ASEAN INDONESIA 2023

LEVERAGING REGIONAL PARTNERSHIPS TO IMPROVE CYBERSECURITY AND DIGITAL TRADE: A CASE STUDY OF INDONESIA

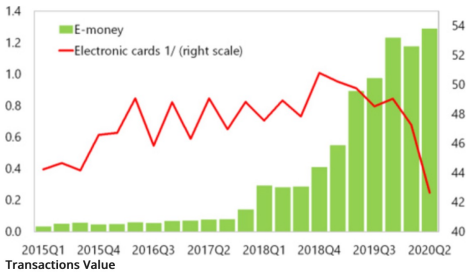
WTO – TECHNICAL BARRIERS TO TRADE

Thematic Session on Regulatory Cooperation Between Members on Cybersecurity

Digital Economy and Why It Matters to Indonesia

Path to a More Inclusive Recovery from COVID-19 Pandemic

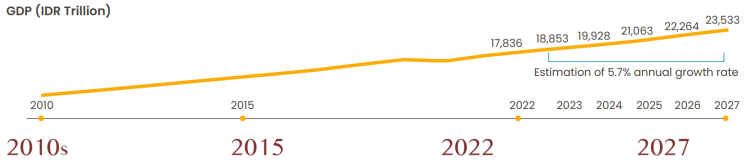
- Indonesia's digital landscape—mainly concentrated in e-commerce and in digital financial services—has expanded rapidly in recent years.
  - The COVID-19 outbreak has seen Indonesia's e-commerce sector surge.
  - The adoption of digital financial payments has accelerated further during the pandemic (30.3% yoy).
  - E-commerce and digital payments services are evolving into digital lending.
  - Digitalization is also advancing in the traditional financial sector, and will likely accelerate further with COVID-19.
  - Banks are responding to this competitive pressure by increasingly collaborating with and investing more in fintech.



Transactions Value

(In percent of GDP)

Digital Economy to Contribute 14% of Indonesia's GDP by 2027



2010s 2015 2022 2027

2015

- Government rolled out Visi Indonesia 2045 with Digital and Technology as the backbone to drive economic growth.

2022

- Digital economy size IDR 1,408 trillion 8% of GDP Indonesia 2022 GDP IDR 17,836 trillion.

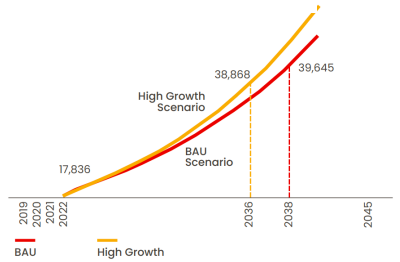
2027

- Digital economy size IDR 3,216 trillion 14% of GDP.
- Indonesia 2027 GDP (IDR 23,533 trillion - 5.7% annual growth rate based on Visi Indonesia 2045).

Digital Technology Can Help Indonesia Achieve High Income Status by 2036

- A Well-Executed Visi Indonesia 2045, together with Digital Technology, will help indonesia achieve **High Income Status by 2036.**
- **Visi Indonesia 2045**, has 4 strategic development pillars:
  - Human development & mastery of sci & tech
  - Sustainable economic development
  - Equitable development
  - National resilience and governance ☑

GDP Projection (IDR Trillion)



