

TECH FOR  
GOOD  
INSTITUTE



Compendium

# Data Sources for Cyber Resilience Research

October 2023



# Table of Contents

---

<b>➤ About This Resource</b>	<b>3</b>
Author	4
Acknowledgements	5
About the Tech for Good Institute	6

---

<b>➤ Chapter 1: Introduction</b>	<b>7</b>
----------------------------------	----------

---

<b>➤ Chapter 2: Cyber Resilience Global Data Sources</b>	<b>9</b>
A. Global Cybersecurity Index	13
B. National Cyber Security Index	15
C. Global Data Regulation Diagnostic Survey	17
D. Cyber Capabilities and National Power: A Net Assessment	18
E. Global Cyber Strategies Index	20

---

<b>➤ Chapter 3: The Way Forward</b>	<b>21</b>
-------------------------------------	-----------

---

<b>➤ References</b>	<b>23</b>
---------------------	-----------



# About This Resource

As the digital economy continues to transform the way we work and live, ongoing research to understand its impact on society and the economy is vital to enable sustainable, inclusive and equitable growth. Sound research, however, relies on good data that are comprehensive, timely and accurate. To encourage robust research across disciplines, the Tech for Good Institute provides a compendium of data sources for key topics of inquiry in the digital economy. While the series is not meant to be exhaustive of all available data sources, it is a good starting point for researchers, policymakers, and stakeholders who are interested in the intersection of policy and technology.



# About The Author

**Keith Detros** is a Programme Manager at the Tech for Good Institute. Keith has more than a decade of experience in government affairs, evidence-based policy research, 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.

## 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 the 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 its respective officers, employees or agents.

Copyright © 2023 by the Tech for Good Institute. All rights reserved.





# Acknowledgments

The author thanks the Tech for Good Institute team for the support, feedback and guidance for this study. The author is also grateful to Priyanka Sahoo and Ethan Yi Ng for their assistance and valuable contribution to this compendium.

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.

# About the Tech for Good Institute

The Tech for Good Institute is a non-profit organisation working to advance 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 while maintaining global connections. Our work is centred on issues at the intersection of technology, society, and the economy, and is intrinsically linked to the region's development. Through research, effective outreach, and evidence-based recommendations, we seek to understand and inform policy with rigour, balance, and perspective.

The Institute was founded by Grab, Southeast Asia's leading superapp, to advance the vision of a thriving and 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](http://www.techforgoodinstitute.org).



## Chapter 1

# Introduction

With rapid digitalisation, new innovative solutions and business models drive the growth and development of economies. Technology promises to enhance the lives of citizens, streamline governance, deliver better public services, and drive innovation. However, the massive opportunities from the digital economy are not without its challenges.

As more people come online, there has been an increase in threats such as scams, data breaches, and cyberattacks. These threats erode trust in the digital economy and dampen technology's potential to fully deliver on its promise of economic growth and social good. Thus, it is crucial for countries to create a safe, secure, and resilient digital economy to maximise its benefits.

To achieve this, raising awareness and understanding of the emerging threat landscape is a key step forward. Both public and private stakeholders in the digital economy need information that would aid them in policy and decision-making processes so policies to protect, identify, detect, respond, and adapt to cyberthreats can be improved.

To encourage more research in the field of cyber resilience, there is a need to amplify publicly available data sources on this topic. This compendium seeks to serve those interested in understanding and monitoring the cyber landscape across various countries, answering key questions such as:

- What are the various ways cybersecurity efforts can be measured?
- How robust is a country's cybersecurity infrastructure?
- What indicators can we use to measure adaptive measures for cyber resilience?
- Which countries can we study to understand current best practices?

It is important to keep in mind that there is no singular “best source” of information as the needs of each researcher may differ. The databases included in this guide have been chosen based on a few criteria: large sample size, balanced geographical cover (including Southeast Asia economies), availability to the public, and time salience.

It should be noted that this is not an exhaustive list. There are data sources from cybersecurity companies, for example, that may not be readily available. Other data sources might be more limited in sample size and scope, and may only be accessible at a point in time.

This guide is intended for analysts, researchers, policymakers, and anyone interested in the field of cyber resilience. This also builds on the Tech for Good Institute's existing research, [Towards a Resilient Cyberspace in Southeast Asia](#), which proposes a framework on how countries can better adapt to cyber risks.

