ASEAN Regional Effort on Cybersecurity and its Effectiveness

MONICA NILA SARI

Introduction

The Association of Southeast Asian Nations (ASEAN), which consist of 10 member countries namely Brunei Darussalam, Cambodia, Lao PDR, Indonesia, Malaysia, Myanmar, Philippines, Thailand, Singapore and Vietnam, is one of the fastest growing Internet markets in the world with 125,000 new users coming online every day. ASEAN has more than 440 million Internet users, and more importantly, 350 millions of them, or about 80%, are digital customers, i.e. Internet users who have bought at least one online service.[1] With a fast-growing base of digital customers and merchants, acceleration in e-commerce and food delivery, ASEAN experienced a positive trend of GDP of more than USD 3.11 trillion in 2020. Resulting in ASEAN to, collectively, become the fifth largest economy in the world.[2] As ASEAN experienced accelerated digitalisation, which has helped to grow the region's digital economy, but have also led to new and novel challenges.

ASEAN countries' Internet penetration is now over 77.6% which is above the global Internet users worldwide (59.5%).[3] With the ASEAN region seeing exponential growth in the digital technology sector, particularly financial technology and e-commerce, there is an increasing demand for Internet and broadband services. However, this increasing reliance on the Internet has created a large number of security threats that can cause immense damage. Based on the ASEAN Cyberthreat Assessment 2021 produced by the INTERPOL ASEAN Cybercrime Operations Desk, ASEAN countries have become a prime target for cyberattack considering their position among the fastest-growing digital economies in the world. An analysis by A.T. Kearney indicated that ASEAN countries are being used as launchpads for cyberattacks - either as vulnerable hotbeds of unsecured infrastructure where numerous computers can be infected easily for large-scale attacks or as hubs for a single point of attack

[1] "e-Conomy SEA report 202", Bain & Company, accessed on May 10, 2022, _sea_2021_report.pdf
[2] "ASEAN Key Figures 2021", the ASEAN Secretariat, https://asean.org/wp-content/uploads/2021/12/ASEAN-KEY-FIGURES-Chapter-1-4-Rev-28-Dec-2021.pdf

[3] Internet penetration in Southeast Asia as of June 2021, Statista, https://www.statista.com/statistics/487965/internet-penetration-in-southeast-asian-countries/

to gain access to the hubs' global connection.[4] Malaysia, Indonesia and Vietnam are global hotspots for major blocked suspicious Web activities – up to 3.5 times the standard ratio, indicating that these countries are being used to launch malware attacks.[5] The said analysis argued that the ASEAN's policy, governance, and cybersecurity capabilities is relatively low.

As one of the most successful regional organisation in the world, ASEAN has an "ASEAN way" approach in the organisation's decision making process which is upholding the consensus principle based on ASEAN Charter. Some scholars argued that this ASEAN way could limit the group of ten in accomplishing substantial achievement in finding common ground and mutually acceptable outcome. ASEAN respects the principle of territorial integrity, sovereignty, non-interference and national identities of ASEAN Member States.[6] The question arises whether this ASEAN way and principle of ASEAN regionalism is effective in dealing with cybersecurity in the region. Moreover, ASEAN is characterized by a high degree of heterogeneity in terms of economic development, which resulted in notable gap in terms of cyber maturity and ASEAN countries' commitment and political will to engage with cybersecurity policy. This paper will analyse how effective the ASEAN's regional approach in dealing with cybersecurity issues in the region, taking into accounts the ASEAN way in consensus decision making and its non-interference principle. In this regard, I will use the theory of effectiveness by by Amos N. Guiora,[7] where cyber security effectiveness relies on policy allocating resources effectively, being based on a cost benefit analysis, and being based on accurate risk assessment. Furthermore, this paper will also present a data breach case in Indonesia as the biggest internet users in ASEAN to assess as well the effectiveness of ASEAN regional approach on cybersecurity. With this case study, it will demonstrate the importance of data protection regulation in strengthening cybersecurity framework, as well as the

[4] "Cybersecurity in ASEAN: An Urgent Call to Action", Cisco and A.T. Kearney, 5, https://www.southeast-asia.kearney.com/documents/1781738/1782318/Cybersecurity+in+ASEAN—An+Urgent+Call+to+Action.pdf/80a880c4-8b70-3c99-335f-c57e6ded5d34
[5] "Internet Security Threat Report Volume 22", Symantec, https://docs.broadcom.com/doc/istr-22-2017-en
[6] The ASEAN Charter, https://asean.org/wp-content/uploads/images/archive/publications/ASEAN-Charter.pdf
[7] Guiora, Amos. N, *Cybersecurity: Geopolitic, Law and Policy*, (Taylor & Francis, Group, 2017)

development of data protection in ASEAN countries. The conclusion of this paper will provide policy recommendation for strengthening ASEAN's cybersecurity framework.