High Growth Scenario

5.7%	2036	USD 23,199
Annual GDP growth	High income nation	GDP per capita in 2045

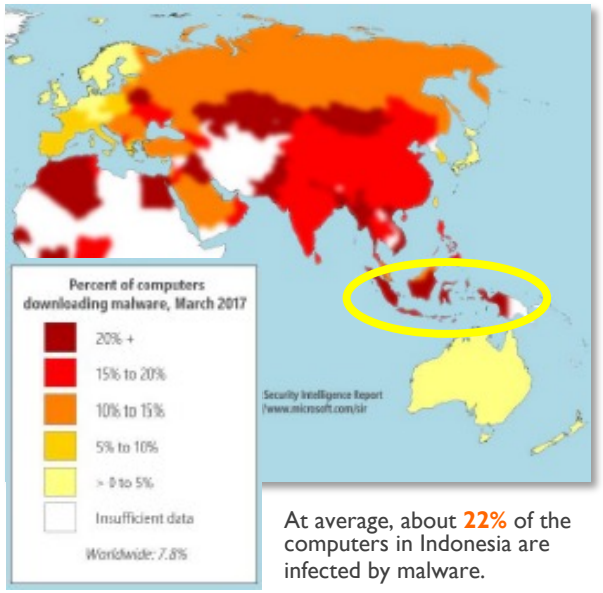
Business as Usual Scenario

5.1%	2038	USD 19,794
Annual GDP growth	High income nation	GDP per capita in 2045

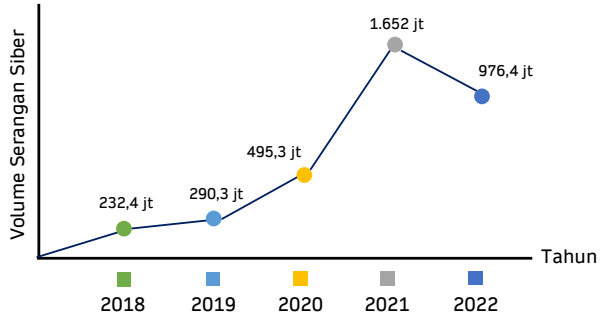
Cybersecurity Challenges

Rapidly Evolving Cyber Threats

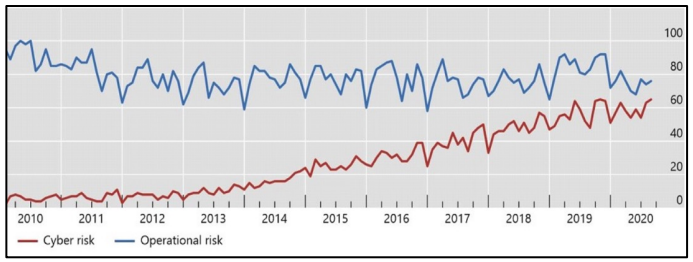
Percentage of Computers Downloading Malware*

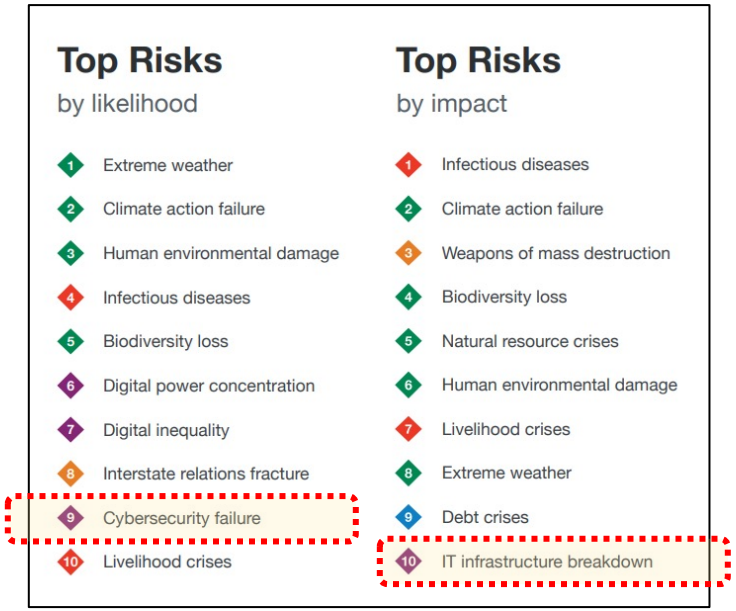


At average, about **22%** of the computers in Indonesia are infected by malware.

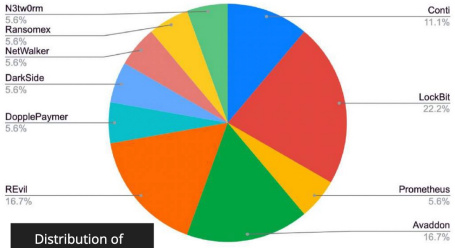


- **Attention to cyber risk has increased** over the past decade, with the trend come near to operational risk.