We hope that this compendium helps to stimulate dialogue and start the building foundations of cyber resilience research.



## Chapter 2

# Cyber Resilience Global Data Sources

This compendium identifies five databases that can be useful in cyber resilience research:

- A. [Global Cybersecurity Index](#)
- B. [National Cyber Security Index](#)
- C. [Global Data Regulation Diagnostic Survey](#)
- D. [Cyber Capabilities and National Power: A Net Assessment](#)
- E. [Global Cyber Strategies Index](#)

Each of these databases are discussed in detail in this chapter, including their frequency, methodology, and focus. Relevant links are also included where applicable to allow users access to raw data.

Table 1 summarises the components of the data sources reviewed.

# Table 1. Summary of Data Sources for Cyber Resilience Research

	Global Cybersecurity Index (A)	National Cyber Security Index (B)	Global Data Regulation Diagnostic Survey (C)	Cyber Capabilities and National Power: A Net Assessment (D)	Global Cyber Strategies Index (E)
Author	International Telecommunication Union	e-Governance Academy	World Bank	International Institute for Strategic Studies	Centre for Strategic and International Studies
Coverage	194 Countries	175 Countries	80 Countries	15 Countries	194 Countries and 13 Territories
Time Period	2014 / 2017 / 2018 / 2020	Live index	2021	2021	2020
Frequency	Updated semi-frequently on an uneven basis	Updated continuously based on government, expert, or public data submissions	One time	One time	One time
No. of Variables	20 indicators	46 indicators	54 indicators	N/A. The Assessment principally employs a qualitative approach for its analysis.	N/A. The GCSI serves as a repository linking users to 7 regulatory categories of relevant cybersecurity legislation.

# Table 1. Summary of Data Sources for Cyber Resilience Research

	Global Cybersecurity Index (A)	National Cyber Security Index (B)	Global Data Regulation Diagnostic Survey (C)	Cyber Capabilities and National Power: A Net Assessment (D)	Global Cyber Strategies Index (E)
Level of disaggregation	The GCI measures cybersecurity efforts across 5 pillars, namely: Legal, Technical, Organisational, Capacity Development, and Cooperative Measures.	The NCSI measures cybersecurity efforts across 3 key categories, namely: General Cyber Security Indicators, Baseline Cyber Security/Prevention Indicators, and Incident and Crisis Management Indicators.	The Survey measures cybersecurity efforts across 7 dimensions organised along the 2 key areas: 1) enablers and 2) safeguards. This is further broken down into: E-commerce / E-transaction, Enablers for Public Intent Data, Enablers for Private Intent Data, Safeguards for Personal Data, Safeguards for Non-personal Data, Cybersecurity and Cybercrime, and Cross-border Data Transfers.	The Assessment covers cybersecurity efforts across 7 key categories, namely: Strategy and Doctrine Governance, Command and Control, Core Cyber-intelligence Capability, Cyber Empowerment and Dependence, Cyber Security and Resilience, Global Leadership in Cyberspace Affairs, and Offensive Cyber Capability.	The GCSI covers cybersecurity efforts across 7 key areas, namely: National Strategy, Military, Content, Privacy, Critical Infrastructure, Commerce, and Crime.

# Table 1. Summary of Data Sources for Cyber Resilience Research


	Global Cybersecurity Index (A)	National Cyber Security Index (B)	Global Data Regulation Diagnostic Survey (C)	Cyber Capabilities and National Power: A Net Assessment (D)	Global Cyber Strategies Index (E)
Usage	Measures a country's commitments towards cybersecurity in 5 key pillars.	Measures a country's preparedness to prevent and manage cyber incidents.	Evaluates a state's maturity and commitment to protect its national infrastructure services.	Gauges how cyber capacities contribute to the overall national power of a state.	Provides links to the existing cyber laws of different countries.
Link	<a href="https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx">https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx</a>	<a href="https://ncsi.ega.ee/ncsi-index/">https://ncsi.ega.ee/ncsi-index/</a>	<a href="https://microdata.worldbank.org/index.php/catalog/3866/study-description">https://microdata.worldbank.org/index.php/catalog/3866/study-description</a>	<a href="https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power">https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power</a>	<a href="https://csis-website-prod.s3.amazonaws.com/s3fs-public/220414_Cyber_Regulation_Index.pdf">https://csis-website-prod.s3.amazonaws.com/s3fs-public/220414_Cyber_Regulation_Index.pdf</a>


