TECH FOR GOOD INSTITUTE

Towards a Resilient Cyberspace in Southeast Asia

Table of Contents

Table of Contents

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

Disclaimer

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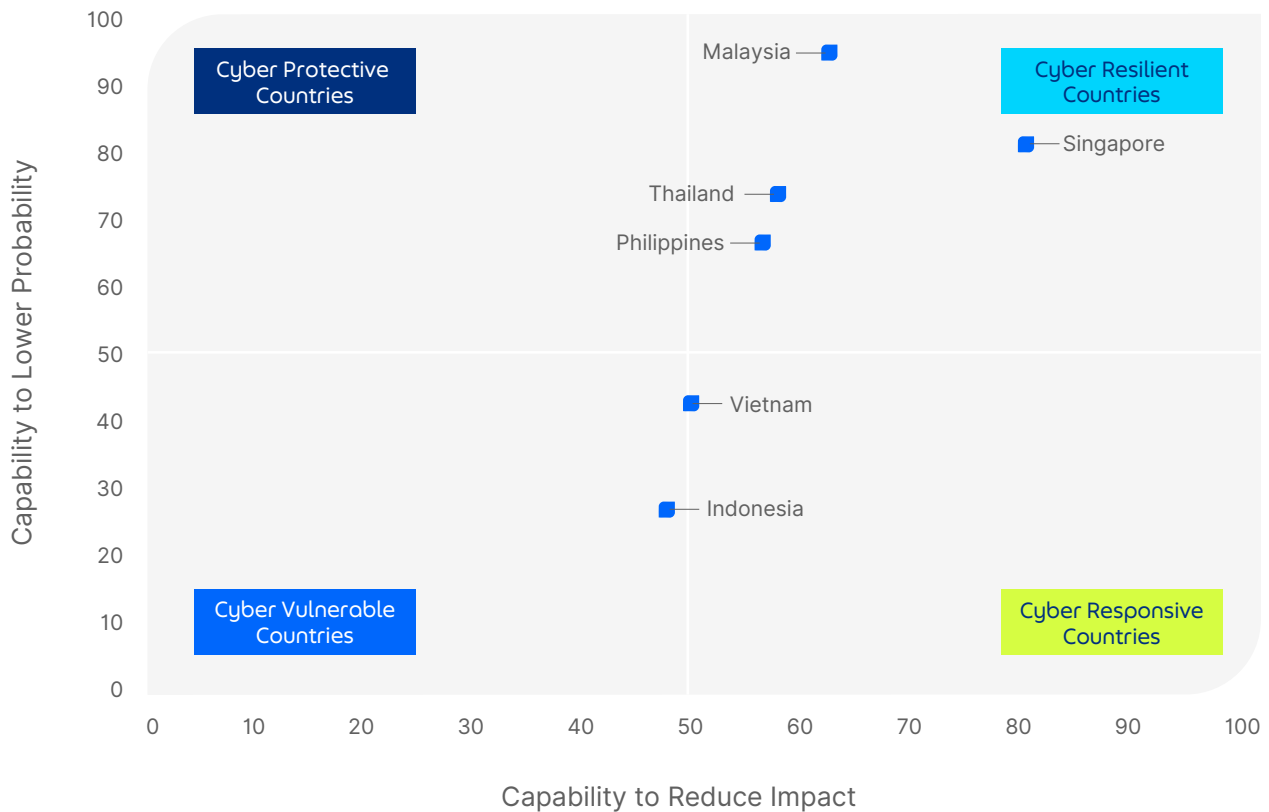
Source: Author's analysis based on the proposed Cyber Resilience Framework

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.

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

1.
Southeast Asia's Digital Decade: Opportunities and Challenges

Key Takeaways

↗ Southeast Asia is the fastest growing internet economy in the world, buoyed by an increasing number of digital users and a rise in e-commerce adoption. By 2030, the internet economy is expected to reach $1 trillion.

↗ COVID-19 catalysed rapid digital transformation in the region, which will in turn drive pandemic recovery.

↗ The cyber threat landscape, however, is continually evolving and, if left unchecked, would hamper the ability of Southeast Asian economies to reap the promised benefits of the digital economy.

The Digital Economy of Southeast Asia

Southeast Asia is undergoing a massive digital transformation. Even before the onset of the global pandemic, countries in the region — particularly the Southeast Asia-6 (SEA-6) that includes Indonesia, Malaysia, Philippines, Singapore, Thailand and Vietnam — had started their digital journ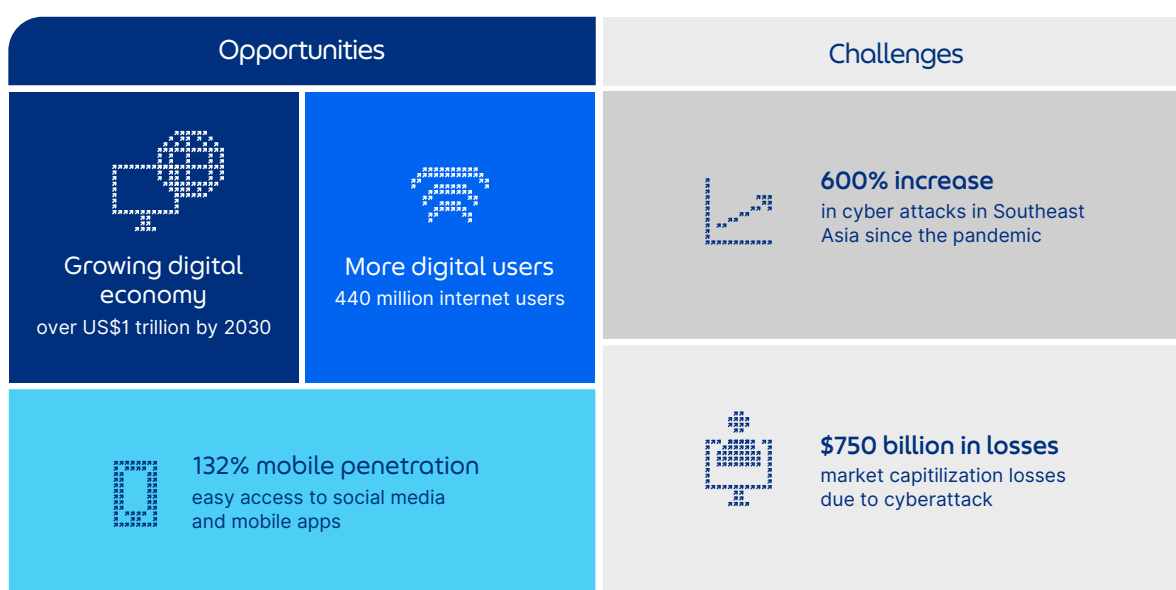ey by improving connectivity and internet infrastructure, increasing adoption of digital services, and promoting trust in digital systems.[6] In 2017, for example, the region's internet economy was already adding US$50 billion to the region's output — outpacing growth projections at that time by 35%.[7]

COVID-19 provided an unexpected acceleration to the region's "digital decade." With the pandemic limiting the movement of people, governments and businesses modified their operations dramatically. Work-from-home arrangements required digital tools for communications and productivity, while some businesses moved their core business processes online to continue transactions. The platform economy in particular, spurred digital adoption amongst micro, small, and medium enterprises (MSMEs).[8] For example, food delivery services and online retails stores experienced a boom because physical stores were closed and foot traffic was not possible. The fear of viral transmission via cash in the early days of the pandemic has also pushed people to adopt digital modes of payment. Even government social protection mechanisms such as cash transfers were released electronically. Bandwidth capacity and stable connectivity became essential as people incorporated the digital realm into their daily lives.

As various stakeholders leveraged technology to adapt during the pandemic, Southeast Asia's digital economy expanded rapidly. The immediate impact was the rise of digital users in the Association of Southeast Asian Nations (ASEAN) region. The number of people online grew from from 360 million in 2019 to 440 million in 2021,[10] raising internet penetration levels to 75%.[11] At the time of writing, around 125,000 new internet users are joining the digital economy daily.[9] Another characteristic of Southeast Asia users is the increasing rate of mobile device usage to access the internet. Mobile internet further increases access to social media and the platform economy to avail of ride hailing and food delivery services. At present, mobile penetration levels in the region have reached up to 132%, indicating that a significant number of users have more than one device connected to the internet.[12]

Figure 1. Opportunities and Challenges in Southeast Asia's Digital Economy

Opportunities	Challenges
Growing digital economy over US$1 trillion by 2030	**600% increase** in cyber attacks in Southeast Asia since the pandemic
More digital users 440 million internet users	
132% mobile penetration easy access to social media and mobile apps	**$750 billion in losses** market capitilization losses due to cyberattack

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

Internet users in Southeast Asia are active digital consumers. Tech for Good Institute noted that a third of consumers started using digital services during the pandemic while one out of two digital consumers in SEA-6 use mobile internet and digital payments in 2021.[13] The same TFGI report noted that one in four digital consumers are using more than three online-to-offline (O2O) services. More significantly, the transition to digital services is a "sticky" one, with 90% of digital consumers expressing that they are likely to continue using digital services in the next 12 months.[14] This growing base will continue to support Southeast Asia's digital boom.

It is expected that the region's digital economy will approach US\$200 billion in gross merchandise value (GMV) in 2022 and up to US\$1 trillion by 2030.[15] Despite the return of traditional physical stores and in-person shopping after the pandemic, the digital economy is still expected to grow 20% by 2025,[16] enabled by the continued adoption of digital financial services.[17] E-commerce, for example, is projected to grow 17% by 2025, accumulating an estimated GMV of US\$211 billion.

As the region continues its digital transformation, it is important to recognise the threats that come with it. The reality is that as more people go online, this increases the threat surface and points of entries for cyber criminals. Users with less experience in the digital economy will become unsuspecting victims of attacks. The cyberthreat landscape continues to evolve globally, and Southeast Asia's rise as one of the fastest growing digital economies will only attract the attention of those who wish to exploit it.

The Cyberthreat Landscape of Southeast Asia

In its 2020 Global Risks Report, the World Economic Forum (WEF) identified cyberthreats as a major man-made risk.[18] As an old adage goes, it is only a matter of "when" and not "if" a cyber-attack happens to a government, organisation, or individual. Globally, cybercrime continues to be a lucrative business for criminals, estimated to be worth US\$6 trillion in 2021, up from US\$3 trillion in 2015.[19] To put it into context, if the cybercrime industry were a country, the 2021 figures would position cybercrime as the third largest economy next to the US and China.

