Research Report

" Cyber Security Measures of Critical Industry Sector" in ASEAN 5 Nations

JISA Team

(1) Research Method

- **Target Nations**
  - Indonesia, Malaysia, Singapore, Thailand, Vietnam
- **Target Critical Industry Sector**
  - Indonesia   : Finance & Bank, ICT, Health, Energy & Mineral Resource, Transportation, Emergency Services, Defense & Strategic Industry, Water Resource, Law Enforcement, Agriculture
  - Malaysia   : Banking & Finance, Information & Communications, Health Services, Energy, Transportation, Emergency Services, National Defense & Security, Water, Government, Food & Agriculture
  - Singapore   : Banking & Finance, Infocomm, Health, Energy, Land Transport, Security & Emergency, Water, Government, Maritime, Aviation, Media
  - Thailand   : Banking & Finance, ICT, Health Services, Energy, Public Service, National Security, NCSC, Supply Chain & Logistics,
  - Vietnam   : Finance, Banking, Information, Healthcare, Energy, Transportation, National Defense, Natural Resources, Snart-City

- **Term**
  - Dec 10, 2021 – Feb 11, 2022
- **Method**
  - Under the ASOCIO's coordination / ATCI, PIKOM, SGTech, VINASA introduce target respondents company
  - JISA provide Secure Sketch platform as an assessment tool: A kind of Third party Risk Management Tool
- **Respondents**
  - More than 10 companies from more than 3 industry sectors per each nation
  - Respondents reply checking the questions on the screen which link was provided by the platform

(2) Questionnaire evaluation category

75 Questions of Secure SketCH consist of 4 Large Category / 20 Medium category

4 Large Category

20 Medium Category

4 Large Category	20 Medium Category
Strategy	1. Security risk response policy 2. Security control
Organization	3. Information management 4. Human resource development and education 5. Physical access control
Technology	6. Configuration management 13. Perimeter defense 7. Network management 14. Cloud service usage management 8. Wireless access management 15. Security log management /storage 9. Data protection 16. Privileged access management 10. Account management 17. Secure development & operation 11. Email management 12. Malware countermeasures
Incident response	18. Disaster response 19. Incident response 20. Training for incident response

(3) Outline of Result (57 Respondents)

- The score is calculated based on the conversion standard prescribed by NRIS, which takes into consideration the weight of each question and the weight of each answer standard.

- Rank is set of 5 levels. Based on the score, S rank (security measures are implemented at a very high level), A rank (security measures are implemented at a high level), B (room for advancement), C rank (weakness reinforcement is essential), D rank Classified as (implementation of security measures is essential)

- Average=778 points of 1,000, High Score =1,000, Low Score =273

	Rank S	Rank A	Rank B	Rank C	Rank D	Average	High Score	Low Score
Indonesia (10)	4	3	2	0	1	741.6	911	497
Malaysia (12)	6	3	1	2	0	784.3	986	546
Singapore (10)	7	1	0	0	2	790.9	1000	273
Thaikand (15)	8	5	1	0	1	798.7	1000	467
Vietnam (10)	4	5	1	0	0	761.4	838	641
Grand total (57)	29	18	5	2	4	777.8	1000	273
Rank/Score	S ≧ 800	800>700	700>600	600>500	500>			

(4) Results by Country : Indonesia
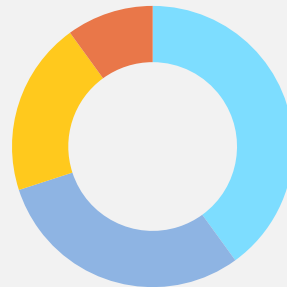
Average Score of 10 Indonesia Companies

742 /1000

Highest Score of 10 Indonesia Companies

911 /1000

Minimum Score of 10 Indonesia Companies

497 /1000

Rank distribution of 10 companies

S	Very high level	4
A	High Level	3
B	There is room for advancement	2
C	Need to reinforce weaknesses	0
D	Implementation of measures is essential	1

- The respondents were 2 finance companies, 3 information and telecommunications companies, 2 energy companies, 2 transportation companies, and 1 chemical company.

- There were 4 companies with S rank, 3 companies with A rank, 2 companies with B rank, and 1 company with D rank.

