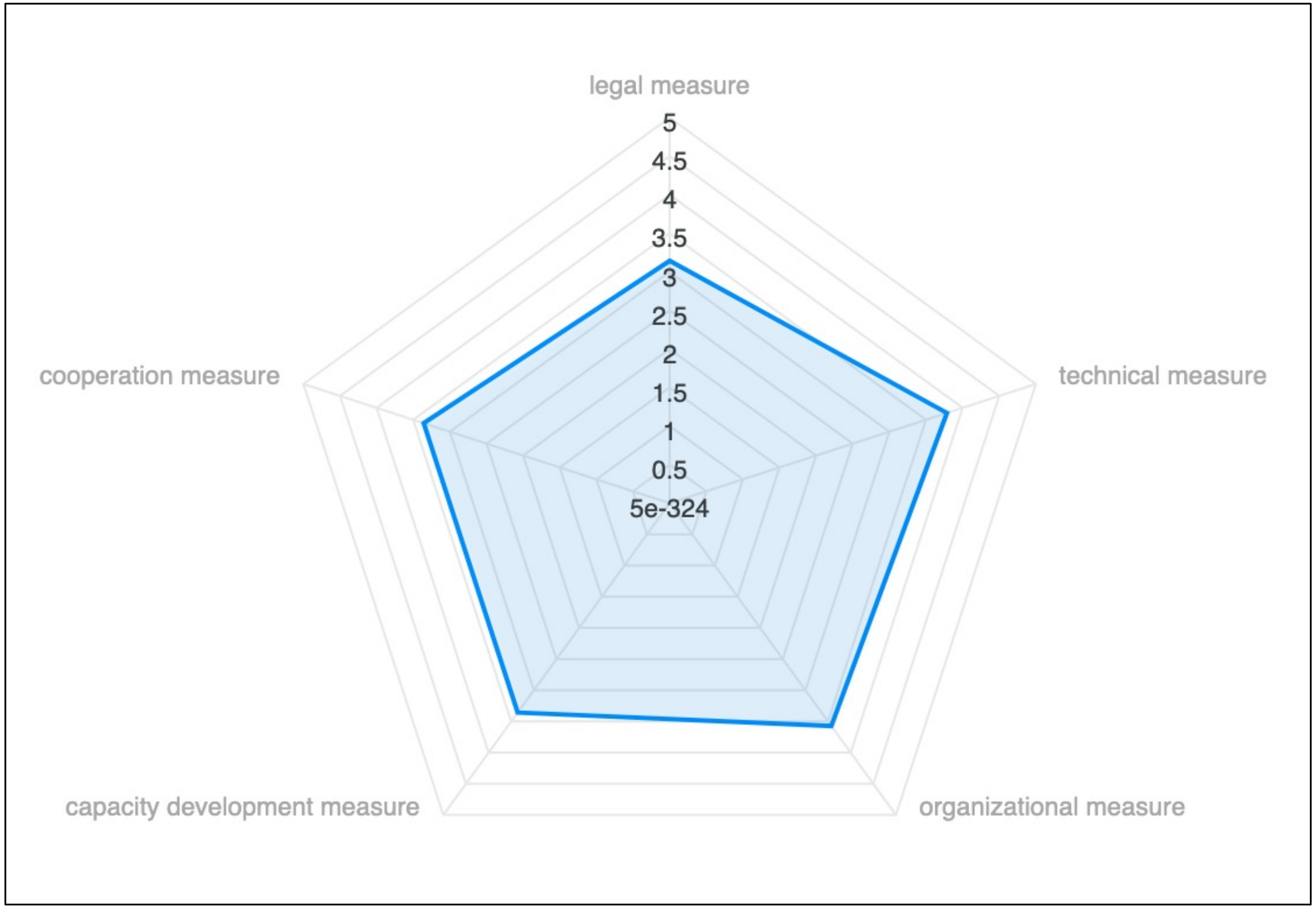


ASEAN JAPAN CYBERSECURITY COMMUNITY ALLIANCE (AJCCA)

AJCCA:
Cybersecurity community view on Cybersecurity ecosystem

ITU's guideline for a country to commit to five pillar namely legal measure, technical measure, organizational measure, capacity development measure and cooperation measure (GCI) to make a better cybersecurity ecosystem

The impact seen by communities
Legal : Closed to Enough
Technical : Closed to Good
Organizational : Closed to Good
Capacity Dev: Closed to Enough
Cooperation : Closed to Enough