Southeast Asia is not spared from cyber-attacks. Countries in the region have felt the rising costs of hacks. The average cost of a data breach in the region is US\$2.71 million per organisation in 2020 in Southeast Asia, an increase from US\$2.62 million in 2019.[20] In 2020, the region has been considered as a hotspot for cyber-attacks as threat actors take advantage of the pandemic.[21] The United Nations Office on Drugs and Crime reports that there has been a 600% increase in cyber-attacks in the region in 2021.[22] In addition to phishing, ransomware has become a prominent tool for such attacks, encrypting an organisation's data before demanding payment (ransom) to restore their network systems. Massive advanced persistent threats (APTs) have been discovered in 2020, with Myanmar and the Philippines as the main targets.[23] Interpol also warned of business email compromise, cyber fraud and scams, e-commerce data interception, and cryptojacking as rising trends of attacks in the region.[24]

Left unchecked, cyber-attacks can have massive economic costs. The top 1,000 companies in Southeast Asia are at risk of losing an estimated US\$750 billion in market capitalisation due to cyberthreats.[25] Compared to the potential US\$1 trillion value of the region's digital economy by 2030, cybercrime could significantly diminish its gains and hamper continued investment in the regional digital economy. In addition, continued threats posed by cyber criminals would erode trust in the digital system. If buyers are not confident that their data, money, or digital assets are safe, adoption of digital technologies will slow dramatically, affecting online transactions from e-commerce to digital payments, to e-government services.

Hence, addressing systemic vulnerabilities is needed to avoid stunting the growth of the digital economy. The region would not be able to leverage the promise of technology without concurrently addressing the need to build a resilient environment for governments, businesses, and consumers to thrive.

2.
Elevating the Discourse: From Cybersecurity to Cyber Resilience

Key Takeaways

↗ Southeast Asia has recognised the importance of protecting the digital system through regional efforts such as the ASEAN Cyber Cooperation Strategy.

↗ Emerging cyberthreat requires a mindset shift from cybersecurity to cyber resilience.

↗ Regional cooperation is key to building cyber resilience.

With governments focused on economic growth, Southeast Asia as a region recognises the importance of protecting the digital economy against cyber-attacks. In the 2018 ASEAN Leader's Statement on Cybersecurity Cooperation, member states agreed that a "peaceful, secure, and resilient cyberspace would be a bedrock of economic progress."[26] The region also released its first ASEAN Cybersecurity Cooperation Strategy from 2017–2020, which served as a roadmap for a shared goal of a safe and secure regional cyberspace. There are continued plans and programmes to improve protection of networks and services, as detailed in the ASEAN Information and Communications Technology (ICT) Masterplans. In addition, a draft of the updated ASEAN Cybersecurity Cooperation Strategy 2021–2025 has also been published.[27]

Challenges to regional cybersecurity development remain. Despite existing masterplans and a regional roadmap, there is still no overarching unifying framework on dealing with cyberthreats.[28] For example, incident reporting and data collection frameworks are not standardised, presenting challenges when sharing information about cross-border cyberthreats. In addition, the focus of the existing ASEAN cyber cooperation strategies has been mainly on capacity building rather than policy development and coordination. This is not surprising given that digital development and cyber capability across the region are in varying stages. As consulting firm A.T. Kearney notes, some countries lack the "strategic mindset" about cybersecurity and governance, which then leads to an underdevelopment of domestic policies. [29]

One critical mindset change is to move beyond cybersecurity to cyber resilience. Cybersecurity and cyber resilience are closely related, but different. The International Telecommunications Union defines cybersecurity as a collection of tools, policies, and guidelines that can be used to **protect** an organisation's assets.[30] On the other hand, cyber resiliency is the ability to anticipate, attack, withstand, recover from, and **adapt** once the assets are compromised.[31] Another way of looking at cybersecurity is that it is concerned with the prevention and detection aspect of a breach, while cyber resilience focuses on what to do to improve the systems once these have been breached. Inherent in cyber resilience are the assumptions that attacks are inevitable, that uncertainty around threats will continue to grow, and that constant development is needed. Elevating the conversation to cyber resilience can help Southeast Asian nations craft forward-looking policies in which governments, policymakers, business leaders, and individuals emphasise continuing development and evolution to keep pace with the rapid pace of change of cyberthreats.

While "secure" and "resilient" have been used in government masterplans, these terms are not usually clearly defined. Cybersecurity has been used as a sweeping term when it comes to addressing the threats in cyberspace. As for resilience, a study by the United Nations University of 14 cybersecurity strategies in Asia Pacific noted that while most countries include the term cyber resilience, only a few have operationalised what it actually means.[32] Singapore, for example, has defined resilience in its national strategy. On the other hand, Malaysia does not use "resilience" but does include the importance of business continuity.[33] In any case, spurring a change in how we think about "cyber resilience" would lend importance not only to protection measures, but adaptation efforts as well.

A discussion on adaptation contributes to a safer cyberspace.[34] As earlier noted, cybersecurity is not just about protecting assets from being hacked. The inevitability of a hack calls for continuous development in capabilities. This would be further explored in succeeding chapters.

3.
Conceptualising a Cyber Resilience Framework

Key Takeaways

↗ The Cyber Resilience Framework is a reconceptualisation of existing cyber governance frameworks, with the aim of highlighting the adaptability component.

↗ Cyber resilience is anchored on four key domains: protect, identify and detect, respond and recover, and adapt.

↗ Cyber resilience emphasises not only bouncing back after an attack but bouncing forward.

↗ Using publicly available global databases, quantifying the pillars of framework can help gauge the state of cyber resilience in Southeast Asia.

There is currently no widely accepted framework for cyber resilience. There are, however, several frameworks from government organisations, industry associations, and the private sector on protecting digital assets. For example, the National Institute for Standards and Technology (NIST) proposes a cyber framework in five stages: identify, protect, detect, respond and recover.[35] US-based organisation MITRE, on the other hand, proposed a four-stage framework to address

cyber-attacks: anticipate, withstand, recover and evolve.[36] Another framework being proposed is the 7Ps framework: patient, persistent, persevering, proactive, predictive, preventive and pre-emptive.[37]

The proposed Cyber Resilience Framework does not reinvent the wheel, but instead builds on existing frameworks. The framework adopts the definition of resilience from the Organisation for Economic Cooperation and Development, referring to "the ability of individuals, communities, and states and their institutions to absorb and recover from shocks, whilst **positively adapting and transforming their structures and means for living in the face of long-term changes and uncertainty."[38]** What the proposed framework offers is a reconceptualisation rather than a complete overhaul of principles. It gives equal weight to the ability of states not only to bounce back after an attack, but to bounce forward and constantly seek improvement of its systems.

The Cyber Resilience Framework: Beyond Response and Recovery

The proposed Cyber Resilience Framework is derived from resilience studies, traditionally rooted in disaster management and climate adaptation. The National Academy of Science (NAS) published a study in 2012 about how system performance is affected by disruptions over time, and how organisations should think about planning, absorbing, recovering and adapting to the continuous threats.[39] The NAS model emphasises the need to minimise the impact of the disruption. It includes planning for future threats, regaining functionality, and developing the system in case of future disruptions. Figure 2 presents how cyber resilience is conceptualised in this paper.

Figure 2. Stages of Resilience
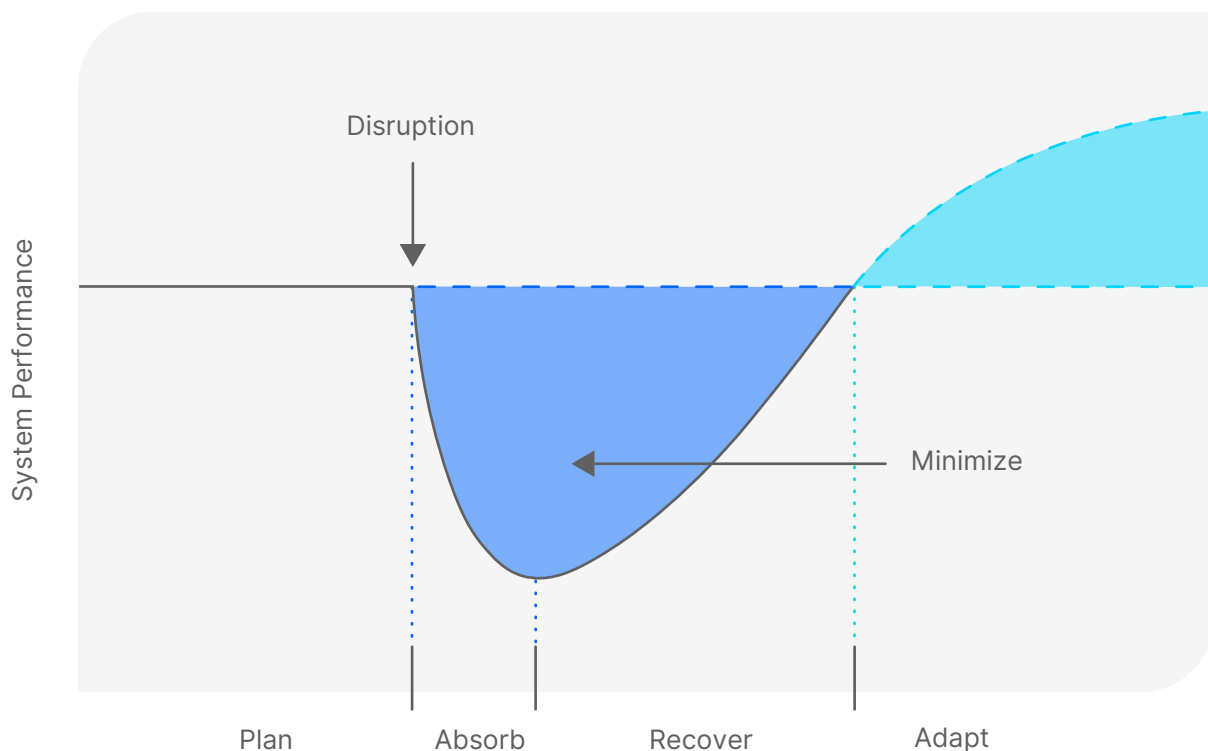
Source: National Acedemy of Science as cited by Linkov and Trump, 2019

How would this be applied in cyberspace? Based on the NAS stages of resilience, Figure 3 illustrates the proposed Cyber Resilience Framework.

