กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม

ETDA

THAILAND CYBERSECURITY **CHALLENGES AND RISK ASPECTS**

Thursday 27th January 2022 | 15.00 – 16.30
at Bangkok Marriott Marquis Queen's Park

1st Executive Education Certificate Program in Cybersecurity

DR.CHAICHANA MITRPANT

Executive Director of the Electronic Transactions Development Agency

Educations:

- PhD in Engineering from the Universitaet DuisburgEssen (Germany)
- MS in Electrical Engineering from the University of Michigan (US)
- BS in Electrical Engineering from Rice University (US).

Dr. Chaichana Mitrpant is currently the Executive Director of the Electronic Transactions Development Agency, Ministry of Digital Economy and Society of Thailand, a primary government agency responsible for developing, promoting, and supporting electronic transactions in Thailand.

During his tenure at ETDA, he has represented Thailand at various international fora and helped negotiate successful collaborations and bilateral meetings at ASEAN, APT, ITU, and the UN. Additionally, he has provided his expert opinions and recommendations to other organizations on numerous occasions.

AGENDA

15.00 – 15.10	Background
	The overview of ETDA and Cybersecurity Authority in Thailand
15.10 – 15.20	Challenges
	ASEAN’s and Thailand cybersecurity challenges based on international reports
15.20 – 15.30	Risk Aspects
	Cybersecurity incidents and financial-related risks
15.30 – 15.40	Way Forward
15.40 – 15.50	Wrap Up
15.50 – 16.20	Interactive Session
	The conduct of N-CERT Service Area Survey, the distribution of E-book collection, and the display Cybersecurity Microlearning Campaign
16.20 – 16.25	Summary
16.25 – 16.30	Q&A

Agenda can be adjusted as appropriate

BACKGROUND

ETDA introduction

ETDA'S AUTHORITY

- Facilitate and expand economic opportunities, build careers and raise incomes towards THAILAND Digital Economy and Society Development
- Building readiness and interoperability by drawing the landscape of critical digital services and standards for service providers
- Improve laws regularly and provide standard
- Regulate digital service businesses
- Create successful opportunities in global online markets
- Encourage more people to become informed citizens

ETDA'S MISSIONS

are to regulate and recommend the standard related to e-transactions. The purpose of the missions is for a secured, concordant,
and trustful environment for all stakeholders

BACKGROUND

EDTA's Other tasks

DIGITALSOCIETY INTERNET FOR A BETTER LIFE

Raised awareness of appropriate and secure digital technology usage for over **5,000** children, young adults and elders

SUPPORT "THAILAND E-COMMERCE SUSTAINABILITY"

Cooperating with leading e-Marketplace to increase trade channels for SMEs Comprehensive professional knowledge & tip sharing Foster knowledge through online learning platform

ONLINE COMPLAINT CENTER (OCC) 1212 SERVICE

hotline phone 1212,
e-mail 1212@mdes.go.th,
and website www.1212occ.com
(Handled over 19,168 cases: during 1st October 2020 – 31st March 2021)

SURVEY IMPORTANT STATISTICS

The value of e-Commerce increased from **USD 0.11 trillion in 2020 to USD 0.12 trillion in 2021**. The estimated growth rate during 2020-2021 was **6.11** percent, and **Thailand ranked #1** in ASEAN of B2C e-Commerce.

BACKGROUND

Cybersecurity Authority in Thailand - The roles and responsibilities of the Authority on cybersecurity

CYBERSECURITY AUTHORITY

- National Security Council
- National Cybersecurity Committee
- Ministry of Digital Economy and Society: MDES
- National Cybersecurity Agency: NCSA
- Cybercrime Investigation Bureau (CCIB)
- National Intelligence Agency (NIA)

NATIONAL SECURITY COUNCIL

- Issue national security policies including cybersecurity
  (National Security Policy 2015-2021)

NATIONAL CYBERSECURITY COMMITTEE

- Draft a National Cybersecurity Policy/Plan
- Cooperate with other national committees and agencies in
  drafting and enforcing the Policy/Plan
- Oversee national cybersecurity performance
- Oversee the National Cybersecurity Agency

MINISTRY OF DIGITAL ECONOMY AND SOCIETY: MDES

- Developing and planning digital economy
- Providing policy government coordination
- Overseeing ETDA/ThaiCERT
- Supporting the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC)

NATIONAL CYBERSECURITY AGENCY: NCSA

- Suggesting policies, strategic plans, and improving cybersecurity laws, including studying and researching, setting guidelines, standards, and related measures under current and future situations.
- Supervise, monitor, monitor, analyze, process, alert and take action to prevent, cope with and mitigate cyber threats.
- Be the centre for coordination, including promoting, supporting and helping government and private sectors both in the nation and overseas to maintain cybersecurity
- Disseminate knowledge and understanding and support the development of cybersecurity personnel

Source: ASEAN-Japan Cybersecurity Reference 2021 TLP:GREEN

BACKGROUND

NATIONAL CSIRT

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

1. Organizational structure of the Government CSIRT

Thailand Computer Emergency Response Team: ThaiCERT

ThaiCERT is a cybersecurity incident response organization under the Electronic Transaction Development Agency (ETDA), Ministry of Digital Economy and Society. It coordinates and cooperates with other domestic sector-based CSIRTs and international CSIRTs. ThaiCERT is a member of regional and global computer emergency response networks including FIRST and APCERT.(https://www.thaicert.or.th/about-en.html)

Roles and responsibilities;

- Incident Coordination
- Threat Intelligence
- Incident Response
- Digital Forensic
- Human Resource Development
- Awareness Raising Activities
- etc.

2. Framework/relationship between CSIRTs

ThaiCERT As a national and Government CSIRT, ThaiCERT coordinates and cooperates with CSIRTs, sector-based CSIRTs and cybersecurity specialist teams in both public and private sectors on a voluntary basis.

BACKGROUND

LAWS AND REGULATIONS

1. Cybersecurity Act

- **National Cybersecurity Act B.E. 2562 (2019)**
- Protect national critical information infrastructure and respond to cyber threats effectively.

2. Criminals related to unauthorized access, creation of virus and sending spam, etc.

- **Computer-Related Crime Act B.E. 2550 (2007)**
- **Computer-Related Crime Act (No.2) B.E. 2560 (2017)**
- Enforce law on unauthorized access, computer misuse, and other computer-related offences.

3. E-signature / Electronic authentication platform

- **Electronic Transactions Act B.E. 2544 (2001)**
- Promote e-transactions
- Enhance trust of electronic information systems
- Provide legal recognition of e-transaction and e-signature
- Supervise e-transaction service providers
- **Electronic Transactions Act (No.2) B.E. 2551 (2008)**
- Transition of paper-based document to electronic documents and vice versa
- **Electronic Transactions Act (No.3) B.E. 2562 (2019)**
- Adoption of selected principles from e-communication convention such as invitation to make offers, use of automated manage systems for contract formation and error in electronic communication.
- **Electronic Transactions Act (No.4) B.E. 2562 (2019)**
- Provide legal recognition of digital identification (Digital ID)

4.Privacy protections

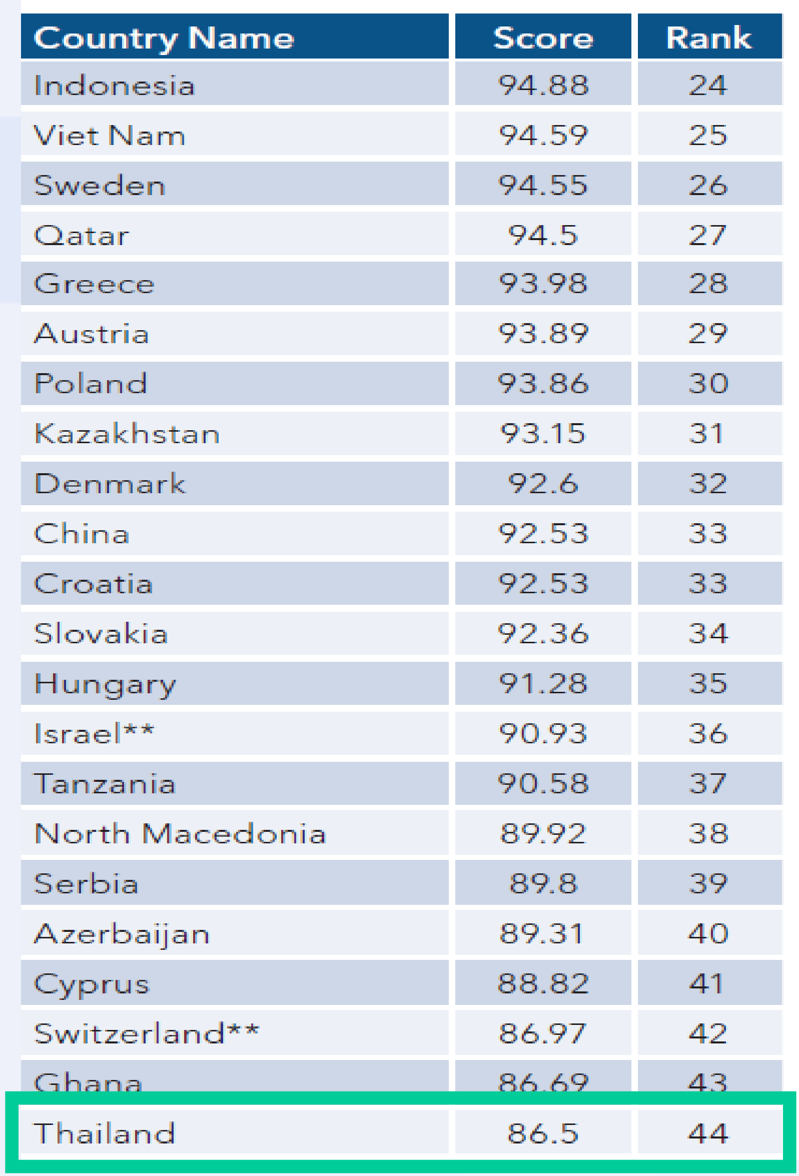
- **Personal Data Protection Act B.E. 2562 (2019)**
- Protect personal data.

5.Other cybersecurity relevant laws the Authority covering

- https://ictlawcenter.etda.or.th/laws (in Thai only)

CHALLENGES

ITU Global Cybersecurity Index 2020

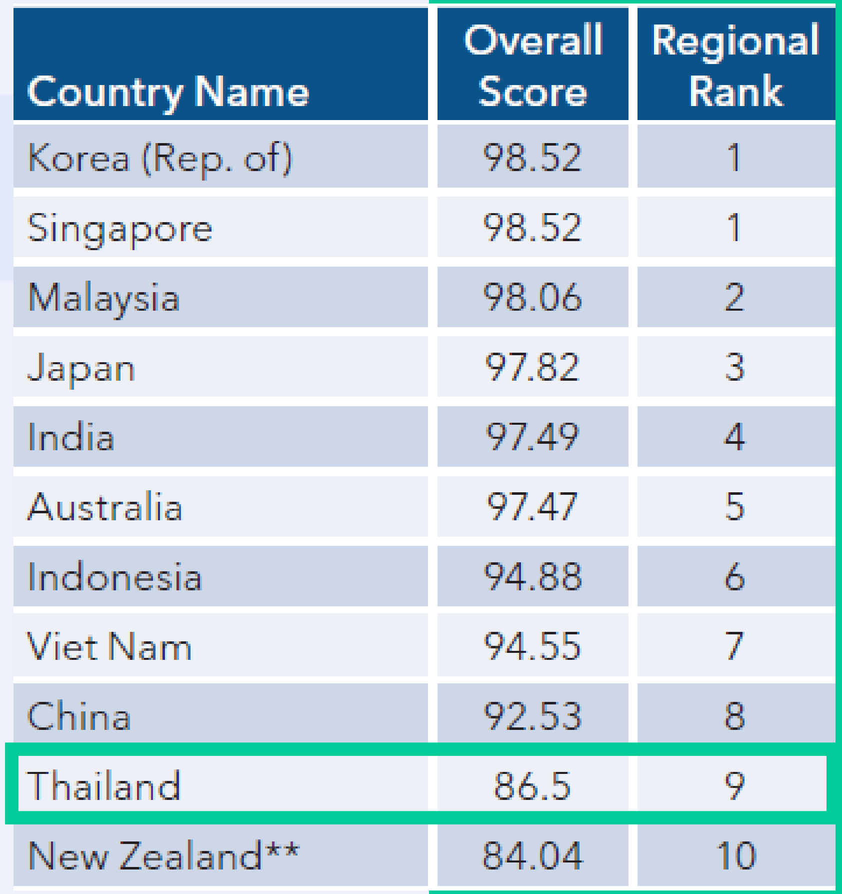


Country Name	Score	Rank
Indonesia	94.88	24
Viet Nam	94.59	25
Sweden	94.55	26
Qatar	94.5	27
Greece	93.98	28
Austria	93.89	29
Poland	93.86	30
Kazakhstan	93.15	31
Denmark	92.6	32
China	92.53	33
Croatia	92.53	33
Slovakia	92.36	34
Hungary	91.28	35
Israel**	90.93	36
Tanzania	90.58	37
North Macedonia	89.92	38
Serbia	89.8	39
Azerbaijan	89.31	40
Cyprus	88.82	41
Switzerland**	86.97	42
Ghana	86.69	43
Thailand	86.5	44

Source: ITU Global Cybersecurity Index 2020

- **The Global Cybersecurity Index (GCI)** was first launched in 2015 by the International Telecommunication Union (ITU) to measure the commitment of **193 ITU Member States** and the State of Palestine to cybersecurity to help them identify areas of improvement and encourage countries to take action, through raising awareness on the state of cybersecurity worldwide.