# A. Global Cybersecurity Index


One of the most widely used cyber indices is the Global Cybersecurity Index (GCI) from the International Telecommunications Union's (ITU). First launched in 2015, the GCI measures a country's commitments towards cybersecurity in five key pillars based on the ITU Global Cybersecurity Agenda: Legal, Technical, Organisational, Capacity Development, and Cooperative measures. Within these pillars, there are 20 indicators based on 82 questions.


Countries are indexed from 0 to 100, with each pillar receiving a score of 20, providing an overall snapshot of the country's performance. The best performing countries score close to 100 in this index.

The five pillars are described as follows:

 **Legal:** This pillar measures the legal and regulatory frameworks present in the jurisdiction, defining activities that are 'illegal' within the cyber realm and the enforcement mechanisms present to investigate and prosecute such offences. Additionally, it also evaluates the baseline measures and compliance systems that exist among national stakeholders and assesses whether national efforts align with international guidelines on cybersecurity.

 **Technical:** This pillar measures the institutional mechanisms and structures in place to deal with cybersecurity or data protection breaches. It involves the presence of the Cyber Emergency Response Teams (CERT), who have the power to take necessary recourse in the incident of a breach.

 **Organisational:** This pillar measures the presence of national strategies for cybersecurity and how effectively it is implemented as part of organisational measures of national entities. This includes demarcation of clear roles and accountability mechanisms in governing national cybersecurity frameworks.

 **Capacity Development Measures:** This pillar measures initiatives taken by the government to generate awareness among the general public about cybersecurity, including training and education programmes for professionals. It also measures incentives posed by the government for cybersecurity capacity development.


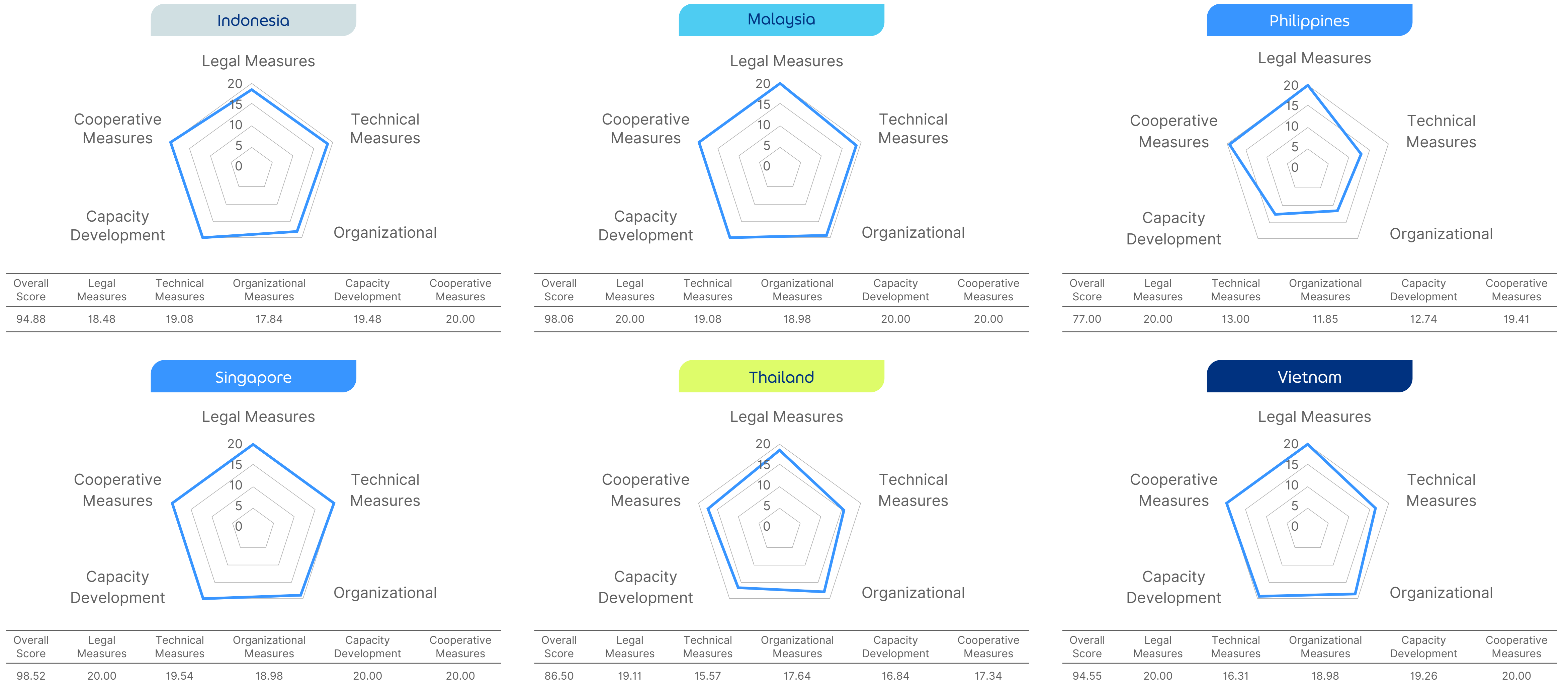
 **Cooperation Measures:** This pillar measures intra-country cooperation mechanisms to ensure a safe cyber ecosystem. It includes whether the country is part of bilateral or multilateral agreements on cybersecurity, ensuring online child protection, etc.