Consider the graph where time is on the x axis, while cyber functionality is on the y axis. The unit of analysis in this example is a government. In this sense, cyber functionality can be a country's healthcare system, banking systems, or elections. It is a representation of how well the systems work in terms of service delivery and operations. At **point A**, the functionality is at a business-as-usual scenario. There are no interruptions and operations are running efficiently. When a cyber-attack happens, however, services are rendered unavailable and operations are crippled, resulting in a decline of functionality. This is the new point of functionality, **point B**. The challenge at this instance is for states to assess what happened and identify and detect the intrusion. After successfully managing the breach, the government can now proceed on several possible paths. The worst-case scenario is if the state does not have the capability to address the attack. At this hypothetical point of no intervention, **point C**, the new cyber functionality will remain crippled and it is less optimal than it was before the attack. The danger of non-intervention is that dips in functionality can spiral out of control. Total loss of the system is a possibility if a government does not do something about the attack. Usually however, states implement response and recovery measures to restore the operations back to the usual state. This path, **point D**, enables governments to regain control of the systems. The danger with staying at point D is when a similar attack happens, the same disruptions can occur again. In the cyber realm, attacks are constant and persistent. This scenario is plausible and functionality can be compromised repeatedly.

Figure 3. Conceptual Framework
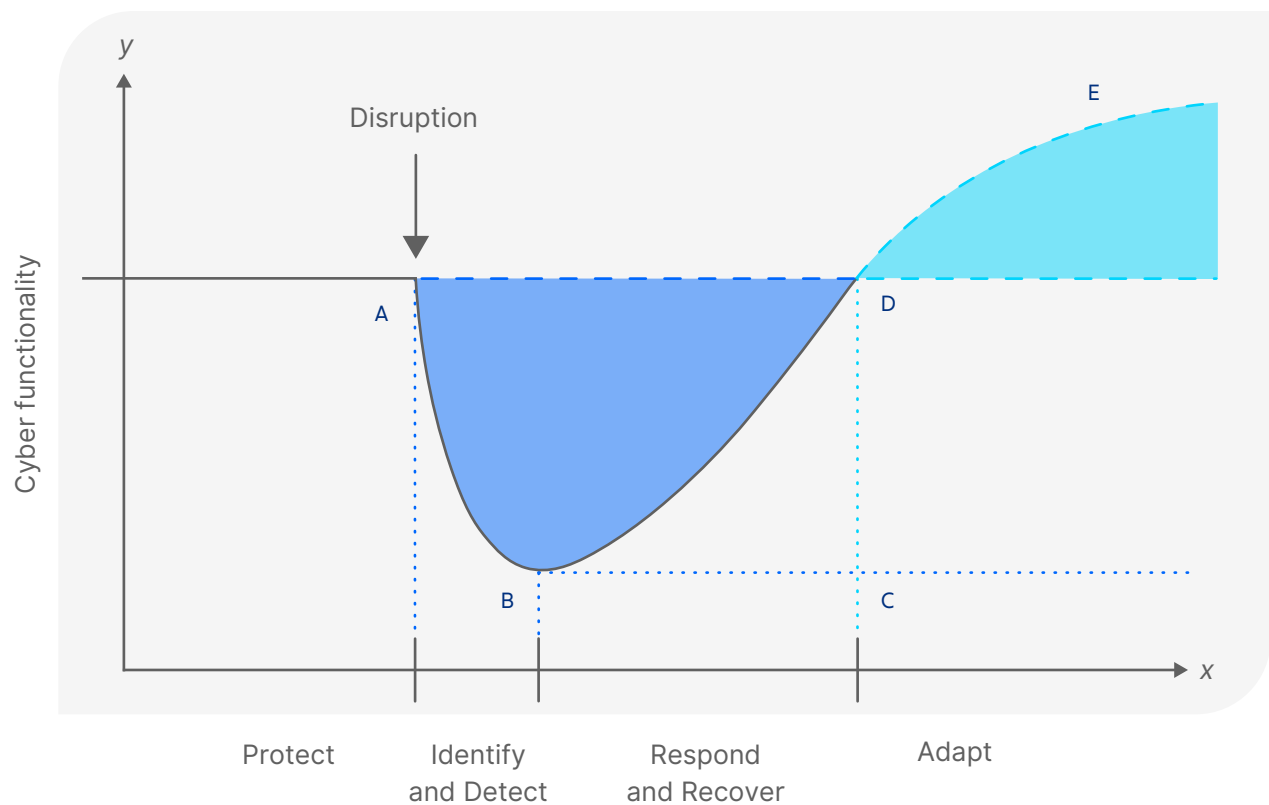
The concept of cyber resilience, however, is that the system not only "responds and recovers," but also adapts beyond the former level of operations and functionality. The goal is to get to **point E.** This is an improved business-as-usual scenario moving forward. The rationale for this mindset is that when the same shock happens in the future, the dip to Point B is theoretically not as severe as the previous. Or, in the ideal world, the same threat would not be able to cripple the systems at all as the new state of functionality has built new defences against it. It is this constant cycle of improvement that advances practices to enable governments to be one step ahead of cyber criminals.

Operationalising Cyber Resilience

Combining existing cybersecurity frameworks and the concept of resilience allows for the operationalisation of cyber resilience. Going back to Figure 3, components of cybersecurity frameworks can be applied at each point. However, there are several questions that highlight the need for resiliency at each state of functionality. Taking the example of a government or state, the following questions can be asked:

↗ At point A, what is the capability of the state to **protect** its assets? Could the attack have been prevented in the first place?

↗ What is the capability of the state to **identify and detect** threats at point B?

↗ What is the capability of the state to **respond and recover** (or move from point B to point D)?

↗ What is the capability of the state to **adapt** to cyberthreats and to improve its systems and networks in the future (to move from point B to point E)?
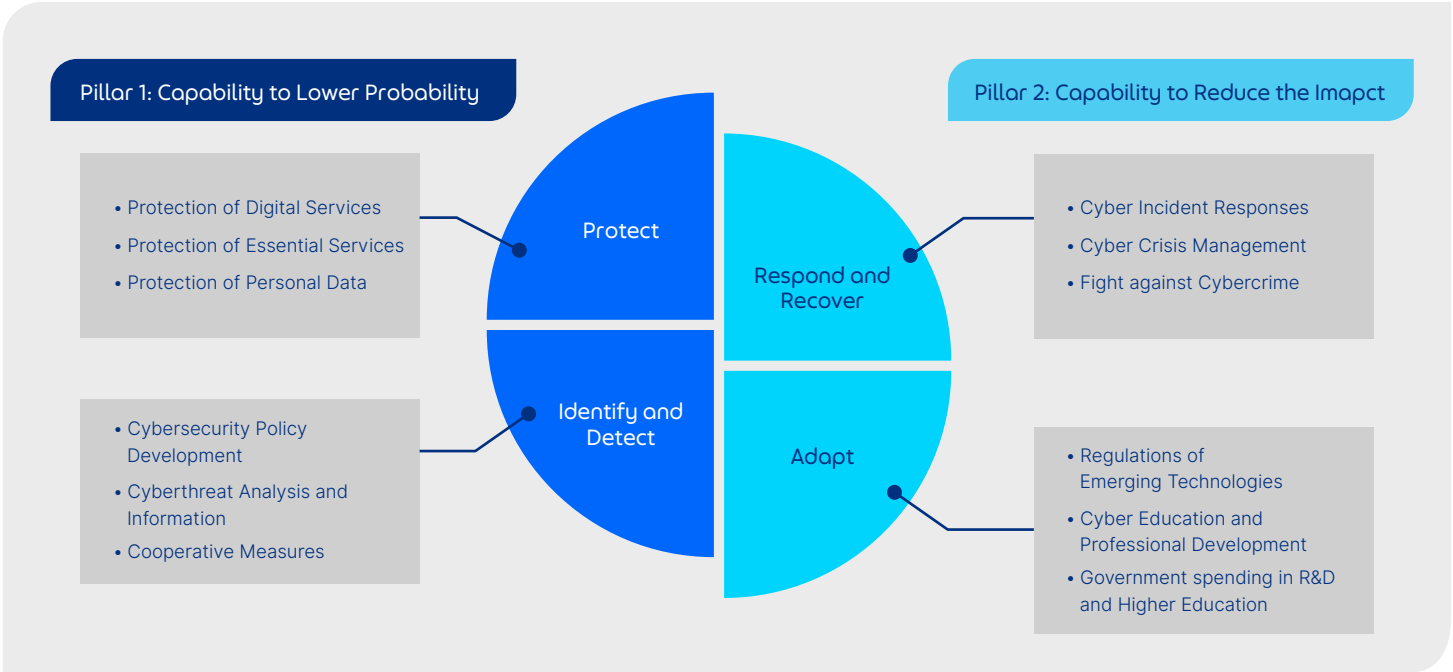
The proposed Cyber Resilience Framework thus builds on NIST's cybersecurity framework of **identify, protect, detect, respond and recover** to add **adapt,** which will be further discussed in the succeeding sections of this chapter.

It is important to note that an attack is not a prerequisite to achieving resiliency. A country need not come from point B before arriving at point E. There is no need for a vulnerability or a disruption to happen. Resiliency can be pursued on its own by the states, by constantly improving digital talent and supply of cyber skills, increasing investment in research and development, as well as crafting new policies to adapt best practices learned from international or industry partners.

What drives the resilience mindset is uncertainty of the next threat, coupled with the recognition of the inevitability of the attack. No matter the level of functionality, there will be big black swan events such as NotPetya, WannaCry or SolarWinds that will catch states off guard. Despite this uncertainty, the aim of cyber resilience is to continually improve so that the impact of such attacks can be managed by lowering the risks of being breached, improving the rate of response and recovery, and continually pursuing improvements in all aspects of cyber capabilities.

Thus, the operationalisation of the proposed Cyber Resilience Framework is two-fold: the capability to lower the likelihood / probability of cyber-attacks and the capability to reduce the impact of cyber-attacks. These form the pillars and overall structure of the Cyber Resilience Framework (Figure 4).

Figure 4. The Structure of the Cyber Resilience Framework

Pillar 1: Capability to Lower Probability

- Protection of Digital Services
- Protection of Essential Services
- Protection of Personal Data

Protect

- Cybersecurity Policy Development
- Cyberthreat Analysis and Information
- Cooperative Measures

Identify and Detect

Pillar 2: Capability to Reduce the Imapct

- Cyber Incident Responses
- Cyber Crisis Management
- Fight against Cybercrime

Respond and Recover

- Regulations of Emerging Technologies
- Cyber Education and Professional Development
- Government spending in R&D and Higher Education

Adapt

Source: Proposed Cyber Resilience Framework

Quantifying the Framework

Existing indicators from publicly-available global databases can be used to build a composite picture of cyber resilience for countries in Southeast Asia. The indicators used in the Framework come from widely-used sources. These sources come from the United Nations International Telecommunications Union, Estonia's e-Governance Academy, and the World Economic Forum's Network Readiness Index. Overall, the framework is composed of two pillars, four domains, and 12 indicators. Indicators are given equal weight and on a scale of 0 to 100, with simple average calculations done for each pillar.

