

Key Messages:

- ASEAN has lost US\$2.87 million due to cyberattacks, which are mostly directed at financial services, with malware attacks being the top concern.
- Investment in cybersecurity in ASEAN has been increasing and will need to be sustained due to increasing digitisation and sustainability efforts involving connectivity.
- Money can buy technologies and systems, but it will not be effective unless clear guidelines and standards are in place. Cybersecurity is also about people – it will take a long time to solve problems such as digital talent gaps in several ASEAN Member States, as well as low awareness of potential events and ignorance of threats.

Michelle Chandra Kasih

Research Associate, Economic Research Institute for ASEAN and East Asia (ERIA)

Fostering ASEAN's Digital Future through Cybersecurity Policies and Human Empowerment

Michelle Chandra Kasih

The adoption of advanced technology comes with the risk of cyberattacks. Despite the remarkable prospects of the digital economy, the cost of cyberattacks has reached millions of US dollars and is projected to increase. Investment is needed to provide cybersecurity to help secure the growth of the digital and sustainable economy and anticipate more advanced attacks. As investment in cybersecurity has started to grow in the Association of Southeast Asian Nations (ASEAN), challenges are present in the intangible form of in-existent or strict policies, skill shortages, and insufficient public awareness, which can halt the effectiveness of such investment. This policy brief proposes four policy recommendations to ensure successful investment in cybersecurity:

- 1. Ensure that cybersecurity policies and legal frameworks are not underdeveloped or overly restrictive.*
- 2. Support small businesses in earning customer trust through cost-effective guidelines.*
- 3. Incentivise and maintain partnerships for education, research, and capacity building with ethical education for future experts.*
- 4. Raise cyber hygiene and establish integrative reporting platforms that help people identify and detect cyber risk.*

Growing Investment in Cybersecurity due to Increasing Digitisation and Cyberattacks

Protection against cyberattacks on data, programmes, and networks has never been more important due to the increasing frequency of such attacks. Cybersecurity Ventures predicted global cybercrime costs to grow by 15% per year, reaching US\$10.5 trillion annually by 2025 (Morgan, 2020). By July 2022, ASEAN had lost US\$2.87 million due to cyberattacks (IBM, 2022). Cyberattacks in ASEAN are mostly directed at financial services, and malware attacks are the top concern (Palo Alto Networks, 2023).

In response to these threats, investment in cybersecurity¹ is increasing in ASEAN, and the cybersecurity market is expected to expand. Cybersecurity revenue in the ASEAN market is projected to reach US\$4.39 billion in 2023, up 13% from 2022 (Statista, n.d.). In Indonesia, many fintech and e-commerce companies, including the central government, have increased their cybersecurity budgets due to the changing threats in the digital space. In 2020, after realising that the data of 91 million of its users was sold on the dark web (CNN Indonesia, 2020), Tokopedia outsourced an international cybersecurity company to investigate these losses and anticipate future attacks (Interpol, 2022). In 2023, the Government of Indonesia approved a budget increase for the National Cyber and Crypto Agency (BSSN) of Rp70 billion following rampant cases of hacking and security breaches in 2022 (Bhwana, 2022). Similarly, in Malaysia, the government proposed to increase the cybersecurity budget to RM73 million in 2023 (Othman, 2022).

Despite increased public and private sector investment, more is needed to combat cyberattacks. For ASEAN, a region that mostly consists of low- to middle-income countries (or developing countries), digitalisation of the economy has been seen as a catalyst for economic growth. It supports efficiencies in payment transfers, access to loans, trading, shopping, and others. A survey by Google, Temasek, and Bain predicted that ASEAN's digital economy is on track to grow to US\$1 trillion gross merchandise value by 2030, as millions of new internet users start to use e-commerce and digital finance (Google, Temasek and Bain, 2021). Sustainable regional policies such as the ASEAN Framework for Circular Economy and the ASEAN Framework on Sustainable Tourism Development in the Post-COVID-19 era include digitalisation as one of their enablers. The use of online platforms and machine learning can enhance value and supply chain efficiency, including the traceability of products, as well as support sustainable tourism and small businesses. Thus, in the context of increasing connectivity, cybersecurity investment could be a deciding factor in achieving sustainable growth in ASEAN.

¹ Definitions of cybersecurity vary, but in essence they refer to the application of technologies, processes, and controls to protect systems, networks, programmes, devices, and data from cyberattacks through malware and denial of service, amongst others.

How Can Developing Countries Ensure the Sustainability and Effectiveness of Cybersecurity Investment?

