ERIA Research Project Report FY2023 No. 19

Operational Technology Security in ASEAN

Edited by

Keita Oikawa

Yoichiro Hatakeyama

Economic Research Institute
for ASEAN and East Asia

Operational Technology Security in ASEAN

Economic Research Institute for ASEAN and East Asia (ERIA)
Sentral Senayan II 6th Floor
Jalan Asia Afrika No. 8, Gelora Bung Karno
Senayan, Jakarta Pusat 12710
Indonesia

ERIA Research Project Report FY2023 No. 19
Published in December 2023

List of Authors

Keita Oikawa
Economist, Economic Research Institute for ASEAN and East Asia (ERIA), Jakarta, Indonesia.

Yoichiro Hatakeyama
Senior Policy Advisor at the Economic Research Institute for ASEAN and East Asia (ERIA), Jakarta, Indonesia.

Koichi Hasegawa
Managing Director & Partner at Boston Consulting Group, Tokyo, Japan.

Masami Shibatani
Associate Director at Boston Consulting Group, Tokyo, Japan.

Eisuke Tanaka
Project Leader at Boston Consulting Group, Tokyo, Japan.

Junichi Ida
Consultant at Boston Consulting Group, Tokyo, Japan.

Yoko Yarimizu
Senior Associate at Boston Consulting Group, Tokyo, Japan.

Table of Contents

	List of Authors	iii
	List of Figures	v
	Executive Summary	vi
Chapter 1	Overview	1
Chapter 2	Current Status of Operational Technology Security	8
Chapter 3	Policy Recommendations for ASEAN–Japan Cooperation on Operational Technology Security	26
	Appendix	32

List of Figures

Figure 1.1	GDP by Industry in ASEAN Member Countries	5
Figure 1.2	GDP in ASEAN Member Countries and its Relationship with Japan	6
Figure 2.1	IEC 62443	12

Executive Summary

This study commemorates the 50th anniversary of Association of Southeast Asian Nations (ASEAN)–Japan friendship and cooperation by examining the challenges and proposing collaborative solutions for operational technology security in the ASEAN region. Multinational companies in Japan established international production networks (IPNs) in ASEAN and East Asia, which proved resilient during the coronavirus disease (COVID-19) pandemic and supported the regional economy. However, maintaining competitiveness requires addressing challenges such as advanced supply chain digitalisation and the associated need for increased security measures. Operational technology security risks, regulatory disparities, and governance frameworks are global concerns in the digitalisation of critical infrastructure. To enhance IPN competitiveness, cyber-resilience across Asia must be improved, prioritising operational technology security in critical infrastructure and manufacturing supply chains. This research bridges the gap between current and desired operational technology security states, proposes policies, and contributes to ASEAN cybersecurity readiness and IPN sustainability in collaboration between ASEAN and Japan.

While awareness of information and communication technology security is rising in ASEAN, operational technology security awareness and preparedness remain insufficient. In ASEAN, few countries have launched initiatives on operational technology security as a country. Singapore has developed its own standards based on International Electrotechnical Commission (IEC) 62443 and has also developed product certification for operational technology security in a way that is tied to government procurement requirements. Malaysia has begun to develop its own standards from 2023, by adopting IEC 62443. However, in other ASEAN countries no national initiatives have yet been seen.

As for current operational technology security level in ASEAN companies, while some are highly sensitive to it due to high awareness of enhanced governance and the occurrence of related incidents, others are not taking measures due to delays in digitalisation and lack of understanding of its necessity. Global companies and some local companies (e.g. companies in industries where operational technology-related incidents have occurred in the past, companies related to critical infrastructure, etc.) tend to take voluntary measures by referring to global standards, regardless of the existence of local standards. However, there are many companies that understand the importance of operational technology security but have yet to take systematic measures due to high cost, lack of experts, or lack of clear government guidelines. There are also many local companies that have not taken measures due to low priority caused by lack of understanding of the importance of operational technology security. In addition, there are companies that are not required to take operational technology measures due to the lack of automation in their plants.

In contrast to current status, ideally, coordinated efforts to enhance operational technology security 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 recent trends, due to the expansion of global supply chains, the importance of coordination throughout the region is increasing more and more, and if countries and companies pursue their individual optimal efforts, they may lose global business opportunities. In this context, Japan can contribute to solving issues that are difficult for governments and companies in ASEAN countries to solve. Specifically, it is believed to be 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 company and product certification system, and the standardisation of procurement requirements, which is support for the development of common systems.