- **Global Scores and Ranking of Thailand:** Thailand is **ranked 44** out of **194** ITU Member States with the score of 86.50/100



Country Name	Overall Score	Regional Rank
Korea (Rep. of)	98.52	1
Singapore	98.52	1
Malaysia	98.06	2
Japan	97.82	3
India	97.49	4
Australia	97.47	5
Indonesia	94.88	6
Viet Nam	94.55	7
China	92.53	8
Thailand	86.5	9
New Zealand**	84.04	10

Source: ITU Global Cybersecurity Index 2020

CHALLENGES

ITU Global Cybersecurity Index 2020

- While being ranked at 44 place worldwide, in ASIA-Pacific region, Thailand's place and score is among the top ten, being ninth place.
- To scope further, Thailand's place in ASEAN region is at the fifth after Singapore, Malaysia, Indonesia, and Vietnam, respectively

CHALLENGES

ITU Global Cybersecurity Index 2020

- Thailand is classified as a **Developing Country** in terms of Development Level.
- The Area of Relative **Strength** for Thailand is **Legal Measures** and of **Potential Growth** is **Technical Measures**
- The overall score of Thailand is 86.50, which can be elaborated into five categories with detailed scores:

19.11 1. **Legal Measures**: Measuring the laws and regulations on cybercrime and cybersecurity

15.57 2. **Technical Measures**: Measuring the implementation of technical capabilities through national and sector-specific agencies

17.64 3. **Organization Measures**: Measuring the national strategies and organizations implementing cybersecurity

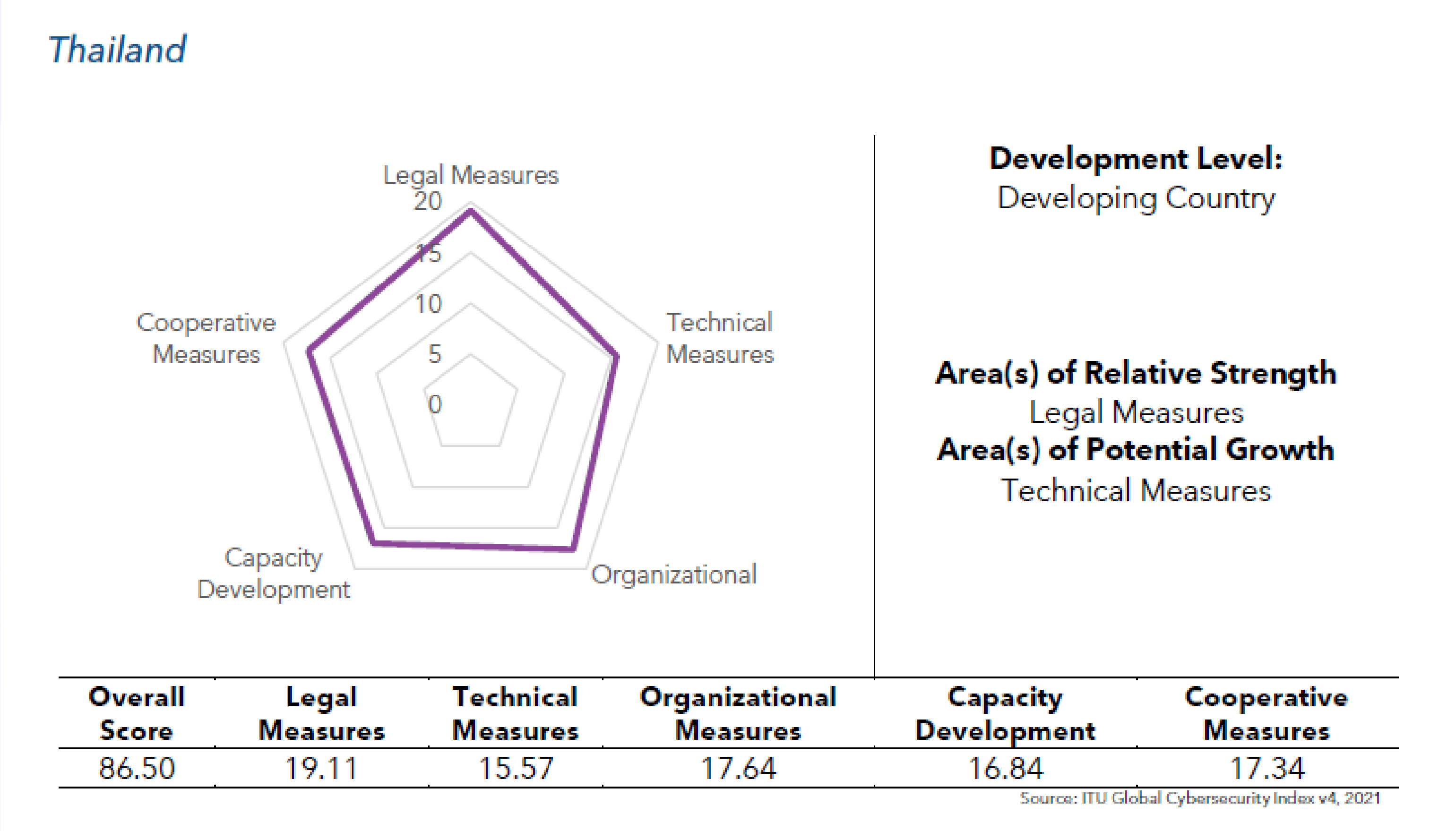
16.84 4. **Capacity Development**: Measuring awareness campaigns, training, education, and incentives for cybersecurity capacity development

17.34 5. **Cooperative Measures:** Measuring partnerships between agencies, firms, and countries

Source: ITU Global Cybersecurity Index 2020

CHALLENGES

ITU Global Cybersecurity Index 2020



Thailand

Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
86.50	19.11	15.57	17.64	16.84	17.34

Source: ITU Global Cybersecurity Index v4, 2021

ITUPublications

International Telecommunication Union
Development Sector

Global Cybersecurity Index
2020

Source: ITU Global Cybersecurity Index 2020

CHALLENGES

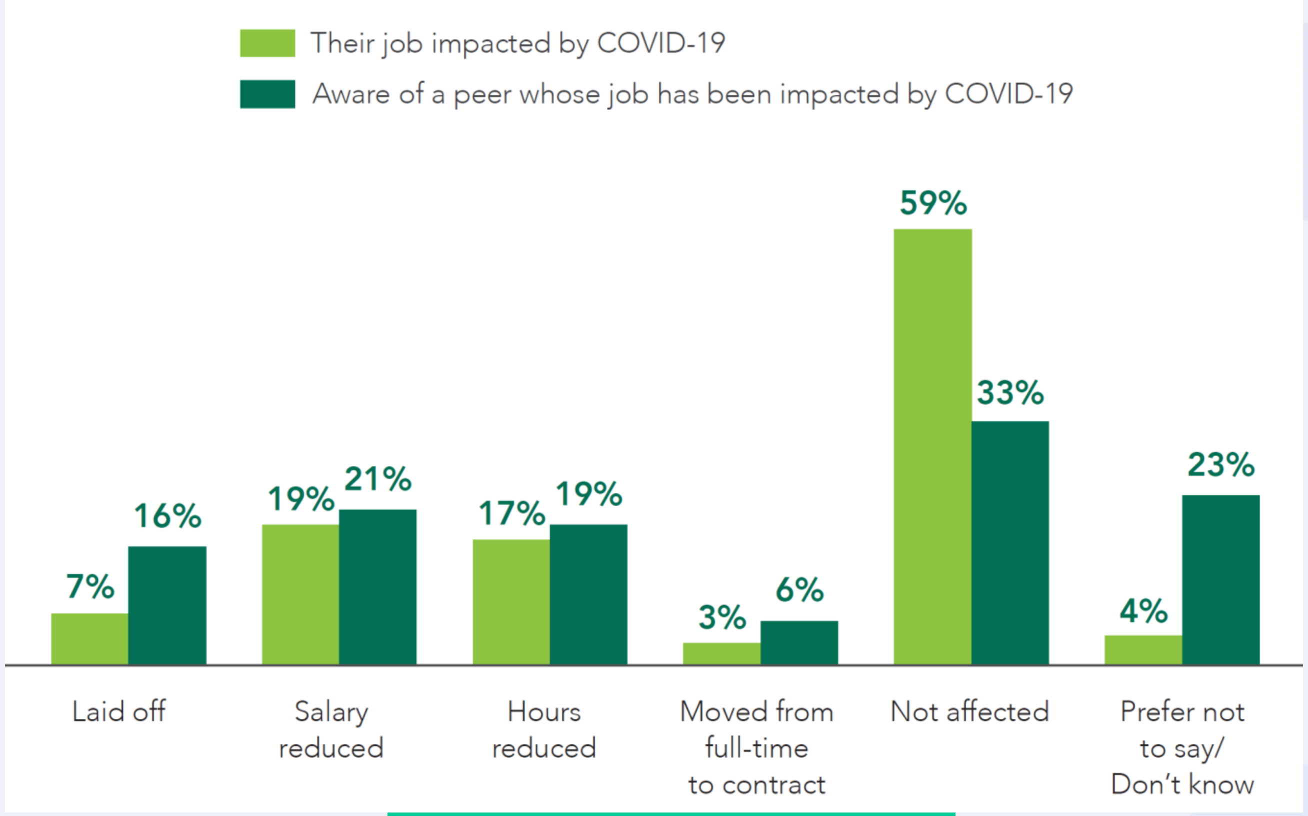
(ISC)² Cybersecurity Workforce Shortage 2020

COVID-19's Impact on Cybersecurity Jobs

- The majority of cybersecurity experts report that their jobs haven't been affected, but others say their hours, salaries, or full-time status have been impacted.
- **17%** of respondents report that their hours have been shortened as a result of the pandemic, while 19% encounter the salary reduction.

Cybersecurity Professionals Stand Up to a Pandemic

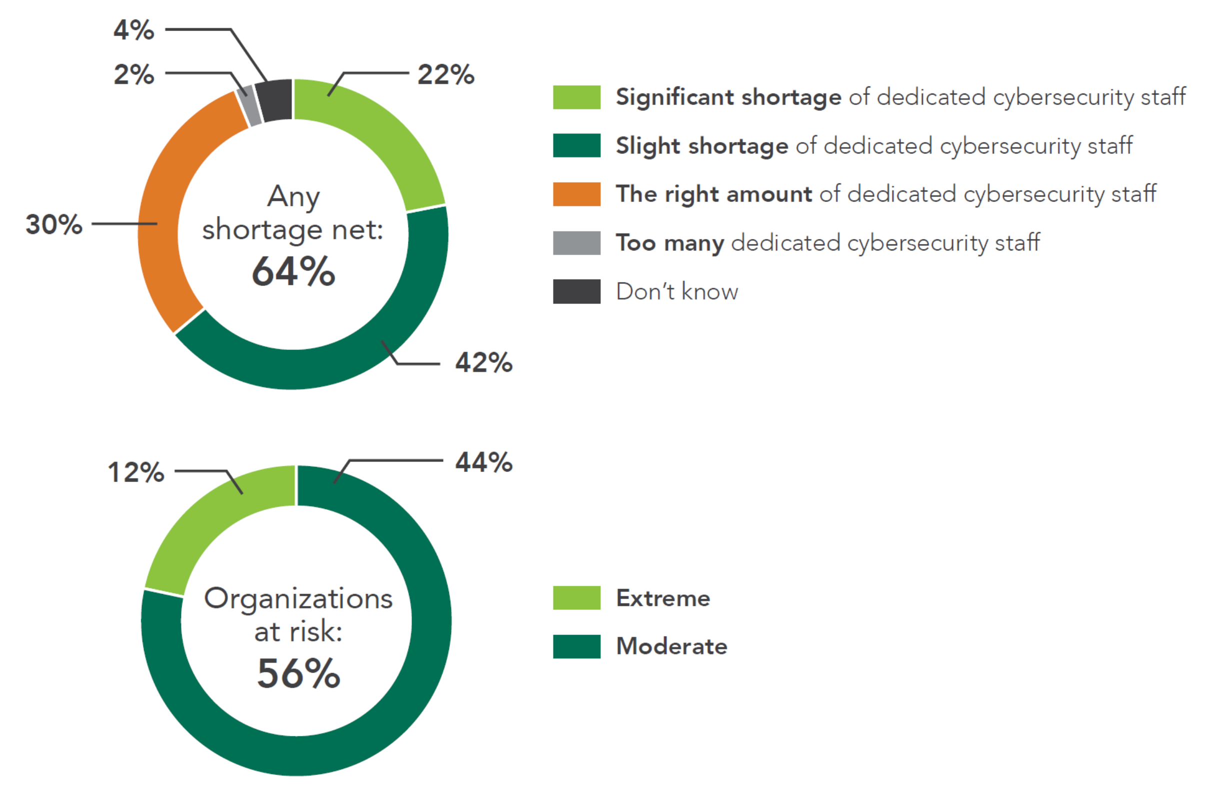
(ISC)² CYBERSECURITY WORKFORCE STUDY, 2020



Source: (ISC)² Cybersecurity Workforce Shortage 2020

CHALLENGES

(ISC)² Cybersecurity Workforce Shortage 2020



64% Shortage net

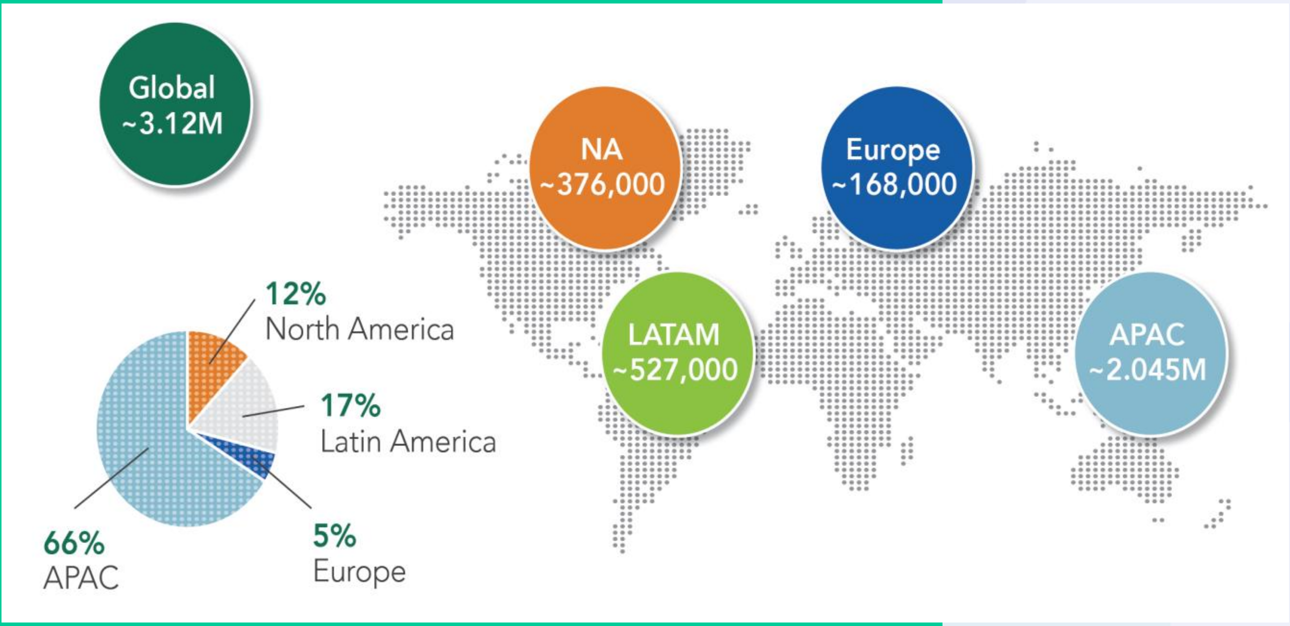
CYBERSECURITY STAFFING LEVELS AND SECURITY RISKS

- **Nearly half of the cybersecurity** professionals report that the staff shortage at their own organizations is still slight, while 30% has sufficient cybersecurity staff at work.
- More than half of respondents (56%) raise their concern that cybersecurity staff shortages are putting their organization at risk.

Source: (ISC)² Cybersecurity Workforce Shortage 2020

CHALLENGES

(ISC)² Cybersecurity Workforce Shortage 2020



THE CYBERSECURITY WORKFORCE GAP BY REGION

- In comparison to past years, the difference between the number of competent professionals required to protect critical assets and the actual capacity available to do so has narrowed significantly in 2020.
- The global cybersecurity gap shrank from **4 million** in 2019 to **3.1 million** in 2020.
- The global cybersecurity workforce gap varies by region, with the Asia-Pacific area having a widest gap of more than 2 million.

