

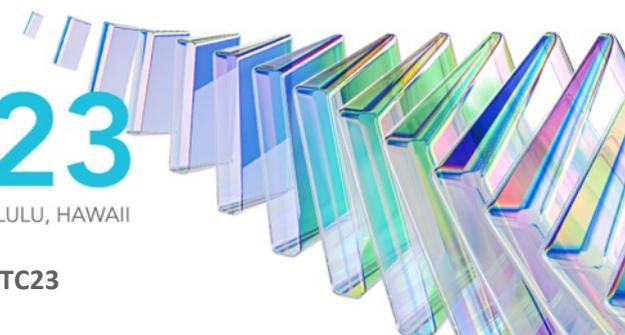


ASEAN Regional Effort on Cybersecurity and Its Effectiveness

Monica Nila Sari

PhD Candidate Keio University

Japan



Content

1. Introduction
2. Existing Cybersecurity Framework
3. Case Study in ASEAN Country
4. Key Challenges
5. Data Protection in ASEAN
6. Analysis
7. Key Recommendation
8. Conclusion

Introduction

- Fastest growing Internet markets (125,000 new users coming online every day)
- 440 million Internet users, and more importantly, 350 millions of them, or about 80%, are digital customers
- ASEAN countries' Internet penetration is now over 77.6% - above the global Internet users worldwide (59.5%)
- Prime target of cyberattacks
- “ASEAN’s way” as limitation

ASEAN's Existing Cybersecurity Framework

1. ASEAN Cybersecurity Cooperation Strategy for 2021 – 2025
2. 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
3. ASEAN Regional Computer Emergency Response Team (CERT) and the ASEAN CERT Information Exchange Mechanism

Case Study in ASEAN Country

- Indonesia's Internet economy : \$146 billion by 2025.

91 million users were leaked

- Tokopedia is the biggest Indonesia's e-commerce company:
 - 865 million products listed
 - Empower 90% MSMEs
 - Sellers' sales volume 133%
 - 86% new entrepreneurs

Key Challenges

1. ASEAN has an “ASEAN way” approach in the organisation’s decision making process which is upholding the consensus principle
2. The gaps among ASEAN countries are ranging from number 4 to 131 among 194 countries in total
3. ASEAN countries have not yet spent enough budget for cybersecurity

Data Protection in ASEAN

- Since 2020, Malaysia, Singapore and the Philippines, and Thailand already have comprehensive general data protection laws, and Indonesia in 2022
- ASEAN Framework on Digital Data Governance
- ASEAN Data Management Framework and the Model Contractual Clauses for Cross Border Data Flows
- Memorandum of Understanding (MOU) for Sharing of Information during Activities of Digital and Technology Network

Analysis

1. **Legal Measures:** ASEAN has yet to develop a legal framework on cybersecurity
2. **Technical measures:** Focus on upgrading the technical capability of its national CERTs
3. **Organisational Measures:** Updates its ASEAN cybersecurity strategy regularly and establishing ASEAN Cybersecurity Coordinating Committee in 2020

Analysis

4. Capacity Development: ASEAN has three regional initiatives on capacity-building:

- ASEAN–Japan Cybersecurity Capacity Building Centre
- ASEAN–Singapore Cybersecurity Center of Excellence
- ADMM Cybersecurity and Information Centre of Excellence

5. International Cooperation: with external partners such as Australia, Canada, China, the EU, India, Japan, Republic of Korea, New Zealand, Russia, the US and the UK.

Recommendation

- Developing technical ability of ASEAN countries CERT
- Developing policy, strategy as well as technical aspects of cybersecurity for ASEAN countries
- Improving the ability and preparedness of cybersecurity professionals
- ASEAN countries with higher cyber maturity could provide their best practices in handling cybersecurity challenges regularly
- Legal umbrella in combating cybercrime

Conclusion

- ASEAN has made significant progresses since 2018
- 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
- ASEAN still needs to learn from other regional effort best practices and continue to strengthen its cooperation with external partners