- Two financial companies, one energy company, and one transportation company have won the S rank.

(5) Results by Country: Malaysia

Average Score of 12 Malaysia Companies

784 /1000

Highest Score of 12 Malaysia Companies

986 /1000

Minimum Score of 12 Malaysia Companies

546 /1000

Rank distribution of 12 companies

S	Very High Level	6
A	High Level	3
B	There is room for advancement	1
C	Need to reinforce weaknesses	2
D	Implementation of measures is essential	0

■ The respondents were 3 Banking & Finance Sector, 3 Health Services, 3 Food & Agriculture Sector, 1 Infocom company, and 1 energy company.

■ There were 6 companies with S rank, 3 companies with A rank, 1 companies with B rank, and 2 companies with C rank.

(6) Results by Country: Singapore

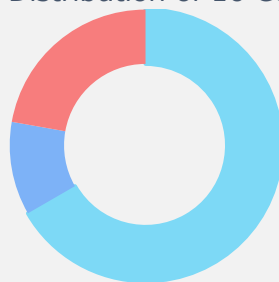**Average Score of 10 Singapore Companies**

791 /1000

Highest Score of 10 Singapore Companies

1000 /1000

Minimum Score of 10 Singapore Companies

273 /1000

Rank Distribution of 10 Companies

S	**Very High Level**	7
A	**High Level**	1
B	**There is room for advancement**	0
C	**Need to reinforce weaknesses**	0
D	**Implementation of measures is essential**	2

- The respondents were 4 Infocom Sector, 2 Health organizations, 1 Food & Agriculture Sector, 1 Banking & Finance, 1 Maritime company, and 1 Transportation company.

- There were 7 companies with S rank, 1 company with A rank. It can be seen that it is excellent, even in cyber security.

- However, it is puzzling that both of the two answers in the health sector were ranked D. There may be other high priority resources and investment allocations in this sector.

(7) Results by Country: Thailand

Average Score of 15 Thailand Companies

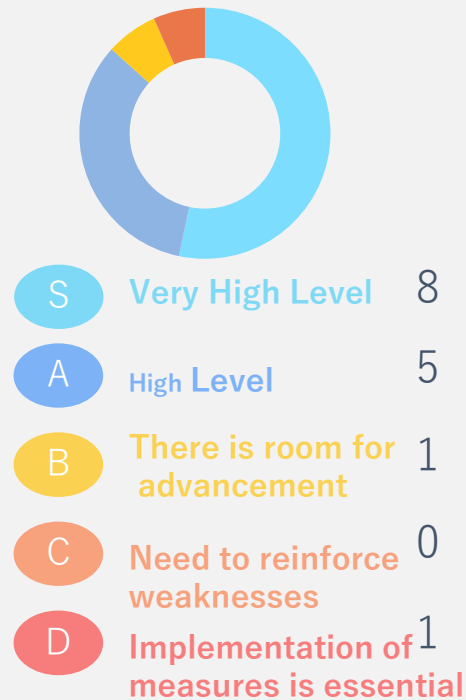**799** /1000

Highest Score of 15 Thailand Companies

1000/1000

Minimum Score of 15 Thailand Companies

467 /1000

Rank Distribution of 15 Companies

S	Very High Level	8
A	High Level	5
B	There is room for advancement	1
C	Need to reinforce weaknesses	0
D	Implementation of measures is essential	1

- The respondents were 8 Central / local Governmental Agencies, 3 Banking and Finance Sector, 2 ICT companies, 1 Health services organization, and 1 public service organizations.

- There were 8 organizations with S rank, 5 organizations with A rank, 1 company with B rank, and 1 company with D rank.

- Of the 8 cases evaluated as S rank, 4 cases were four central and local government agencies, 2 cases were in finance, 1 case was for ICT, and 1 case was in the Health service.

- The government and public services fields are all ranked A or higher, and it can be inferred that this field and finance are making a significant contribution to improving cybersecurity in Thailand.