ASEAN's Effort on Cybersecurity

ASEAN leaders shared the vision of a peaceful, secure and resilient regional cyberspace that serves as an enabler of economic progress, enhanced regional connectivity and betterment of living standards as stated in the ASEAN Leaders' Statement on Cybersecurity Cooperation.[8] Moreover, ASEAN recognises the multi-faceted nature of cybersecurity and the different dimensions of cybersecurity cooperation are discussed under each of the three pillars of ASEAN. On the ASEAN Political-Security Community pillar, it specifically addresses the need to strengthen cooperation on cybersecurity from all aspects, including developing and improving laws and capacity building for law enforcement. Under the ASEAN Economic Community pillar, cybersecurity is discussed from the angle of cyber infrastructure and information protection, whereas discussion on cybersecurity within the ASEAN Socio-Cultural Community pillar is focused on the promotion of cyber wellness through policy initiatives and activities that relate to developing digital literacy and mitigating the harmful effects of fake news.[9]

ASEAN Mechanism

Relevant ASEAN Sectoral Bodies and ASEAN-led mechanisms[10] have been working on cyber security issues, namely the ASEAN Digital Ministers' Meeting (ADGMIN) and the ASEAN Digital Senior Officials' Meeting (ADGSOM) as its subsidiary body, the ASEAN

[8] "ASEAN Leaders' Statement on Cybersecurity Cooperation", 2018, https://asean.org/wp-content/uploads/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf
[9] Ibid
[10] ASEAN's constructive engagement with its external partners, through ASEAN-led mechanisms such as the ASEAN Plus-One, ASEAN Plus Three (APT), East Asia Summit (EAS), ASEAN Regional Forum (ARF) and ASEAN Defence Ministers' Meeting Plus (ADMM-Plus), in building mutual trust and confidence as well as reinforcing an open, transparent, inclusive and rules-based regional architecture with ASEAN at the centre.

Regional Forum (ARF), the ASEAN Ministerial Meeting on Transnational Crime (AMMTC), the East Asia Summit (EAS), the ASEAN Defence Ministers' Meeting (ADMM)-Plus.

On the area of cybercrime, the ASEAN Ministerial Meeting on Transnational Crime (AMMTC) has the mandate to discuss the said issue. Under this mechanism, ASEAN has adopted ASEAN Declaration to Prevent and Combat Cybercrime in 2017. Recognising the need to address the rapid growth of cyber-security threats, the ARF established the ARF Inter-Sessional Meeting on Security of and in the Use of ICTs in 2017. It serves as a specific platform for ARF Participants to promote mutual understanding as well as to discuss and coordinate ARF's efforts on ICTs security, to implement the ARF Work Plan on Security of and in the Use of ICTs as well as to enhance trust and confidence through capacity building whilst ensuring that in the conduct of its activities. To guide the work of the ISM on ICTs Security, the ARF Work Plan on Security of and in the Use of ICTs was adopted in 2015. It serves to promote a peaceful, secure, open and cooperative ICT environment and to develop transparency and confidence-building measures to prevent conflict in cyberspace between states in the ARF region through capacity building. ARF recently adopted "ARF Terminology in the Field of Security of and in the use of ICTs" in September 2020 to encourage discussion among ARF participants on their domestic views and definitions pf key ICTs related terminologies utilised in their respective countries.

Initiatives on cybersecurity under the ASEAN Economic Community pillar is under the mechanism ASEAN Digital Ministers 'Meeting (ADGMIN). This mechanism before was named ASEAN Telecommunication and Information Technology Ministers Meeting (TELMIN), and it changed in 2019 to reflect the widening scope of work of the ICT ministries across ASEAN.[11] On cyber defence, in 2021 ADMM has adopted concept papers on ASEAN Cyber Defence Network and the ADMM Cybersecurity and Information Centre of Excellence, as important milestones in promoting practical cybersecurity cooperation in ASEAN. These

[11] ASEAN Secretariat, www.asean.org

efforts serve as Confidence-Building Measures (CBMs) within the region, and ASEAN would like to encourage other regions to adopt similar measures, towards building trust and confidence at the global level. In order to reinforce the Leaders' intention to strengthen cooperation in cybersecurity, this issue has been increasingly featured under the ambit of the East Asia Summit (EAS). This mechanism has provided workshop regional cyber capacity building as well as Leaders' commitment to promote open, secure, stable, accessible and peaceful cyberspace.

ASEAN has various mechanisms dealing with cybersecurity with the aim to facilitate the deliberations of cybersecurity cooperation under the three pillars of ASEAN. In order to strengthen cross-sectoral coordination as cybersecurity is a cross-cutting issue, in 2020 ASEAN established the ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber-CC) to tackle the coordination challenges, and to promote cross sectoral and cross-pillar cooperation and strengthen cybersecurity in the region. Under this new mechanism, ASEAN is now developing a Regional Action Plan on the Implementation of the Norms of Responsible State Behaviour in Cyberspace to assist with the prioritization and implementation of the 11 voluntary, non-binding norms of responsible State behaviour in the use of ICTs.

These ASEAN Sectoral Bodies and ASEAN-led mechanisms are not only aiming to produce Chairman's Statement or to adopt agreed documents. Its regular meetings among regional leaders and officials provide diplomatic ecosystem where many informal and side-line engagements take place. ASEAN meetings engender a sense of familiarity and a give-and-take approach which in turn facilitate consensus-building on contentious issues. These mechanisms are also forum for ASEAN countries and partners to discuss relevant issues related to cybersecurity.