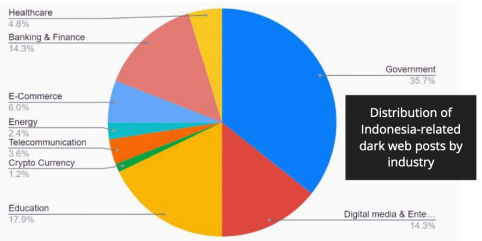




- Indonesia is a prime **target for nation-state-sponsored actors as well as financially motivated ransomware gangs** in recent years.
  - Indonesian companies and public agencies are observed to attract the attention of ransomware groups such as REvil, Conti, Avaddon, and LockBit.
  - Nearly 20,000 phishing attacks targeting Indonesia have been detected since the start of 2021, a 38% increase from last year (SOCRadar, 2022).



Distribution of ransomware gang activities.
Source: SOCRadar **DarkMirror**



Distribution of Indonesia-related dark web posts by industry

*"The threat landscape is **evolving**, becoming more **sophisticated** and doing so at a **faster pace** than many organisations are able to keep up with."*

Cybersecurity Cooperation in Support of Digital Economy Agreement

The ASEAN Cybersecurity Cooperation Strategy

- The ASEAN region holds **tremendous potential with its strong economic fundamentals**, such as a 670-million strong market, a young, tech-savvy population and rising Internet penetration.
- **Cybersecurity is a key enabler** of economic progress in the ASEAN digital economy.
- Introduced in 2017, the 2021 – 2025 Cybersecurity Cooperation Strategy builds on the foundation laid by **incident response, CERT and capacity-building cooperation, and considers the rapid cybersecurity landscape changes** for the purpose of creating a safer regional cyberspace.
- In Indonesia's case, certain strategy activities **directly impacted the country's commitment** to cybersecurity.

Cybersecurity in Support of ASEAN's Digital Ambitions

ASEAN Smart Cities Network
Improve the lives of ASEAN citizens using technology as an enabler

ASEAN Declaration on Industrial Transformation to Industry 4.0
A well-prepared ASEAN able to maximise the opportunities of Industry 4.0 to foster regional economic growth and maintain ASEAN centrality as a key player in global production networks

ASEAN Digital Masterplan (ADM) 2025
ASEAN as a leading digital community and economic bloc, powered by secure and transformative digital services, technologies and ecosystem

All digital activities undergirded by building secure and resilient cyberspace

Dimension 1: Advancing Cyber Readiness Cooperation	Dimension 2: Strengthening Regional Cyber Policy Coordination	Dimension 3: Enhancing Trust in Cyberspace	Dimension 4: Regional Capacity Building	Dimension 5: International Cooperation
• CERT Coordination – incidence response and threat information sharing ✓ • Coordination on regional CII protection ✓	• Norms implementation ✓ • Coordination on cybersecurity and related digital security issues ✓	• Promoting International Cybersecurity Standards ✓ • Cyber hygiene and digital inclusion	• Multi-disciplinary, modular, measurable multi-stakeholder capacity building programmes	• Multilateral Engagement with Dialogue Partners
Lead ASEAN Sectoral Body/Forum	**Lead ASEAN Sectoral Body/Forum**	**Lead ASEAN Sectoral Body/Forum**	**Lead ASEAN Sectoral Body/Forum**	**Lead ASEAN Sectoral Body/Forum**
○ ANSAC ○ ASEAN Cyber CC	○ ADGMIN ○ ATRC ○ ASEAN Cyber CC ○ ARF ISM on ICTs Security	○ ADGSOM and ATRC ○ ASCN ○ ANSAC ○ SOMRI Working Group on Information	○ ADGSOM + Japan ○ ADMM	○ ARF ISM on ICTs Security ○ ANSAC ○ ASEAN Cyber CC

✓ *Most influential activities impacted to a higher score in Global Cybersecurity Index.*

Advancement in Regional Cybersecurity

Opening Up Opportunities Ahead

- Cybersecurity Cooperation Strategy has proven to **stimulate advancements** across all ASEAN Member States, including Indonesia.
- Opportunities for **greater intra-ASEAN coordination efforts** and network partnerships with the private sector.