(8) Results by Country: Vietnam

Average Score of 10
Vietnam Companies

761 /1000

Highest Score of 10
Vietnam Companies

838 /1000

Minimum Score of 10
Vietnam C0mpanies

641 /1000

Rank Distribution of 10 Companies
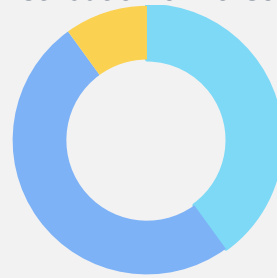
S	Very High **Level**	4
A	High Level	5
B	There is room for sophistication	1
C	Need to reinforce weaknesses	0
D	Implementation of measures is essential	0

- The respondents were 7 information and communications, 2 banks, and 1 insurance.

- There were 4 companies with S rank, 5 companies with A rank, and 1 company with B rank.

- Three information companies and one bank were evaluated as S rank.
- It can be said that companies in the ICT sector are advancing cyber security measures in Vietnam.

(9) Summary

Since the definitions of important infrastructure fields are slightly different in each country, we asked ASOCIO member associations in each country to include companies in the BFSI sector and companies in ICT sector so that we can make a common comparison as much as possible in this survey. It became a tendency like below.

- 17 responses in the ICT Sector and 12 responses in the finance (BFSI) Sector.
- As for the response status of companies in the ICT Sector, 8 of 17 companies are S rank and 7 companies are A rank.
- Of the 12 companies in the BFSI Sector, 7 are S rank and 3 are A rank.
- The energy Sector also has the highest S rank, with 3 out of 4 companies having S rank.

(10) References: Comparison ASEAN 5 + Japan in 4 Large Evaluation Category

- A comparison of 28 major Japanese critical infrastructure-related companies and the similar industries of 5 ASEAN countries (40 companies)
- In the comparative analysis, the answers with a perfect score of 1000 were excluded.
- In a country-by-country comparison of 40 companies in five countries, there is a large difference by country in the "organization" category.
- Singapore excels in every category

Legend: Indonesia (10社) | Malaysia (7社) | Singapore (7社) | Thailand (6社) | Vietnam (10社) | Japan (28社)

Category	Indonesia	Malaysia	Singapore	Thailand	Vietnam	Japan
Strategy	78%	84%	89%	79%	80%	84%
Organization	65%	74%	85%	79%	74%	82%
Technology	74%	83%	89%	78%	75%	77%
Incident Response	78%	86%	91%	81%	78%	78%
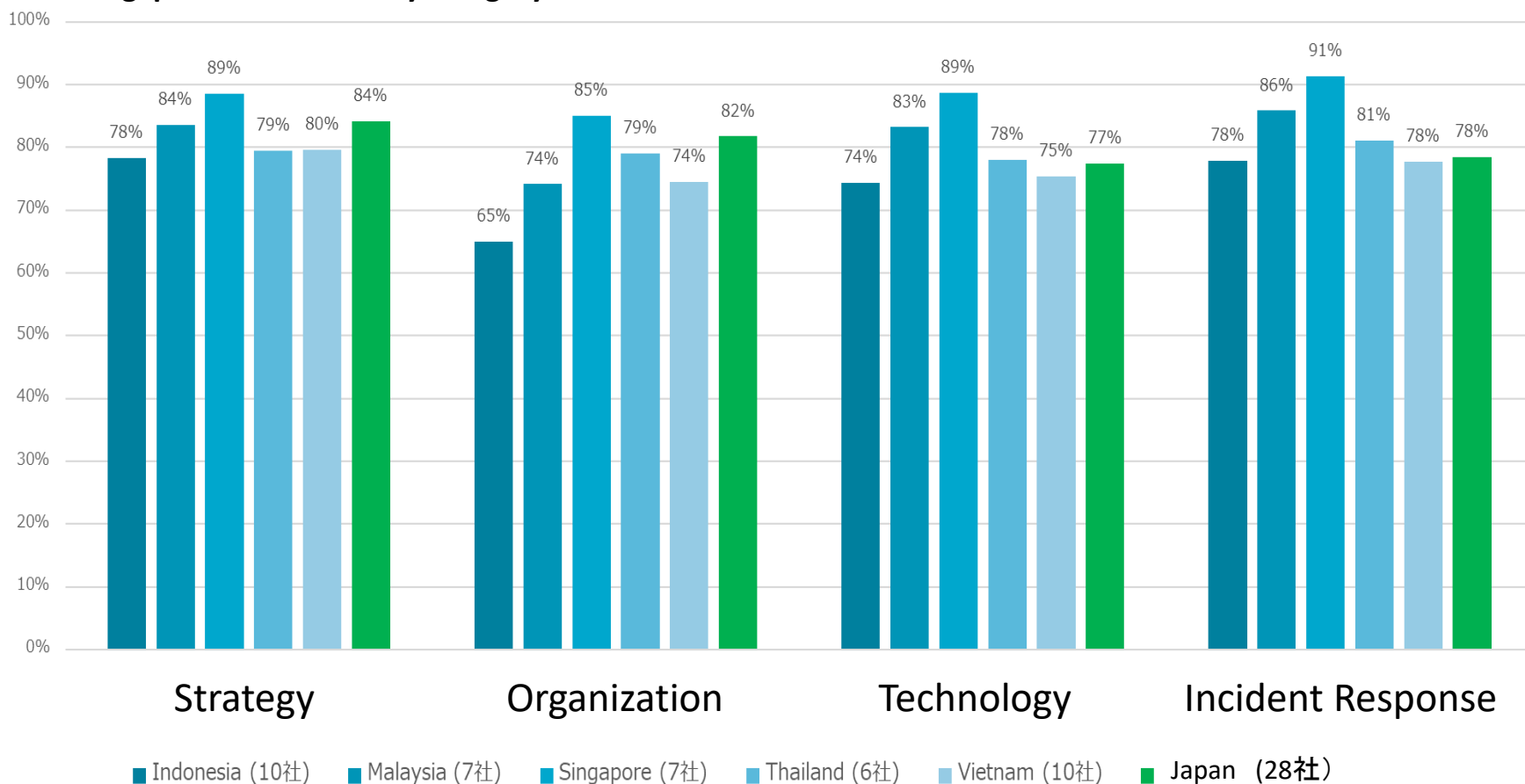
(11) References: Comparison / ASEAN 5 average vs Japan average in 20 Medium Evaluation Category