Regional Framework

Over the past few years, the ASEAN region has shown the way forward on how to build a regional cybersecurity cooperation framework. First, ASEAN has updated its cybersecurity

cooperation strategy as reflected in the ASEAN Cybersecurity Cooperation Strategy for 2021 – 2025 in response to the newer cyber developments to strengthen collective efforts to secure cyberspace for the region and to promote digital's economy and community to grow. The updated Strategy contains five dimensions of work: (1) advancing cyber readiness cooperation, (2) strengthening regional cyber policy coordination, (3) enhancing trust in cyberspace, (4) regional capacity building, and (5) international cooperation.

Second, ASEAN is the first and only regional organisation to have subscribed, in principle, to the United Nation's 11 voluntary, non-binding norms of responsible state behaviour in cyberspace.[12] This is important to underpin ASEAN's active contribution to maintaining peace and security in the cyberspace. In this regard, ASEAN is developing ASEAN Regional Plan on the Implementation of UNGGE Norms of Responsible State Behaviour in Cyberspace which are categorized into several focus areas including international cooperation, development of policy, awareness-rising, strengthening national cybersecurity and cybercrime laws, cybercrime cooperation, incident response cooperation and creation of trustworthy ecosystem.[13] This initiative have increased the understanding and awareness of ASEAN countries on key cybersecurity issues and will act as useful guides in ASEAN's work on norms implementation.

Third, ASEAN is establishing ASEAN Regional Computer Emergency Response Team (CERT) and the ASEAN CERT Information Exchange Mechanism. ASEAN recognized the urgency to secure the growing digital economy in ASEAN in the face of increasingly sophisticated transboundary cyber-attacks, therefore it would be valuable to establish ASEAN CERT to facilitate the timely exchange of threat and attack-related information among AMS (ASEAN Member States) National CERTs and foster CERT-related capacity building and coordination.[14]

---

[12] "ASEAN Cybersecurity Cooperation Strategy 2021-2025", accessed on May 10, 2022, https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf
[13] Ibid
[14] "ASEAN Cybersecurity Cooperation Strategy 2021-2025", accessed on May 10, 2022, https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

Key Challenges in ASEAN on Cybersecurity

First, as one of the most successful regional organisation in the world, ASEAN has an "ASEAN way" approach in the organisation's decision making process which is upholding the consensus principle based on ASEAN Charter. Some scholars argued that this ASEAN way could limit the group of ten in accomplishing substantial achievement in finding common ground and mutually acceptable outcome. Moreover, ASEAN respects the principle of territorial integrity, sovereignty, non-interference and national identities of ASEAN Member States.[15] The question arises whether this ASEAN way and principle of ASEAN regionalism is effective in dealing with cybersecurity in the region.

Second, according to ITU's Global Cybersecurity Index (GCI) 2020, the gaps among ASEAN countries are ranging from number 4 to 131 among 194 countries in total (Table 1).

Table 1: Cybersecurity Maturity of ASEAN Countries

Country	Rank	Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
Singapore	4	98.52	20.00	19.54	18.98	20.00	20.00
Malaysia	5	98.06	20.00	19.08	18.98	20.00	20.00
Indonesia	24	94.88	18.48	19.08	17.84	19.48	20.00
Vietnam	25	94.55	20.00	16.31	18.98	19.26	20.00
Thailand	44	86.50	19.11	15.57	17.64	16.84	17.34
Philippines	61	77.00	20.00	13.00	11.85	12.74	19.41
Brunei Darussalam	85	56.07	14.06	14.19	10.84	12.85	4.12
Myanmar	99	36.41	9.39	3.64	4.71	8.92	9.75
Lao PDR	131	20.34	11.77	3.27	0.00	1.23	4.07
Cambodia	132	19.12	7.38	2.50	1.69	3.29	4.26

Source: ITU's Global Cybersecurity Index 2020

Third, ASEAN countries have yet spent enough budget for cybersecurity to secure a sustained commitment to cybersecurity and investment gap. A.T. Kearney report argued that to secure sustained commitment to cybersecurity and address the investment gap, ASEAN

[15] The ASEAN Charter, https://asean.org/wp-content/uploads/images/archive/publications/ASEAN-Charter.pdf

countries need to spend between 0.35 and 0.61 percent of their GDP – or US$ 171 billion collectively – on cybersecurity in the period spanning 2017-2025.[16] Based on the *State of Cyber Security in* ASEAN in 2020 by Palo Alto Networks, cybersecurity has risen to the top of leadership agenda for many ASEAN business with a vast majority (92%) believing to be priority for their business considering growing volume of cyberthreats in the region. As surveyed, most ASEAN organizations increased their security investments in 2019. In fact, 46% allocated at least half their total IT budget to cybersecurity. It is also mentioned that more than half (53%) of Singapore companies allocated over half their IT budget to cybersecurity and 84% of Indonesian companies increased their cybersecurity budgets between 2019 and 2020 which was the biggest jump in ASEAN.[17] For government allocated fund, Singapore, as the leading country in ASEAN in terms of cyber maturity, has allocated US$1 billion to build up the Government's cyber and data security capabilities for 2020-2023 budget.[18] While Malaysia allocated US$6 million in 2021 to strengthen the nation's cybersecurity capacity[19] and Indonesia allocated US$89 million in 2021 for the ICT development.[20] However, other countries in ASEAN have yet allocated the same proportion of budget for cybersecurity.