Costly estimated impacts of cyberattacks on AMS's economic development

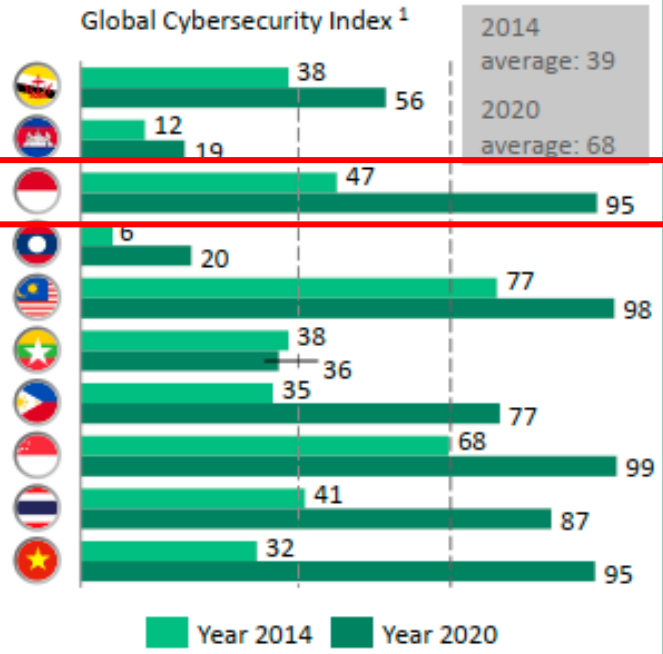
>USD 4.4 Mn[2]

Average cost of a data breach

280 days[2]

Time taken to identify and contain breach

Notable improvements in cybersecurity maturity, especially in VN & ID



Gaps remain in establishment of legal frameworks, national strategy & network partnerships

1. Several AMS **yet to introduce clear CS legislation**; and degree of advancement varies significantly

2. Every AMS has a national CERT; but there are **gaps in sector-specific CERTs** and **limited network partnerships**

3. Some countries **yet to introduce CS strategy**; opportunity to align for better intra-government coordination

Further Support of Digital Economy and Trade

The ASEAN Digital Integration Framework Action Plan 2019 - 2025

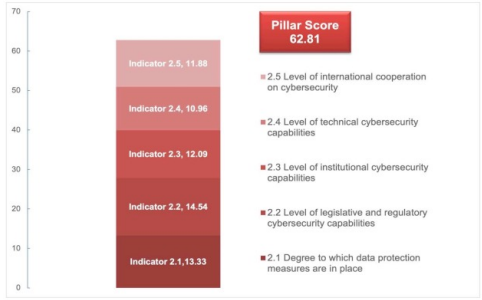
Ratified at the 18th ASEAN Economic Community meeting on 31 of October 2019

The 5 priorities:

- Facilitating seamless trade, — **Priority Area 1**
- Protecting data while supporting digital trade, — **Priority Area 2**
- Enabling seamless digital payments, — **Priority Area 3**
- Developing a digital workforce and, — **Priority Area 4**
- Fostering entrepreneurship — **Priority Area 5**

Priority Area 2
Protecting Data While Supporting Digital Trade and Innovation

a. Level of international cooperation on cybersecurity;
b. Level of technical cybersecurity capabilities;
c. Level of institutional cybersecurity capabilities;
d. Level of legislative and regulatory cybersecurity capabilities;
e. Degree to which data protection measures are in place.



ASEAN Agreement on e-Commerce (2019)

Consumers in the region stand to benefit from lower costs and improvement in the speed and reliability of supply chains in cross-border e-Commerce transactions. Consumers can also look forward to more robust consumer protection measures for e-Commerce transactions.

