



**TECH FOR
GOOD
INSTITUTE**



This is not an ADB material. The views expressed in this document are the views of the author/s and/or their organizations and do not necessarily reflect the views or policies of the Asian Development Bank, or its Board of Governors, or the governments they represent. ADB does not guarantee the accuracy and/or completeness of the material's contents, and accepts no responsibility for any direct or indirect consequence of their use or reliance, whether wholly or partially. Please feel free to contact the authors directly should you have queries.

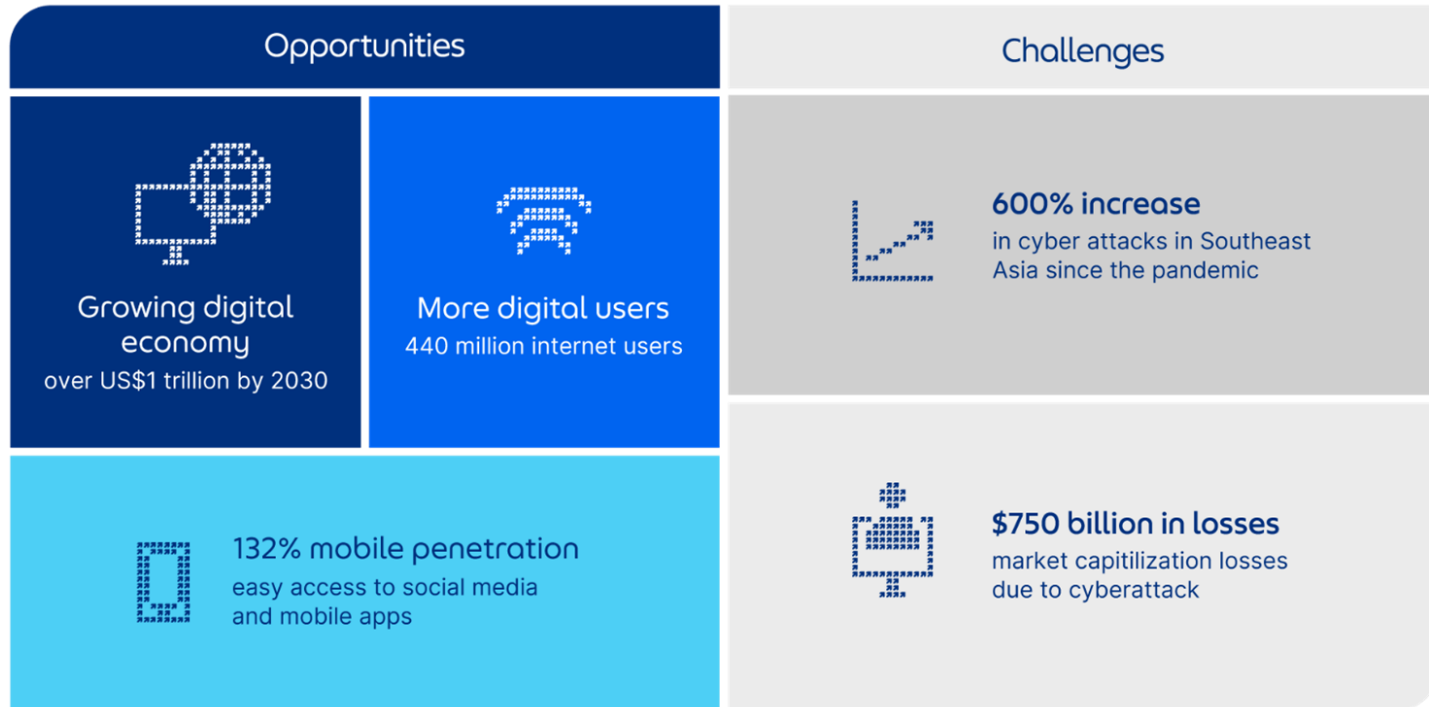


Keith Detros, Programme Lead Tech for Good Institute

Towards a Resilient Cyberspace in Southeast Asia



Southeast Asia's digital economy is full of opportunities, but it is not without risks.



Source: Google, Temasek, & Bain and Company (2022); We are Social (2021); United Nations Office on Drugs and Crime (2021); AT Kearney (2018).