Case Study of Data Breach in Indonesia

ASEAN countries' Internet penetration is now over 77.6% which is above the global Internet users worldwide (59.5%).[21] With the ASEAN region seeing exponential growth in the digital technology sector, particularly financial technology and e-commerce, there is an

[16] "Cybersecurity in ASEAN: An Urgent Call to Action", Cisco and A.T. Kearney, 5, https://www.southeast-asia.kearney.com/documents/1781738/1782318/Cybersecurity+in+ASEAN—An+Urgent+Call+to+Action.pdf/80a880c4-8b70-3c99-335f-c57e6ded5d34

[17] "The State of Cybersecurity in ASEAN", Palo Alto Networks, 2020, https://www.paloaltonetworks.sg/apps/pan/public/downloadResource?pagePath=/content/pan/en_SG/resources/whitepapers/the-state-of-cybersecurity-in-asean-2020

[18] Lim Min Zhang, Singapore Budget 2020: $1b over next 3 years to shore up cyber and data security capabilities, The Straits Times, February 18, 2020, https://www.straitstimes.com/singapore/singapore-budget-2020-1b-over-next-3-years-to-shore-up-cyber-and-data-security

[19] Angelin Yeoh, Budget 2021: RM27mil allocation for CyberSecurity Malaysia hailed by industry players, The Star, February 6, 2020, https://www.thestar.com.my/tech/tech-news/2020/11/06/budget-2021-rm27mil-allocation-for-cybersecurity-malaysia-hailed-by-industry-players

[20] Indonesia Ministry of Finance, www.kemenkeu.go.id

[21] Internet penetration in Southeast Asia as of June 2021, Statista, https://www.statista.com/statistics/487965/internet-penetration-in-southeast-asian-countries/

increasing demand for Internet and broadband services. However, this increasing reliance on the Internet has created a large number of security threats that can cause immense damage. Based on the ASEAN Cyberthreat Assessment 2021 produced by the INTERPOL ASEAN Cybercrime Operations Desk, ASEAN countries have become a prime target for cyberattack considering their position among the fastest-growing digital economies in the world. One of the most serious cyberattacks, which occurred in the ASEAN region in 2020, is the data breach incident of Indonesia's e-commerce Tokopedia's which 91 million users' information were leaked.[22]

Indonesia is the biggest country in ASEAN, it has more than 275 million population and according to Statista, as of July 2021, online penetration in the country stood at around 70 percent. With over 171 million internet users, Indonesia is one of the biggest online markets worldwide. One of the most serious cyberattacks, which occurred in the ASEAN region in 2020, is the data breach incident of Indonesia's e-commerce Tokopedia's which 91 million users' information were leaked.[23]

Tokopedia is considered to be the largest e-Commerce marketplace in Indonesia, which provides ample business opportunities to various small scale vendors and SMEs, resulting the marketplace become a preferred selling and shopping destination. Tokopedia's webpage became the most visited e-commerce site in Indonesia with monthly web traffic reached 157 million.[24] Indonesia, being one of the fastest growing economies in ASEAN, continues to be one of the most vibrant digital financial services markets due to its relatively open regulatory framework, and is showing rapid growth across fintechs and digital platforms. Based on the Google, Temasek and Bein, e-Conomy SEA 2021 report, Indonesia's Internet economy will likely reach $146 billion by 2025.

---

[22] "ASEAN Cyber Threat Assessment 2021", INTERPOL file:///Users/monica/Downloads/ASEAN%20Cyberthreat%20Assessment%202021%20-%20final%20(7).pdf
[23] "ASEAN Cyber Threat Assessment 2021", INTERPOL file:///Users/monica/Downloads/ASEAN%20Cyberthreat%20Assessment%202021%20-%20final%20(7).pdf
[24] "The Map of E-commerce in Indonesia", iPrice, accessed on May 20, 2022, https://iprice.co.id/insights/mapofecommerce/en/

After the data breach incident, CEO of Tokopedia, Mr. William Tanuwijaya, reported to the Indonesian Parliament how the company solved the cyberattack. At that time, since there was not yet a regulation on data protection in Indonesia, the company then claimed to follow the international standards by delivering transparency to its customers through providing explanation to its customers which data had been breached. Furthermore, Tokopedia provided regular updates to its customers on how the attack was being handled by the company and improved its system internally to prevent future attacks.[25]

If we refer to the effectiveness theory of cybersecurity policy by Amos N. Guiora,[26] the Tokopedia's data breach incident could be analyzed by answering these questions: what is the impact significance of a data breach of 91 million users' information? To what extent, from a policy perspective, does this data breach warrant significant attention and resources? And finally, from a policy perspective, what is the impact of Tokopedia's data breach towards the overall development and assessment of cybersecurity in Indonesia? The question is put forward in the context of *resource prioritization, cost-benefit analysis, and risk assessment*

