Chapter 3

Policy Recommendations for ASEAN–Japan Cooperation on Operational Technology Security

December 2023

This chapter should be cited as

ERIA study team (2023), 'Policy Recommendations for ASEAN–Japan Cooperation on Operational Technology Security', in Oikawa, K. and Y. Hatakeyama (eds.), *Operational Technology Security in ASEAN.* ERIA Research Project Report FY2023 No. 19, Jakarta: ERIA, pp.26-31.

Chapter 3

Policy Recommendations for ASEAN–Japan Cooperation on Operational Technology Security

Finally, with an understanding of the current initiatives by governments and companies in ASEAN, and the OT security initiatives in the US and EU where OT security measures are relatively advanced, we discussed the necessary efforts for ASEAN–Japan cooperation to enhance OT security in ASEAN. Please note that we have prioritised infrastructure industry and manufacturing industry as the highest focus for enhancing OT security, as explained in 1.4. The following recommendations are mainly formulated with these industries in mind. While there are several sectors within the manufacturing industry, such as heavy industry and light industry, and their priorities for OT security measures may vary, the overall approach to OT security remains unchanged, as explained in chapter 2. Therefore, we believe that these efforts can be applied to any manufacturing industry.

1. Summary

In making policy recommendations, we considered measures in the following steps, with implications drawn from Chapter 2.

Step 1: Current overview of operational technology security in ASEAN enterprises

Step 2: Issues in ASEAN enterprises and what they expect from ASEAN governments

Step 3: Current overview of operational technology security in ASEAN governments

Step 4: Issues in ASEAN governments and what they need for the region

As explained in Chapter 2, the current status of operational technology security measures in ASEAN is such that there are hardly any initiatives taken across the entire region, and only some countries and companies are independently promoting initiatives. On the other hand, ideally, coordinated efforts should be promoted throughout the region, and regulations should be introduced by each government based on a regional agreement, and corporate operational technology security measures should mature based on these regulations. In fact, in regions where operational technology security measures are being promoted, such a picture is being realised. The EU is developing common legal and certification systems throughout the region, and each government is introducing regulations based on a common mechanism. The US government is adopting compliance with its own standards, which have expanded international standards, as procurement requirements, and is raising the operational technology security measures of domestic companies.

Due to the expansion of global supply chains, the importance of coordination throughout the region has been increasing, and if countries and companies pursue their individual optimal efforts, they may lose global business opportunities. It is beneficial to deepen support in the following two directions. The first is to foster and horizontally develop operational technology security measures using a third-party perspective, such as hosting meetings where government, industry groups, and major companies gather to share best practices, or conducting cybersecurity exercises for major companies.

The second is to support the development of a common ASEAN framework based on global standards, the establishment of a common ASEAN company and product certification system, and the standardisation of procurement requirements, which is support for the development of common ASEAN systems.

In the following sections, we will explain in detail about the challenges and policy proposals.

2. Current Overview of Operational Technology Security in ASEAN Enterprises

Currently, there are four types of maturity levels for operational technology security in ASEAN companies.

(i) Companies less involved in global supply chains (GSCs) that have no operational technology security measures at all (mainly local small and medium-sized enterprises)

(ii) Companies involved in GSCs that have no operational technology security measures at all (mainly local small and medium-sized enterprises)

(iii) Companies involved in GSCs that have only ad hoc and passive operational technology security measures (mainly local large enterprises)

(iv) Companies involved in GSCs that have organized and integrated measures (mainly global companies and some local large enterprises)

The group of companies in (i) has not progressed in automation, is not aware of the need for operational technology security in the first place, and has no capability for strengthening operational technology security.

The group of companies in (ii) has not progressed in automation but recognises the need for operational technology security due to their relationship with companies in the supply chain. However, they have no capability for strengthening operational technology security, and have not taken any measures.

The group of companies in (iii) has advanced in automation across networks in one or multiple locations and recognises the need for operational technology security. However, the capability for strengthening operational technology security is insufficient, and measures remain ad hoc.

The group of companies in (iv) has advanced in automation across networks in one or multiple locations and recognises the need for operational technology security. On top of that, they have high capability for strengthening operational technology security and are currently able to take high-level operational technology security measures on their own.