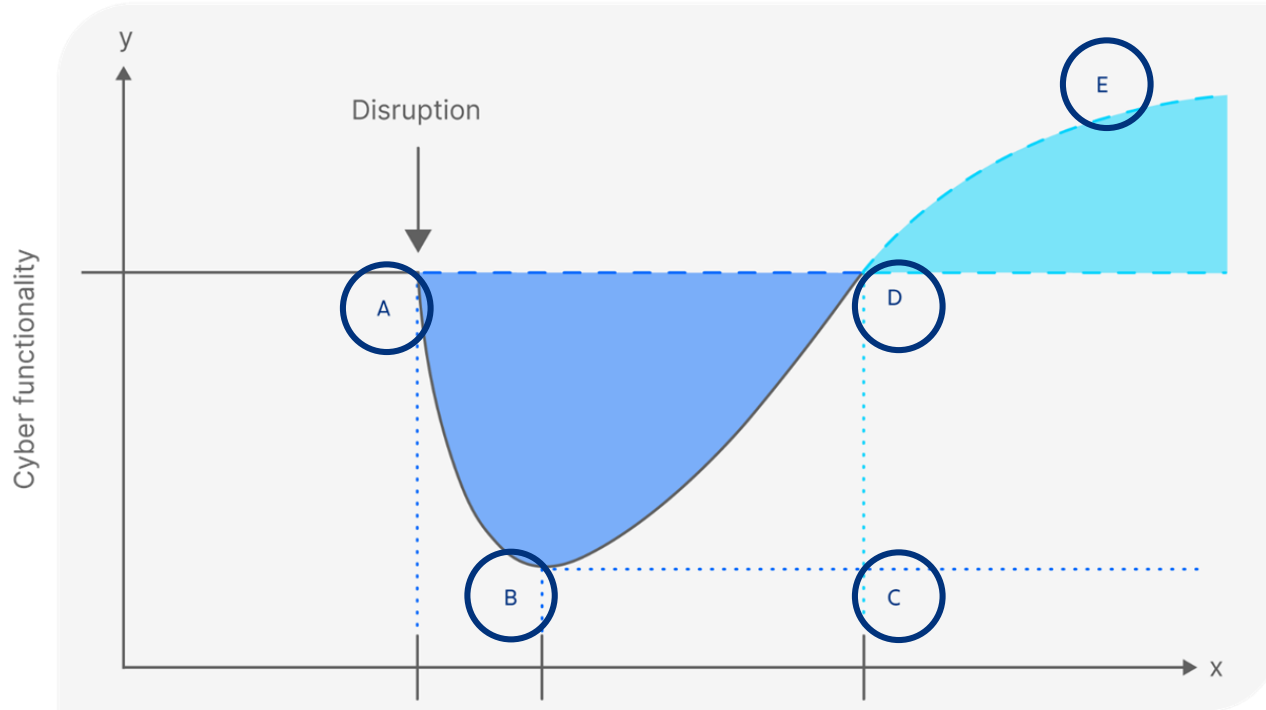
Building cyber resilience is key to maximising the benefits of the region's digital economy.

ASEAN has a vision of a peaceful, secure and **resilient** regional cyberspace that serves as an enabler of economic progress.