Paperless Trading
Promote greater efficiency and reliability through the digitisation of documents

Electronic Payments
Encourage interoperable electronic payment systems for cross-border transactions and e-commerce

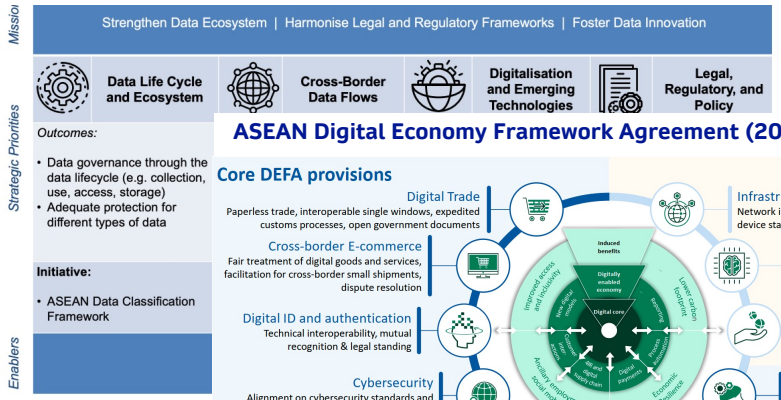
Cross-border Transfer of Information
Facilitate the transfer of data across borders for efficient operations and digital services

Logistics
Improve speed a in cross-border e timely fulfilment

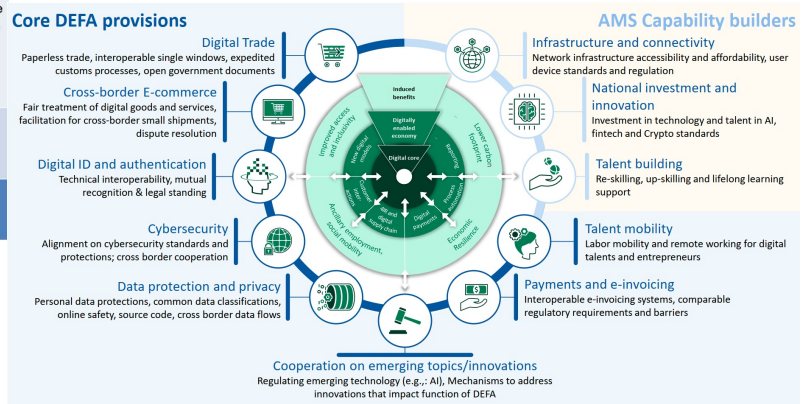
Consumer Protection

Domestic Regulatory Framework

ASEAN Framework on Digital Data Governance



ASEAN Digital Economy Framework Agreement (2023)



Recommendation Focused on Using Regulatory Cooperation to Improve Cybersecurity

01	**Develop a shared understanding of cybersecurity risk**	▪ As a first step, governments need to develop a common understanding as to the scope of cybersecurity and what could constitute a cybersecurity measure. ▪ While the nature of cybersecurity threats are evolving, there are doing so within the constraints of how technology exposes people and the economy to cyber threats through connections to the internet and the free flow of data.
02	**Agree to a risk-based approach to cybersecurity**	▪ The notion of risk is central to cybersecurity. Risk-based cybersecurity measures are increasingly a global norm. ▪ Moreover, how to assess risk and determine what is needed to reduce it requires a risk assessment. A risk assessment could inform what cybersecurity measures to adopt, what risk reduction can be expected, and at what cost. ▪ The rapidly changing nature of cybersecurity threats means that addressing risk is a dynamic process that requires regular reassessment of risk and consideration of what else might be needed to reduce risk to acceptable levels.
03	**Ensure compliance with cybersecurity standards**	▪ Cybersecurity standards can build a common approach to addressing cybersecurity risks based on best practice. ▪ Tying cybersecurity policy to international standards will also support the development of globally consistent and least trade-restrictive approaches to cybersecurity. ▪ Using international standards as a basis for cybersecurity policy can also help address concerns that cybersecurity regulation is a disguised restriction on trade aimed at supporting domestic industry.
04	**Enhance information sharing**	▪ Real-time sharing of information on threats and vulnerabilities—to promote awareness, plan responses, and help targets adapt and respond—has become an important feature of cybersecurity policies. ▪ The trust issues implicit in sharing proprietary or classified information in the domestic context are compounded when dealing with governments or organizations across national borders.