TECH FOR GOOD INSTITUTE

Paper — May 2023

Towards a Resilient Cyberspace in Southeast Asia

About This Study

As the digital economy continues to drive growth for Southeast Asia, we need an environment that is safe, secure and resilient. The Tech for Good Institute believes that confidence in the digital ecosystem is a prerequisite for unlocking the economic and social potential of an increasingly digitalised economy and society. Cyber resilience serves as a foundation for such confidence. With a focus on Southeast Asia-6 (Malaysia, Indonesia, Philippines, Thailand, Singapore, and Vietnam), this research contributes to conversations towards broadening the debate on cybersecurity and fostering trust that will enable growth and innovation.

Author

Keith Detros

Keith Detros is a programme lead at the Tech for Good Institute. Keith has almost a decade of experience in government affairs, evidence-based policy research, and stakeholder engagement, and currently works on areas at the nexus of technology and public policy. He previously served as a digital economy specialist at the US Embassy in Manila, where he covered entrepreneurship, innovation, technology policy and cybersecurity. Earlier in his career, he worked as a Research Specialist at the Philippine Institute of Development Studies. Keith holds a Master's Degree in International Affairs from the National University of Singapore's Lee Kuan Yew School of Public Policy and a Bachelor's Degree in Political Science from the University of the Philippines Manila.

Acknowledgements

The author is grateful to the Tech for Good Institute for the support, feedback, and guidance for this study.

An earlier version of this study was presented as a white paper at the National University of Singapore's Lee Kuan Yew School of Public Policy as part of the author's Master's programme requirements. The author would like to thank Professors Adam Liu, Selina Ho, and Vinod Thomas for the valuable feedback on the initial model and conceptualisation of the framework.

The author is also grateful to Senior Research Adviser Mamello Thinyane of the United Nations University Institute in Macau for offering his insights on improving cyber resilience in Southeast Asia and helping organise a research seminar at which ideas in this paper were refined.

This study is funded by TFGI’s founding donor, Grab. We are grateful to Grab for supporting TFGI's mission of leveraging the promise of technology and the digital economy for inclusive, equitable, and sustainable growth in Southeast Asia. The views expressed in this study are those of the author and should not be attributed to TFGI, its advisors, directors, or funders. Funders do not determine research findings nor the insights and recommendations of research.

Disclaimer

The information in this paper is provided on an “as is” basis. This paper is not to be considered as a recommendation for investments in any industry. This document is produced by Tech for Good Institute and has been prepared solely for information purposes over a limited time period to provide a perspective on the region. The Institute and any of its affiliates or any third party involved make no representation or warranty, either expressed or implied, as to the accuracy or completeness of the information in the report and no responsibility or liability whatsoever is accepted by any person of the Institute, its affiliates, and their respective officers, employees, or agents.

About the Tech for Good Institute

TFGI is a non-profit organisation on a mission to leverage the promise of technology and the digital economy for inclusive, equitable and sustainable growth in Southeast Asia.

With a population twice the size of the US and strong demographics, Southeast Asia's digital economy is evolving rapidly. At the same time, the region's trajectory will be unique, shaped by its diverse cultural, social, political, and economic contexts. The Tech for Good Institute serves as a platform for research, conversations and collaborations focused on Southeast Asia but connected to the rest of the world. Our work is centred on issues at the intersection of technology, society, and the economy, and that are intrinsically linked to the region's development. We seek to understand and inform policy with rigor, balance and perspective, through research, effective outreach and evidence-based recommendations.

The Institute was founded by Grab, Southeast Asia's leading superapp, to advance the vision of a thriving, innovative Southeast Asia for all. We welcome opportunities for partnership and support, financial or in-kind, from organisations and individuals committed to fostering responsible innovation and digital progress for sustainable growth in the region. More information about the Institute can be accessed at www.techforgoodinstitute.org.

Executive Summary

Southeast Asia is one of the fastest growing regional economies in the world, with a combined gross domestic product of US$3.2 trillion in 2019.[1]

Catalysed by the pandemic, the region's digital economy is currently serving an estimated 440 million people online, of which 40 million are new digital consumers.[2] By 2030, Southeast Asia's internet economy is projected to grow to US$1 trillion, buoyed by 125,000 new digital consumers joining the internet every day.[3]

However, the gains in the digital economy has seen corresponding growth in risks and challenges posed by cybercriminals.

In particular, perpetrators are taking advantage of how digital adoption has outpaced digital literacy and cyber-awareness amongst users. Post-pandemic, Southeast Asia will continue to be a target for cyber-attacks, as the region seeks economic cooperation through digital trade and connectivity.[4] This can have catastrophic impacts on the region's digital economy, with studies showing that the top 1,000 companies in Southeast Asia are at risk of losing US$750 billion in market capitalisation because of cybersecurity threats.[5]

To address this concern, building cyber resilience in Southeast Asia is key to maximising the benefits of digitalisation.