Figure 1.  
Global Cybersecurity Index: SEA-6, 2020



Source: ITU Global Cybersecurity Index v4, 2020

## B. National Cyber Security Index

Another index-based study on the cybersecurity capacity of governments is e-Governance Academy's National Cyber Security Index (NCSI). Similar to the GCI, the NCSI is an index updated regularly to reflect the preparedness of countries to manage cyber incidents. The NCSI is based on publicly available resources and includes 46 indicators across 12 capabilities, under three key categories. The three key categories covered by the NCSI are: General Cyber Security Indicators, Baseline Cyber Security/Prevention Indicators, and Incident and Crisis Management indicators.

Countries are then scored on a scale of 0 to 100. The country that achieves a score closest to 100 in this index is regarded as the top-performing one.

The three key categories are described as follows:




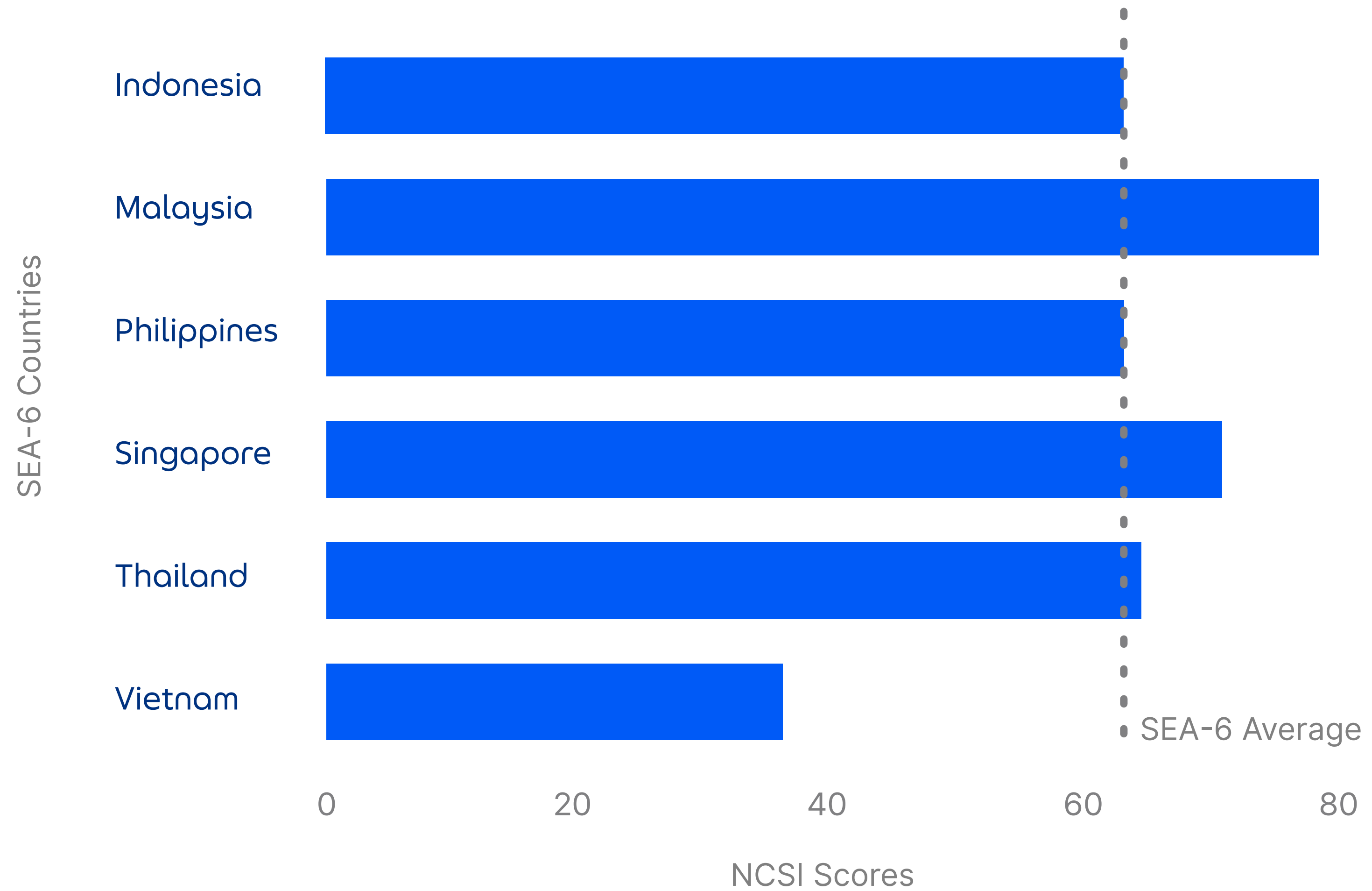
-  **General Cyber Security Indicators:** This category measures a country's cybersecurity policy development, capacity for cyberthreat analysis, preparedness in terms of education and professional development of the public, and its contribution to the global discourse on cybersecurity.
-  **Baseline Cyber Security/Prevention Indicators:** This category measures a country's existing standards to enable trust and promote usage of digital and essential services, including protection of personal data.
-  **Incident and Crisis Management Indicators:** This category measures a country's existing mechanisms to respond to a cyber incident, manage a cyber crisis, fight against a cybercrime, and military cyber operation capabilities.

