ATKearney

Cybersecurity in ASEAN: An Urgent Call to Action

As the region is poised to take its position amongst the world's top digital economies, the doors are wide open for cyberattacks. A radical agenda can help policy makers and industry leaders defend and capture a wealth of value.

Contents

Executive Summary

The ASEAN region is a prime target for cyberattacks

The digital economy in the Association of Southeast Asian Nations (ASEAN)[1] has the potential to add $1 trillion to GDP over the next 10 years. However, cyber risks could impede trust and resilience in the digital economy and prevent the region from realizing its full digital potential. ASEAN countries have already been used as launchpads for attacks, either as vulnerable hotbeds of unsecured infrastructure or as well-connected hubs to initiate attacks.

The region's growing strategic relevance makes it a prime target for cyberattacks. Cyber resilience is generally low, and countries have varying levels of cyber readiness. Specifically, there is a lack of a strategic mindset, policy preparedness, and institutional oversight relating to cybersecurity. The absence of a unifying framework makes regional efforts largely voluntary, leads to an underestimation of value-at-risk, and results in significant underinvestment. In addition, because cyber risk is perceived to be an information technology (IT) rather than a business problem, regional businesses do not have a comprehensive approach to cybersecurity. The region's nascent cybersecurity industry faces shortages of home-grown capabilities and expertise along with fragmented products and solutions and few comprehensive solution providers. Multiple vendor relationships and product deployments are creating operational complexity and, in some cases, increasing vulnerability.

The situation will escalate over time

The increase in trade, capital flows, and cyber linkages across ASEAN countries imply that the cyber threat landscape will generate even greater complexity in the future, further escalating the region's cybersecurity challenges:

- Growing interconnectedness will intensify the systemic risk, making the region only as strong as its weakest link.
- Diverging national priorities and varying paces of digital evolution will foster a pattern of sustained underinvestment.
- Limited sharing of threat intelligence, often because of mistrust and a lack of transparency, will lead to even more porous cyber defense mechanisms.
- Rapid technological evolution makes threat monitoring and response more difficult, especially with the rise of encryption, multi-cloud operations, the proliferation of the Internet of Things (IoT), and the convergence of operation technology (OT) and IT.

Because of these factors, the top 1,000 ASEAN companies could lose $750 billion[2] in market capitalization, and cybersecurity concerns could derail the region's digital innovation agenda—a central pillar for its success in the digital economy.

[1] The ASEAN region includes Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand, and Vietnam.

[2] Based on erosion in market capitalization for corporations that have been victims of mega data breaches

An urgent call to action

The response to these challenges must be comprehensive, engaging an array of stakeholders to deal with the scale of the threat and to ensure that ASEAN's leap into the digital economy is unobstructed. An active defense mindset is required to work together to defend and leverage collective ASEAN resources.

The ideal regional cybersecurity defense playbook needs to address a four-point agenda (see figure 1):

- Elevate cybersecurity on the regional policy agenda.
- Secure a sustained commitment to cybersecurity.
- Fortify the ecosystem.
- Build the next wave of cybersecurity capability.

Figure 1
Regional cybersecurity defense playbook

Elevate cybersecurity on the regional policy agenda	• Concerted coordination to steer the implementation of a Rapid Action Cybersecurity (RAC) Framework • Elevate cybersecurity to the top of the agenda in economic dialogue (for example, establish a regional coordination platform and multilateral agreement to have "cybersafe" trading partners)
Secure a sustained commitment to cybersecurity	• Pursue a commitment to address the regional cybersecurity spending gap • Define and track cybersecurity metrics through a cyber-hygiene dashboard
Fortify the ecosystem	• Foster a risk-centric mindset in the corporate sector • Instill a culture around sharing threat intelligence • Extend cyber resilience across the supply chain (i.e. to business partners) • Implement regional public–private partnerships and encourage industry alliances
Build the next wave of cybersecurity capability	• Develop the next generation of security professionals • Strengthen the local cybersecurity industry through deeper cooperation and collaboration with global players • Drive R&D around emerging threat vectors, including artificial intelligence and blockchain • Anchor world-class capabilities

Source: A.T. Kearney analysis

Elevating cybersecurity on the regional policy agenda calls for the immediate implementation at national levels of a Rapid Action Cybersecurity Framework to harmonize cyber resilience across the region. The Rapid Action Cybersecurity Framework is a comprehensive 12-point action agenda for national governments to address gaps in strategy, policy, legislation, and governance related to cybersecurity. In addition, adopting an ASEAN-initiated multilateral regime around cybercrime can bring strategic and operational benefits to the region, particularly in rapid law enforcement cooperation. National governments should take the lead in implementing the framework with support, guidance, and oversight from the ASEAN Ministerial Conference on Cybersecurity (AMCC). The ASEAN secretary-general's annual report should be expanded to include a scorecard that tracks each country's progress in achieving milestones set by the Rapid Action Cybersecurity Framework. To **secure a sustained commitment to cybersecurity** and address the investment gap, ASEAN countries need to spend[3] between 0.35 and 0.61 percent of their GDP—or $171 billion collectively—on cybersecurity in the period spanning 2017 to 2025. This is a small price to pay considering the value-at-risk and the fact that ASEAN governments spend up to 3.4 percent of GDP[4] on other items, including defense.