Source: (ISC)² Cybersecurity Workforce Shortage 2020

CHALLENGES

GFCE CSIRTs In Low Income Countries 2022 – National CERT (N-CSIRT) SERVICE ROADMAP

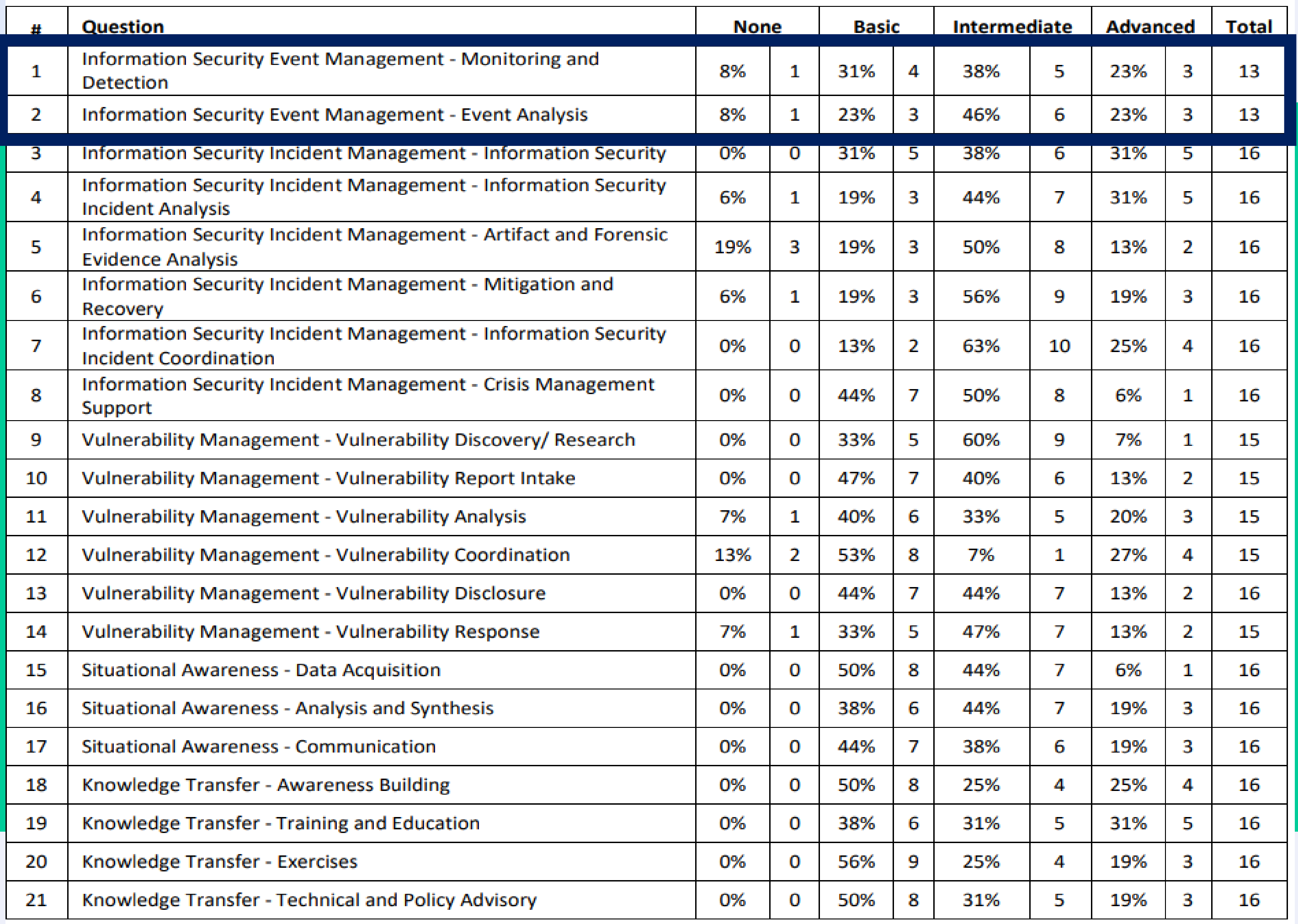
The Global Forum on Cyber Expertise (**GFCE**)'s research team conducted surveys with 16 N-CSIRTs in low-income or developing countries to better understand the technical and organizational aspects of N-CSIRT services and sufficiently grasp the needs of the corresponding countries. In these surveys and follow-up semi-structured interviews with three of these N-CSIRTs, we explored which services those CSIRTs deliver, what type of technical and organizational capabilities they have, their medium and long-term goals, and their best practices in capacity building

CSIRT Services Framework classifies CSIRT services into five areas,

1. Information Security Event Management (ISEM),
2. Information Security Incident Management (ISIM),
3. Vulnerability Management (VM),
4. Situational Awareness (SA), and
5. Knowledge Transfer (KT).

Source:
FIRST is the global Forum of Incident Response and Security Teams
NIST 800-181 Rev. 1 Workforce Framework for Cybersecurity (NICE Framework)
CSIRT Services Competencies https://bit.ly/348BEii

CHALLENGES Current CSIRT Service Offerings

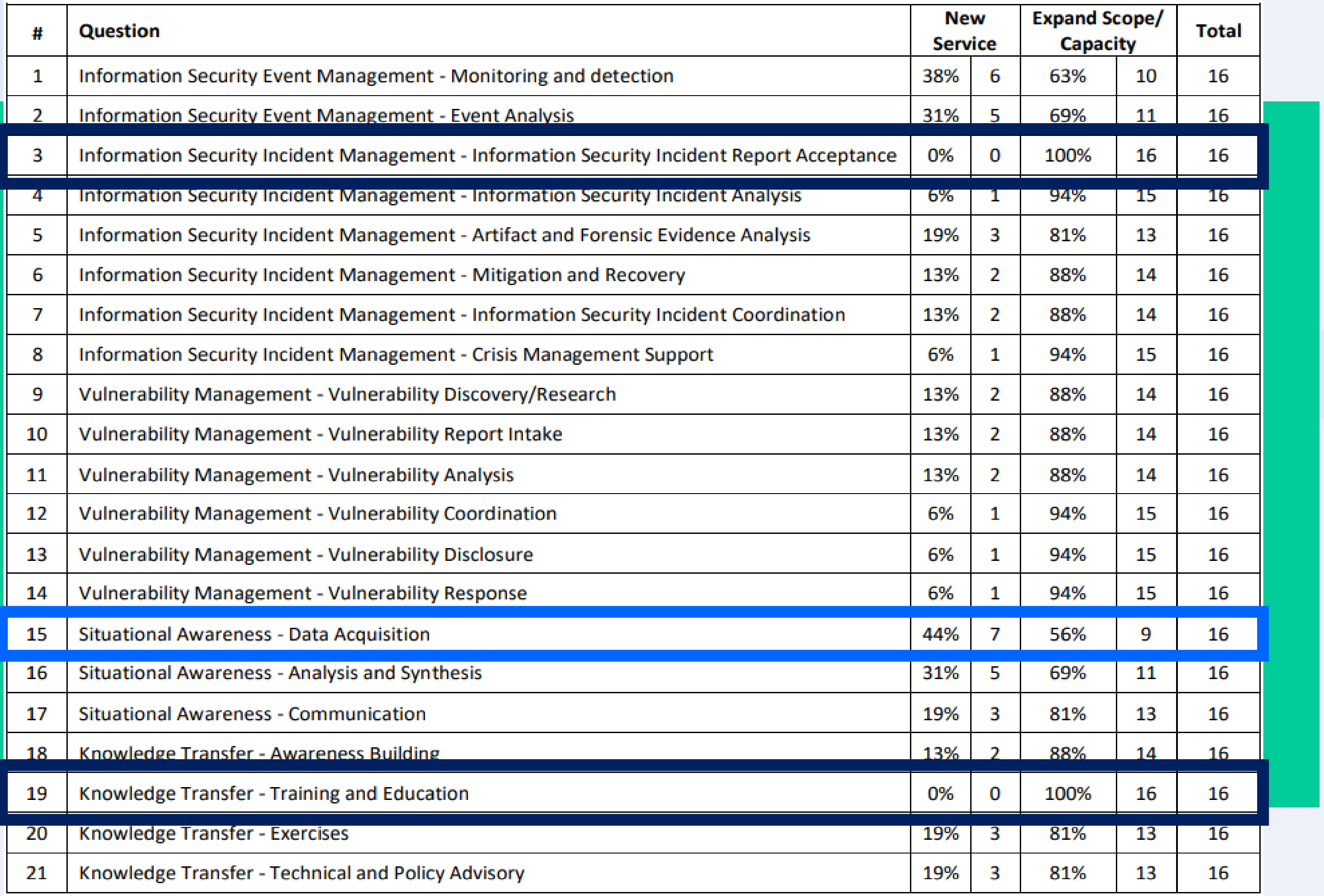


#	Question	None		Basic		Intermediate		Advanced		Total
1	Information Security Event Management - Monitoring and Detection	8%	1	31%	4	38%	5	23%	3	13
2	Information Security Event Management - Event Analysis	8%	1	23%	3	46%	6	23%	3	13
3	Information Security Incident Management - Information Security	0%	0	31%	5	38%	6	31%	5	16
4	Information Security Incident Management - Information Security Incident Analysis	6%	1	19%	3	44%	7	31%	5	16
5	Information Security Incident Management - Artifact and Forensic Evidence Analysis	19%	3	19%	3	50%	8	13%	2	16
6	Information Security Incident Management - Mitigation and Recovery	6%	1	19%	3	56%	9	19%	3	16
7	Information Security Incident Management - Information Security Incident Coordination	0%	0	13%	2	63%	10	25%	4	16
8	Information Security Incident Management - Crisis Management Support	0%	0	44%	7	50%	8	6%	1	16
9	Vulnerability Management - Vulnerability Discovery/ Research	0%	0	33%	5	60%	9	7%	1	15
10	Vulnerability Management - Vulnerability Report Intake	0%	0	47%	7	40%	6	13%	2	15
11	Vulnerability Management - Vulnerability Analysis	7%	1	40%	6	33%	5	20%	3	15
12	Vulnerability Management - Vulnerability Coordination	13%	2	53%	8	7%	1	27%	4	15
13	Vulnerability Management - Vulnerability Disclosure	0%	0	44%	7	44%	7	13%	2	16
14	Vulnerability Management - Vulnerability Response	7%	1	33%	5	47%	7	13%	2	15
15	Situational Awareness - Data Acquisition	0%	0	50%	8	44%	7	6%	1	16
16	Situational Awareness - Analysis and Synthesis	0%	0	38%	6	44%	7	19%	3	16
17	Situational Awareness - Communication	0%	0	44%	7	38%	6	19%	3	16
18	Knowledge Transfer - Awareness Building	0%	0	50%	8	25%	4	25%	4	16
19	Knowledge Transfer - Training and Education	0%	0	38%	6	31%	5	31%	5	16
20	Knowledge Transfer - Exercises	0%	0	56%	9	25%	4	19%	3	16
21	Knowledge Transfer - Technical and Policy Advisory	0%	0	50%	8	31%	5	19%	3	16

CSIRT has limited some services such as Monitoring and Detection, Event Analysis, etc.

The level of offered services (Basic, Intermediate and advanced) describes the maturity of each CSIRT.

CHALLENGES Services to Expand or Offer in Next 5 Years



#	Question	New Service		Expand Scope/ Capacity		Total
1	Information Security Event Management - Monitoring and detection	38%	6	63%	10	16
2	Information Security Event Management - Event Analysis	31%	5	69%	11	16
3	Information Security Incident Management - Information Security Incident Report Acceptance	0%	0	100%	16	16
4	Information Security Incident Management - Information Security Incident Analysis	6%	1	94%	15	16
5	Information Security Incident Management - Artifact and Forensic Evidence Analysis	19%	3	81%	13	16
6	Information Security Incident Management - Mitigation and Recovery	13%	2	88%	14	16
7	Information Security Incident Management - Information Security Incident Coordination	13%	2	88%	14	16
8	Information Security Incident Management - Crisis Management Support	6%	1	94%	15	16
9	Vulnerability Management - Vulnerability Discovery/Research	13%	2	88%	14	16
10	Vulnerability Management - Vulnerability Report Intake	13%	2	88%	14	16
11	Vulnerability Management - Vulnerability Analysis	13%	2	88%	14	16
12	Vulnerability Management - Vulnerability Coordination	6%	1	94%	15	16
13	Vulnerability Management - Vulnerability Disclosure	6%	1	94%	15	16
14	Vulnerability Management - Vulnerability Response	6%	1	94%	15	16
15	Situational Awareness - Data Acquisition	44%	7	56%	9	16
16	Situational Awareness - Analysis and Synthesis	31%	5	69%	11	16
17	Situational Awareness - Communication	19%	3	81%	13	16
18	Knowledge Transfer - Awareness Building	13%	2	88%	14	16
19	Knowledge Transfer - Training and Education	0%	0	100%	16	16
20	Knowledge Transfer - Exercises	19%	3	81%	13	16
21	Knowledge Transfer - Technical and Policy Advisory	19%	3	81%	13	16

Most CSIRTs are expanding their services in 5 years. The most expansion is Training and Education, and Information Security Incident Report Acceptance at **100%** Growth Rate.

Data Acquisition is the least expansion in CSIRT's responses at a **56%** growth rate.

New services provided by CSIRT are varied to achieve each N-CERT's requirements and goals.

RISK ASPECTS ThaiCERT Statistics 2021

ecsirt.net taxonomy	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total
Abusive Content	0	1	0	0	0	1	0	0	0	5	2	5	**14**
Availability	0	0	1	0	1	0	1	0	0	2	0	0	**5**
Fraud	46	20	26	16	27	16	13	10	9	13	9	7	**212**
Information Gathering	12	24	49	25	29	27	42	20	11	4	4	1	**248**
Information Security	4	5	0	0	2	2	0	2	9	3	1	2	**30**
Intrusion Attempts	21	15	25	20	14	5	6	4	2	4	13	95	**224**
Intrusions	32	27	29	8	15	15	11	14	11	14	4	3	**183**
Malicious Code	8	29	21	10	12	9	11	5	23	96	128	127	**479**
Vulnerability	31	5	121	64	81	94	77	75	35	31	25	35	**674**
Other	0	0	0	0	0	0	0	0	0	0	0	0	**0**
Total	**154**	**126**	**272**	**143**	**181**	**169**	**161**	**130**	**100**	**172**	**186**	**275**	**2069**

ThaiCERT collected incident statistics in 2021. The information uses ecsirt.net taxonomy in reporting, represents in month's period.