Figure 2.  
National Cyber Security Index SEA-6,2023



Source: e-Governance Academy, 2023





# C. Global Data Regulation Diagnostic Survey

The Global Data Regulation Diagnostic is a comprehensive assessment of the quality of the data governance environment, covering both enabler and safeguard regulatory practices across 80 countries. It provides indicators to assess and compare relative performances.

The survey is based on questionnaires completed by lawyers specialising in data governance and ICT, providing a detailed desk review of seven dimensions organised along two key areas of enablers and safeguards. The seven dimensions covered by the World Bank are: E-commerce/E-transaction, Enablers for Public Intent Data, Enablers for Private Intent Data, Safeguards for Personal Data, Safeguards for Non-personal Data, Cybersecurity and Cybercrime, and Cross-border Data Transfers.

Using objective and standardised indicators and normative interpretation, a “Yes/No” designation is assigned to each country for every facet of data governance if the existing frameworks are deemed adequate.

The two key areas are described as follows:

-  **Enablers:** This area focuses on legal requirements related to e-signature, data portability, interoperability, digital ID systems, open data, and other mechanisms to enable and promote the use, reuse, and sharing of public and private sector data.
-  **Safeguards:** This area focuses on the legal requirements that protect fundamental rights in personal/mixed/sensitive data and commercial rights in non-personal data. Issues covered include data protection, cybersecurity and cybercrime, cross-border data flows, and intermediary liability.