Cybersecurity investment covers a range of measures such as software and hardware adoption, employee training, and incident response, depending on the necessity. More investment in cybersecurity could translate to partnerships with start-ups to fill gaps in businesses' needs (Daglioglu, 2022). Innovations in the cybersecurity sector, such as the integration of artificial intelligence (AI) and cyber insurance, are on the rise. However, without clear guidelines on accountability, increased spending on cybersecurity technology and infrastructure may not be effective. Cybersecurity is also about people. Resolving digital talent gaps in several AMS, as well as low awareness of potential events and ignorance of threats, may take considerable time and effort.

(1) Ensure that cybersecurity policies and legal frameworks are not underdeveloped or overly restrictive

Having cybersecurity or data protection laws could imply the commitment of the state and increase confidence in the market that cybersecurity investment and businesses are protected. The presence of laws also ensures that businesses and organisations take the necessary measures to protect their data and systems, investing in technologies and human resources. An example of this is the impact of the General Data Protection Regulation (GDPR), implemented by the European Union (EU) in 2018. To comply with GDPR standards of data protection and privacy for individuals in the European Union, a survey by a firm in the United Kingdom recorded that 68% of European businesses and 75% of British companies have invested in cybersecurity (RSM, 2020). A study by Capgemini also reported that compliance with data protection regulations has led to better reputations and more trust, which could lead to increased revenue (Capgemini Research Institute, 2019).

ASEAN does not have a cybersecurity framework. Nonetheless, ASEAN cited cybersecurity as a significant factor in the ASEAN Digital Masterplan 2025; ASEAN Cybersecurity Cooperation Strategy, 2021–2025; ASEAN Framework on Personal Data Protection; ASEAN Framework on Digital Data Governance; and ASEAN Data Management Framework, including the Implementing Guidelines

for ASEAN Data Management Framework and ASEAN Cross Border Data Flows Mechanism. Other ASEAN documents also included cybersecurity as a consideration in developing 5G ecosystems and in protecting critical information infrastructure (CII). Initiatives have been taken, amongst others, to strengthen legal, regulatory, and policy aspects under the ASEAN Data Protection and Privacy Forum, as well as enhancing coordination through the ASEAN Cybersecurity Coordinating Committee. Regarding international agreements, the Philippines is the only AMS that has ratified the Budapest Convention on Cybercrime (2001).

Cybersecurity policies and legal frameworks often refer to the protection of CII, identifying key sectors and designating institutions to respond to and mitigate CII attacks. However, not all AMS have both legislation and action plans on cybersecurity. Indonesia, Singapore, Thailand, and Viet Nam have dedicated laws for securing CII. Brunei Darussalam, Malaysia, the Philippines, Singapore, and Viet Nam have cybersecurity national strategies or plans. These AMS share the same sectoral classification of CII – government administration, energy, transport, finance, health, and information and communication technology.

In terms of related cybersecurity policies and legislation, such as data protection, each AMS takes a diverse approach. Indonesia, the Lao People's Democratic Republic (Lao PDR), Malaysia, the Philippines, and Singapore have laws focused on data protection. Brunei Darussalam has a national data protection policy, while in Myanmar and Viet Nam, data protection measures are still scattered across various laws and regulations. On the other hand, Cambodia does not have any data protection laws or regulations. Learning from the impact of the GDPR, the presence of comprehensive cybersecurity policies, especially binding legal instruments, facilitates compliance through effective reporting systems and sanctions, which could help cybersecurity investment increase and work in a clear direction.

In addition to policies, cybersecurity requires necessary measures. Countries can establish standards that ensure data protection and offer consumers better information about their smart devices. For example, Singapore established the Cybersecurity Labelling Scheme in 2019, which allows consumers to identify the level of cybersecurity of smart devices through official ratings. This labelling system has gained

mutual recognition from Finland and Germany (Cyber Security Agency of Singapore, n.d.). On the other hand, cybersecurity has increasingly been invoked as an aspect of 'national security', which is considered an important factor that impacts international trade and investment policy (Huang, Madnick, and Johnson, 2019). Restrictions and bans on businesses in the name of cybersecurity coincided with rising geopolitical tensions. Examples include bans on products from Kaspersky Lab, Huawei, and ZTE in the US due to suspicion of espionage (BBC, 2022; Reuters, 2017) and LinkedIn's restriction in Russia because of a refusal to comply with data localisation measures (Breene, 2016). Scholars also argue that data localisation could create barriers for businesses, particularly in big data and cloud computing, and reduce operational efficiency (Chen, 2022). Data localisation is often imposed to protect essential data for national security and to promote the local economy (McKinsey & Company, 2022), as applied by Indonesia and Viet Nam for data managed by public electronic system operators² and cyberspace service providers,³ respectively. In line with data localisation measures, Indonesia needs to apply a clearer cross-border personal data transfer requirement, to identify which countries have an equal or higher level of protection.⁴ It is understood that each AMS has its own challenges and standards, but the purpose of their cybersecurity policies, laws, and regulations must be clarified legally and transparently to avoid excessive restrictions (Chen et al., 2019).