There were 2,069 incidents as follows:

1 Vulnerability
674 (32.6%)

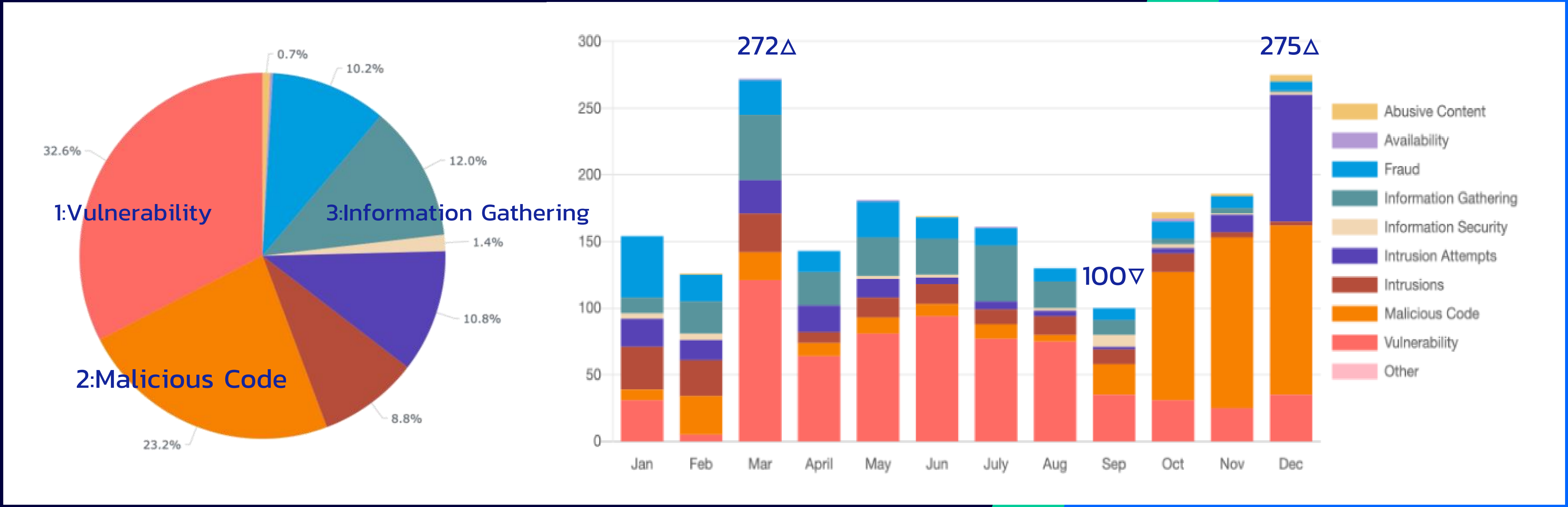
2 Malicious Code
479 (23.2%)

3 Information Gathering
248 (10.8%)

Source: https://www.thaicert.or.th/statistics/statistics.html

RISK ASPECTS ThaiCERT Statistics 2021

In 2021, the statistic showed many incidents in March and December with **272** and **275** cases, respectively. In September, there were 100 incidents at the lowest point of the year.

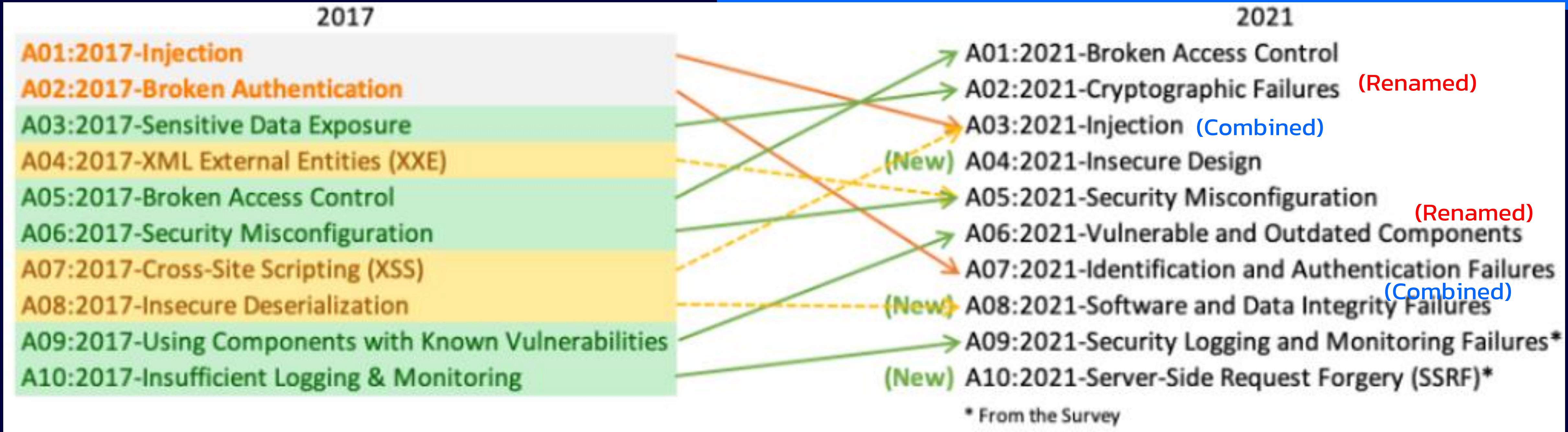


Source: https://www.thaicert.or.th/statistics/statistics.html

RISK ASPECTS

The Open Web Application Security Project (OWASP)

OWASP-TOP10 :2021



2017	2021
A01:2017-Injection	A01:2021-Broken Access Control
A02:2017-Broken Authentication	A02:2021-Cryptographic Failures (Renamed)
A03:2017-Sensitive Data Exposure	A03:2021-Injection (Combined)
A04:2017-XML External Entities (XXE)	(New) A04:2021-Insecure Design
A05:2017-Broken Access Control	A05:2021-Security Misconfiguration
A06:2017-Security Misconfiguration	(Renamed) A06:2021-Vulnerable and Outdated Components
A07:2017-Cross-Site Scripting (XSS)	A07:2021-Identification and Authentication Failures
A08:2017-Insecure Deserialization	(Combined) (New) A08:2021-Software and Data Integrity Failures
A09:2017-Using Components with Known Vulnerabilities	A09:2021-Security Logging and Monitoring Failures*
A10:2017-Insufficient Logging & Monitoring	(New) A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

Footnotes:

CVSS – The Common Vulnerability Scoring System (CVSS) is a system widely used. CVSS Scores provides a numerical (0-10) representation of the severity of an information security vulnerability

CVE – Common Vulnerabilities and Exposures (CVE) is a list of publicly disclosed vulnerabilities and exposures that is maintained by MITRE.

NVD – The National Vulnerability Database (NVD) is a database, maintained by NIST, that is fully synchronized with the MITRE CVE list.

RISK ASPECTS

OWASP-TOP10 :2021 : New positions

A04:2021-Insecure Design

is a new category for 2021, with a focus on risks related to design flaws. If we genuinely want to "move left" as an industry, we need more threat modeling, secure design patterns and principles, and reference architectures. An insecure design cannot be fixed by a perfect implementation as by definition, needed security controls were never created to defend against specific attacks

A08:2021-Software and Data Integrity Failures

is a new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWEs in this category. A8:2017-Insecure Deserialization is now a part of this larger category.

A10:2021-Server-Side Request Forgery

is added from the Top 10 community survey (#1). The data shows a relatively low incidence rate with above average testing coverage, along with above-average ratings for Exploit and Impact potential. This category represents the scenario where the security community members are telling us this is important, even though it's not illustrated in the data at this time.

Footnotes:
CVSS – The Common Vulnerability Scoring System (CVSS) is a system widely used. CVSS Scores provides a numerical (0-10) representation of the severity of an information security vulnerability
CVE – Common Vulnerabilities and Exposures (CVE) is a list of publicly disclosed vulnerabilities and exposures that is maintained by MITRE.
NVD – The National Vulnerability Database (NVD) is a database, maintained by NIST, that is fully synchronized with the MITRE CVE list.

RISK ASPECTS

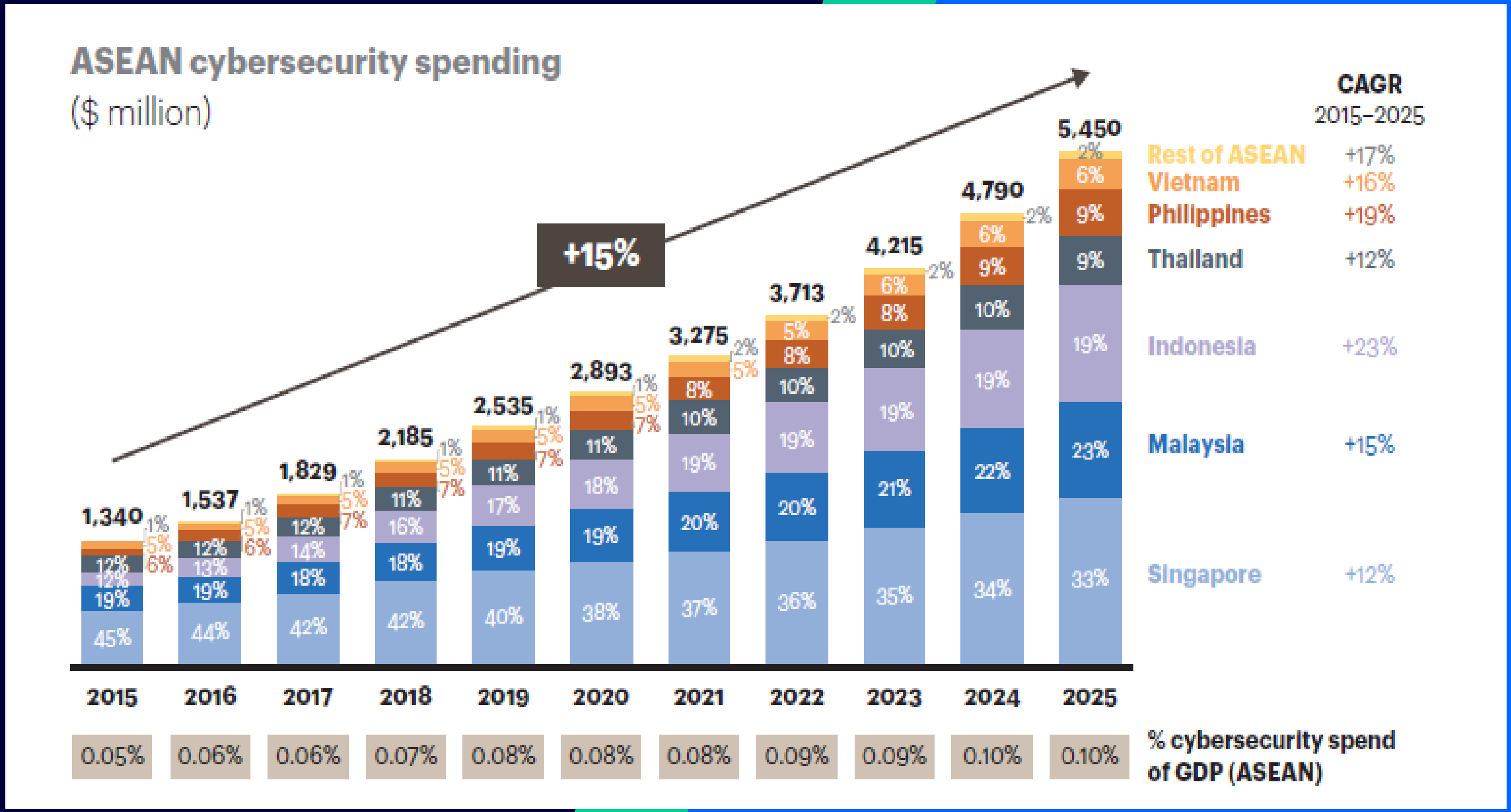
Cybersecurity Investment per GDP in ASEAN

- ASEAN's cybersecurity spend was estimated to be **$3.3 billion** in 2021, representing **0.08** percent of the region's GDP.

- The spend is forecasted to grow at 15 percent CAGR from 2015 to 2025 with **Singapore, Malaysia, and Indonesia** as a prime potential growth driver.

- The contribution to CAGR growth of Thailand from 2015 - 2025 will be approximately around **12%**, following Singapore, Malaysia, and Indonesia.

- Although the anticipated growth seems to be constantly increasing, most ASEAN countries **fall below** the global average, creating a **potential risk** of insufficient spend relative to a rapidly escalating threat landscape

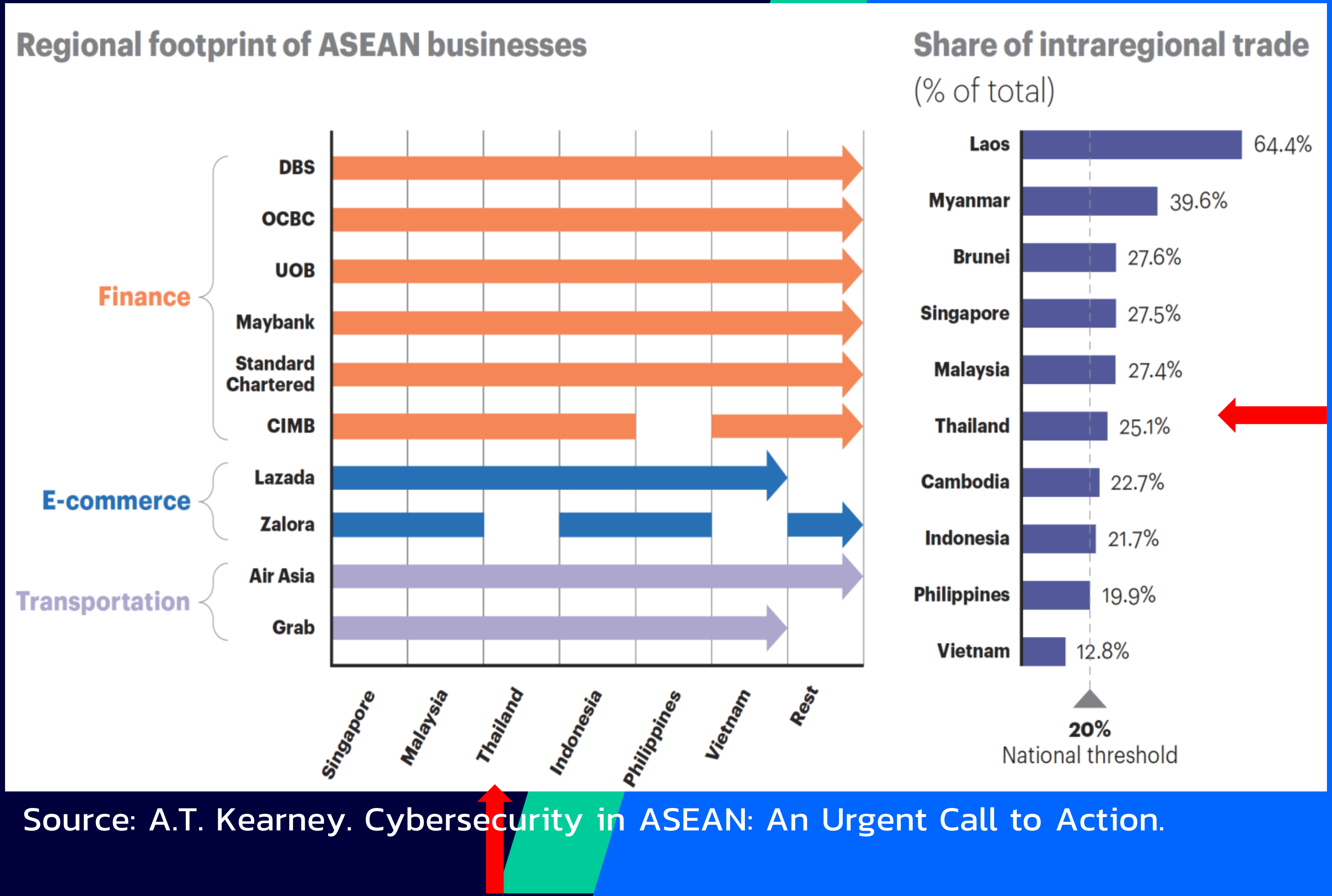


Source: A.T. Kearney. Cybersecurity in ASEAN: An Urgent Call to Action.