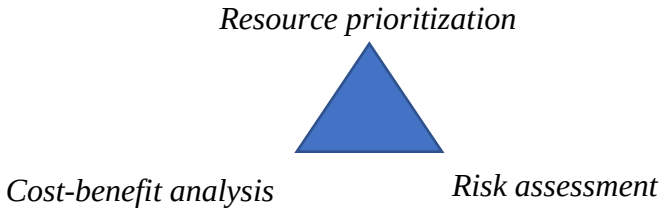

Figure 1: Resource triangle

During this incident, Indonesia does not have a comprehensive personal data protection regulation. What does exist is a multitude of laws and regulations in many sectors governing personal data protection, namely Law No. 11 of 2008 on Electronic Information and Transactions, Government Regulation No. 71 of 2019 on Implementation of Electronic Systems and Transactions and Minister of Communications and Informatics Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems.

[25] Fanny Potkin, "Indonesia's Tokopedia probes alleged data leak of 91 million users", *Reuters*, May 3, 2020, https://www.reuters.com/article/us-tokopedia-cyber-idUSKBN22E0Q2
[26] Guiora, Amos. N, *Cybersecurity: Geopolitic, Law and Policy*, (Taylor & Francis, Group, 2017)

In this regard, *what is the impact of significance of a data breach of 91 million users' information?* The significant impact was data relating to names, emails and telephone numbers of 91 million users had been partly compromised although Tokopedia explained that financial data were safe. The hackers claimed that email addresses and encrypted passwords from the company's user database were put for sale on the dark web for US$5,000.[27] Since there was not yet a regulation on data protection when the incident occurred, the Tokopedia's users could not claimed and protect its rights. The users were only advised to change their password on other digital platforms and not sharing OTP (One-Time Pin) codes. *To what extent, from a policy perspective, does this data breach warrant significant attention and resources?* The Tokopedia's data breach incident pushed and reminded the Indonesia Government of the need to develop and enact a regulation on personal data protection. On the resource dimension, Tokopedia announced that it has appointed independent global institution specializing in cybersecurity to improve its security system including the safety and security of its users' accounts and transactions. *And finally, from a policy perspective, what is the impact of Tokopedia's data breach towards the overall development and assessment of cybersecurity in Indonesia?* Indonesia has prioritized to draft a regulation on data protection since businesses need to know they can operate in a secure environment while customers need to know that public services supporting their continued safety, health and welfare remain accessible. Since there is not yet a model on data protection in ASEAN regional framework, Indonesia refers to the European Union General Data Protection. Thus, the impact of the Tokopedia's incident is significant toward the development of cybersecurity framework. At this time, Indonesia's draft regulation on data protection is being discussed intensively at Parliament level.

Based on the above case and the report from the Indonesia National Cyber and Crypto Agency that in 2021 there were 1.65 billion cyberattacks in Indonesia.[28], it demonstrates that Indonesia's cybersecurity framework is in urgent need to be further strengthened and

[27] Fanny Potkin, "Indonesia's Tokopedia probes alleged data leak of 91 million users", *Reuters*, May 3, 2020, https://www.reuters.com/article/us-tokopedia-cyber-idUSKBN22E0Q2
[28] "The 2021 Security Monitoring Result", The National Cyber and Crypto Agency, www.bssn.go.id

developed. In this regard, this paper argues that ASEAN cybersecurity framework has not contributed effectively towards one of the biggest ASEAN country, particularly on the legal measures on data protection and technical measures in countering the cyber-attacks.

Data Protection in ASEAN Countries

The case study in Indonesia has clearly demonstrated that Indonesia is one of the ASEAN countries which in urgent need to enact a law on data protection. After the Tokopedia incident, on October 2022, Indonesia had enacted its first Data Protection Law. Based on the risk assessment of the data breach of 91 million users' information in Indonesia, the Government of Indonesia had prioritized to enact Data Protection law and with this law, it contributes to the strengthening of cybersecurity policy in Indonesia.

Besides Indonesia, since 2020, Malaysia, Singapore and the Philippines, and Thailand already have comprehensive general data protection laws in place, while other six are pending passage or covered within various legislations.[29] While other ASEAN countries do not have a comprehensive data protection regulation.

Countries	Data Protection Policy and Regulation
Brunei Darussalam	Authority for Info-Communications Technology Industry (AITI) issued a Public Consultation Paper in 2021 to seek feedback on the proposed Personal Data Protection Order (PDPO) for the private sector in Brunei Darussalam.[30]
Cambodia	Data Protection regulation is still on the agenda
Indonesia	Personal Data Protection Law No. 27 Year 2022 as enacted in October 2022
Lao PDR	The government has enacted the Law on Prevention and Combating of Cyber Crime in 2015 and the Electronic Data Protection Act in

[29] TRPC (2020) TRPC Data Protection Index 202, https:/trpc.biz/old_archive/wp-contents/uploads/TRPC_DPI2020.pdf.
[30] https://www.aiti.gov.bn/regulatory/pdp/public-consultation-paper-on-personal-data-protection-for-the-private-sector-in-brunei-darussalam/