Key indicators are selected to assess the capability to lower the probability of an attack (Pillar 1) and the capability to reduce the impact of an attack (Pillar 2). The pillars are further broken down into domains. Pillar 1 is composed of (1) the capability to **protect** critical data and services, and (2) the capability to **identify and detect** intrusions. On the other hand, Pillar 2 is further broken down into (1) the capability to **respond and recover** from an attack, and (2) the capability to **adapt** or build back better. Table 1 below details the indicators and sources used in quantifying the framework.

Table 1. The Indicators of Cyber Resilience Framework

Indicators	Year	Source
Pillar 1: Capability to Reduce Probability		
Protect		
Protection of Digital Services	2021	e-Governance Academy
Protection of Essential Services	2021	e-Governance Academy
Protection of Personal Data	2021	e-Governance Academy
Identify and Detect		
Cybersecurity Policy Development	2021	e-Governance Academy
Cyberthreat Analysis and Information	2021	e-Governance Academy
Cooperative Measures	2020	International Telecommunications Union
Pillar 2: Capability to Lower Impact		
Respond and Recover		
Cyber Incident Responses	2021	e-Governance Academy
Cyber Crisis Management	2021	e-Governance Academy
Fight against Cybercrime	2021	e-Governance Academy
Adapt		
Regulation of Emerging Technology	2022	Network Readiness Index
Cyber Education and Professional Development	2019	e-Governance Academy
Government spending in R&D and higher education	2022	Network Readiness Index

A Focus on Adaptability Indicators

As noted, the Cyber Resilience Framework is a combination of the NIST Framework plus an *adapt* component. The NIST framework (protect, identify, detect, respond, and recover) are traditional, commonly-used indicators for measuring cybersecurity capability. For adaptability indicators, the Cyber Resilience Framework again borrows on received industry standards.

In managing cyber risks, organisations usually build their information management security systems on three key factors: people, process, and technology. These factors are consistent with ISO/IEC 27001 as set by the International Standards Organization and the International Electrotechnical Commission.[40] Given that the study of cyber resilience is an evolving body of knowledge, some proxy indicators are selected to inform how countries can continue their cyber resilience initiatives.

↗ People

In the cyber realm, people refers to manpower and digital skills that enable a country to cope with cyberthreats through upskilling its citizens. This measure takes into account the presence (or absence) of education programmes in the country, including cyber education in the primary and secondary levels, bachelor's degrees, master's degrees, doctorate degrees, and involvement in cyber professional associations.

↗ Process

Processes encompass rules and regulations in cyber governance. With the rapid advancement of technology, governments should exhibit agility in legal and regulatory environments. This proxy measure references the adaptability of a country's legal framework to adapt to emerging technologies, including artificial intelligence, robotics, app- and web-enabled markets, big data analytics, and cloud computing.

↗ Technology

Technology involves the use of innovative solutions to make cyber governance effective and smarter. To be ahead of cyberthreats, countries should invest in building their capacities through research and development (R&D). This is a proxy indicator for adaptability and measures a combined expenditure of governments and higher education institutions on R&D as percentage of GDP.

Figure 5. Foundational Frameworks of Cyber Resilience
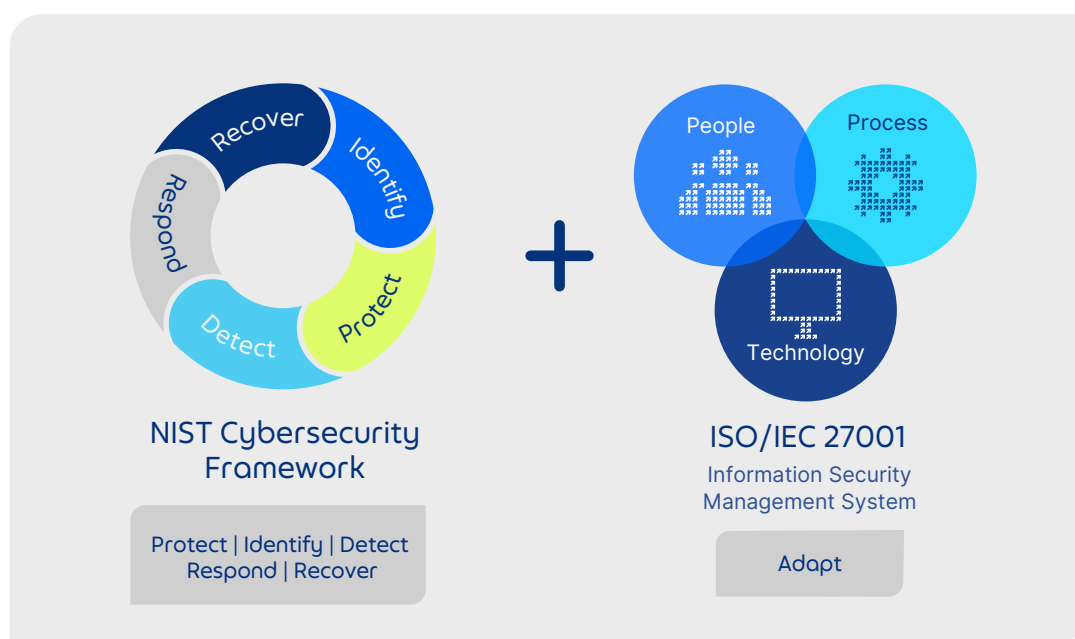
Source: NIST and ISO/IEC 27001

Categorisation in Cyber Resilience

The reconceptualisation of cyber resilience also offers an opportunity for categorical analysis. Converting Pillar 1 (Capability to Reduce Probability) and Pillar 2 (Capability to Reduce Impact) into a matrix, countries in the region can be classified as:

Vulnerable: low capability to reduce probability, low capability to reduce impact

Protective: high capability to reduce probability, but low capability to reduce impact

Responsive: low capability to reduce probability, but high capability to reduce impact

Resilient: high capability to reduce probability, high capability to reduce impact

The next section is an application of the framework to answer one pressing question:
What is the state of cyber resilience among SEA-6 countries?

4.

# The State of Cyber Resilience in Southeast Asia

Key Takeaways

↗ Southeast Asia-6 is in varying levels of cyber resilience, with Singapore leading the region in resilience efforts.

↗ There is a need for national data protection agencies to cooperate with their counterparts in other countries.

↗ Cybersecurity expertise will critical to secure and further digital progress of each country.

↗ Computer security incident response teams will benefit from coordination within and beyond national borders.

↗ Governments need to build a culture of cyber resilience across the whole of society, through awareness and competency development, from the very young to the elderly.

SEA-6 countries have shown commitment towards cyber resilience. Singapore, Malaysia, Thailand, and the Philippines have made strides in their resilience journey, having taken actions to both improve the capability to lower the likelihood of an attack, and also reduce the impact when an attack does happen. On the other hand, there is room for improvement with Vietnam and Indonesia. Figure 5 shows the main findings of the study.

Singapore leads the region in cyber resiliency. This is no surprise as Singapore has been spearheading the regional efforts in cybersecurity efforts. Since the establishment of the Cyber Security Agency in 2015, Singapore has been active in the region with its cyber initiatives. The Singapore government has committed over US$736 million to continue to develop security capabilities that would enable the country to protect critical infrastructure and mitigate cyber risk.[41]

Figure 7. The State of Cyber Resilience in Southeast Asia
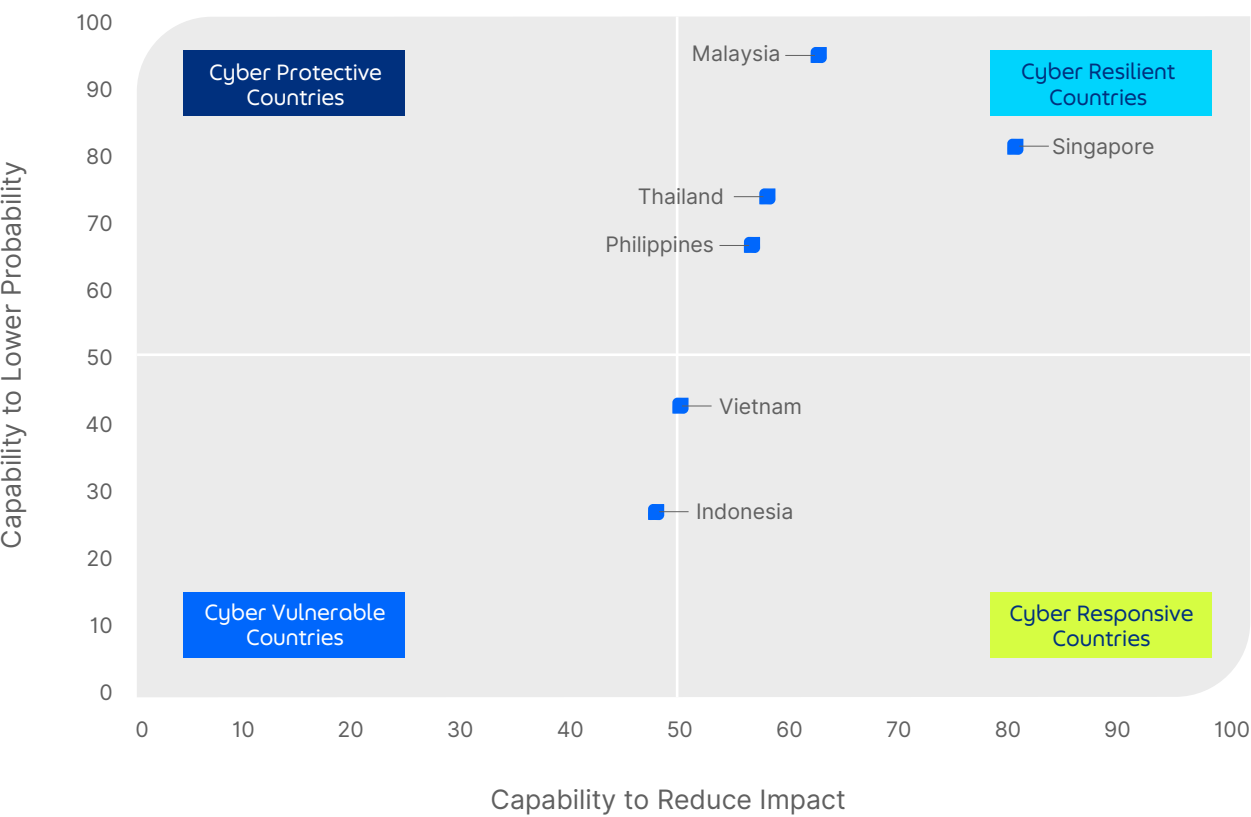
Source: Cyber Resilience Framework

Malaysia protects its assets well, with room for improvement in adaptive measures. Interestingly, Malaysia scores the highest in Pillar 1, owing to a robust regulatory environment that governs its efforts to protect, identify, and detect intrusions. As for Pillar 2, Malaysia needs to further develop adaptive measures, including its spending on cyber research and development.