Last
But Not
Least

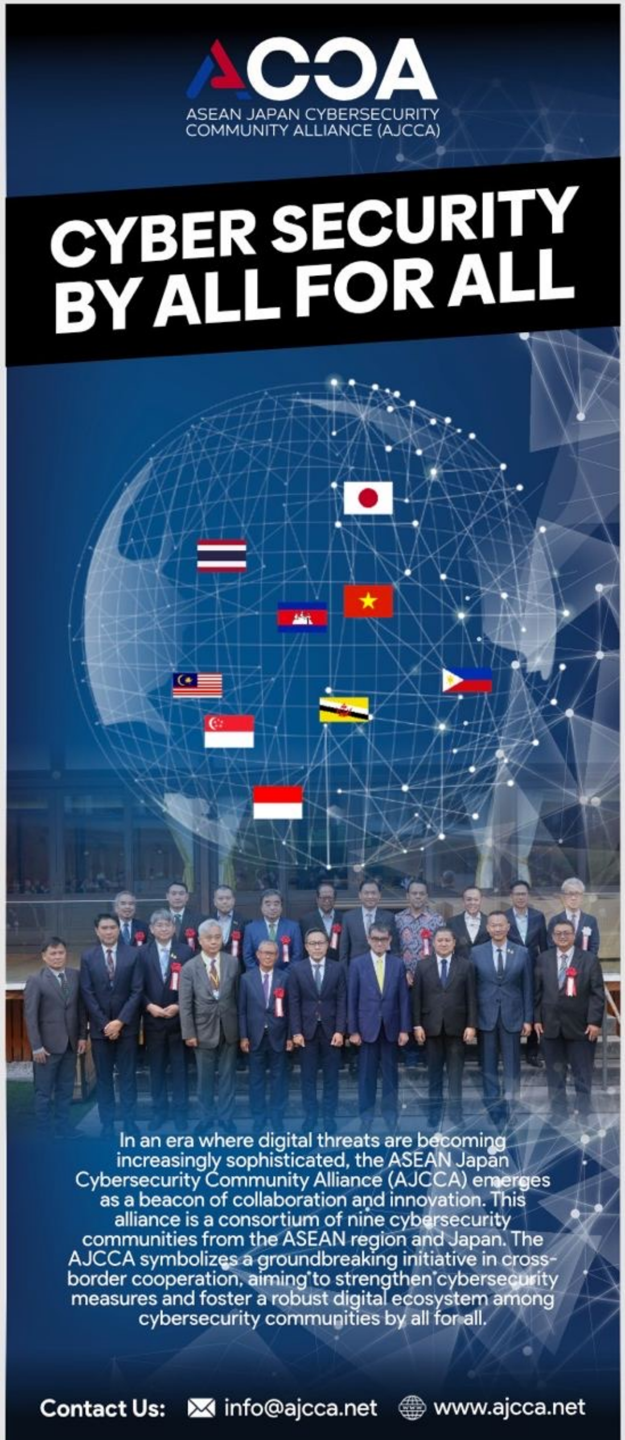
Barrack Obama

- What makes cyber security difficult is because it's not just a government problem. It is a private sector and government problem. And there's got to be a lot more cooperation

- Safety and security don’t just happen, **they are the result of collective consensus and public investment**.
- We owe our children, the most vulnerable citizens in our society, a life free of violence and fear

Public Private Cooperation and Cybersecurity Ecosystem

https://ajcca.net/form/arAPI



ASEAN JAPAN CYBERSECURITY COMMUNITY ALLIANCE (AJCCA)

CYBER SECURITY BY ALL FOR ALL

In an era where digital threats are becoming increasingly sophisticated, the ASEAN Japan Cybersecurity Community Alliance (AJCCA) emerges as a beacon of collaboration and innovation. This alliance is a consortium of nine cybersecurity communities from the ASEAN region and Japan. The AJCCA symbolizes a groundbreaking initiative in cross-border cooperation, aiming to strengthen cybersecurity measures and foster a robust digital ecosystem among cybersecurity communities by all for all.

Contact Us: ✉ info@ajcca.net 🌐 www.ajcca.net

Thank You

- info@ajcca.net

ASEAN JAPAN Security Working Group Meeting
Day 2 Session (9) Joint Government-Industry-Academia, 9:30-11:30

Minutes of Meeting

The Session started and opened by Mr Kato. He gave an introduction of Government Industry Academia program up to now included international conference on ASEAN Japan Cybersecurity Community which was held last year on October.