	2017 to strengthen cybersecurity and protection of personal information. While there is no overarching law on data protection.
Malaysia	The Personal Data Protection Act 2010 (PDPA) was passed in 2010, and came into force in 2013, while the government consulted in February 2020 on revisions to update the PDPA to consider digital developments around the world.
Myanmar	There is no general data protection law in Myanmar, elements of data protection are covered within "the Myanmar Official Secret Act", "the Telecommunication Law", "the Electronic Transaction Law" and "the Law for Protection of Personal Privacy and Personal Security of Citizens".[31] On 15 February 2021, the amendment of Electronic Transactions Law was adopted and includes a new article on "Personal Data Protection".
Philippines	Philippines was the front runner in ASEAN in enacting its Data Privacy Act in 2012
Singapore	Singapore's Personal Data Protection Act 2021 was amended to more adequately respond to and safeguard consumers' in the digital age and keep pace with technological advances and new business models.
Thailand	Thailand in May 2019 passed the Personal Data Protection Act (PDPA)
Vietnam	Vietnam has a draft Personal Data Protection decree, which was released for discussion in February 2020.

ASEAN Digital Senior Officials' Meeting (ADGSOM), have adopted the ASEAN Framework on Digital Data Governance, which aims to align baseline principles and standards

[31] MLIS, https://www.mlis.gov.mm/

for data protection, advance digital innovation and the use of open and big data, and facilitate data flows.[32] In particular, the ASEAN Data Management Framework and the Model Contractual Clauses for Cross Border Data Flows were approved by the 1st ASEAN Digital Ministers' Meeting (ADGMIN) in January 2021.[33] In addition, the ASEAN Cybersecurity Resilience and Information Sharing Platform (CRISP) has fully operationalized with the entry into force for the participating AMS that have signed the Memorandum of Understanding (MOU) for Sharing of Information during Activities of Digital and Technology Network (DTN) on 1 February 2021, which allows information sharing to combat cybersecurity threats and to develop collaborative mitigation actions for ASEAN Central Banks.

However, data protection and cybersecurity are continuously ongoing processes. In order to support the development of regional regulatory environment, ASEAN countries need to make sure their domestic data protection laws are updated regularly to remain relevant to the digital economy, such as enacting coherent and simple rules to both enable and protect cross-border data flows, clear obligations and responsibilities defined for data processors and data controllers, transparent data breach notification process, and others. In this regard, ASEAN may eventually create a regional framework on data protection in order to mitigate cybercrime in the region.

ASEAN's Regional Approach Analysis

ASEAN member countries have become a prime target for cyberattacks considering its position among the fastest-growing digital economies in the world. Some of the most serious cyberattacks which occurred in the ASEAN region in 2020 including Indonesia's e-commerce Tokopedia data breach which 91 million users' information leaked in May 2020, ransomware of 1.5 terabytes sensitive data stolen from subsidiary of ST Engineering Aerospace in June

[32] ASEAN (2018) Framework on Digital Data Governance, https://asean.org/storage/2012/05/6B-ASEAN-Framework-on-Digital-DataGovernance_Endorsedv1.pdf
[33] ASEAN (2021), ASEAN Data Management Framework, https://asean.org/storage/2-ASEAN-Data-Management-Framework_Final.pdf

2020, ransomware of hospital and businesses targeted in Thailand in September 2020, data breach of 1.1 million accounts of RedMart were compromised in October 2020. Besides the cyberattacks and data breaches, there is also an increase in COVID-19-related online fraud, including the sale of medical equipment and personal protective equipment. Compared with 2019, there is a marked increase in the number of online scammers who are impersonating government officials from the Ministry of Health and other agencies, chiefs of police and other notable officials to obtain people's confidential details by fraudulent means. The trend has shown an upward hill and will likely continue to rise exponentially in the future.

In order to analyse the effectiveness of ASEAN regional effort on cybersecurity, this paper review it by measuring cybersecurity commitments across five pillars (Table 2).[34]

Table 2: Five Pillars of Cybersecurity Commitments

Pillars	ASEAN Commitments
Legal Measures	ASEAN is yet to develop a legal framework on cybersecurity. In the case of Indonesia, it demonstrated the urgency to have a legal framework on data protection.
Technical Measures	• ASEAN is focused on upgrading the technical capability of ASEAN's national CERTs. Based on the ASEAN Cybersecurity Cooperation Strategy 2021-2025, each ASEAN countries shall assess the technical capability of their national CERT in the areas of cyber threat monitoring, incident handling, vulnerability handling, evidence handling, alerts and advisory drafting towards achieving a defined level of competency. • ASEAN is also establishing ASEAN CERT to facilitate the timely exchange of threat and attack-related information