RISK ASPECTS

Region's developing intraregional trade and business linkages

- With the **region's developing intraregional trade and business linkages**, the potential of contagion in the event of cyberattacks among ASEAN countries is significant.
- Banks, e-commerce enterprises, and transportation corporations all have a **large** influence in the region.
- Intra-regional trade accounts for more than **20%** of total trade in **8 of the 10** ASEAN countries and intra-ASEAN investment has been continuously expanding over the year.
- Manufacturing, financial services, and real estate are among the **20 industries** with the largest proportion of intra-regional investment.



Source: A.T. Kearney. Cybersecurity in ASEAN: An Urgent Call to Action.

RISK ASPECTS

Correlation between digital maturity and cybersecurity spend

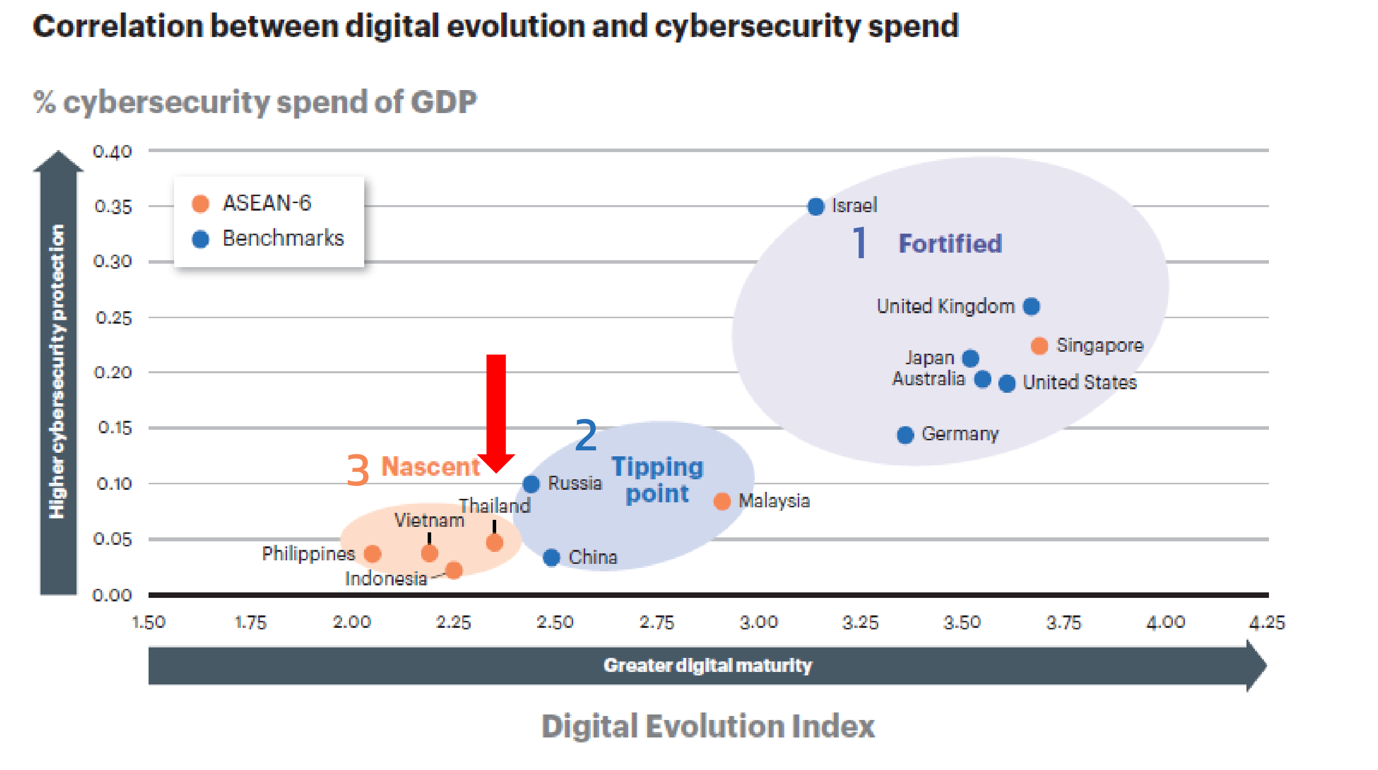
- **Digital Planet** analyst reports by **World Bank** suggested that there is a correlation between digital maturity and cybersecurity spend.

- Most nations are on a strong digital growth trajectory but without a commensurate increase in spend. Only **0.06** percent of the region's collective GDP are accounted for cybersecurity, which **is five time lower** than the relative proportion of world's top countries' GPD.

- It can be seen that the higher percentage cybersecurity spend there is , the higher digital maturity there will be.

- The **level of maturity** can be categorized into three different levels:
  1. Fortified
  2. Tipping Point
  3. Nascent (display signs of future potential)

- **Thailand** is on the Nascent level with many other ASEAN states, except for **Singapore** which is in Fortified and **Brunei** in Tipping Point levels.



Correlation between digital evolution and cybersecurity spend

Source: A.T. Kearney. Cybersecurity in ASEAN: An Urgent Call to Action.

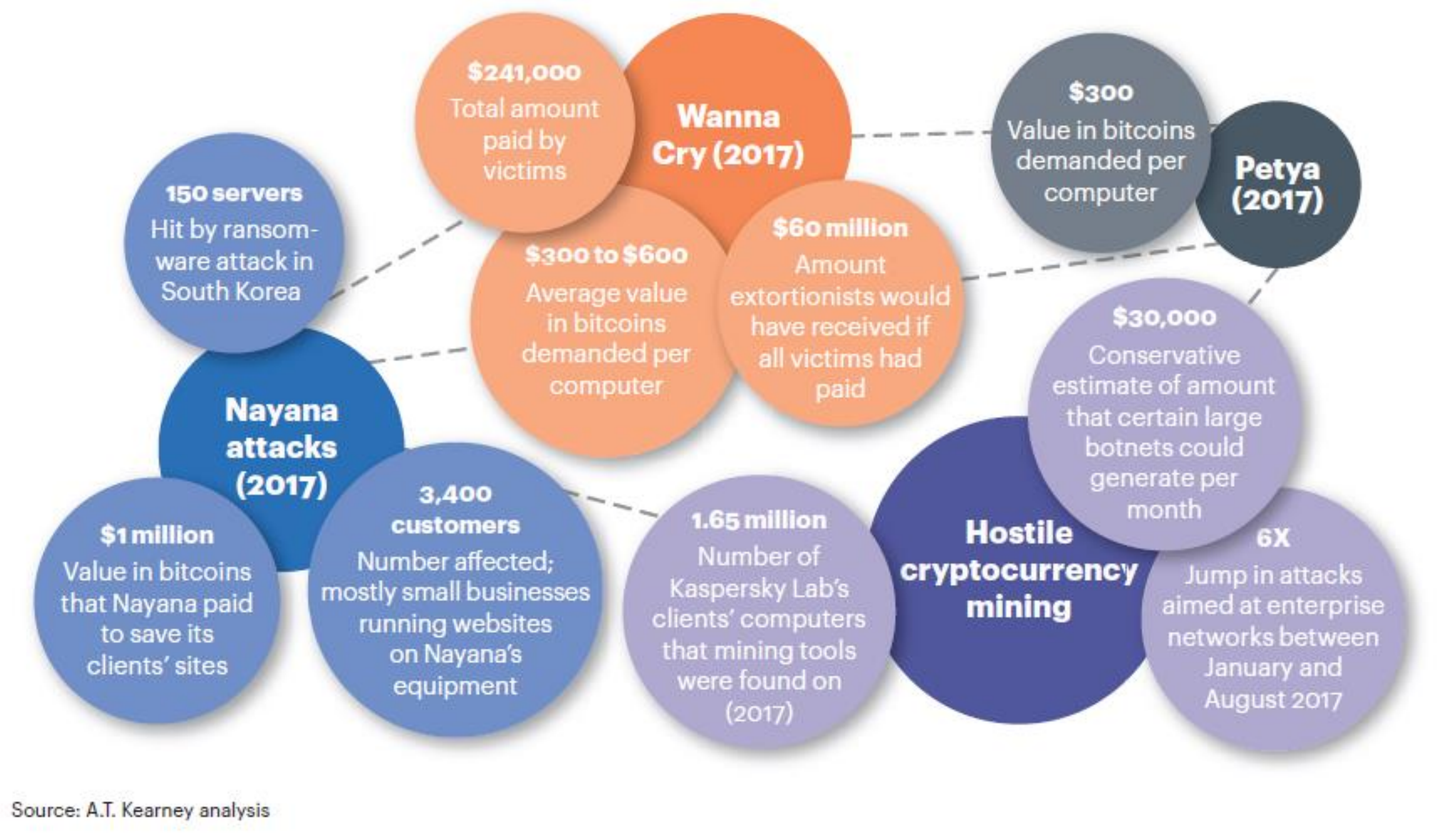
RISK ASPECTS

Virtual currency is increasingly a target for cyberattacks

Security experts have seen a spike in attacks over the past year, aimed at stealing computer power for cryptocurrency mining operations. Researchers have detected several large botnets set up to profit from cryptocurrency mining along with a growing number of attempts to install mining tools on organizations' servers.

Illegal mining operations set up by insiders, which can be much more difficult to detect, are on the rise. These are often carried out by employees with high-level network privileges and the technical skills needed to turn their company's computing infrastructure into a currency mint.

Source: A.T. Kearney. Cybersecurity in ASEAN: An Urgent Call to Action.



Wanna Cry (2017)
$241,000
Total amount paid by victims
$300 to $600
Average value in bitcoins demanded per computer
$60 million
Amount extortionists would have received if all victims had paid
Petya (2017)
$300
Value in bitcoins demanded per computer
Nayana attacks (2017)
150 servers
Hit by ransom-ware attack in South Korea
$1 million
Value in bitcoins that Nayana paid to save its clients' sites
3,400 customers
Number affected; mostly small businesses running websites on Nayana's equipment
Hostile cryptocurrency mining
1.65 million
Number of Kaspersky Lab's clients' computers that mining tools were found on (2017)
$30,000
Conservative estimate of amount that certain large botnets could generate per month
6X
Jump in attacks aimed at enterprise networks between January and August 2017

Source: A.T. Kearney analysis

In the ASEAN region, the recognition of the threat posed by virtual currencies is nascent with almost *no policy alignment* across member states.

RISK ASPECTS

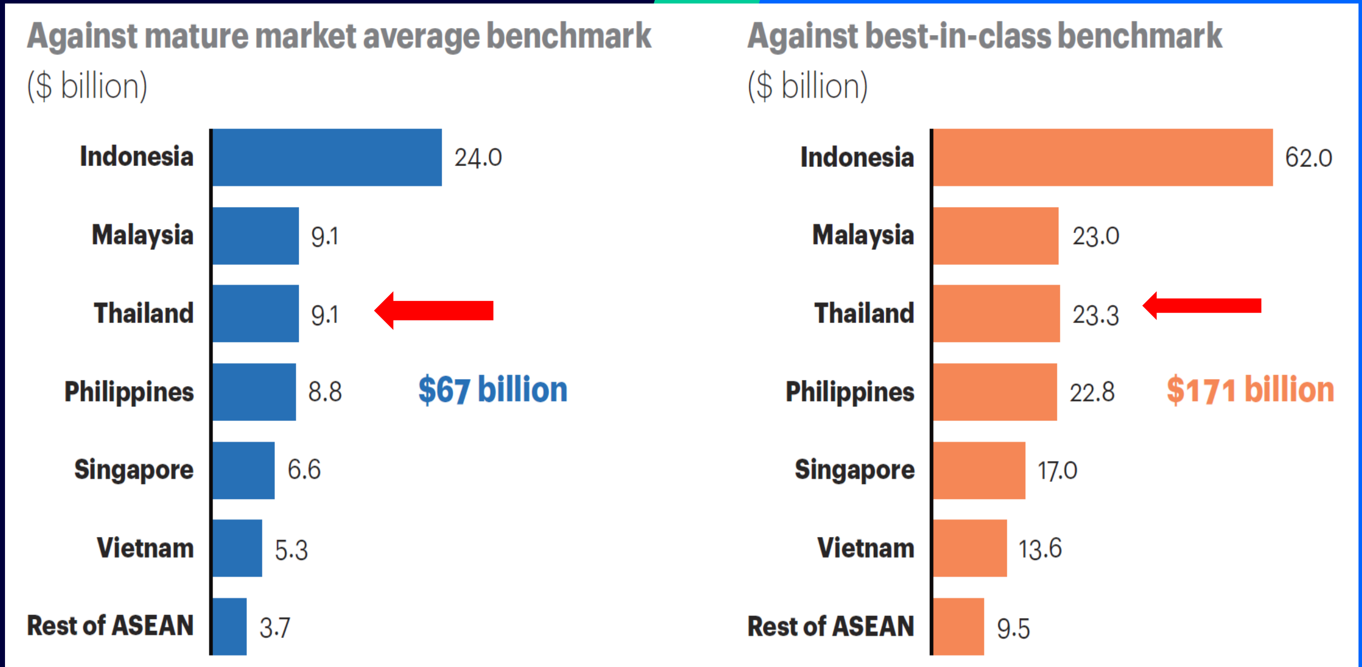
Target Cumulative Cybersecurity Spend in 2017 to 2025

- Currently, ASEAN countries are underspending in cybersecurity, therefore, a **significant increase in an investment is required** to reach benchmark levels of cybersecurity spending.

- If each ASEAN country spends **0.35** to **0.61** percent of its GDP on cybersecurity each year between **2017** and **2025**, spending would be comparable to *best-in-class countries*

- The estimates suggest that this translates into a **$171** billion collective spend for the region in **2017** to **2025**.

- Indonesia stands out as a country that could require a **massive investment** since its digital economy is likely to grow dramatically in the coming years.



Source: A.T. Kearney. Cybersecurity in ASEAN: An Urgent Call to Action.

RISK ASPECTS

Thailand Electronic Transaction Commission – Security Policy and Data Protection Policy

ETDA is responsible for facilitating the **Electronic Transactions Commission** to drive policy into action as the commission's secretary by approving Security and Data Protection policy for government agencies. As of 2021, **173** Government agencies have approved their **security policy (SP)** approved; and the commission has successfully approved only **28** data **protection policies (DP)**.

The number covers only 43% in security and less than 7% data protection of all governments in Thailand*.

ETDA relates to Laws and Regulations as follows:

RECAP!