Concerted efforts need to be made to **fortify the ecosystem** by advocating for businesses to adopt a risk-centric, layered defense approach to cyber threats. This includes instilling a culture that enables the sharing of threat intelligence, extending cyber resilience across the supply chain, and encouraging the development of regional public–private partnerships (PPPs) and industry alliances. Finally, because cybersecurity is a continuously evolving challenge, the region must **build the next wave of cybersecurity capability** by cultivating the future generation of security professionals and driving research and development around innovative technologies that can address emerging and unforeseen threats. Given the magnitude and complexity of the region's challenges and its unique context, ASEAN must embrace a game-changing approach, based on greater cohesion and a collective use of resources, to achieve a cyber resilient future.

1 The ASEAN Region: A Prime Target for Cyberattacks

With a combined GDP of more than $2.7 trillion, the ASEAN region is the world's seventh largest market and is swiftly becoming an economic force to reckon with. Nominal GDP is expected to grow at a CAGR of 8.2 percent, exceeding $4 trillion by 2022. With a population of 645 million people—over 100 million more than the European Union (EU)—ASEAN is the third most populous market in the world.

The region is strategically positioned to capture trade with other growth powerhouses, both geographically and diplomatically. Trade with China alone is expected to reach $1 trillion by 2020, partly because of partnerships such as the ASEAN–China Free Trade Area. The region's global significance can also be seen in its relationship with the United States. US foreign direct investments into ASEAN have grown at a CAGR of 12 percent since 2004. In fact, the region has received more investments from the United States than from China, India, Japan, and South Korea combined.[5]

Although ASEAN is behind its global peers in terms of contribution of the Internet economy, the region has the potential to enter the world's top five digital economies by 2025. Over the next 10 years, ASEAN's digital economy could add $1 trillion to its GDP.[6] This digital revolution could transform daily life, making physical cash obsolete and regional cities smarter, safer places to live (see figure 2 on page 4). The region could also pioneer the development of new digital services, especially advanced mobile financial services and e-commerce—sectors that are likely to see the emergence of local digital champions. Failing to address the risks will impede trust and resilience in the digital economy and prevent the region from realizing its full economic potential.

The region's growing strategic relevance and expanding digitalization make it a prime target for cyberattacks. Although countries are beginning to extend their policies to encompass the digital playing field, cybersecurity is a very real danger for several reasons:

[3] Includes both public- and private-sector cybersecurity spend

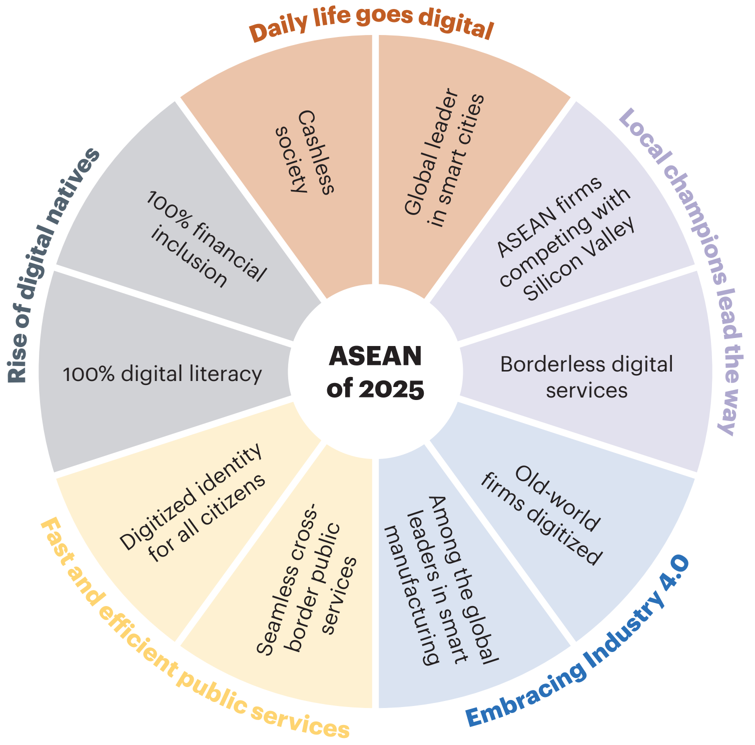
[4] World Bank

[5] *ASEAN Matters for America*, The East–West Center, 2017

[6] For more information, see The A.T. Kearney ASEAN Digital Revolution at www.atkearney.com

Figure 2

A digital revolution will transform ASEAN by 2025


Daily life goes digital
Cashless society
Global leader in smart cities
Local champions lead the way
ASEAN firms competing with Silicon Valley
Borderless digital services
Embracing Industry 4.0
Old-world firms digitized
Among the global leaders in smart manufacturing
Fast and efficient public services
Seamless cross-border public services
Digitized identity for all citizens
Rise of digital natives
100% digital literacy
100% financial inclusion
ASEAN of 2025

Sources: *The ASEAN Digital Revolution*; A.T. Kearney analysis

1. ASEAN countries have emerged as launchpads for cyberattacks.
2. Policy preparedness is still nascent, with a lack of institutional oversight and low levels of spending to fortify digital economies.
3. A nascent local cybersecurity industry faces shortages of home-grown capabilities and expertise.
4. Perception that cyber risk is an IT risk results in the absence of a holistic approach to cyber resilience.
5. Multiple vendor relationships and product deployments result in operational complexity, slowing times to detect and respond to attacks.