After finishing the explanation, he handed over the next turn to Mr Rudi as the chairman of AJCCA. Mr Rudi Explain the contents of his presentation: first is about AJCCA, second self-introduction of member of AJCCA and last is explanation the new report results by AJCCA on the public private cooperation in cybersecurity field.

In first part Mr Rudi explain about AJCCA profile. Its establishment on 5 October 2023, its nine-community member from ASEAN Countries and the community member selection criteria. Community criteria are 1. They have their own community or member to server, 2. They have routine activities that they conduct monthly or at least annually, 3. They are nonprofit and usually funded by them self or from sponsor, 4. They are independent from any intervention, 5. They may have already cooperation agreement with other international organization or communities and 6. They have the same understanding about the important of community role. He Explained also about AJCCA Vision, Mission and logo. The AJCCA vision is to become a dynamic and resilient cybersecurity community in our region through trustworthy and respectful collaboration. The AJCCA missions are 1. Facilitate Exchanges Among Organizations, 2. Exchange Information on Cyber Threats for better cyber resilience. 3. Improve and Enhance Sustainable Cybersecurity Capacity. The most important things, Mr Rudi also explained about AJCCA article of organization, its activities and this year calendar activities.

In second part Mr Rudi introducing its member and asked them to do self-introduction of each: There are nine member introductions from BCSA (Brunei Cyber Security Association), ISAC-Cambodia, IdNSA from Indonesia, JNSA from Japan, rawSEC from Malaysia, Philippine CERT or PhCERT from Phillippine, AiSP from Singapore, TISA from Thailand and VNISA from Vietnam.

In third part Mr Rudi explained new result of AJCCA survey about public partnership or cooperation - community report. The background of the survey, objectives, focus area and expected output. The objectives are to assess the level of current cooperation and level satisfaction, to identify areas of improvement and to gather feedback on current initiatives. Mr Rudi explained that by look at the result of this survey we can get valuable insight, identify some areas to improve and strengthen the cooperation between public and private. This will be very useful reference for those who are seeking and want to improve this partnership.

after his explanation, Mr Rudi gave time to the floor to discuss regarding the topic and findings. There are some questions arose to strengthen the finding and also open new program for collaboration between public and private. After the discussion, Mr Rudi closed his turn and handed over back to Mr Kato. Mr Kato then closed the session.

サイバーセキュリティ関連情報リンク集

（第 1.0 版）

2016 年　6 月　24 日

一般社団法人情報通信ネットワーク産業協会

通信ネットワーク機器セキュリティ分科会

１．まえがき

通信ネットワーク機器セキュリティ分科会では、CIAJ 内でセキュリティに対して専門的な検討を行う組織として、会員に対してサイバーセキュリティ情報の提供を行うべく検討を行っています。本資料は、サイバーセキュリティ情報として有益な情報を入手することができるHP(Home Page)について表形式にまとめました。これらの HP へのアクセスにより、各種のセキュリティ関連情報が得られると同時に警報やインシデントの発生についても知ることができます。定期的なセキュリティ情報の収集のためにも有効に活用をお願いします。

2. サイバーセキュリティー関連情報

区分	No	項目	内容	HP アドレス
政府省庁 関連機関	1	内閣官房 内閣サイバーセキュリティセンター(NISC)	・ 内閣サイバーセキュリティセンターの活動報告・情報分析 ・ サイバーセキュリティ政策に関する計画立案 ・ サイバーセキュリティ技術動向等の調査・研究分析 ・ サイバー攻撃等に関する最新情報の収集・集約 ・ 標的型メール及び不正プログラムの分析 ・ その他サイバー攻撃事案の調査分析 ・ 広報啓発活動：みんなでしっかりサイバーセキュリティ	http://www.nisc.go.jp/
	2	総務省 国民のための情報セキュリティサイト	・ インターネットと情報セキュリティの知識習得、利用方法に応じた情報セキュリティ対策を講じるための基本情報を提供 ・ 一般利用者のセキュリティ対策と企業・組織の対策をそれぞれ分けて提示	http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.html
	3	経済産業省 情報･セキュリティ政策 HP	・ 経産省 商務情報政策局 情報セキュリティ政策室による情報セキュリティ政策情報 ・ 政策・制度中心だが、脆弱性情報を含む	http://www.meti.go.jp/policy/netsecurity/
	4	警察庁@police	・ 警察庁によるインターネット定点観測データ、セキュリティ啓発情報を含む ・ 子供向け、一般 PC ユーザ向け、システム管理者向けに分けて学習情報を掲載 ・ PC やスマホの各種ソフトのアップデート情報	http://www.npa.go.jp/cyberpolice/index.html https://www.npa.go.jp/cyberpolice/detect/observation.html
	5	IPA ((独)情報処理推進機構)	・ IPA セキュリティセンター、サイバー情報共有イニシアティブ（J-CSIP、サイバーレスキュー隊 J-CRAT 等による具体的なセキュリティ対策活動 ・ 各種セキュリティ関連情報提供 ・ セミナー開催等によるセキュリティ対策啓蒙・普及活動等の実施	https://www.ipa.go.jp/
	6	NICT ((国研)情報通信研究機構)	・ サイバー攻撃に対する早期発見、分析、防御、侵入感知に関するサイバーセキュリティ技術の研究 ・ サイバー攻撃対策総合研究センター（CYREC：サイレック）：標的型攻撃等の新たなサイバー攻撃の抜本的な解決を目指す ・ インシデント分析センター nicter：サイバー攻撃を実時間で高精度に分析	http://www.nict.go.jp/research/cyber-security.html http://nict.go.jp/cyrec/ http://www.nict.go.jp/info/event/2012/06/120605_interop08.html