(2) Support small businesses through cost-effective guidelines

Cyber criminals target companies of all sizes, and small and medium-sized enterprises (SMEs) are the most vulnerable. According to *Forbes*, 43% of cyberattacks are aimed at SMEs, but only 14% are prepared to defend themselves (Brooks, 2022). In ASEAN, SMEs are the backbone of the ASEAN economy, contributing to more than half of total employment and 95%–99% of all business establishments in 2019 (ERIA, 2019). SMEs often have limited technical capabilities,

² Article 20 of Government Regulation No. 71 of 2019 on the Organisation of Electronic Systems and Transactions.

³ Article 26.3 of the Vietnamese Law on Cybersecurity, 2018.

⁴ Indonesia's Law No. 27 of 2022 on Personal Data Protection and Government Regulation No. 80 of 2019 on E-commerce allows cross-border personal data transfer if the destination country has equal or better data protection mechanisms.

time, and resources, and cyberattacks can have broader consequences. Looking at the contribution of SMEs to the ASEAN economy, ASEAN can build cost-effective guidelines for SMEs to comply with existing policies and legislation and to carry out training. These efforts can be complemented with government-based cybersecurity certification for SMEs that have met good practice standards in the technical aspect of cybersecurity, especially for those that are having difficulties in achieving international standards (Cardiff University's Centre for Cyber Security Research, n.d.).

(3) Incentivise and maintain partnerships in education, research, and capacity building with ethics for future experts

Countries with higher-skilled and better educated workforces tend to attract more greenfield foreign direct investment (FDI) projects (Caon, 2020). However, despite an enlarging market, several AMS (e.g. Cambodia, Indonesia, Lao PDR, and Myanmar) have a shortage of cybersecurity experts (National Cyber Security Index, n.d.). Some cybersecurity companies in Indonesia have reported talent deficits as one of the challenges to balancing rapid technological development (Suhartadi, 2016). However, this could present an opportunity for cybersecurity investment by facilitating training of existing employees and the identification of future talent.

Developed countries have also faced the need to generate cybersecurity talent (Executive Office of the President, 2016). In 2016, the United States launched its Cybersecurity National Action Plan, which focused on investing in modern information technology, as well as offering scholarships and loan forgiveness programmes for students interested in cybersecurity education to join the government. In addition, public-private partnerships were established to enhance cybersecurity research and development, which aimed to develop and deploy technical solutions to cybersecurity challenges (White House, 2016). At the ASEAN level, the establishment of the ASEAN Cybercrime Operations Desk, the ASEAN Cyber Capacity Development Project, and the ASEAN Regional Computer Emergency Response Team aim to build the cyber capacity of AMS, threat information-sharing, and coordination on incidence response. In some AMS, such as Cambodia, the government has offered scholarships for students interested in digital technology (Matthew, 2023).

Encouraging students at a young age to enter the field can provide societal benefits. This can be done by offering cybersecurity lessons in the education system and assured employment after finishing their studies, with a good salary and promising career path. This could include attention to ethics, so that experts not only know what they can do, but also what they should do. Moreover, as the effectiveness of policy and laws partially depends on how they are enforced, laws also need to identify and ensure the capabilities of regulatory bodies and law enforcement agencies. Countries can collaborate with each other and international organisations to share best practices, expertise, and resources on cybersecurity. For example, regional trade agreements such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)⁵ have recognised the importance of capacity building for emergency response and collaboration in identifying malicious intrusions. Multilateral arrangements can help build capacity and strengthen cybersecurity efforts.