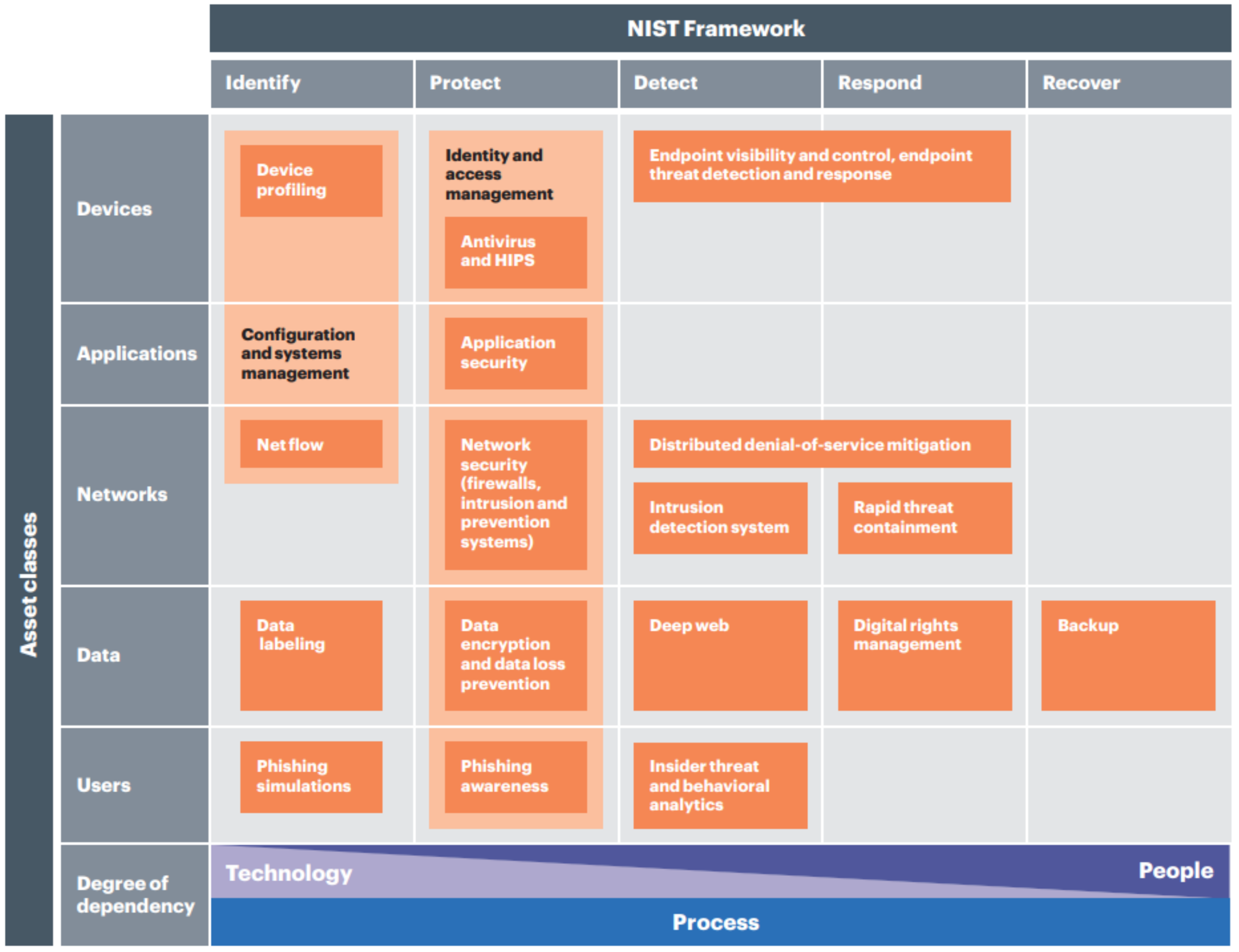
- **Electronic Transactions Act B.E. 2544 (2001)**
  - ➢Promote e-transactions
  - ➢Enhance trust of electronic information systems
  - ➢Provide legal recognition of e-transaction and e-signature
  - ➢Supervise e-transaction service providers
- **Electronic Transactions Act (No.2) B.E. 2551 (2008)**
  - ➢Transition of paper-based document to electronic documents and vice versa
- **Electronic Transactions Act (No.3) B.E. 2562 (2019)**
  - ➢Adoption of selected principles from e-communication convention such as invitation to make offers, use of automated manage systems for contract formation and error in electronic communication.
- **Electronic Transactions Act (No.4) B.E. 2562 (2019)**
  - ➢Provide legal recognition of digital identification (Digital ID)
- **(Draft) Digital Platform Act B.E. … (…)**
  - ➢ Provide legal measures and controls to regulate Digital platform services, and actionable items for business owners to enhance their digital services

•The estimated number of government agencies in Thailand is more than four hundred, with changes

WAY FORWARD

A cyber-defense matrix can help optimize the cybersecurity portfolio

- The growing interconnectedness across the region and geographical dispersion of the physical supply chain will intensify systemic risk, making the region only as strong as **its weakest link**.
- Diverging national priorities and varying paces of digital evolution will continue to foster a sustained **pattern of underinvestment**.
- Limited sharing of threat intelligence, often because of mistrust and a lack of transparency, will lead to even more porous cyber defense mechanisms.
- **Technological evolution** will render threat monitoring and response more complex, particularly given the rise of encryption, multi-cloud operations, proliferation of IoT, and convergence of OT and IT environments.



		NIST Framework				
Asset classes		Identify	Protect	Detect	Respond	Recover
	Devices	Device profiling	Identity and access management Antivirus and HIPS	Endpoint visibility and control, endpoint threat detection and response		
	Applications	Configuration and systems management	Application security			
	Networks	Net flow	Network security (firewalls, intrusion and prevention systems)	Distributed denial-of-service mitigation Intrusion detection system	Rapid threat containment	
	Data	Data labeling	Data encryption and data loss prevention	Deep web	Digital rights management	Backup
	Users	Phishing simulations	Phishing awareness	Insider threat and behavioral analytics		
	Degree of dependency	Technology		Process		People

Note: HIPS is host-based intrusion prevention system. NIST is National Institute of Standards and Technology.
Sources: RSA, National Institute of Standards and Technology; A.T. Kearney analysis

WAY FORWARD

Rapid Action Cybersecurity Framework

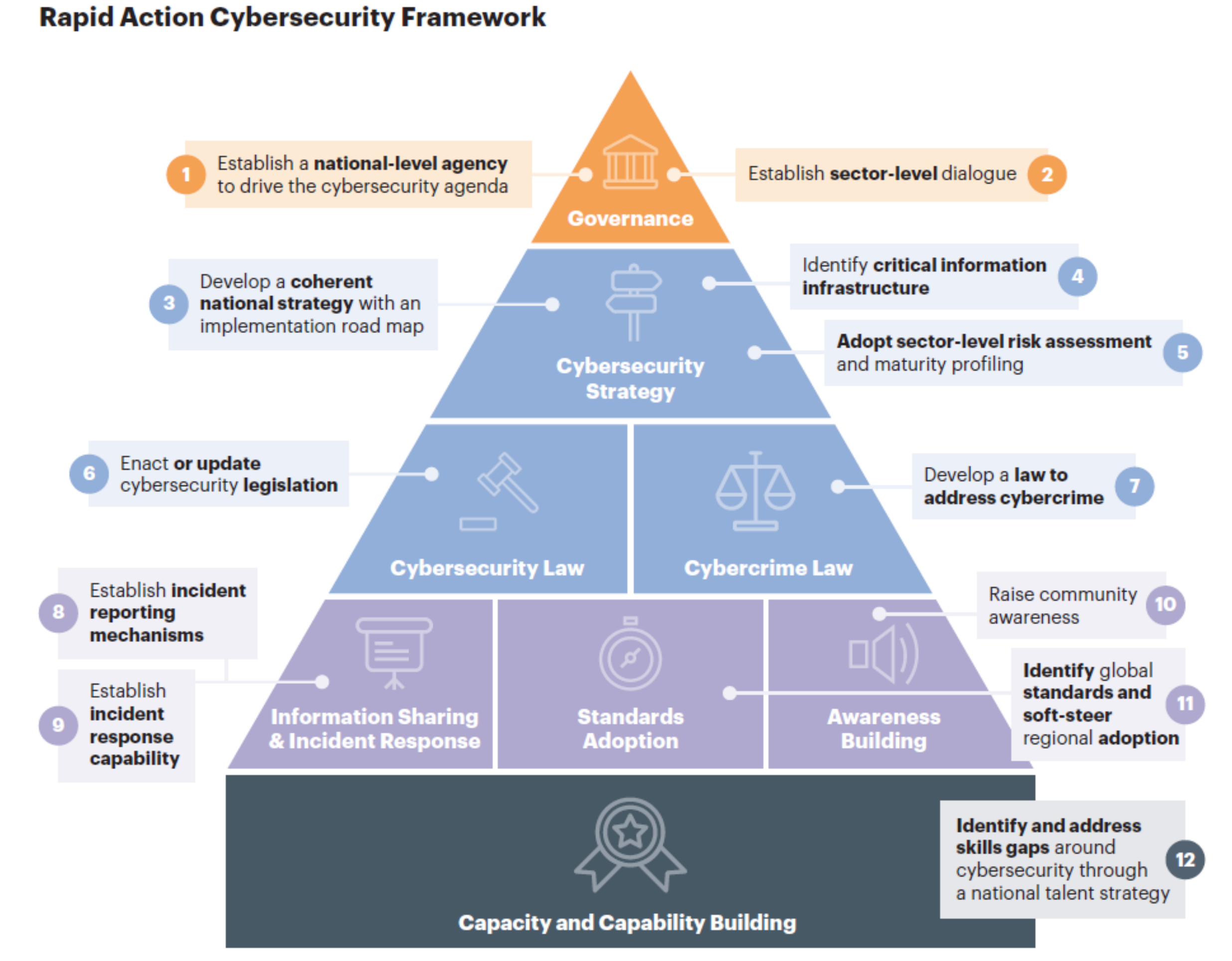
- ASEAN Ministerial Conference on Cybersecurity (AMCC) has taken steps to extend collaboration on cybersecurity across the region using "A Rapid Action Cybersecurity Framework"

- Despite having cybersecurity national strategy and implementation road map, the pace, urgency, and the level of harmonization of the region remains too slow.

- **A Rapid Action Cybersecurity Framework** is established to focus on addressing current weaknesses in cyber resilience in each state and to be a readiness threshold for some countries to accelerate their institutional frameworks implementation.

- The framework envisages **12 strategic imperatives**, aimed at fixing the basics related to cybersecurity across the region, and the national governments of each member state should be a harbinger in implementing the framework.

Sources: RSA, National Institute of Standards and Technology; A.T. Kearney analysis



Rapid Action Cybersecurity Framework

Governance

1 Establish a **national-level agency** to drive the cybersecurity agenda

2 Establish **sector-level** dialogue

Cybersecurity Strategy

3 Develop a **coherent national strategy** with an implementation road map

4 Identify **critical information infrastructure**

5 **Adopt sector-level risk assessment** and maturity profiling

Cybersecurity Law

Cybercrime Law

6 **Enact** or **update** cybersecurity **legislation**

7 Develop a **law to address cybercrime**

Information Sharing & Incident Response

Standards Adoption

Awareness Building

8 Establish **incident reporting mechanisms**

9 Establish **incident response capability**

10 Raise community awareness

11 **Identify** global **standards and soft-steer** regional **adoption**

Capacity and Capability Building

12 **Identify and address skills gaps** around cybersecurity through a national talent strategy

Note:
HIPS is host-based intrusion prevention system.
NIST is National Institute of Standards and Technology.

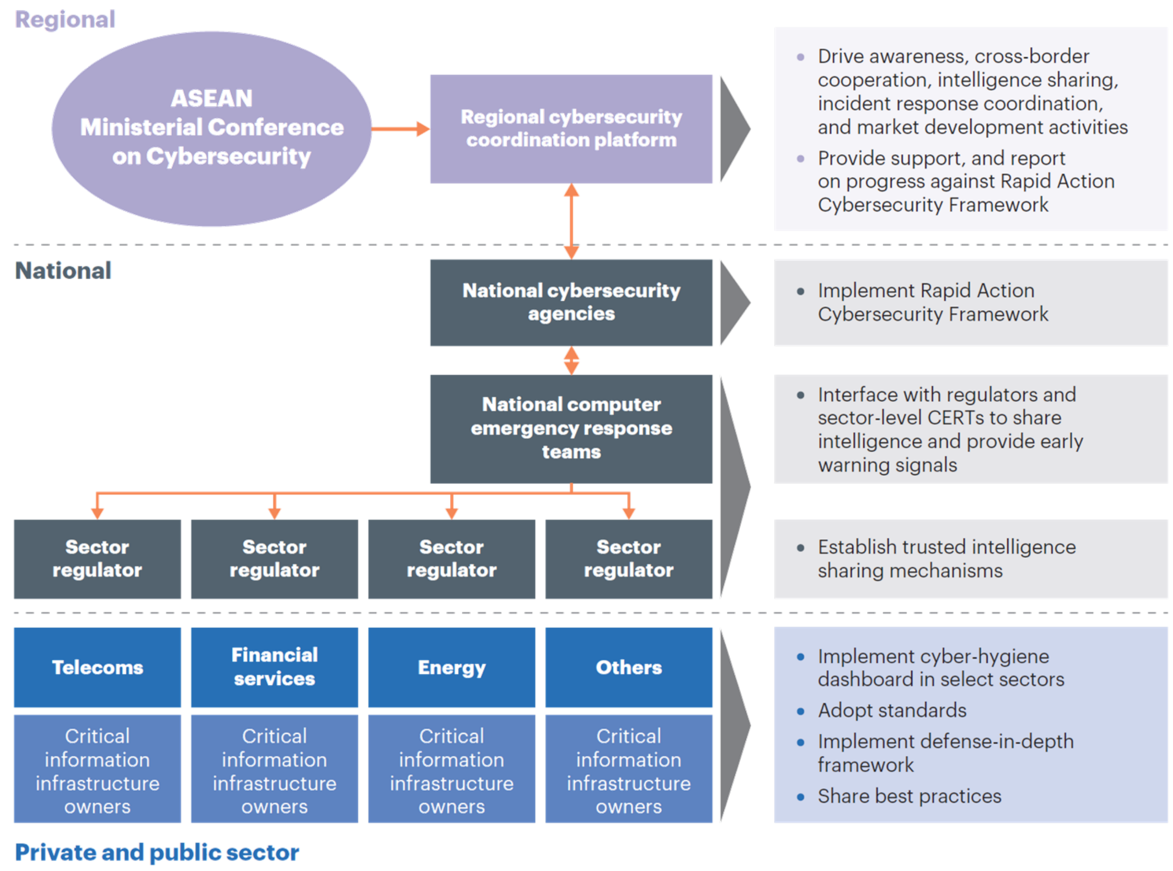
WAY FORWARD

From Regional to National

- To interface with numerous national agencies, a regional operational coordination platform is required. This allows *awareness-raising*, *cross-border cooperation*, and *market development initiatives*, such as **standard adoption** and **harmonization**.