# D. Cyber Capabilities and National Power: A Net Assessment

There are also qualitative assessments of cyber capacity that adopt broader concepts of cyber power. In 2021, the International Institute for Strategic Studies (IISS) released the Cyber Capabilities and National Power: A Net Assessment, designed to gauge how cyber capacities contribute to the overall national power of a state. IISS' approach stands out for its broad scope, as it takes into account the intersection of cybersecurity measures with international security, economic competition, and military affairs. This goes beyond the typical index-based methodologies used in other assessments.

This report covers a snapshot of the cyber capabilities of 15 nations, which includes most of the Five Eyes intelligence allies and a selection of their partners, a handful of states widely considered to pose cyberthreats to Western interests and several other countries at earlier stages of their cyber power development across seven key capabilities. The seven key capabilities covered by the IISS are: National Strategy and Doctrine, Governance, Command and Control, Core Cyber-intelligence Capability, Cyber Empowerment and Dependence, Cyber Security and Resilience, Global Leadership in Cyberspace Affairs, and Offensive Cyber Capability.

Each country is then assessed qualitatively across these key capabilities and then categorised into three tiers: Tier 1 (world-leading strengths in all categories), Tier 2 (world-leading strengths in some categories), and Tier 3 (world-leading strengths in some categories but with significant weaknesses in others).

The seven key capabilities are described as follows:

-  **National Strategy and Doctrine:** This capability evaluates government documents that set out priorities and budgets for cybersecurity, evaluating each country for its evolution and quality rather than noting its mere existence, unlike other indices.
-  **Governance, Command, and Control:** This capability evaluates the operational and governance mechanisms that exist within top-level government and military structures, assessing its effectiveness and evolution over time.
-  **Core Cyber-intelligence Capability:** This capability evaluates a country's situational awareness in cyberspace, comprising its ability to detect and understand threats, and opportunities in cyberspace.

➔ **Cyber Empowerment and Dependence:** This capability evaluates how best a state can protect itself from adversaries in an increasingly connected world. This intends to assess the digital sovereignty of a country in the cyber domain. The index uses assessments or research into and use of artificial intelligence as a proxy indicator.

➔ **Cyber Security and Resilience:** This capability evaluates a country's ability to ensure cybersecurity, including responding and recovering from cyberattacks. It considers the creation of security standards, technological advancement, industry-specific risk management, the efficiency of the domestic cybersecurity sector, and the extent to which the nation has been able to grow and diversify its cyber specialist workforce. To standardise this measure, this index also references the country's ranking in the Global Cybersecurity Index 2018, as compiled by the International Telecommunication Union (ITU).

➔ **Global Leadership in Cyberspace Affairs:** This capability evaluates the extent to which the country is involved in pushing forth international collaborations and agreements in cybersecurity and resilience. It includes participation in international diplomacy, formal alliances, treaties, and agreements to achieve better cyber resilience for the country itself and other cooperating countries.

➔ **Offensive Cyber Capability:** This capability evaluates a country's offensive competence in delivering an impact, rather than merely collecting intelligence information. This is essential for deterring potential cyberattacks. These operations can be carried out during both peace and conflict, either on civilians or military personnel, and vary from those intended to have cognitive impacts to those intended to cause physical destruction. Factors such as political will, legal regime, and ethical frameworks while planning an offensive cyberattack by a state are also taken into consideration.

For Southeast Asia, the index includes Indonesia, Malaysia and Vietnam. The methodology however offers an opportunity for further research to include other SEA-6 countries of Singapore, Philippines, and Thailand.

Figure 3.  
Cyber Capabilities and National Power: SEA-6, 2021

**SEA-6 Countries included in the assesment are all in Tier 3**



Source: International Institute for Strategic Studies, 2021

# E. Global Cyber Strategies Index

To evaluate the existing cyber laws of different countries, the Centre for Strategic and International Studies (CSIS) has come out with [Global Cyber Strategies Index \(GCSI\)](#), which includes a repository of cyber legislation relevant to seven key regulatory categories. The seven regulatory categories covered by the GCSI are: National Strategy, Military, Content, Privacy, Critical Infrastructure, Commerce, and Crime.

This index is not intended to evaluate or rank countries based on their regulatory efforts or capabilities. Instead, it compiles and provides access to pertinent regulations and legislation within each of the seven categories.