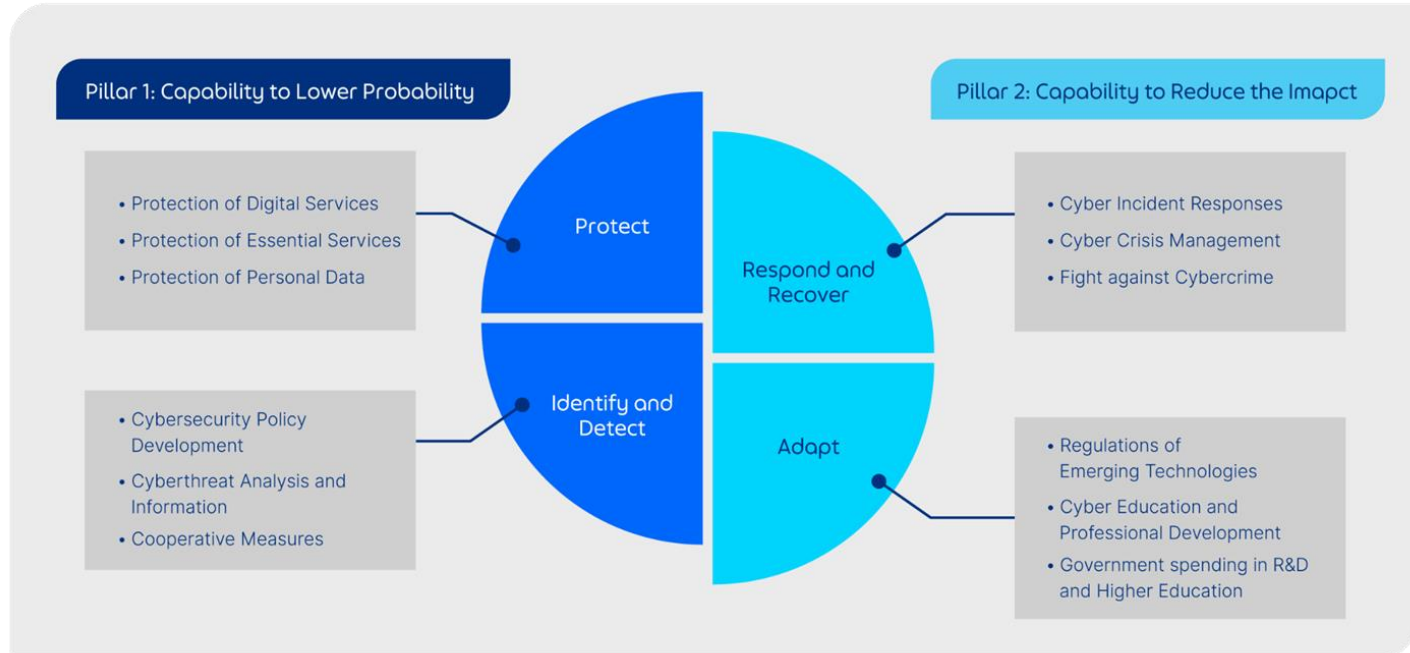
- ASEAN Leader's Statement of Cybersecurity Cooperation, 2018

- There is opportunity to operationalise “resilience”.
- Resilience includes the recognition that:
 - attacks are inevitable;
 - uncertainty is constant;
 - adaptability is important.

Cyber resilience is the capability to adapt to constantly evolving cyber threats.



The Cyber Resilience Framework uses publicly available resources.

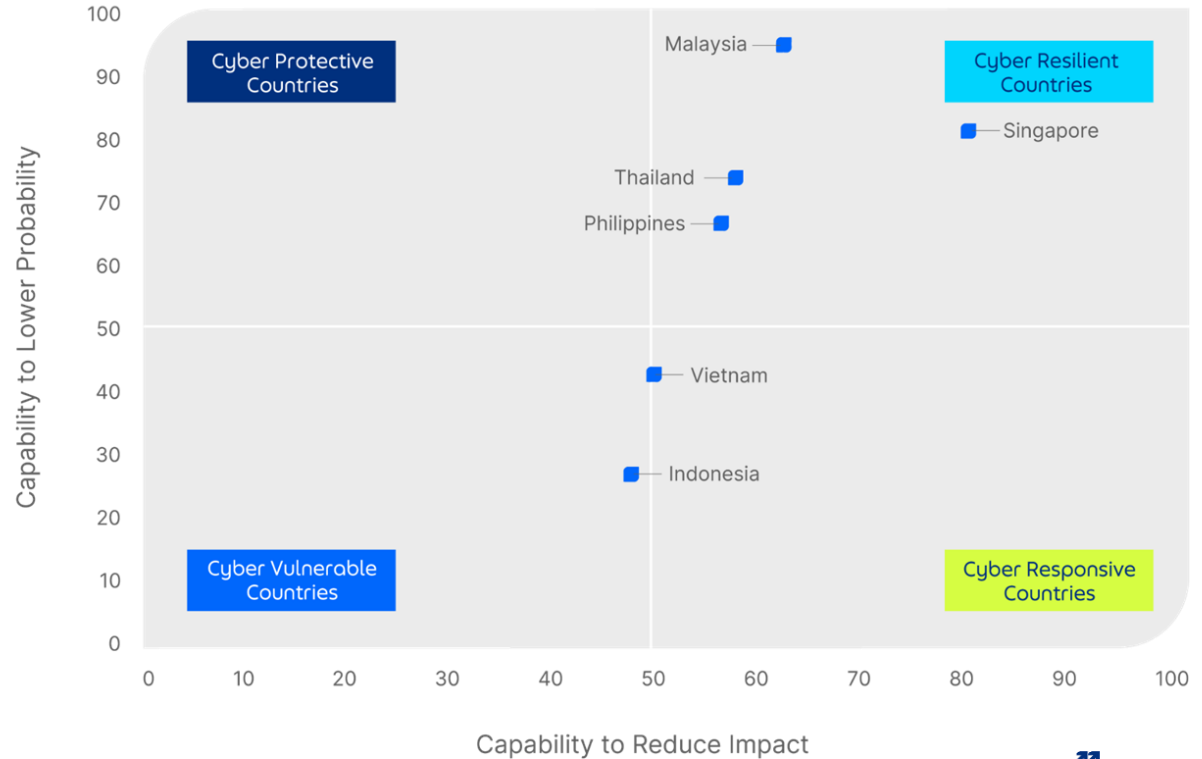


Source: Proposed Cyber Resilience Framework

Southeast Asia's cyber resilience journey varies.