(4) Raise cyber hygiene and establish integrative reporting platforms that help people identify and detect cyber risk

Raising awareness about cybersecurity is crucial because human error is a major vulnerability that even the best technology and employees cannot fix. This can come in the form of weak passwords, email misdelivery, or careless clicks. According to IBM, negligent actions by employees or contractors accounted for 21% of data breaches worldwide in 2021 (IBM, 2022). Public campaigns could enhance the public's ability to avoid, detect, and respond to cyber incidents. Information on how citizens, SMEs, and institutions can secure data with multi-factor authentication, data backup, and what to do after a cyberattack, can make a difference. This campaign requires continuous efforts to keep up with the evolving cybersecurity landscape, as cyberattacks are expected to increase the scale of the dissemination and sophistication of social engineering methods (Interpol, 2022).

Simultaneously, initiatives and cooperation between ministries and society can minimise the cost of cyberattacks. For example, in Indonesia, people have

⁵ Article 14.16 of the CPTPP on Cooperation on Cybersecurity Matters. ASEAN members of the CPTPP are Malaysia, Singapore, and Viet Nam.

used social media to warn others not to click on and download suspicious attachments sent by unknown users to their WhatsApp accounts. However, such measures are sporadic and may not reach all individuals. A live reporting platform accessible to the public could assist society in anticipating possible threats. Potential cyberattacks could be tagged and checked. Such systems can help societies anticipate and respond to cyber threats more efficiently.⁶

Policy Recommendations

Cybersecurity is a major factor in digital trust. As internet use becomes more prevalent, the costs associated with repairing damage from cyberattacks will outweigh the costs of reducing such damage. Investment in cybersecurity in ASEAN is rising. To foster it, governments need to address several aspects. First, AMS could prioritise the development of cybersecurity policies and legal frameworks that strike a balance between allowing investment and national defence. Over-regulation may increase the cost of investment, while under-regulation could affect trust. Harmonisation of cyber regulations for different CII sectors could help ease of doing business. Regionally, an overarching cybersecurity framework aligned with international best practices and standards could help create a safer cyberspace for all. Second, to create a guideline specifically for SMEs that lack experience and resources to protect their data and respond to cyberattacks. A cybersecurity certification scheme could be a valuable marketing asset that would reassure customers. Third, many AMS suffer from talent deficits, which could affect FDI flow in cybersecurity. International partnerships and cooperation with the private sector should be strengthened in capacity building and incentivising students and interested workers to take up cyber education or cybersecurity to address national (and regional) skill shortages in cybersecurity. Last, enhancing awareness through public campaigns and providing facilities to report cyberattacks would increase the effectiveness of cybersecurity investment and promote a more secure ASEAN digital community.

⁶ For example, see Cisco (n.d.).

References

- ASEAN (n.d.-a), Key Documents. <https://asean.org/our-communities/economic-community/asean-digital-sector/key-documents/>
- ASEAN (n.d.-b), Overview. <https://asean.org/our-communities/economic-community/resilient-and-inclusive-asean/development-of-micro-small-and-medium-enterprises-in-asean-msme/>
- ASEAN (2016), 'ASEAN–Japan Critical Information Infrastructure Protection Guidelines, Version 3.0'. <https://asean.org/wp-content/uploads/2012/05/01-CIIP-Guidelines-Ver3.0.pdf>
- ASEAN (2022), 'Development of Best Practice Guides for 5G Ecosystem Development in ASEAN'. <https://asean.org/wp-content/uploads/2022/02/03-ASEAN-5G-Ecosystem-Best-Practices-Guide-Final-Report-SG-ASEC-TL-PH-MY.pdf>
- BBC (2022), 'US Bans Sale of Huawei, ZTE Tech amid Security Fears', 26 November. <https://www.bbc.co.uk/news/world-us-canada-63764450>
- Bhwana, P.G. (2022), 'Rp70bn BSSN Budget Raise; PSI Calls for Transparency over Cyber Security Plan', *Tempo*, 26 September. <https://en.tempo.co/read/1638408/rp70bn-bssn-budget-raise-psi-calls-for-transparency-over-cyber-security-plan>
- Breene, K. (2016), 'As Russia Blocks LinkedIn: These Countries Already Deny Access to Social Networks', World Economic Forum, 17 November. <https://www.weforum.org/agenda/2016/11/russia-is-about-to-block-linkedin-these-6-countries-already-deny-access-to-social-networks/>
- Brooks, C. (2022), 'Cybersecurity in 2022 – A Fresh Look at Some Very Alarming Stats', *Forbes*, 21 January. <https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=139a08706b61>
- Caon, V. (2020), 'FDI Drivers and the Quest for Talent', *Investment Monitor*, 23 November. <https://www.investmentmonitor.ai/features/fdi-drivers-and-the-quest-for-talent/>
- Capgemini Research Institute (2019), 'Championing Data Protection and Privacy: A Source of Competitive Advantage in the Digital Century'. https://www.capgemini.com/de-de/wp-content/uploads/sites/5/2019/09/Report_GDPR_Championing_DataProtection_and