The seven regulatory categories are described as follows:

- ➔ **National Strategy:** Comprehensive frameworks guiding national and coordinated deterrents and responses to cyberthreats.
- ➔ **Military:** Strategies detailing offensive or defensive capabilities of a nation's military in cyberspace.
- ➔ **Content:** Laws regulating or limiting certain types of digital content.
- ➔ **Privacy:** Strategies overseeing the collection and management of personal data.
- ➔ **Critical infrastructure:** Strategies designed to mitigate cybersecurity risks for critical infrastructure networks, and enhance its resilience.
- ➔ **Commerce:** Laws that regulate digital trade and the delivery of internet services.
- ➔ **Crime:** Strategies or laws aimed at combating cybercrime.

## Chapter 3

# The Way Forward

The selection of databases outlined in this guide present a global source of information, embracing multiple facets of cyber resilience. Academics, researchers, and policymakers can use the data to inform their studies and policies depending on their needs and areas of interest.

# The Way Forward

With a mission to raise understanding, the Tech for Good Institute released a [Cyber Resilience Framework](#) which offers a conceptual understanding of resilience and borrows indicators from some of the publicly available resources cited here. The framework is another resource for those interested in cyber resilience to use as a reference in gauging the capabilities of countries in addressing the cyber risks, especially in Southeast Asia.

It is important to note that as technology evolves, data needs will also continue to evolve. The rise and increased prevalence of new technologies such as artificial intelligence, blockchain, and quantum computing may need the development of new indicators to reflect the risks these new technologies may bring. Furthermore, as more sectors adopt technological solutions, new gaps in data will inevitably appear. For example, the agriculture and healthcare sector will have its own unique challenges and thereby require sector-specific data.

In light of this, the Tech for Good Institute believes it is crucial for researchers to use these databases as a starting point in exploring further research. As noted, a key goal of this guide is to shed light on these publicly accessible datasets in order to spur further conversations on how to drive a safe and secure cyberspace forward.

## Areas of future research in cyber resilience



### Cyber resilience of MSMEs:

Micro, Small and Medium Enterprises (MSMEs), which constitutes the majority of businesses in Southeast Asia, often lack robust cybersecurity defences, making them easy targets for cyberattacks. By having data and in-depth research on MSMEs' cyber resilience, we can glean critical insights into this pivotal business segment that drives the economies of many developing nations.



### Cyber resilience of the non-profit sector

Non-profit organisations play an increasingly indispensable role in aiding societal development and equity. Despite the vital and often sensitive data they handle and the integral services they provide, these organisations often operate under tight resource constraints, potentially leading to insufficient investment in robust cybersecurity measures. Thus, increased study and data in this sector can help identify unique vulnerabilities and formulate better strategies to bolster defences.



# References

Cyber Capabilities and National Power: A Net Assessment. (2021). The International Institute for Strategic Studies. Retrieved 2 February 2023 from <https://www.iiss.org/research-paper//2021/06/cyber-capabilities-national-power>

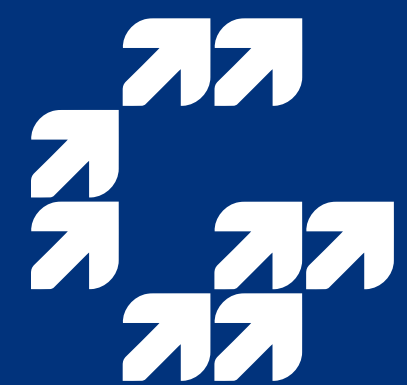
Global Cyber Strategies Index. (n.d.). Center for Strategic and International Studies. Retrieved 2 February 2023 from <https://www.csis.org/programs/strategic-technologies-program/archives/cybersecurity-and-governance/global-cyber>

Global Data Regulation Diagnostic Survey. (2021). The World Bank. Retrieved 2 March 2023 from <https://microdata.worldbank.org/index.php/catalog/3866>

International Telecommunications Union (ITU). (2023). Global Cybersecurity Index. 2021. International Telecommunications Union. Retrieved 2 March from <https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTML-E>

National Cyber Security Index. (2023). e-Governance Academy. Retrieved 2 March 2023 from <https://ncsi.ega.ee/ncsi-index/>





**TECH FOR  
GOOD  
INSTITUTE**