Thailand has also made significant developments in improving its cyber resilience posture. The country's Cybersecurity Act and the Personal Data Protection Act were both passed in 2019 — foundational policies for protecting digital assets.[42] Thailand's capability to identify and detect cyberthreats is just behind Malaysia and Singapore. The country, however, lacks a cyber crisis management plan, which will affect its ability to effectively respond and recover from cyberthreats. The country also has a low score in the adaptability of the country's legal framework to emerging technologies.
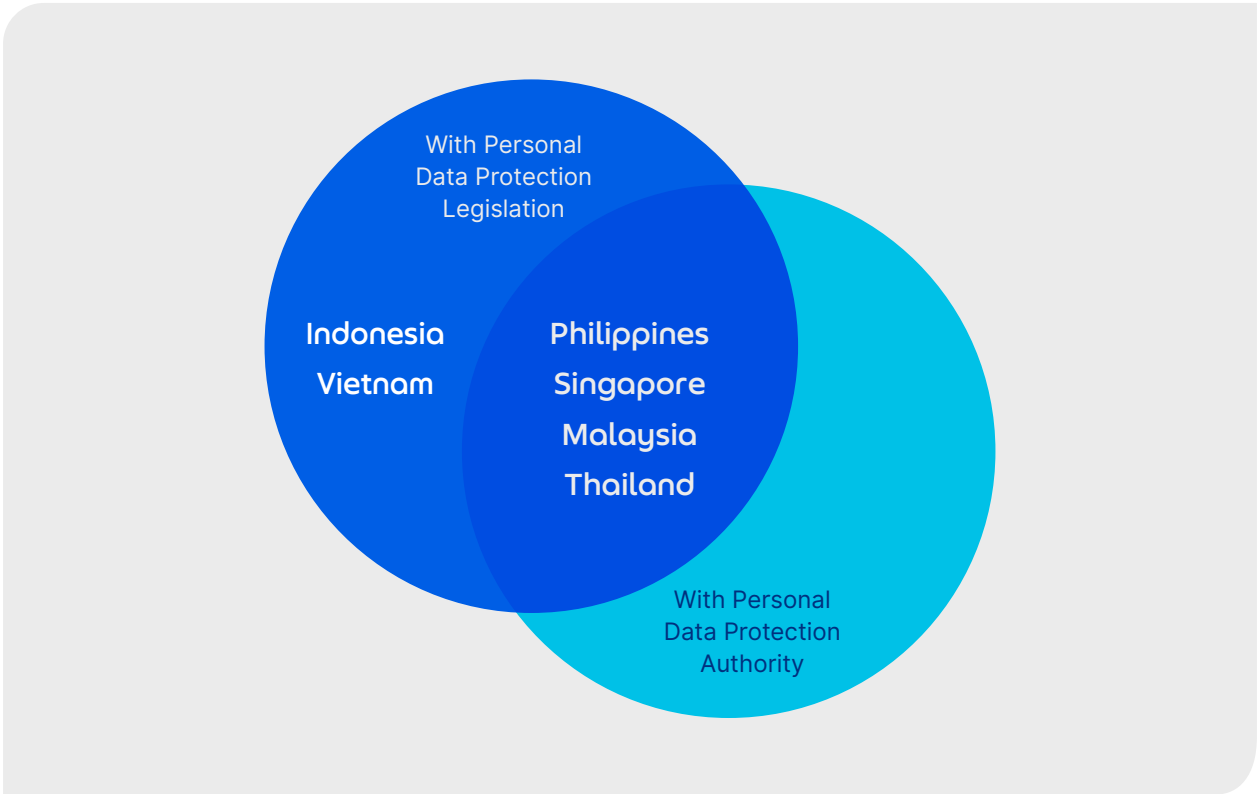
The Philippines is another country that continues its cyber resilience journey towards a positive trend. The Philippines scores high in its capability to identify and detect cyberthreats, due to dedicated cyber units and a cooperative international framework that allows for exchange of information with international partners. The Philippines, however, scores low in cyber adaptation initiatives.

Vietnam has taken up measures to improve its cyber resilience, but still has room for improvement. Despite a comprehensive data privacy law still in draft form, Vietnam has guidelines in place for the protection of digital services enshrined in several government documents and has formed a dedicated cyber response unit. Vietnam has also recently approved its cybersecurity law decree in 2022. In terms of adapting to cyberthreats, Vietnam has made efforts in cyber education with the introduction of cyber curricula at both tertiary and master's level education. Unlike the more cyber-resilient countries in the region, Vietnam does not have doctorate level programmes.

Despite having a large economy and rapid digital adoption, Indonesia is behind the other SEA-6 countries in terms of cyber resilience, in both protection and adaptation domains. Indonesia has instituted policies related to fighting cybercrime. In addition, where Indonesia shines relative to all indicators is in its international cooperative frameworks. Similar to the Philippines, Indonesia has mechanisms in place for sharing its best practices with international partners.

Based on the data, there are several themes for discussion for each of the domains of cyber resilience.

Figure 8. Current Personal Data Protection Landscape (Southeast Asia-6)

With Personal
Data Protection
Legislation

Indonesia
Vietnam

Philippines
Singapore
Malaysia
Thailand

With Personal
Data Protection
Authority

Source: Author's interpretation

Protect: Coordination among Data Protection Authorities

Data breaches, especially concerning personally identifiable data, continue to be one of the most serious organisational risks globally. Southeast Asia is no exception. In 2020 for example, the average cost of data breach in the region is US$2.62 million, with an average leak of 22,500 records per breach.[43] Some of the notable cases include the Singapore's Ministry of Health data leak in 2018. The breach was Singapore's worst cyber-attack with health records of 1.5 million people stolen, including confidential information of Prime Minister Lee Hsien Loong and other government officials.[44] The presence of a robust legal and regulatory environment helps mitigate the exposure to data breaches. All states should have an independent authority to ensure that data protection laws are developed and fit-for-purpose, and implemented consistently. In addition, coordination between data protection authorities will be key in adapting to the increasing risks of data breaches. Sharing of best practices, alignment of data protection policies, and knowledge-exchange between privacy authorities will facilitate the creation of responsive data policies in Southeast Asia.

Identify and Detect: The Need for Cyber Professionals

Like the rest of the world, cybersecurity professionals are in short supply in SEA-6. This limits the capability of states to identify and detect cyberthreats, evidenced by the long threat dwell times in the region. This poses problems as the region already suffers from long threat dwell times. Dwell time is measured in the number of days from the moment of intrusion to the moment of detection of the threat. Median dwell time in Southeast Asia as of 2017 is at 172 days, which is 73 days above the global median dwell time of 99 days.[45] The International Information System Security Certification Consortium, the leading cybersecurity professional organisation in the world, grants the certification of Certified Information Systems Security Professional (CISSP). CISSP is one of the most coveted certifications of cybersecurity experts. As of July 2021, there are 149,174 CISSP holders across 172 countries, of which 62% are in the United States.[46] In Southeast Asia, there are 3,707 cybersecurity CISSPs, 72% of whom are based in Singapore.

Table 2. Cybersecurity Experts, ASEAN-6:2021

	CISSP
ASEAN	3,707
Singapore	2,683
Malaysia	377
Thailand	258
Philippines	183
Indonesia	122
Vietnam	76

Source: (ISC)[2],2021

Respond and Recover: Building Capacity of CSIRTs

A key factor for responding to cyberthreats is the formation of a computer security incident response team (CSIRT), also called a Computer Emergency Response Team (CERT). A positive highlight is that all the countries in Southeast Asia have CSIRTs that are responsible for coordinating key actions if a government is hacked. The ongoing priority for the region is further capacitating these CSIRTs. In line with this, Singapore launched the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE).[47] The Centre aims to train officials from ASEAN member states and will allow for CSIRT-to-CSIRT information sharing.

Adapt: Building a Culture of Cyber Resilience Through Education

There have been important strides made in the region to build up a pool of cybersecurity professionals through the formal education system. Singapore, Malaysia, and Thailand all have bachelors, masters, and doctorate programmes specifically for cybersecurity. There is a gap, however, in introducing the cyber competencies at the primary and secondary levels in the region. This is important as the pandemic has increased the rate of using digital technologies for education, especially the children. It would be prudent to equip the students, even children in the primary and secondary levels, with some basic cyber hygiene to protect themselves from the dangers of the internet. Except for Singapore and Malaysia, SEA-6 economies have yet to incorporate cyber safety and computer safety practices into pre-university curricula.

Table 3. Cyber Education and Professional Cyber Association in Southeast Asia

	Primary/ Secondary	Bachelor's	Masters	PHD	Industry Associations
Indonesia	✗	✓	✗	✗	✓
Malaysia	✓	✓	✓	✓	✓
Philippines	✗	✓	✓	✗	✓
Singapore	✓	✓	✓	✓	✓
Thailand	✗	✓	✓	✓	✓
Vietnam	✗	✓	✓	✗	✓

Source: e-Governance Academy,2021

5.

The Cyber Resilience Playbook: Towards a Secure and Resilient Digital Economy

Key Takeaways

↗ Cyber resilience at a national level will be challenging to achieve without collective cyber resilience at the regional level.

↗ Southeast Asia needs to ramp up its spending to develop cyber resilience. The Cyber Resilience Framework offers strategic insights on which areas countries can prioritize.

↗ Crosscutting recommendations across countries include improving public-private partnerships to address cyber workforce gaps and building a culture of cyber resilience by training the vulnerable population.

Given the ever-changing threat landscape, the future of keeping the integrity of digital systems depends not only on protecting them from a breach, but also ensuring that resilient networks are in place. Southeast Asia would benefit from a unifying framework that is built on the concept of bouncing forward in response to cyber-attacks. As earlier noted, while ASEAN roadmaps and masterplans have been mentioning cyber resilience, the operationalisation with actual actionable steps for countries should also be identified. The current Cybersecurity Regional Action Plan focuses

on the adoption of the UN Group of Governmental Experts (GGE) Norms of responsible state behaviour, which governs state-to-state interactions and includes a confidence-building measure for states not to attack each other in the digital world. A similar regional action plan, with focus on cyber resilience, would benefit the region.