Privacy.pdf

- Chen, L. (2022), 'The Indo-Pacific Partnership and Digital Trade Rule Setting: Policy Proposals', *ERIA Discussion Paper Series*, No. 466. Jakarta: Economic Research Institute for ASEAN and East Asia.
- Chen, L., W. Cheng, D. Chiuriak, and F. Kimura (2019), 'The Digital Economy for Economic Development: Free Flow of Data and Supporting Policies', T20 Japan 2019. <https://t20japan.org/wp-content/uploads/2019/03/t20-japan-tf8-4-digital-economy-economic-development.pdf>
- Cisco (n.d.), Cisco Talos Intelligence Group – Comprehensive Threat Intelligence (accessed 24 March 2023).
- CNN Indonesia (2020), 'Complete Chronology of 91 million Tokopedia Accounts Leaked and Sold', 3 May. <https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual>
- Cyber Security Agency of Singapore (n.d.), Cybersecurity Labelling Scheme (CLS). <https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme>
- Daglioglu, A.B. (2022), 'In the era of the global start-up, countries must step up their game to attract FDI', World Economic Forum, 19 July. <https://www.weforum.org/agenda/2022/07/globalized-startup-countries-attract-fdi/>
- ERIA (2019), 'Study on MSMEs Participation in the Digital Economy in ASEAN', Study on MSMEs Participation in the Digital Economy in ASEAN: Nurturing ASEAN MSMEs to Embrace Digital Adoption (eria.org)
- Executive Office of the President (2016), 'Federal Cybersecurity Workforce Strategy', Memorandum, 12 July. https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2016/m-16-15.pdf
- Google, Temasek and Bain (2021), 'e-Conomy SEA 2021', e-Conomy report SEA 2021 (bain.com)
- Huang, K., S. Madnick, and S. Johnson (2019), 'Framework for Understanding Cybersecurity Impacts on International Trade', *Working Paper CISL*, No. 2019-23. Cambridge, MA: Massachusetts Institute of Technology. <http://web.mit.edu/smadnick/www/wp/2019-23.pdf>
- IBM (2022), 'Cost of a Data Breach Report 2022'. <https://www.ibm.com/downloads/cas/3R8N1DZJ#:~:text=Average%20total%20cost%20of%20a,million%20in%20the%202020%20report>
- Interpol (2022), 'ASEAN Cyberthreat Assessment 2021'. Singapore: Interpol.
- IT Governance (n.d.), What is Cyber Security? Definition and Best Practices. <https://www.itgovernance.co.uk/what-is-cybersecurity>
- McKinsey & Company (2022), 'Localization of Data Privacy Regulations Creates Competitive Opportunities', 30 June. <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/localization-of-data-privacy-regulations-creates-competitive-opportunities>
- Matthew, M. (2023), '500 "Techo Digital Talent Scholarships" up for grabs', *Khmer Times*, 4 January. <https://www.khmertimeskh.com/501213433/500-techo-digital-talent-scholarships-up-for-grabs/>
- Morgan, S. (2020), 'Cybercrime to Cost the World \$10.5 Trillion Annually By 2025', *Cybercrime Magazine*, 13 November. <https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/>
- National Cyber Security Index (n.d.), <https://ncsi.egee/compare/>
- Othman, N.Z. (2022), '#TECH: Tech Companies Laud Proposed Budget Allocation to Boost Nation's Cybersecurity', *New Straits Times*, 11 October. <https://www.nst.com.my/lifestyle/bots/2022/10/839601/tech-tech-companies-laud-proposed-budget-allocation-boost-nations>
- Palo Alto Networks (2023), 'State of Cybersecurity Report ASEAN 2022' (Infographic). <https://s3.ap-southeast-1.amazonaws.com/cdn.thinklogicmarketing.com/CybersecAsia/Infographics/%5BInfographic%5D+Palo+Alto+Networks+State+of+Cybersecurity+Report+ASEAN+2022.pdf>
- Reuters (2017), 'Israeli Spies Found Russians Using Kaspersky Software for Hacks: Media', 11 October. <https://www.reuters.com/article/us-usa-security-kaspersky/israeli-spies-found-russians-using-kaspersky-software-for-hacks-media-idUSKBN1CG05P>