- **Of the 20 medium security categories, half is above the Japanese average and half are below the Japanese average.**
- **It can be said that the survey results reflect the mutual characteristics well, rather than whether Japan or ASEAN is superior, and it is possible to share and complement each**

Legend:
- ASEAN CII 40 Companies Average
- Japan CII 28 Companies Average
- Japan All Industry 3,100 companies Average

Categories:
1. Security risk response policy
2. Security control
3. Information Management
4. HRD/Education
5. Physical access control
6. Configuration Management
7. Network Management
8. Wireless access management
9. Data Protection
10. Account Management
11. Email Management
12. Malware Countermeasures
13. Perimeter defense
14. Cloud service usage management
15. Security log management / storage
16. Privileged access management
17. Secure Development Operation
18. Disaster Response
19. Incident response
20. Training for incident response

Legend: Indonesia (10社), Malaysia (7社), Singapore (7社), Thailand (6社), Vietnam (10社), Japan CII (28社), ASEAN 5 Average (40)

Categories:
1. Security risk response policy
2. Security control
3. Information Management
4. HRD/Education
5. Physical access control
6. Configuration Management
7. Network Management
8. Wireless access management
9. Data Protection
10. Account Management
11. Email Management
12. Malware Countermeasures
13. Perimeter defense
14. Cloud service usage management
15. Security log management/storage
16. Privileged access management
17. Secure Development Operation
18. Disaster Response
19. Incident response
20. Training for incident response

(13) Reference: Answer to 75 Question

The status of question and answer of the company is shown below .

- The pink frame indicates that no measures have been taken.
- The yellow frame indicates that measures are being taken, but more complete measures are needed.

The second column from the left shows BFSI, Infocom, and Energy in order of dark blue. In each country, there are few pink and yellow frames in the dark blue part.

For the following items that are often pink or yellow, it is recommended to improve the countermeasures.

- Responding to cyber attacks using email
- Log management of malware infection response (EDR, etc.)
- Correlation analysis of logs
- Outgoing email security
- Cloud service related security policy / management / control
- Incident response training