3. Issues in ASEAN Enterprises and What They Expect from ASEAN Governments

The challenges faced and the required measures for governments vary according to the current maturity levels outlined in 3.2.

The problem faced by the group of companies in (i) is their failure to recognise the need for advancing operational technology security measures amidst a lack of digitalisation. Ideally, they should strive for a state of preparedness by proactively increasing the security level, rather than waiting until digitalisation progresses and security risks become apparent. Therefore, ASEAN governments are

required to carry out educational activities to emphasise the necessity of operational technology security measures. Specifically, it is necessary to raise awareness about industry trends such as operational technology-related incidents, rising geopolitical risks, and the benefits of strengthening operational technology security.

The problem faced by the groups of companies in (ii) and (iii) is insufficient knowledge and resources to tackle operational technology security measures. Ideally, they should aim for a state where their own operational technology security measures have sufficiently advanced without compromising their own interests. Therefore, ASEAN governments are required to provide specific knowledge and resources to advance operational technology security measures. This includes establishing national standards/guidelines for reference when formulating security policies and roadmaps, and defining skills and developing training for operational technology security personnel to enhance their capabilities.

The problem faced by the group of companies in (iv) is a lack of motivation to continuously update their operational technology security measures and a limited ability to disseminate these measures to suppliers. Ideally, they should aim for a state where their own operational technology security measures are constantly updated, and they are able to promote security measures amongst their suppliers. Therefore, ASEAN governments are required to provide incentives for updating operational technology security and to develop policy tools to involve suppliers. Specifically, for motivation, it is necessary to establish a corporate/product certification system for operational technology security that can be used to build external trust. Additionally, policy tools such as procurement requirements (including government subsidies) should be implemented to ensure compulsory assurances.

4. Current Overview of Operational Technology Security in ASEAN Governments

As detailed in section 3.3, each government is expected to provide enlightenment activities that explain the necessity of operational technology security measures, provide specific knowledge and resources, and provide update incentives and policy tools to involve suppliers. However, the current situation of the ASEAN governments is that while the Singapore government is responding to a certain extent, other countries are not catching up; in Singapore, CSA is disseminating the government's approach to security both domestically and internationally through an event called Singapore International Cyber Week, but in other countries, there is no national initiative.

As for providing specific knowledge and resources, Singapore is implementing part of global standards as national standards and providing training for the development of related personnel. Malaysia has just standardised part of the global standards in 2023, but in other countries, no national initiatives are seen.

In terms of providing incentives to update operational technology security and policy tools to involve suppliers, in Singapore, there are the ICT/IoT product certification systems such as CLS and NITES, and considerations are underway for updating and new certification with operational technology measures in mind. Also, Singapore mandates NITES evaluations for products handling data from government agencies. On the other hand, in other countries, initiatives such as certification and procurement requirements are not seen.

5. Issues in ASEAN Governments and What They Need

As outlined in Section 3.4, the ASEAN governments are currently not fully addressing the requirements expected of them, and there is a need to support regional efforts.

Regarding enlightenment activities, there is a lack of a unified approach amongst ASEAN countries, and while Singapore wishes to lead these activities, it cannot do so justifiably as it is only one member country. However, each government should aim to promote enlightenment activities quickly and broadly to their domestic enterprises.

In terms of providing specific knowledge and resources, there is a risk that disparate systems that deviate from global standards due to each government's limitations might proliferate in each country. However, each government should aim to provide knowledge and resources to their domestic enterprises involved in the global supply chain to ensure their continued participation in it.

Regarding providing incentives, the hurdle for regional collaboration is high. However, each government should aim to implement wide-ranging security regulations based on regional agreements, and to mature and scale them.

To bridge the gap between these challenges and the intended objectives, support is sought in two directions. The first is support for momentum building and lateral development of operational technology security measures, leveraging a third-party position. Specifically, translation and dissemination of global standards into the languages of each ASEAN country, hosting events for governments, industry associations, and major corporations to share best practices, and implementation of cybersecurity exercises for major corporations are all required on a regional basis. The second is support for the establishment of common systems amongst ASEAN countries. Specifically, support is sought for establishing a common framework for ASEAN countries based on global standards, such as the standard based on IEC 62443 and the development of skill definitions and training for operational technology security personnel. In addition, support for inter-country collaboration for further strengthening is also sought. Specifically, the establishment of a common company/product certification system within ASEAN and the adoption of procurement requirements compliant with operational technology security are required.