- National operation surfaces to implement Rapid Action Cybersecurity Framework and intelligence sharing mechanism as well as to coordinate with sector regulators to share intelligence.

- The operation of Private and public sectors, including Telecoms, Financial Service, Energy, and others is executed to implement "**cyber-hygiene dashboard"** and defense framework as well as share best practices among one another.



Regional

ASEAN Ministerial Conference on Cybersecurity

Regional cybersecurity coordination platform

- Drive awareness, cross-border cooperation, intelligence sharing, incident response coordination, and market development activities
- Provide support, and report on progress against Rapid Action Cybersecurity Framework

National

National cybersecurity agencies

- Implement Rapid Action Cybersecurity Framework

National computer emergency response teams

- Interface with regulators and sector-level CERTs to share intelligence and provide early warning signals

Sector regulator

Sector regulator

Sector regulator

Sector regulator

- Establish trusted intelligence sharing mechanisms

Telecoms

Financial services

Energy

Others

Critical information infrastructure owners

Critical information infrastructure owners

Critical information infrastructure owners

Critical information infrastructure owners

- Implement cyber-hygiene dashboard in select sectors
- Adopt standards
- Implement defense-in-depth framework
- Share best practices

Private and public sector

Source: A.T. Kearney analysis

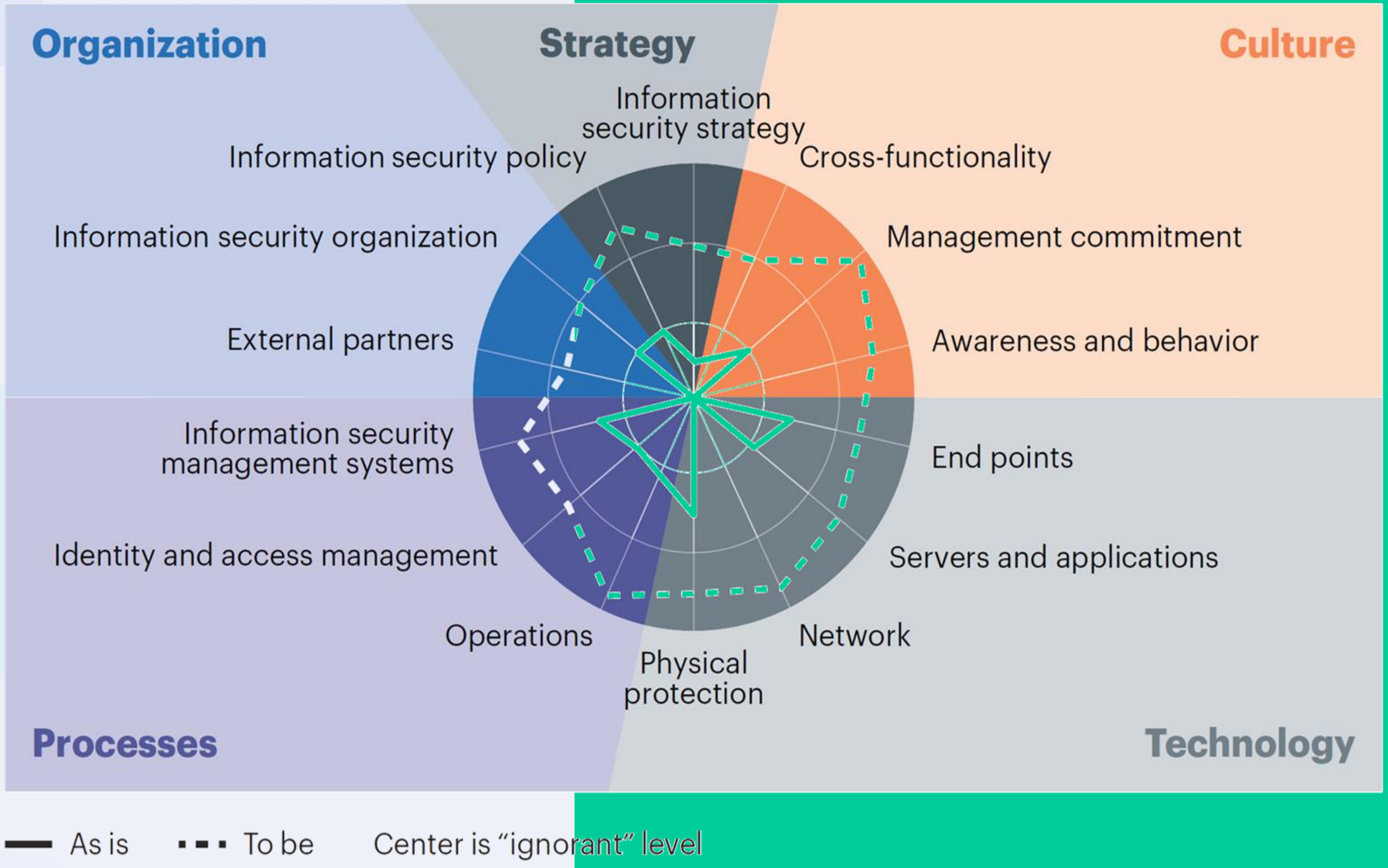
WAY FORWARD

A cyber-hygiene dashboard

A cyber-hygiene dashboard should be an integral part of monitoring company performance system, and internal **readiness** tracking on strategy, culture, technology, operations, and organization.

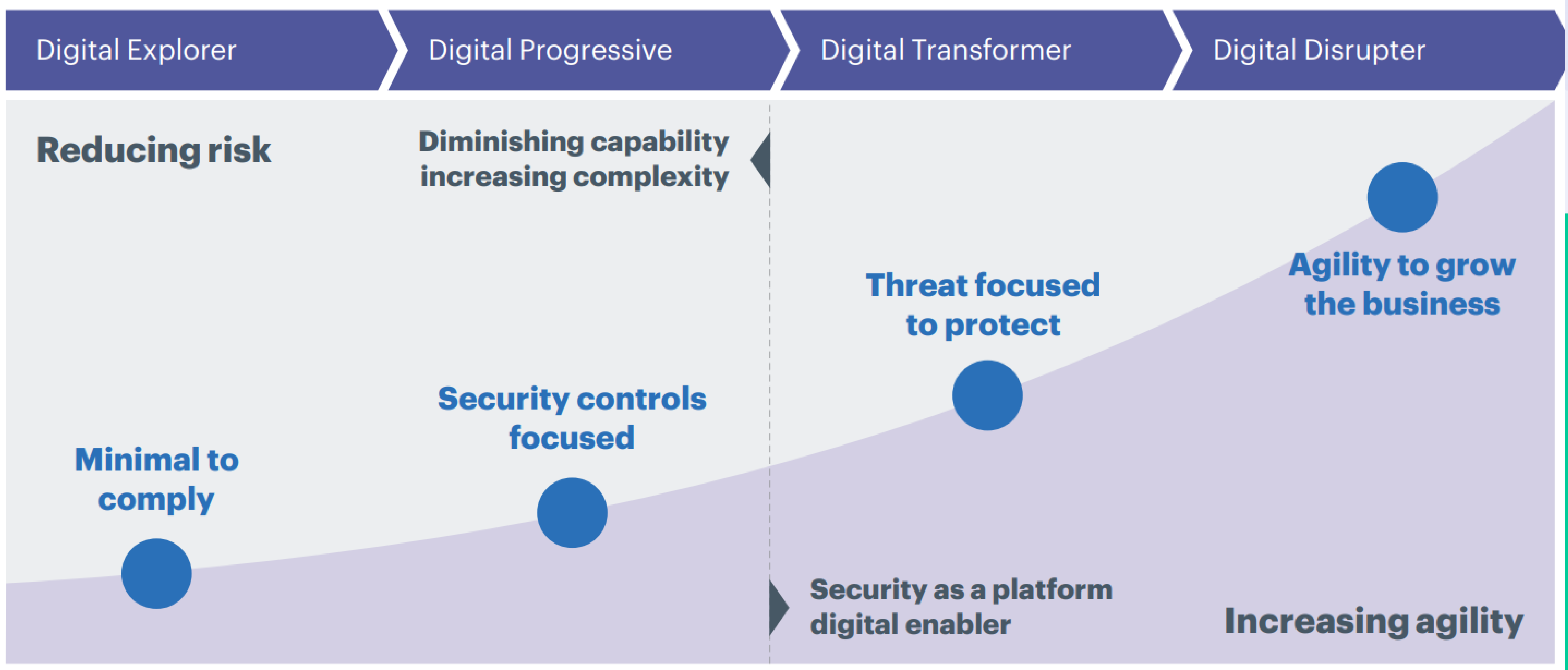
The dashboard shows the readiness of the national country-level in AMS in a detailed manner influenced by the regional plan (ASEAN).

Sources: A.T. Kearney analysis



WAY FORWARD

Security as a digital enabler



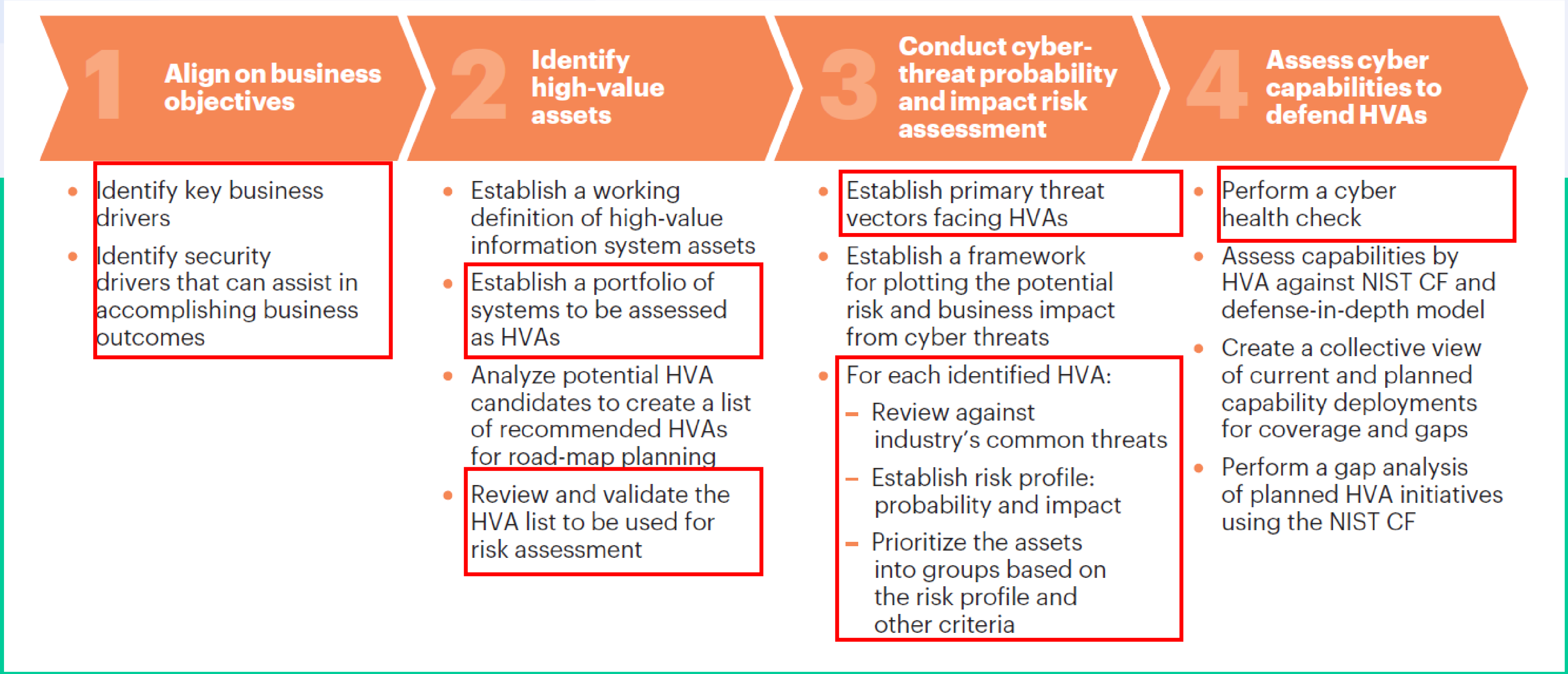
Digital Explorer
Digital Progressive
Digital Transformer
Digital Disrupter
Reducing risk
Diminishing capability increasing complexity
Minimal to comply
Security controls focused
Threat focused to protect
Agility to grow the business
Security as a platform digital enabler
Increasing agility

Sources: A.T. Kearney analysis

WAY FORWARD

the lack of a holistic approach around strategy, governance, organization, and culture often results **in organizations being highly vulnerable** despite relying on the best vendors and products.

A four-step approach can help companies define their cybersecurity strategy



1 Align on business objectives

- Identify key business drivers
- Identify security drivers that can assist in accomplishing business outcomes

2 Identify high-value assets

- Establish a working definition of high-value information system assets
- Establish a portfolio of systems to be assessed as HVAs
- Analyze potential HVA candidates to create a list of recommended HVAs for road-map planning
- Review and validate the HVA list to be used for risk assessment

3 Conduct cyber-threat probability and impact risk assessment

- Establish primary threat vectors facing HVAs
- Establish a framework for plotting the potential risk and business impact from cyber threats
- For each identified HVA:
  - Review against industry's common threats
  - Establish risk profile: probability and impact
  - Prioritize the assets into groups based on the risk profile and other criteria

4 Assess cyber capabilities to defend HVAs

- Perform a cyber health check
- Assess capabilities by HVA against NIST CF and defense-in-depth model
- Create a collective view of current and planned capability deployments for coverage and gaps
- Perform a gap analysis of planned HVA initiatives using the NIST CF

Sources: A.T. Kearney analysis

Notes: HVA is high-value asset. NIST CF is the National Institute of Standards and Technology Cybersecurity Framework.