This is an effort that requires cooperation across governments, as digital technologies and the services they enable are often transboundary in nature. Regional policy alignment can benefit all participating economies. One key opportunity is to share a cyber resilience framework that would enable a more holistic understanding of managing cyber risks. Quantifying the framework further gauges how well different states protect, identify and detect, respond and recover, and adapt in response to the constantly changing cyberthreat landscape.

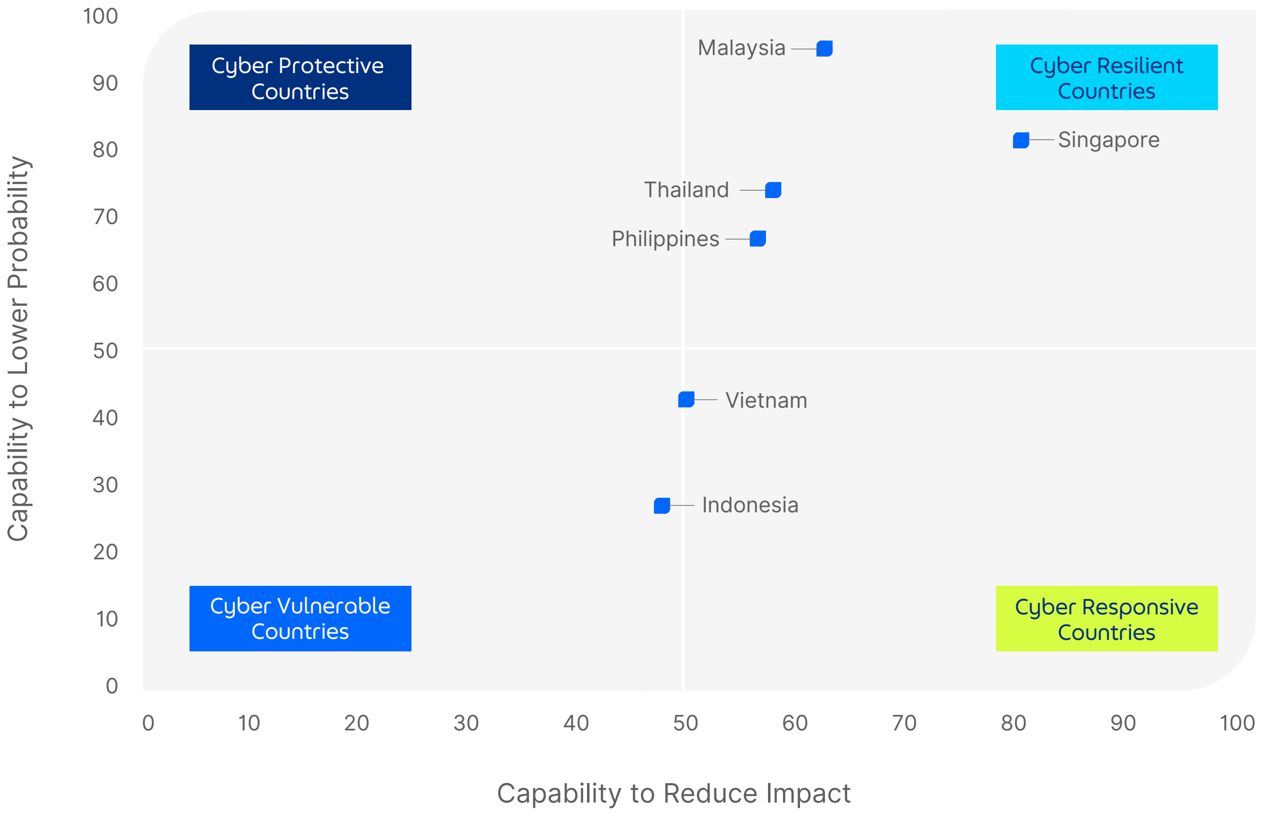
Using publicly-available global databases, the Cyber Resilience Framework proposed in this paper builds on existing cybersecurity indicators, with emphasis on both lowering the likelihood of cyber attacks and reducing their impact.

The framework borrows from current enterprise and industry standards as a basis for resilience. With such a conceptual definition of cyber resilience, this paper shows how six Southeast Asian states are prepared to ensure a safe, secure and thriving digital economy.

Within this Framework, we find that countries in Southeast Asia are at varying stages of cyber resiliency.

Singapore, Malaysia, Thailand, and the Philippines have instituted policies that protect their governments, citizens, and businesses from the constantly evolving cyberthreats. Vietnam and Indonesia, are starting to implement policies to improve protection of their digital economy, although there are still areas for improvement.