On top of the existing ASEAN Cyber Cooperation Strategy, an ASEAN cyber resilience regional action plan will offer specific guidelines towards cyber resilience. Building on the emphasis of cyber resilience as proposed by the Cyber Resilience Framework, such a plan should have tangible targets in investing in people, process, and technology in order to ensure adaptability.

In addition, further general recommendations can be pursued individually by SEA-6 economies. These are general in nature, but can serve as a step towards a resilient digital economy.

a) Ramp up spending to develop cyber resilience.

As of 2017, Southeast Asian countries collectively spent US$1.9 billion or 0.06% of the regional GDP on cybersecurity. Benchmarking this across the world, this is half of the global average (0.13% of GDP). The average for mature economies is 0.16% of GDP, while Israel, considered one of the leading countries in cyber capabilities, is at 0.35% of GDP. [48]

As for ASEAN economies, Singapore leads the region at 0.22% of GDP, above the global average and mature economies average. Malaysia (0.08% of GDP) is spending above ASEAN's average, while the rest of ASEAN hovers around 0.04%. Figure 9 shows the spending levels of Southeast Asia in 2017.

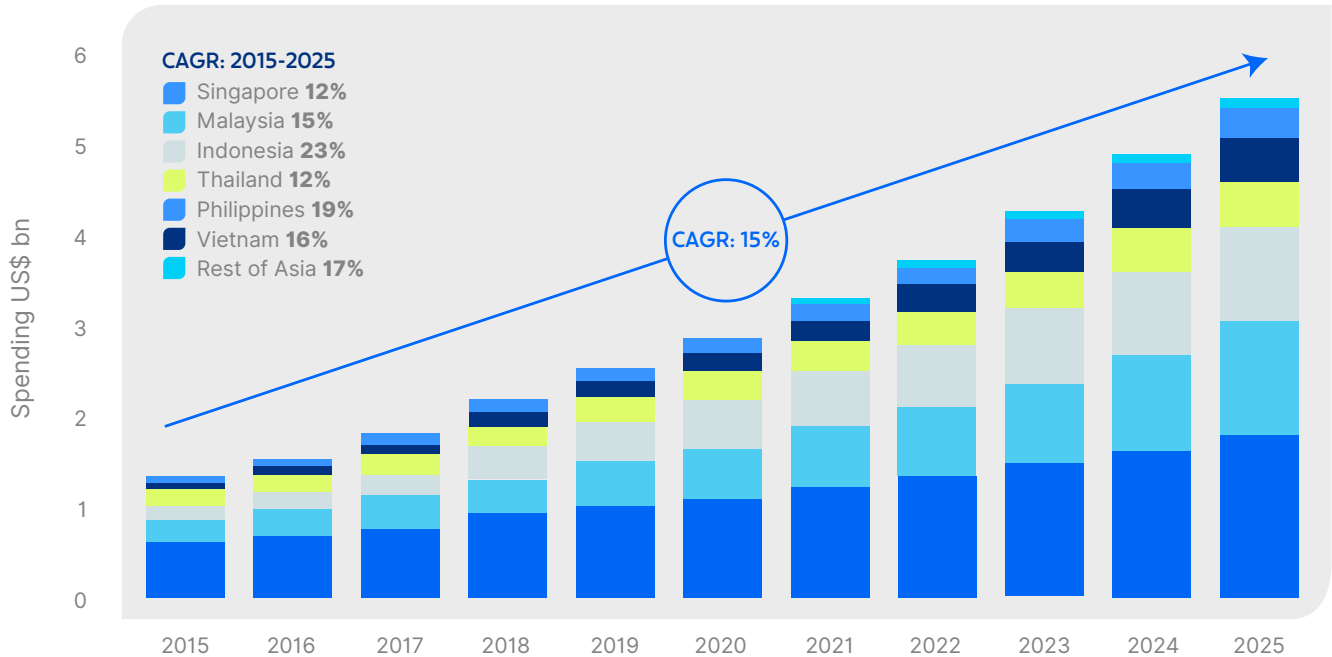Figure 9. Cybersecurity Spending, Southeast Asia and Selected Countries, 2017
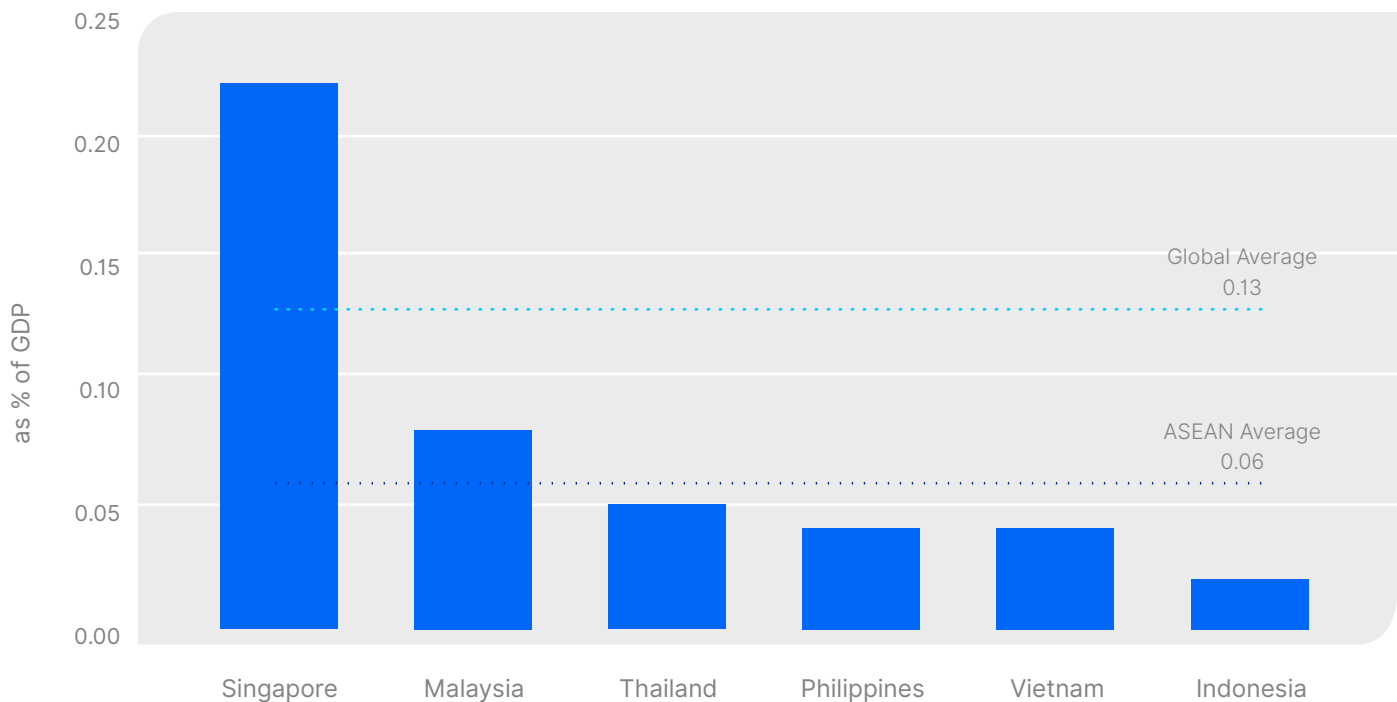
Source of raw data: A.T. Kearney, 2018

Despite some shortfalls in spending, a silver lining for the region is that it is expected to increase its investments in protecting its networks by 2025. A compound annual growth rate of 15% is projected to be spent towards cybersecurity initiatives (Figure 10). Singapore, Malaysia, and Indonesia are the drivers of this growth, accounting for almost 75% of total investments in the period. Indonesia (23%), the Philippines (19%), Vietnam (16%), and Malaysia (15%) are expected to see the highest growth as they address gaps in infrastructure and as the managed service landscape evolves.[49]

In relation to the increase in overall spending, the proposed Cyber Resilience Framework allows for countries to identify which areas should be their strategic priorities for investment in order to achieve cyber resilience. Analysing the framework, domains with the most room for growth would be the strategic priority. For example, Indonesia and Vietnam can focus on the domains which can help them protect against cyberthreats, while Thailand and the Philippines can improve on their adaptability to cyberthreats. Appendix 2 shows a detailed breakdown per country.

Figure 10. Cybersecurity Spending Projections in Southeast Asia, 2015-2025

CAGR: 2015-2025
■ Singapore **12%**
■ Malaysia **15%**
■ Indonesia **23%**
■ Thailand **12%**
■ Philippines **19%**
■ Vietnam **16%**
■ Rest of Asia **17%**

CAGR: 15%

Source of raw data: A.T. Kearney, 2018

b) Regularly publish ASEAN Threat Landscape Reports.

Threat landscape reports are the backbone of policymaking in cybersecurity. Currently, most of the reports come from the private sector and international organisations. National CERTs have a wealth of information on what countries face on a day-to-day basis. Compiling, analysing and publishing an ASEAN-level report from the national CERTs would enable a more comprehensive view of the threats that ASEAN-member states face. This would lead to more responsive policies specific to the region and would allow countries to better calibrate responses.

c) Establish a regional baseline for cybersecurity standards.

Cyber resilience among ASEAN member states varies widely. There is a need to coordinate, at the very least, the minimum standards across the region. A common framework for cybersecurity standards would encourage states to protect their systems and ensure that there are no weak links in the regional efforts towards cyber resilience. The framework for a regional baseline, however, must be periodically reviewed to ensure that it remains relevant and fit-for-purpose.

d) Address the gap in cybersecurity workforce through public-private partnerships.

Countries have already developed cybersecurity curricula in tertiary education institutions to address the shortage of cybersecurity professionals in the region. There is, however, a need to augment such efforts with public-private partnerships especially focusing on reskilling and upskilling the existing workforce.

➔ ***Establish learning hubs for cybersecurity.*** Similar to the initiative of the World Economic Forum, establishing a learning hub will help increase awareness among individuals.[50] A learning hub is an online platform where public and private stakeholders can share industry frameworks and cybersecurity resources. This would democratise information and would also encourage more to take on cybersecurity jobs.

➔ ***Synergise private sector needs with close coordination to education policy.*** Governments should provide a platform where the private sector and their ministries for higher education can exchange information on the supply and demand of cyber professionals. The private sector can offer projections on their needs and educational institutions can design strategies to equip graduates with the skills needed to meet the growing demand for a cyber workforce.

e) Build a culture of cyber resilience.