6. Recommended Policies for ASEAN–Japan Cooperation on Operational Technology Security

As explained in section 3.5, ASEAN governments face challenges and, as such, are seeking support from Japan for the promotion and widespread adoption of operational technology security measures from a neutral third-party perspective and assistance in the establishment of common regulations amongst ASEAN countries. The following provides detailed policy proposals. Going forward, it is expected that Japan will cooperate with ASEAN governments to contribute to the overall strengthening of operational technology security across ASEAN countries.

<u>Translation and dissemination of global standards in each ASEAN language</u>

Dissemination of global standards in a form that is easy for each country's government, industry groups, and major companies to refer to.

- Translation of IEC 62443 into each country's language

- Dissemination of information through websites, text messages, and various events, etc.

Organising events where all the governments, industry groups, and major companies from each country meet and share best practices

Aiming to build momentum, share knowledge, and strengthen relationships by sharing knowledge at events where each organisation comes together.

- Host annual events where governments, industry groups, and major companies from each country gather to share best practices in digitalisation through operational technology and efforts to strengthen operational technology security in ASEAN countries from Japan's perspective.
- Hosting sessions where each government, industry group, and major company shares their initiatives on operational technology security as a main theme for 30 minutes each.

Implementing cybersecurity drills for major companies

Conduct exercises for major companies aimed at acquiring correct knowledge for security enhancement, building momentum, and spreading knowledge.

- To acquire correct knowledge, provide information on global standards (conduct lectures to learn about governance establishment methods defined in IEC 62443 and key points for strengthening security during integrated management as explained in SP 800-82).
- To build momentum, share enlightenment activities and the status of initiatives in ASEAN countries (explain industry trends such as increasing incident/geopolitical risks and benefits from strengthening operational technology security. Also, share the status of initiatives such as domestic standards, certified qualifications, training, etc. in ASEAN countries).
- Conduct case studies and hands-on exercises utilising the advantages of drills, as well as exchanging opinions between companies.

Establishment of standards based on IEC 62443

Establish and expand standards compliant with IEC 62443, starting with the bare minimum requirements.

- Start by showing the steps of countermeasures for companies based on the defined requirements.
- It is assumed that effective enlightenment and guideline creation, conscious of gradually raising the Security Level (technical level) and Maturity Level (company maturity level) defined in IEC 62443, will be effective.
- For example, regarding system security requirements, start with achieving SL1 as the minimum line, and then gradually advance to achieve the necessary security level for each company.
- In addition, Singapore and Malaysia have experience in using IEC 62443 as their national standard, so it may be possible to proceed smoothly if implemented in cooperation with these countries.

Skill definition and training for operational technology security personnel

Develop training in line with the phased establishment and expansion of standards to help resolve the shortage of personnel in companies.

- Define the skills of operational technology security personnel in conjunction with the common standard development and expansion in ASEAN countries to clarify the personnel required by companies to strengthen operational technology security.
- Referring to the initiatives of ICSCoE, create training menus that match the digital progress of companies and organise nurturing training to secure the necessary security personnel at each stage to assist in resolving the personnel shortage.

Establishment of a common company/product certification system in ASEAN

Establish a system to certify efforts toward the established standards, taking into account each initiative.

- Refer to the operational system and certification framework established in Japan's CSMS certification to establish a system to certify efforts towards the established standards compliant with IEC 62443.
- One idea is to establish a certification system for product groups related to operational technology, referring to the efforts of Singapore's CLS.

Adoption of operational technology security compliance as procurement requirements

Adopt standards as common procurement requirements in ASEAN to strengthen supply chain security and facilitate collaboration.

- The US has strengthened supply chain security by adopting NISTSP800-171, and the Japan Defense Equipment Agency has adopted the Defense Industry Cybersecurity Standard as procurement standards.
- Strengthen supply chain security and facilitate collaboration between countries by adopting ASEAN common standards as operational technology security procurement requirements in each government.