WAY FORWARD

A Guide to Understanding Cybersecurity & Data Protection Documentation

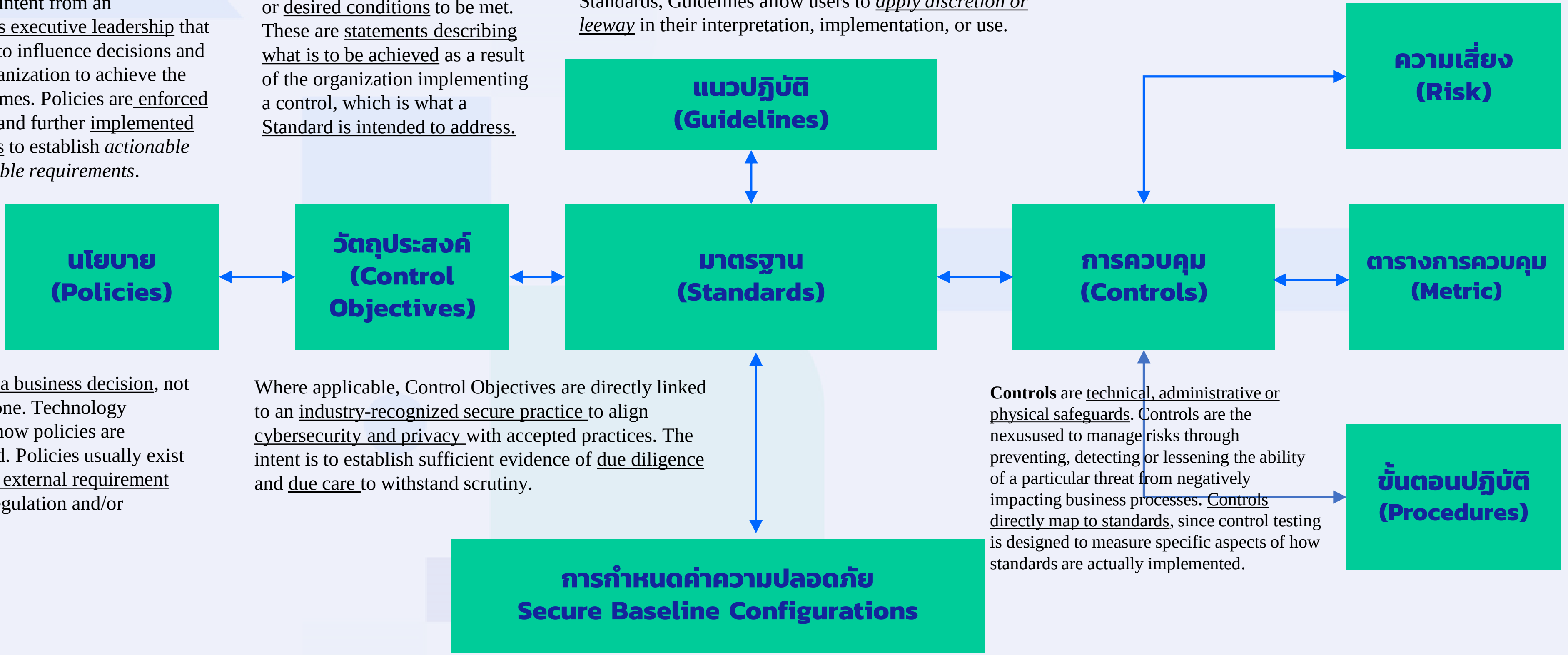
Policies are high-level statements of management intent from an organization's executive leadership that are designed to influence decisions and guide the organization to achieve the desired outcomes. Policies are enforced by standards and further implemented by procedures to establish *actionable and accountable requirements*.

Control Objectives are targets or desired conditions to be met. These are statements describing what is to be achieved as a result of the organization implementing a control, which is what a Standard is intended to address.

Guidelines are recommended practices that are based on industry-recognized secure practices. Guidelines help augment Standards when discretion is permissible. Unlike Standards, Guidelines allow users to *apply discretion or leeway* in their interpretation, implementation, or use.

Risks represent a situation where someone or something valued is exposed to danger, harm or loss(noun) or to expose someone or something valued to danger, harm or loss (verb).

Metrics provide a "point in time" view of specific, discrete measurements, unlike trending and analytics that are derived by comparing a baseline of two or more measurements taken over a period of time. Analytics are generated from the analysi sof metrics.



Policies are a business decision, not a technical one. Technology determines how policies are implemented. Policies usually exist to satisfy an external requirement (e.g., law, regulation and/or contract).

Where applicable, Control Objectives are directly linked to an industry-recognized secure practice to align cybersecurity and privacy with accepted practices. The intent is to establish sufficient evidence of due diligence and due care to withstand scrutiny.

Controls are technical, administrative or physical safeguards. Controls are the nexusused to manage risks through preventing, detecting or lessening the ability of a particular threat from negatively impacting business processes. Controls directly map to standards, since control testing is designed to measure specific aspects of how standards are actually implemented.

Good metrics are those that are **SMART(Specific, Measurable, Attainable, Repeatable, and Time-dependent)**

Procedures are a documented set of steps necessary to perform a specific task or process in conformance with an applicable standard. Procedures help address the question of how the organization actually operationalizes a policy, standard or control. Without documented procedures, there can be defendable evidence of due care practices.

Secure baseline configurations are technical in nature and specify the required configuration settings for a defined technology platform. Leading guidance on secure configurations come from the following sources: 1) Center for Internet Security 2) DISASTIGs and 3) Vendor recommendations

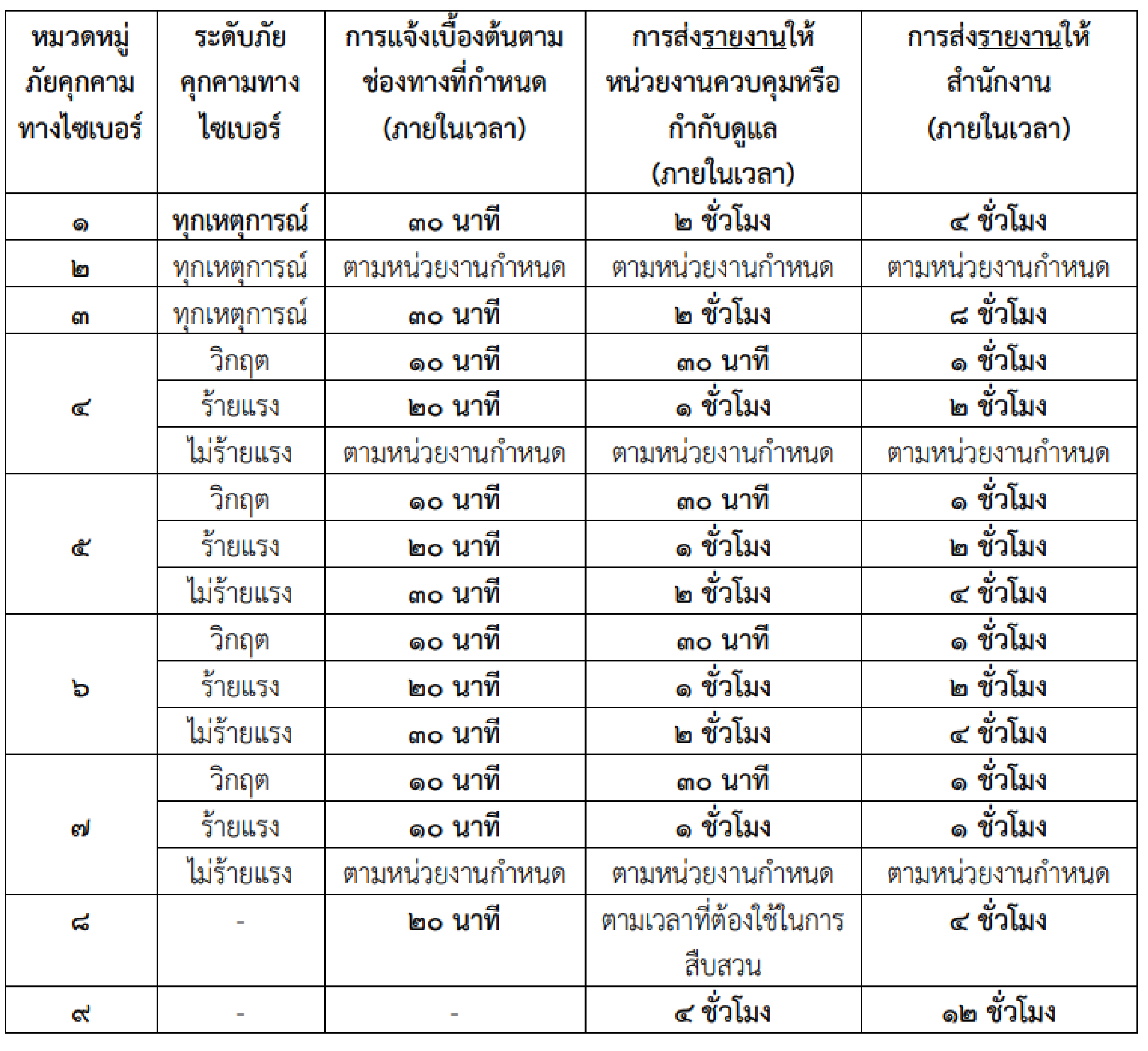
Source: ComplianceForge 2021

WAY FORWARD

Laws and Regulations – Cybersecurity Act B.E. 2562 (2019) ("Cybersecurity Act") and its Ancillary law

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง **ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ** (พ.ศ. ๒๕๖๔)

- การจำแนกหมวดหมู่ของภัยคุกคามทางไซเบอร์
- ตัวอย่างลักษณะภัยคุกคามทางไซเบอร์แยกตามระดับต่าง ๆ
- ตัวอย่างกำหนดระยะเวลาในการแจ้งและรายงานภัยคุกคามทางไซเบอร์



หมวดหมู่ภัยคุกคามทางไซเบอร์	ระดับภัยคุกคามทางไซเบอร์	การแจ้งเบื้องต้นตามช่องทางที่กำหนด (ภายในเวลา)	การส่งรายงานให้หน่วยงานควบคุมหรือกำกับดูแล (ภายในเวลา)	การส่งรายงานให้สำนักงาน (ภายในเวลา)
๑	ทุกเหตุการณ์	๓๐ นาที	๒ ชั่วโมง	๔ ชั่วโมง
๒	ทุกเหตุการณ์	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด
๓	ทุกเหตุการณ์	๓๐ นาที	๒ ชั่วโมง	๘ ชั่วโมง
๔	วิกฤต	๑๐ นาที	๓๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๒๐ นาที	๑ ชั่วโมง	๒ ชั่วโมง
	ไม่ร้ายแรง	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด
๕	วิกฤต	๑๐ นาที	๓๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๒๐ นาที	๑ ชั่วโมง	๒ ชั่วโมง
	ไม่ร้ายแรง	๓๐ นาที	๒ ชั่วโมง	๔ ชั่วโมง
๖	วิกฤต	๑๐ นาที	๓๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๒๐ นาที	๑ ชั่วโมง	๒ ชั่วโมง
	ไม่ร้ายแรง	๓๐ นาที	๒ ชั่วโมง	๔ ชั่วโมง
๗	วิกฤต	๑๐ นาที	๓๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๑๐ นาที	๑ ชั่วโมง	๑ ชั่วโมง
	ไม่ร้ายแรง	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด
๘	-	๒๐ นาที	ตามเวลาที่ต้องใช้ในการสืบสวน	๔ ชั่วโมง
๙	-	-	๔ ชั่วโมง	๑๒ ชั่วโมง

Source: http://www.ratchakitcha.soc.go.th/DATA/PDF/2564/E/303/T_0003.PDF

TAKE A SURVEY

- In the next session, we will focus on **National CERT Competency Survey 2022.**
- The survey can be completed at https://forms.office.com/r/uCsideKgAC
- This survey is used to gauge the demands of five service areas of national CERT referred to FIRST Services Framework, ranging based on the basis of importance during 1st Executive Education Certificate Program in Cybersecurity on Thursday 27th January 2022 at 15.00 – 16.30. The five areas include:

QR Code to the survey
(For participants)

- The survey consist of 3 sections and 9 questions as follows:

  SECTION 1 : Survey Profiling (5 questions)
  SECTION 2 : Quality Measurement for CSIRT services (2 questions)
  SECTION 3 : Prioritizing Service Areas for Roadmap Development(2 questions)

- Your **anonymity** is preserved in completing the survey

INTERACTIVE SESSION

N-CERT SERVICE AREA SURVEY (1/3)

SECTION 1 : SURVEY PROFILING

Your **anonymity** is preserved in completing the survey

- Field of Work/ Industries Distribution
- Years of Experience in Working Fields
- Gender
- Age
- Education

QR Code to the survey
(For participants)

See Survey results (For presenter)

INTERACTIVE SESSION

N-CERT SERVICE AREA SURVEY (2/3)

SECTION 2 :
QUALITY MEASUREMENT FOR CSIRT SERVICES

Your **anonymity** is preserved in completing the survey

- Importance of Areas
- Budget Allocation Worthiness of Areas

QR Code to the survey
(For participants)

See Survey results (For presenter)

INTERACTIVE SESSION

N-CERT SERVICE AREA SURVEY (3/3)

SECTION 3 :
PRIORITIZING SERVICE AREAS FOR ROADMAP DEVELOPMENT

Your **anonymity** is preserved in completing the survey

- Opinion towards a promotion of a particular area
- Opinion towards a demotion of a particular area

QR Code to the survey
(For participants)

See Survey results (For presenter)

กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม

ETDA

INTERACTIVE SESSION

ETDA's E-book Collection

INTERACTIVE SESSION

Cybersecurity Microlearning Campaign

Top 5 Takeaways 3 Week Lessons 5 – 10 min

As the world has become more digitalized than ever, the necessity in raising cybersecurity awareness has thus become more important in preventing oneself from cyber threats. How to do so is briefly explained these following topics.

WEEK 1 : AWARENESS

Security Basic & Password
Phishing & Social Engineering
Dangers from Hackers
Malware, and Mobile Devices

Awareness Micro-learning

Note: No application installed need

ETDA Thailand

@ETDA.Thailand · หน่วยงานราชการ

สวัสดี! มีอะไรให้เราช่วยไหม

Facebook

ETDA Thailand

SUMMARY (1/2)

1. **ETDA**'s missions, goals and Authority and The roles and responsibilities of the Authority on Cybersecurity
2. Report on Cybersecurity includes **ITU** Global Cybersecurity Index 2020, **(ISC)²** Cybersecurity Workforce Shortage 2020, The Global Forum on Cyber Expertise (**GFCE**) 's research at CSIRTs In Low-Income Countries.
3. **ThaiCERT** Statistics 2021, **OWASP** Top-10 2021, and Cybersecurity Investment per GDP in ASEAN. Virtual currency is increasingly a target for cyber attacks response to the COVID-19 crisis

SUMMARY (2/2)

4. Cybersecurity Framework for National-Level, Sector-Level to organization level through "**right-amount**" of cybersecurity policy
5. Cybersecurity Act B.E. 2562 (2019) ("**Cybersecurity Act**") + its Ancillary law and other most recent standards and guidelines
6. The NICE Frameworks areas include 1. Information Security Event Management (ISEM), 2. Information Security Incident Management (ISIM), 3. Vulnerability Management (VM), 4. Situational Awareness (SA), and 5. Knowledge Transfer (KT).
7. ETDA's **E-book Collection** and **Cybersecurity Microlearning Campaign**

Q&A

Please feel free to ask any questions.

References

- ASEAN-Japan Cybersecurity Reference 2021 TLP:GREEN
- A.T. Kearney. Cybersecurity in ASEAN: An Urgent Call to Action.
- Global Forum on Cyber Expertise, Global Affairs Canada, & AfricaCERT. (2022). Cyber Incident Management in Low-Income Countries.
- International Telecommunication Union. (2021). Global Cybersecurity Index 2020.
- (ISC)2 CYBERSECURITY WORKFORCE STUDY (2020)
- The Open Web Application Security Project. (2021). OWASP Top 10:2021
- Compliance Forge, A Guide to Understanding Cybersecurity & Data Protection Documentation (2021)

THANK YOU

Electronic Transactions Development Agency
The 9th Tower Grand Rama9 Building (Tower B) Floor 20-22
33/4 Rama 9 Road, Huai Khwang, Bangkok 10310

CALL CENTER : 02 123 1234
email : info@etda.or.th
Web : www.etda.or.th

กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม

ETDA