The widespread adoption of technology also increased access to all segments of society. Aside from focusing mainly on tertiary education that would feed talent directly into the cyber workforce, governments in the region should also incorporate initiatives for cyber awareness across all segments of society. These might include:

➔ ***Introducing cyber hygiene in primary and secondary education.*** With the rise of remote and hybrid learning models for education, gadgets such as mobile phones and tablets have become an indispensable part of a child's daily life. Unfortunately, children may be susceptible to hacks, phishing, fraud, and scams. Southeast Asian nations would be better off by starting cyber hygiene training at a young age. Not only would this help raise cyber awareness among the young but it could also spark interest among the youth to pursue careers in cybersecurity. Gamification of cyber best practices can also help achieve this goal.

↗ ***Launch a senior's programme for cyber education.*** The older segments of the population also need to be educated about cyber security. A survey conducted by Kaspersky in 2018 reveals that the elderly sector is not well-equipped to protect themselves online.[51] In addition, the older population might not be as technologically savvy and might find the online environment unfamiliar.[52] A 2012 study by the Stanford Centre of Longevity also notes that people over the age of 65 are 35% more likely to be a victim of scams or fraud than those under 30.[53] This makes the elderly easy targets for cybercriminals. Educating seniors helps build a culture of cyber resilience in the region. It also promotes trust in the digital systems when governments can protect the most vulnerable.

6.
Conclusion

The Cyber Resilience Framework is a conceptualisation of cyber resilience for countries, with this paper focusing on Southeast Asia-6. The framework provides a nuanced approach in understanding cyber capabilities focusing on two key pillars: the capability to lower the likelihood of an attack, and the capability to reduce the impact of an attack. The framework also allows for gauging specific domains: 1) protect, 2) identify and detect, 3) respond and recover, and 4) adapt.

Adaptability is a core but under appreciated contribution to cyber resilience. This is in line with the value of resilience in general, in which continual development in people, process and technology increases capability to cope with uncertainty. Amidst the growing and evolving cyber threats, economies need to invest in cyber resiliency in a holistic manner, so as to sustainably protect digital networks. The Framework can shape important conversations on how the region can formulate actionable policies and move towards making Southeast Asia's digital economy secure and resilient.

The Cyber Resilience Framework is in line with what industry observers have been promoting–a shift from cybersecurity to cyber resiliency. This includes crafting policies with the recognition that a hack will be inevitable. This helps address policy myopia and encourages ASEAN member states not to rest on their laurels when it comes to protecting the integrity of the digital economy. In addition, the Framework's focus on resilience can become the foundation of future cyber roadmaps and technology masterplans. Aside from the recommendation of crafting a regional Cyber Resilience Action Plan, there are general recommendations that ensure the digital economy remains safe and secure as the region continues its path towards regional integration. Finally, policymakers can use the Framework as a tool for identifying national strategic priorities to improve their systems. In-depth country studies and local stakeholder consultations can support the crafting of responsible national-level recommendations to improve cyber resilience for each country.

Appendix 1: The Cyber Resilience Framework

Indicators are on a scale of 0 – 100, with higher scores indicating a more resilient state. Given that some of the indicators are on different scales, a minimum-maximum normalisation method was used to keep the data comparable.
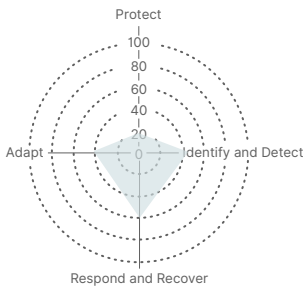
Indicators	Indonesia	Malaysia	Philippines	Singapore	Thailand	Vietnam
Cyber Resilience Framework	38	79	62	82	66	47
Pillar 1: Capability to Reduce Probability	28	94	67	81	74	43
Protect	15	93	46	67	57	43
Protection of Digital Services	20	80	20	0	20	80
Protection of Essential Services	0	100	17	100	50	50
Protection of Personal Data	25	100	100	100	100	0
Identify and Detect	40	95	88	95	91	43
Cybersecurity Policy Development	0	86	86	86	86	29
Cyberthreat Analysis and Information	20	100	80	100	100	0
Cooperative Measures	100	100	97	100	87	100
Pillar 2: Capability to Lower Impact	48	63	57	82	59	50
Respond and Recover	55	56	81	76	68	57
Cyber Incident Responses	67	50	83	50	100	100
Cyber Crisis Management	20	40	60	100	60	60
Fight against Cybercrime	78	78	100	78	44	11
Adapt	41	71	33	88	49	44
Regulation of Emerging Technologies	62	59	26	94	43	53
Cyber Education and Professional Development	44	100	67	100	89	67
Government spending in R&D and higher education	18	53	7	72	16	11

Source: The Cyber Resilience Framework

Appendix 2: Country Radar Chart of Southeast Asia, by Domain

Country scores per country are shown below. A larger area in the radar chart reflects a more cyber resilient state.
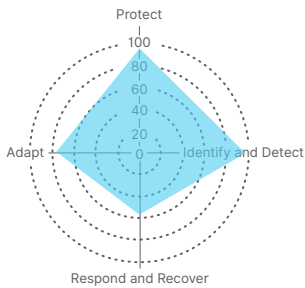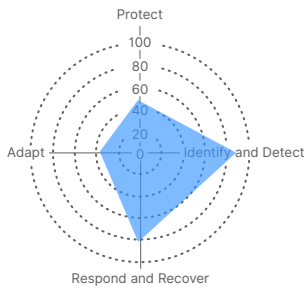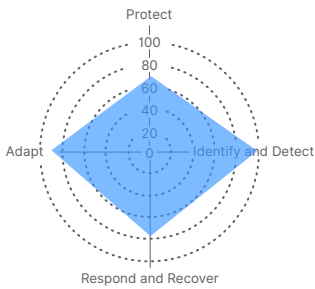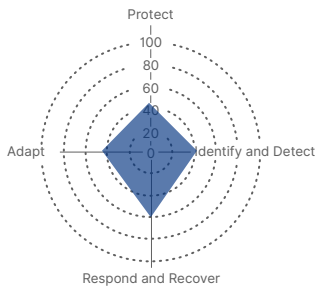
Source: See Appendix 2

Appendix 3: Indicator Selection and Definitions

PILLAR 1: Capability to Reduce Probability

This pillar is composed of the domains of Protect and Identify & Detect.

1.1. Protect

1.1.1   **Protection of Digital Services.** This indicator is a composite score which assigns points to governments if there is evidence of cyber security responsibility for digital service providers (1 point), cyber security standard for the public sector (1 point), and competent supervisory authority (3 points). The total score for this indicator is 5 points, normalised to be comparable. This data is from the e-Governance Academy.

1.1.2   **Protection of Essential Services.** This indicator is a composite score which assigns points to governments if operators of essential services are identified (1 point), if there are cyber security requirements for operators of essential services (1 point), if there is a competent supervisory authority (3 points), and if there is regular monitoring of security measures (1 point). The total score for this indicator is 6 points, normalised to be comparable. This data is from the e-Governance Academy.

1.1.3   **Protection of Personal Data.** This indicator is a composite score which assigns points to governments if there is evidence of personal data protection legislation (1 point) and if there is personal data protection authority (3 points). The total score for this indicator is 4 points, normalised to be comparable. This data is from the e-Governance Academy.

1.2. Identify & Detect

1.2.1   **Cybersecurity Policy Development.** This indicator is a composite score which assigns points to governments if there is evidence of a cyber security policy unit (3 points), cyber security policy coordination format (2 points), cyber security strategy (1 point), and cyber security strategy implementation plan (1 point). The total score for this indicator is 7 points, normalised to be comparable. This data is from the e-Governance Academy.

1.2.2   **Cyberthreat Analysis and Information.** This indicator is a composite score which assigns points to governments if there is evidence of a cyberthreat analysis unit (3 points), if public cyberthreat reports are published annually (1 point), and if there is a cyber safety and security website (1 point). The total score for this indicator is 5 points, normalized to be comparable. This data is from the e-Governance Academy.

1.2.3   **Cooperative Measures.** The indicator measures a country's involvement in cybersecurity agreements in various capacities including bilateral, multilateral, inter-agency partnerships, private sector partnerships, and international mechanisms. This indicator gives out zero to 20 points, normalised to be comparable. This data is from the International Telecommunications Union.

PILLAR 2: Capability to Lower Impact

This pillar is composed of the domains of Respond & Recover and Adapt.

2.1. Respond and Recover

2.1.1   ***Cyber Incident Responses.*** This indicator is a composite score which assigns points to governments if there is evidence of a cyber incident response unit (3 points), if the reporting responsibilities are clear (1 point), and if there is a single point of contact for international coordination (2 points). The total score for this indicator is 6 points, normalised to be comparable. This data is from the e-Governance Academy.

2.1.2   ***Cyber Crisis Management.*** This indicator is a composite score which assigns points to governments if there is evidence of a cyber crisis management plan (1 point), a national-level cyber crisis management exercise (2 points), participation in international cyber crisis exercises (1 point), and operational support of volunteers in cyber crises (1 point). The total score for this indicator is 5 points, normalised to be comparable. This data is from the e-Governance Academy.

2.1.3   ***Fight against Cybercrime.*** This indicator is a composite score which assigns points to governments if there is evidence that cybercrimes are criminalised (1 point), if there is a cybercrime unit (3 points), if there is a digital forensics unit (3 point), and if there is a 24/7 contact point for international cybercrime (2 points). The total score for this indicator is 9 points, normalised to be comparable. This data is from the e-Governance Academy.

2.2. Adapt

2.2.1   ***Regulation of emerging technologies.*** This is a proxy indicator for a country's ability to change its legal framework for cybersecurity and the evolving processes involved in technology. This indicator is a sub-indicator from the Network Readiness Index 2020 and can also be found on the WEF Executive Opinion Survey 2018–2019. The scores are normalised to be comparable. It is a mean score of the answer to the question: In your country, how adequately is the legal framework adapting in Artificial intelligence, Robotics, app- and web-enabled markets, big data analytics, and Cloud computing?

2.2.2   ***Cyber Education and Professional Development.*** This indicator is a proxy indicator for adaptability, especially for manpower and the future of cybersecurity skills in a country. This indicator is a composite score which assigns points if there is evidence of cyber safety competencies in primary or secondary education (1 point), bachelor's level cyber security programme (2 points), master's level cyber security programme (2 points), PhD level cyber security programme (2 points), and cyber security professional association (2 points). The total score for this indicator is 9 points, normalised to be comparable. This data is from e-Governance Academy.