- RSM (2020), 'Impact of the GDPR on Cyber Security Outcomes'. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/906691/Impact_of_GDPR_on_cyber_security_outcomes.pdf
- Statista (n.d.), Cybersecurity – ASEAN. <https://www.statista.com/outlook/tmo/cybersecurity/asean>
- Statista (2022), 'Value of the e-commerce market in Southeast Asia from 2019 to 2022 and a forecast for 2025'. <https://www.statista.com/statistics/958414/southeast-asia-e-commerce-market-value/#:~:text=In%202022%2C%20the%20e%2Dcommerce,approximately%20131%20billion%20U.S.%20dollars>
- Suhartadi,I.(2016), 'Indonesia Lacks Cyber Security Talent', *Berita Satu*, 26 December. <https://www.beritasatu.com/ipitek/406490/indonesia-kekurangan-bakat-cyber-security>
- WEF (2022), 'Earning Digital Trust: Decision-Making for Trustworthy Technologies'. https://www3.weforum.org/docs/WEF_Earning_Digital_Trust_2022.pdf
- White House (2016), 'FACT SHEET: Cybersecurity National Action Plan'. <https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>

Previous Policy Briefs

- Sefrina, M. (2023), *Understanding the ASEAN Digital Economy Framework Agreement: A Means to Support ASEAN Integration*. ERIA Policy Brief, No. 2023-01, April 2023.
- Ing, L.Y. and I. Markus (2023), *ASEAN Digital Community 2040*. ERIA Policy Brief, No. 2022-11, February 2023.
- Isono, I. and S. Kumagai (2023), *ASEAN's Role in the Threat of Global Economic Decoupling: Implications from Geographical Simulation Analysis*. ERIA Policy Brief, No. 2022-10, January 2023.
- Afifi, F.A.R., V. Anbumozhi, D. Chen, A. Halimaussadiah, V. Hardjono, R.E.G. Lutfi, D. Lutfiana, J. Mauricio, A.J. Purwanto, W.W. Purwanto, J. Roychoudhury, C.E.N. Setyawati, M.A. Suwailem, and W.T. Woo (2023), *Reframing of Global Strategies and Regional Cooperation Pathways for an Inclusive Net-Zero Strategy in the Energy Transition Framework*. ERIA Policy Brief, No. 2022-09, January 2023.
- Isono, I., S. Kumagai, and K. Oikawa (2023), *Geographical Simulation Analysis for CADP 3.0*. ERIA Policy Brief, No. 2022-08, January 2023.
- Ramadhan, R.M. and P.A. Muchtar (2023), *Facilitating Global Trade and Investment and Leveraging Value Added in Downstream Industries*. ERIA Policy Brief, No. 2022-07, January 2023.
- Sapulette, M.S and P.A. Muchtar (2023), *Redefining Indonesia's Digital Economy*. ERIA Policy Brief, No. 2022-06, January 2023.
- Markus, I. and P.A. Muchtar (2023), *The Global Economic Outlook and the State of Indonesia*. ERIA Policy Brief, No. 2022-05, January 2023.
- Arima, J., H. Hashimoto, H. Moghaddam, Y.D. Priadi, and A.J. Purwanto (2022), *Exploring Short-term Solutions to the Global Gas Crisis*. ERIA Policy Brief, No. 2022-04, December 2022.
- Thangavelu, S.M., F. Kimura, S. Urata, and D. Narjoko (2022), *New Dynamism in ASEAN and East Asia: The Role of the RCEP as a 'Living' Agreement*. ERIA Policy Brief, No. 2022-03, December 2022.
- Singh, R. (2022), *Inclusive Education: Overcoming Barriers for Students with Disability in ASEAN*. ERIA Policy Brief, No. 2022-02, October 2022.


ERIA policy briefs from previous years can be found at:



©ERIA, 2023.

DISCLAIMER:

The findings, interpretations, and conclusions expressed herein do not necessarily reflect the views and policies of the Economic Research Institute for ASEAN and East Asia, its Governing Board, Academic Advisory Council, or the Institutions and governments they represent. All rights reserved. Material in this publication may be freely quoted or reprinted with proper acknowledgement.

 Economic Research Institute for ASEAN and East Asia
Sentral Senayan 2, 5th, 6th, and 15th floors
Jalan Asia Afrika No.8
Senayan, Central Jakarta 10270, Indonesia
Tel: (62-21) 57974460
Fax: (62-21) 57974463
E-mail: contactus@eria.org