➤ Varying levels of cyber resiliency in Southeast Asia.

➤ Commitment of some countries to resiliency with the important need for everyone converge.



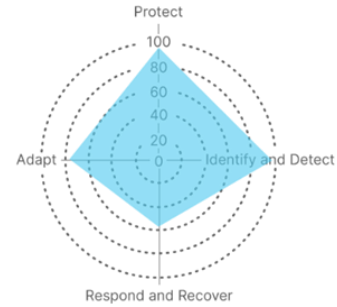
Source: Cyber Resilience Framework

Country Profiles

Indonesia



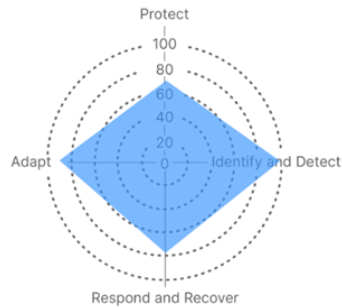
Malaysia



Philippines



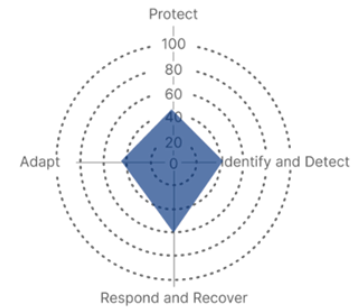
Singapore



Thailand



Vietnam



Key considerations to improve resilience in Southeast Asia

Pillar 1: Capacity to Lower Probability

Protect

Need for data protection agencies and coordination with one another.

Identify and Detect

Increasing importance of talent to secure digital progress.

Pillar 2: Capacity to Reduce the Impact

Respond and Recover

CSIRTs will benefit from coordination within and beyond borders.

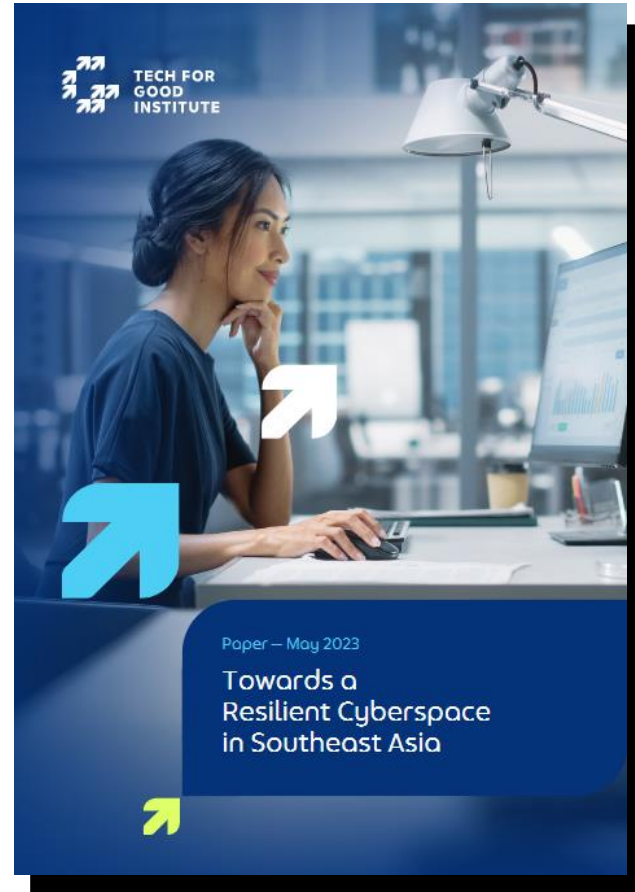
Adapt

Build a culture of cyber resilience.

Read our full paper:



<https://techforgoodinstitute.org/research/tfgi-reports/towards-a-resilient-cyberspace-in-southeast-asia/>





**TECH FOR
GOOD
INSTITUTE**