2.2.3 **_Government spending in R&D and higher education._** This indicator is a proxy indicator for adaptability, especially in the ability of governments to cope with ever-changing technology and cyberthreats. This data is a sub-indicator from the Network Readiness Index 2020 and can also be sourced from the UNESCO Institute for statistics. The indicator is a combined expenditure of governments and higher education institutions on research and development as percentage of GDP.

References

1	Association of Southeast Asian Nations (ASEAN). (2020). ASEAN key figures 2020. Retrieved March 22, 2022 from https://www.aseanstats.org/wp-content/uploads/2020/11/ASEAN_Key_Figures_2020.pdf
2	Google. (2021). e-Conomy report 2021. Retrieved November 22, 2022 from https://economicimpact.google.com/
3	World Economic Forum. (n.d.). Digital ASEAN. Retrieved February 6, 2022 from https://www.weforum.org/projects/digital-asean.
4	AT Kearney. (2018). Cybersecurity in ASEAN: An urgent call to action. Retrieved February 6, 2022 from https://www.southeast-asia.kearney.com/documents/1781738/1782318/Cybersecurity+in+ASEAN%E2%80%94An+Urgent+Call+to+Action.pdf/80a880c4-8b70-3c99-335f-c57e6ded5d34.
5	AT Kearney. (2018).
6	World Bank. (2019). The digital economy in Southeast Asia: Strengthening the foundations for future growth. Information and Communications for Development. World Bank, Washington, D.C. License: Creative Commons Attribution CC BY 3.0 IGO. Retrieved April 2, 2022 from https://openknowledge.worldbank.org/bitstream/handle/10986/31803/The-Digital-Economy-in-Southeast-Asia-Strengthening-the-Foundations-for-Future-Growth.pdf?sequence=1&isAllowed=y
7	Anandan, R. and Sipahimalani, R. (2017). 330 million internet users accelerating the growth of Southeast Asia's internet economy. Google. Retrieved April 17, 2022, from https://blog.google/around-the-globe/google-asia/sea-internet-economy/
8	Tech for Good Institute. (2021). The platform economy report. Retrieved April 30, 2022 from https://techforgoodinstitute.org/blog/reports/the-platform-economy-southeast-asias-digital-growth-catalyst/
9	World Economic Forum. (n.d.). Digital ASEAN.
10	Google, Temasek, & Bain and Company. (2021). e-Conomy SEA. Retrieved April 2, 2022 from https://services.google.com/fh/files/misc/e_conomy_sea_2021_report.pdf.
11	Google, Temasek, & Bain and Company. (2021).
12	We Are Social. (2021). Southeast Asia: Digital life intensified. Retrieved March 3, 2022 from https://wearesocial.com/sg/blog/2021/03/southeast-asia-digital-life-intensified/#:~:text=Southeast%20Asia%20is%20also%20leading,132%25%20of%20the%20total%20population
13	Tech for Good Institute (2021).
14	Tech for Good Institute (2021).
15	Google, Temasek, & Bain and Company. (2022). e-Conomy SEA Report. Retrieved November 15, 2022 from https://services.google.com/fh/files/misc/e_conomy_sea_2022_report.pdf
16	Google, Temasek, & Bain and Company.(2022).
17	Tech for Good Institute. (2022). Digital financial services for financial inclusion in Southeast Asia. Retrieved November 5, 2022 from https://techforgoodinstitute.org/blog/reports/digital-financial-services-for-financial-inclusion-in-southeast-asia/

18	World Economic Forum (2020). The Global Risks Report 2020. Retrieved 05 October 2020 from http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf
19	Morgan, S. (2020). Cybercrime to cost the world $10.5 trillion annually by 2025. Cybercrime Magazine. Retrieved April 17, 2022, from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
20	Henderson, J. (2020). Data breaches cost ASEAN businesses $2.71m. Channel Asia. Retrieved April 17, 2022, from https://www.channelasia.tech/article/681831/data-breaches-cost-asean-businesses-minimum-2-71m/
21	Tan, A. (2020). Southeast Asia remains hotspot for cyber-attacks. Computer Weekly. Retrieved June 14, 2022 from https://www.computerweekly.com/news/252490194/Southeast-Asia-remains-hotspot-for-cyber-attacks.
22	United Nations Office on Drugs and Crime. (2021). Ransomware attacks, a growing threat that needs to be countered. UNODC Regional Office for Southeast Asia and the Pacific. Retrieved April 17, 2022, from https://www.unodc.org/roseap//en/2021/10/cybercrime-ransomware-attacks/story.html
23	Kaspersky. (2021). Rare, mass advanced threat campaign targets more than a thousand users in Southeast Asia. Retrieved April 17, 2022, from https://www.kaspersky.com/about/press-releases/2021_rare-mass-advanced-threat-campaign-targets-more-than-a-thousand-users-in-southeast-asia
24	Interpol. (2021). ASEAN Cyberthreat assessment 2021: Key cyberthreat trends outlook from the ASEAN Cybercrime Operations Desk. Retrieved March 20, 2022 from https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-charts-top-cyberthreats-in-Southeast-Asia.
25	AT Kearney. (2018)
26	Association of Southeast Asian Nations. (2018). ASEAN leader's statement on cyber cooperation. Retrieved March 20, 2022 from https://asean.org/wp-content/uploads/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf
27	Association of Southeast Asian Nations. (2022). ASEAN cyber security cooperation strategy 2021–2025 [Draft]. Retrieved March 20, 2022 from https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf
28	Benincasa, E. (2020). The role of regional organisations in building cyber resilience: ASEAN and the EU. Issues and Insights: Working Paper. Vol. 20. Retrieved March 20, 2022 from https://pacforum.org/wp-content/uploads/2020/06/issuesinsights_Vol20WP3-1.pdf
29	AT Kearney. (2018)
30	International Telecommunications Union. (2008). Overview of Cybersecurity. Retrieved March 12, 2023 from https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items.
31	National Institute for Standards and Technology. (2020). Glossary: Cyber Resiliency. Retrieved February 2, 2022 from https://csrc.nist.gov/glossary/term/cyber_resiliency.
32	Christine, D. and Thinyane, M. (2020). Cyber resilience in Asia-Pacific: A review of national cybersecurity strategies. United Nations University. Retrieved March 22, 2022 from https://collections.unu.edu/eserv/UNU:7760/n2020_Cyber_Resilience_in_Asia-Pacific.pdf

33	Christine, D. and Thinyane, M. (2020).
34	An upcoming study by the Tech for Good Institute is a compendium of global cybersecurity databases to guide policymakers and researchers in their work towards securing the region's digital economy.
35	National Institute for Standards and Technology. (2018). Cybersecurity Framework. Retrieved February 4, 2022 from https://www.nist.gov/cyberframework.
36	Bodeau, D., Graubart, R., Picciotto, J., and McQuaid, R. (2011). Cyber resiliency engineering framework. MITRE. Retrieved February 2, 2022 from http://www.mitre.org/work/tech_papers/2012/11_4436/%5Cnpapers2://publication/uuid/F03 D9287-780F-4B61-AC47-E77BEDC3F939.
37	Carayannis, E.G., Grigoroudis, E., Rehman, S.S., & Samarakoon, N. (2021). Ambidextrous cybersecurity: The seven pillars (7Ps) of cyber resilience. IEEE Trans. Eng. Manag. 2021, 68, 223–234. Retrieved February 4, 2022 from doi: 10.1109/TEM.2019.2909909.
38	Organisation for Economic Co-operation and Development. (2013). Retrieved January 17, 2022 from https://www.oecd.org/dac/conflict-fragility-resilience/docs/May%2010%202013%20FINAL% 20resilience%20PDF.pdf.
39	National Academy of Sciences (NAS) Committee on Science, Engineering, and Public Policy. (2012). Disaster resilience: A national imperative. The National Academies Press. See also: Linkov & Trump. (2019). The science and practice of resilience. Springer Link.
40	International Standards Organisation. (2013). ISO/IEC 27001 – Information technology – Security techniques – Information security management systems – Requirements. Retrieved February 2, 2022 from https://www.iso.org/standard/54534.html.
41	Economic Development Board. (2021). Fortifying Singapore's Cybersecurity Capabilities. Retrieved January 17, 2022 from https://www.edb.gov.sg/en/business-insights/insights/- fortifying-singapore-s-cybersecurity-capabilities.html.
42	Somwaiya, K. (2019). Thailand's cyber security act and personal data protection act passed. LawPlus Ltd. Retrieved April 17, 2022, from https://www.lawplusltd.com/2019/03/thailands-cyber-security-act-personal-data-protecti on-act-passed
43	IBM Security. (2019). Cost of Data Breach 2019. Retrieved February 8, 2022 from https://www.ibm.com/downloads/cas/RDEQK07R#:~:text=The%20global%20average%20cost %20of,by%201.5%20percent%20from%202018.
44	Tham, I. (2018). Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber-attack. Strait Times. Retrieved February 10, 2022 from https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-includin g-pm-lee-stolen-in-singapores-most.
45	Barbaschow, A. (2018). Median 'dwell' time for cyber intrusion highest in APAC at 172 days: FireEye. ZDNet. Retrieved April 17, 2022, from https://www.zdnet.com/article/median-dwell-time-for-cyber-intrusion-highest-in-apac-at- 172-days-fireeye/
46	International Information System Security Certification Consortium. (2022). (ISC)2 Member Counts. Retrieved March 15, 2022 from https://www.isc2.org/About/Member-Counts#.

47	Cyber Security Agency. (2021). ASEAN Singapore Cybersecurity Centre of Excellence. Retrieved February 2, 2022 from https://www.csa.gov.sg/News-Events/Press-Releases/2021/asean-singapore-cybersecurity-centre-of-excellence.
48	AT Kearney. (2018).
49	AT Kearney. (2018).
50	World Economic Forum. (n.d.). Cybersecurity Learning Hub. Retrieved January 17, 2022 from https://www.weforum.org/projects/cybersecurity-learning-hub
51	Kaspersky. (2018). Concern for the online security of our older relatives is not converting into care, warns Kaspersky Lab. Retrieved March 20, 2022 from https://www.kaspersky.com/about/press-releases/2018_online-security-of-older-relatives.
52	Fong, J. (2017). Protecting the elderly from cyber-attacks. TODAY. Retrieved April 17, 2022 from https://www.todayonline.com/singapore/protecting-elderly-cyber-attacks
53	Lee, V. (2018). Police drive to educate seniors amid spike in loan scams. The Straits Times. Retrieved April 17, 2022, from https://www.straitstimes.com/singapore/police-drive-to-educate-seniors-amid-spike-in-loan-scams

TECH FOR GOOD INSTITUTE