区分	No	項目	内容	HP アドレス
海外機関･サイト	1	NIST （米国国立標準技術研究所）	・ NIST「重要インフラのサイバーセキュリティを向上させるためのフレームワーク」 1.0 版 ・ 他にも米国 NIST の関連情報を IPAHP 内に掲載	http://www.nist.gov/ https://www.ipa.go.jp/security/publications/nist/ https://www.ipa.go.jp/files/000038957.pdf
	2	ITU-T SG17 （ITU 電気通信標準化部門）	・ 情報セキュリティ関連標準化（SG17）動向	http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/default.aspx
	3	ISO/IEC JTC1 SC27	・ ISO（国際標準化機構）、IEC（国際電気標準化会議）の JTC1（第１合同委員会）SC27 によるセキュリティ標準化情報	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45306
	4	Internet Storm Center Dshield	・ インターネット定点観測データ	https://www.dshield.org/port.html
	5	SecurityFocus	・ 海外ニュース等、ソフトのアップデート情報、セキュリティイベント情報	http://www.securityfocus.com/
国内 民間団体	1	JPCERT/CC （(一社)JPCERT ｺｰﾃﾞｨﾈｰｼｮﾝｾﾝﾀｰ）	・ JPCERT/CC: Japan Computer Emergency Response Team Coordination Center ・ セキュリティ注意情報・早期警戒、脆弱性対策 ・ インターネット定点観測 ・ コンピュータセキュリティの情報を収集し、インシデント対応の支援、コンピュータセキュリティ関連情報の発信	https://www.jpcert.or.jp/
	2	CSIRT （日本シーサート協議会）	・ CSIRT: Computer Security Incident Response Team ・ インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定等実施 ・ 配下に１３の WG を設置	http://www.nca.gr.jp/
	3	産業競争力懇談会（COCN）	・ 安全・安心・快適を実現する空間ソリューション ・ アグリ・イノベーション・コンプレックスの構築 ・ 安定な未利用エネルギーによる水素社会の実現 ・ ３次元位置情報を用いたサービスと共通基盤整備 ・ IoT 時代におけるプライバシーとイノベーションの両立 ・ IoT、CPS を活用したスマート建設生産システム	http://www.cocn.jp/report.html
国内 企業サイト	1	Kaspersky Lab	・ 2016 年のサイバーセキュリティ動向予測 ・ ウィルスニュース、マルウェア・スパム情報	http://www.kaspersky.co.jp/about/news/virus/2015/vir10122015
	2	トレンドマイクロ	・ 2016 年のサイバーセキュリティ動向予測	http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20151208083916.html
	3	Symantec	・ マルウェア、セキュリティリスク、脆弱性、スパム等の情報	http://www.symantec.com/ja/jp/security_response/
	4	Intel Security (McAfee)	・ 脅威情報，マルウェア情報	http://www.mcafee.com/jp/threat-center.aspx
	5	Security NEXT	・ サイバーセキュリティの日刊ニュース ・ 政府・業界動向、マイナンバー関連情報、セキュリティメルマガ	http://www.security-next.com/category/cat179
	6	ScanNetSecurity	・ 海外ニュース、中国動向、教委・脆弱性情報等	http://scan.netsecurity.ne.jp/