[34] "Global Cybersecurity Index 2020", ITU, https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

	among ASEAN countries national CERTs and foster CERT related capacity building and coordination.
Organizational Measure	• ASEAN has an cybersecurity strategy as reflected in the document "ASEAN Cybersecurity Cooperation Strategy 2021-2025" and it is updated from the 2017-2020 document. In this regard, ASEAN updates its cybersecurity regularly. • ASEAN has created a new mechanism in 2020 to strengthen cross-sectoral coordination as cybersecurity which is the ASEAN Cybersecurity- CC. • ASEAN countries have established their national CERT. • To date, only Singapore, Malaysia, Indonesia, Brunei Darussalam and Myanmar have national cyber agency, while other ASEAN counties are being represented by its relevant Ministries. • Development of ASEAN Critical Information Infrastructure Protection (CIIP) Coordination Framework, built upon the 2020 ASEAN CIIP Framework which is to provide strategic recommendations and coordinated approaches to create more resilient cybersecurity across ASEAN's critical information infrastructure.
Capacity Development	• ASEAN has three regional initiatives on capacity building namely: 1. ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) 2. ASEAN-Singapore Cybersecurity Center of Excellence (ASCCE)

	3. ADMM Cybersecurity and Information Centre of Excellence (ACICE) • Besides the three Center above, ASEAN also organize and provide targeted capacity building through various ASEAN mechanisms, such as ARF, ADMM, ADMM-Plus, AMMTC, EAS, ADGMIN.
Cooperation	• ASEAN has established framework for ASEAN to widen and deepen its relations with external parties through the conferment of the formal status of Dialogue Partners with Australia, Canada, China, European Union, India, Japan, Republic of Korea, New Zealand, Russia, United States and United Kingdom. • With these Dialogue Partners, ASEAN established ASEAN + 1 process to discuss and review the state cooperation between ASEAN and the Dialogue Partner as well as strengthening cooperation in priority area such as cybersecurity. • Through ASEAN+1 process, ASEAN has managed to enhance cybersecurity cooperation as reflected, for example, in the 2018 ASEAN-US Leaders' Statement on Cybersecurity Cooperation, the 2019 ASEAN-EU Statement on Cybersecurity Cooperation, inaugural ASEAN-Australia Cyber Policy Dialogue, ASEAN-Japan Cybersecurity Working Groups and Policy Meetings, annual workshop on network security with China.

Based on the analysis above, ASEAN countries need to develop and strengthen the following measures. First, ASEAN needs to update its ASEAN cybersecurity strategy regularly by assessing current risks, prioritize cybersecurity interventions, and track progress and has a clear set of objectives on the protection of critical infrastructure. From the ITU's GCI, we learn that the lack of adequate organizational measures can contribute to a lack of clear responsibilities and accountability in the national cybersecurity governance, and it can prevent effective intra-government and inter-sector coordination. If all ASEAN countries have established an effective national cybersecurity, this will contribute to the development of ASEAN cybersecurity strategy. Brunei Darussalam, Indonesia, Malaysia, the Philippines, Singapore, Thailand, and Vietnam have already developed national strategies related to cybersecurity and can do more to promote regional alignment and assist other ASEAN countries which have yet to craft their own cybersecurity roadmaps or implementation strategies.

Second, ASEAN needs to focus to strengthen its technical measures. While legislation and regulation are important, but the actual implementation of cyber threat detection systems and the capability to handle cyber risks are more important. In order to improve the technical capabilities, ASEAN should enhance its capacity building programme.

Third, considering the huge maturity gap among ASEAN countries, the regional capacity building should focus on: (i) developing technical ability of ASEAN countries CERT, (ii) developing policy, strategy as well as technical aspects of cybersecurity for ASEAN countries officials and cybersecurity professionals, and (iii) improving the ability and preparedness of cybersecurity professionals within ASEAN region for cybersecurity and trusted digital services.

Fourth, ASEAN need to establish legal umbrella in combating cybercrime similar to Budapest Convention. However, taking into account "ASEAN way" approach in the organisation's decision-making process which is upholding the consensus principle and the principle of non-interference, creating a legal document would be complex and lengthy.

Lastly, to narrow the gap among ASEAN countries, ASEAN can consider focusing on the capacity building in the three Center (AJCCBC, ASCCE, ACICE) in enhancing organizational measures and technical measures. The capacity building programme can be focused towards improving those two dimensions for ASEAN countries with the lowest by improving the capability of national CERT, training in areas covering cybersecurity norms and policy, and regular assessments of their cybersecurity commitments. At the same time, ASEAN countries with higher cyber maturity could provide their best practices in handling cybersecurity challenges regularly. ASEAN has experiences with its Initiative for ASEAN Integration (IAI) to provide a framework for regional cooperation by which the more developed ASEAN countries could provide assistance for ASEAN countries that most need it, with a view of narrowing the development gap and to enhance ASEAN's competitiveness in the region. This IAI has shown its effectivity through ASEAN's positive GDP trend and becoming the fifth largest economy in the world. With this experience, ASEAN could undertake similar regional approach on cybersecurity by narrowing the gap among ASEAN countries to improve its cybersecurity framework.