Figure A. The State of Cyber Resilience in Southeast Asia



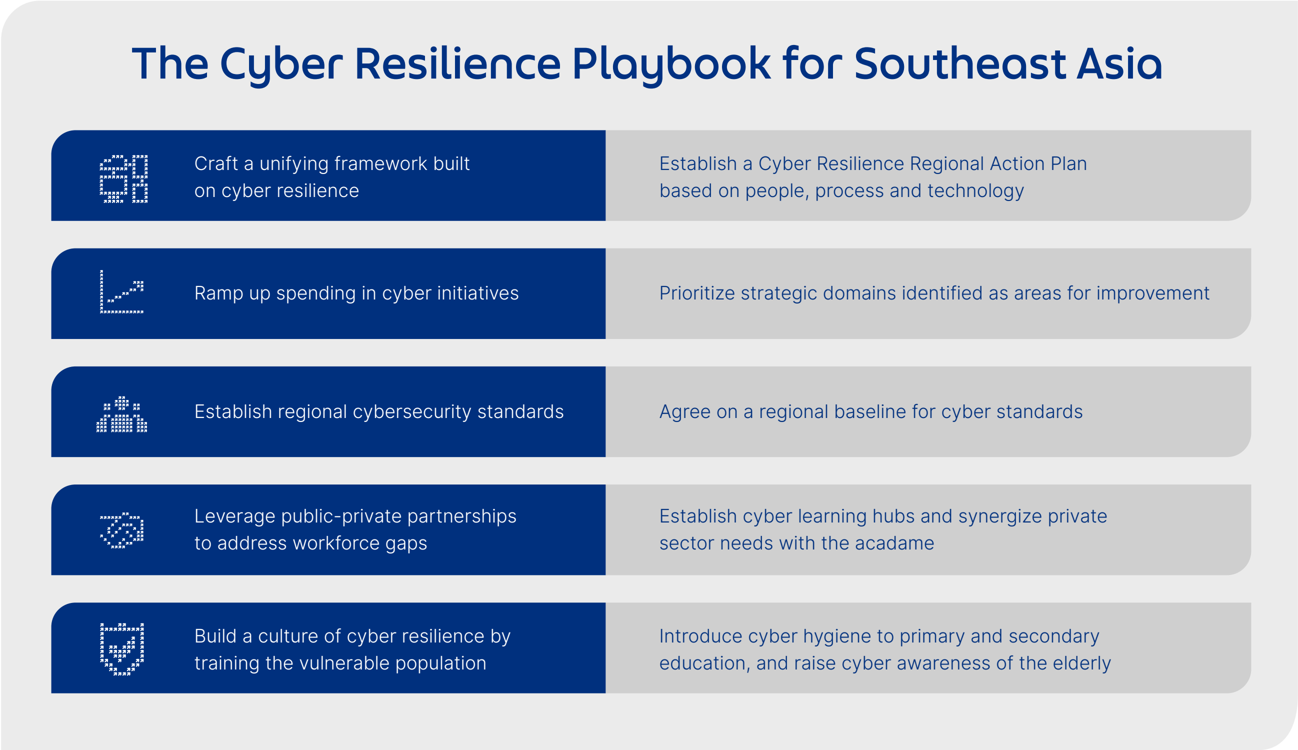
Source: Author's analysis based on the proposed Cyber Resilience Framework

While diverse in their digital and cyber resilience journeys, Southeast Asia can focus on key themes in order to improve the resiliency in the region. These are:

- Increasing regional cooperation amongst agencies responsible for national data protection;
- Facilitating coordination within and beyond national borders of computer security incident response teams;
- Nurturing cybersecurity expertise; and
- Building a culture of cyber resilience across the whole of society, through awareness and competency development from the very young to elderly.

A cyber resilience playbook offers recommendations for key policy actions. However, it is important to note that each government in the region must craft responsive and specific strategies aligned with each country's national priorities.

Figure B. The Cyber Resilience Playbook for Southeast Asia



The Cyber Resilience Playbook for Southeast Asia

Craft a unifying framework built on cyber resilience	Establish a Cyber Resilience Regional Action Plan based on people, process and technology
Ramp up spending in cyber initiatives	Prioritize strategic domains identified as areas for improvement
Establish regional cybersecurity standards	Agree on a regional baseline for cyber standards
Leverage public-private partnerships to address workforce gaps	Establish cyber learning hubs and synergize private sector needs with the acadame
Build a culture of cyber resilience by training the vulnerable population	Introduce cyber hygiene to primary and secondary education, and raise cyber awareness of the elderly

TECH FOR GOOD INSTITUTE

in Tech For Good Institute

www.techforgoodinstitute.org