Conclusion

Since the ASEAN Leaders' committed to enhance cybersecurity cooperation in 2018, ASEAN has made significant progresses. ASEAN has strengthen its cybersecurity effort in: (i) technical dimension by enhancing CERT cooperation, (ii) organization dimension by updated its Strategy and established the ASEAN Cybersecurity Coordinating Committee, (iii) capacity building with the three ASEAN initiatives and targeted capacity building training, and (iv) cooperation within ASEAN countries and also with ASEAN external partners in a way that is mutually beneficial and effective.

However, ASEAN as a regional organization has its limitation in finding mutually acceptable outcome and implementing the agreed regional framework considering ASEAN's principle of non-interference and ASEAN way of consensus decision making process. In the

case of cybersecurity, this limitation becomes more substantial since ASEAN countries have high degree of heterogeneity in terms of economic development which resulted in wide disparity of ASEAN countries' commitment and political will to engage with cybersecurity policy. This is shown in the notable gap among ASEAN countries in terms of cyber maturity. Therefore, ASEAN countries needs to narrow its gap in cyber maturity. ASEAN has provided forums through various ASEAN mechanisms to discuss cybersecurity among ASEAN countries and with external partners. This regular interaction between relevant stakeholders subsequently serve to increase knowledge and understanding between relevant actors, and also strengthen the cybersecurity development. If the trust-based relationships can be built, then solutions to cybersecurity challenges can be found.

There is no best cybersecurity standard or framework as new technologies and delivery mechanisms develop, it will continue to accommodate change and expand in order to address various fields of cybersecurity, but there are already good example of existing cybersecurity framework. Therefore, ASEAN still needs to learn from other regional effort best practices and continue to strengthen its cooperation with external partners.

Bibiliography

Angelin Yeoh, Budget 2021: RM27mil allocation for CyberSecurity Malaysia hailed by industry players, The Star, February 6, 2020, https://www.thestar.com.my/tech/tech-news/2020/11/06/budget-2021-rm27mil-allocation-for-cybersecurity-malaysia-hailed-by-industry-players

ASEAN Cybersecurity Cooperation Strategy 2021-2025

ASEAN-Japan Cybersecurity Capacity Building Center, https://www.ajccbc.org

ASEAN Secretariat, www.asean.org

AITI,https://www.aiti.gov.bn/regulatory/pdp/public-consultation-paper-on-personal-data-protection-for-the-private-sector-in-brunei-darussalam/

Bain & Company, e-Conomy SEA report 202", accessed on May 10, 2022, _sea_2021_report.pdf

Caitríona H. Heinl, "Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime", Asia Policy, Number 18, July 18, 2014

Cisco and A.T. Kearney, Cybersecurity in ASEAN: An Urgent Call to Action, 5, https://www.southeast-asia.kearney.com/documents/1781738/1782318/Cybersecurity+in+ASEAN—An+Urgent+Call+to+Action.pdf/80a880c4-8b70-3c99-335f-c57e6ded5d34

Cyber Security Agency Singapore website, https://www.csa.gov.sg/News/Press-Releases/asean-singapore-cybersecurity-centre-of-excellence

Fanny Potkin, "Indonesia's Tokopedia probes alleged data leak of 91 million users", *Reuters,* May 3, 2020, https://www.reuters.com/article/us-tokopedia-cyber-idUSKBN22E0Q2

Jirapon Sunkpho, Sarawut Ramjan, Chaiwat Ottamakorn, "Cybersecurity Policy in ASEAN Countries", *Research Gate,* (March 2018)

Kishore Mahbubani and Jeffry Sng, *The ASEAN Miracle: A Catalyst for Peace*, (Ridge Books Singaporer: 2017)

Lim Min Zhang, Singapore Budget 2020: $1b over next 3 years to shore up cyber and data security capabilities, The Straits Times, February 18, 2020, https://www.straitstimes.com/singapore/singapore-budget-2020-1b-over-next-3-years-to-shore-up-cyber-and-data-security

International Telecommunication Union, *Global Cybersecurity Index 2020,* https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

Indonesia Ministry of Finance, www.kemenkeu.go.id

International Business Machine, Cost of a Data Breach Report 2020, https://www.ibm.com/downloads/cas/QMXVZX6R

INTERPOL, ASEAN Cyber Threat Assessment 2021

MLIS, https://www.mlis.gov.mm/

Palo Alto Networks, The State of Cybersecurity in ASEAN, 2020, https://www.paloaltonetworks.sg/apps/pan/public/downloadResource?pagePath=/content/pan/en_SG/resources/whitepapers/the-state-of-cybersecurity-in-asean-2020

Statista, Internet penetration in Southeast Asia as of June 2021, https://www.statista.com/statistics/487965/internet-penetration-in-southeast-asian-countries/

Symantec, Internet Security Threat Report Volume 22, https://docs.broadcom.com/doc/istr-22-2017-en

TRPC (2020) TRPC Data Protection Index 202, https:/trpc.biz/old_archive/wp-contents/uploads/TRPC_DPI2020.pdf.

The National Cyber and Crypto Agency, The 2021 Security Monitoring Result, www.bssn.go.id

The ASEAN Secretariat, ASEAN Key Figures 2021,
https://asean.org/wp-content/uploads/2021/12/ASEAN-KEY-FIGURES-Chapter-1-4-Rev-28-Dec-2021.pdf