> "Some countries are being more offensive as opposed to defensive, leading to state-sponsored attacks. Even hacktivism has evolved in complexity."
>
> **—chief executive officer, CyberSecurity Malaysia**

> "Cyber espionage is an important emerging threat vector."
>
> **—deputy chief executive, Cyber Security Agency of Singapore**

1.1 ASEAN countries have emerged as launchpads for cyberattacks

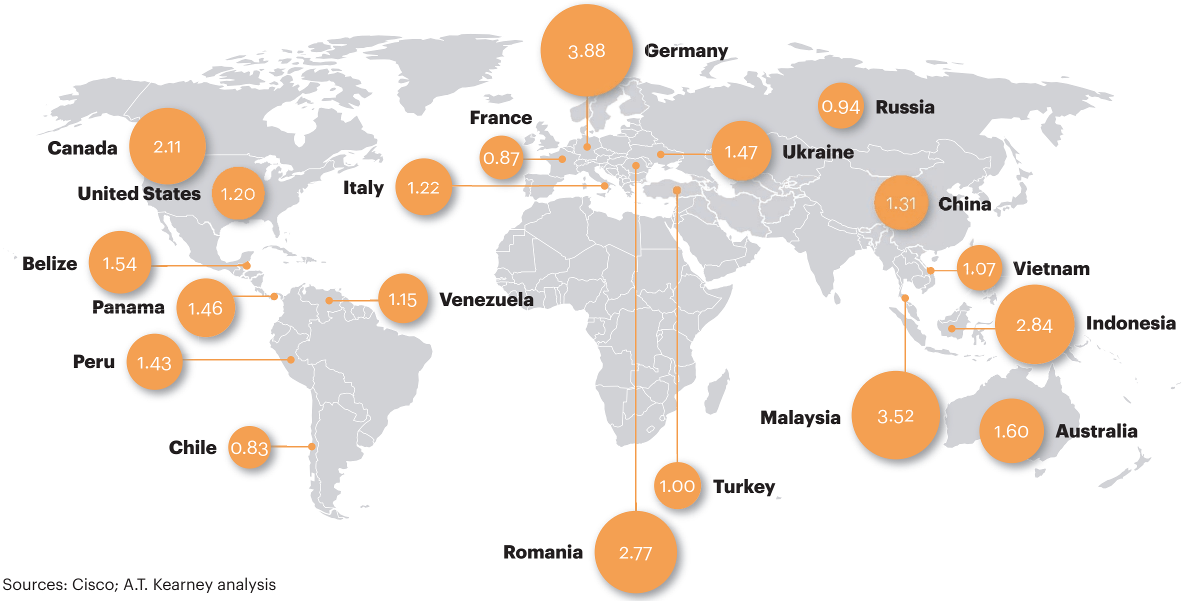
ASEAN countries are being used as launchpads for cyberattacks—either as vulnerable hotbeds of unsecured infrastructure where numerous computers can be infected easily for large-scale attacks or as hubs for a single point of attack to gain access to the hubs' global connections.

Malaysia, Indonesia, and Vietnam are global hotspots for major blocked suspicious Web activities—up to 3.5 times the standard ratio, indicating that these countries are being used to launch malware attacks (see figure 3). Spam botnets are also finding ASEAN countries to be attractive hosts for their attacks. For example, Vietnam registered 1.68 million IP blocks from December 2015 to November 2016, and the country is number five in the world's top countries from which attacks against IoT devices originated in 2016.[7, 8]

> "In our country, there are still many weaknesses in information security, including lack of awareness and action plans at leadership levels, lack of policies to promote human resource development and nurture talent in information security, and a lack of cohesiveness amongst information security stakeholders in general."
> **—ASEAN national CERT**

Figure 3

Blocked suspicious Web activity, by country of origin (expected ratio = 1.0)



Sources: Cisco; A.T. Kearney analysis

[7] IP blocks are spam messages that are blocked immediately by spam-detecting technology because the sender has a bad reputation score. Examples include messages that originate from known spam-sending botnets or compromised networks.

[8] *Internet Security Threat Report Volume 22*, Symantec, April 2017

State-sponsored cyberattacks, such as those from North Korea, are another threat. This combination of criminal and state-sponsored threats increases ASEAN's risk profile, creating obstacles for foreign investment and hampering the growth of the digital economy.

1.2 Policy preparedness is still nascent with a lack of institutional oversight and limited funding to fortify digital economies

The region's cyber resilience is low, particularly around policy, governance, and cybersecurity capabilities. The absence of a unifying regional governance framework makes it difficult to collaborate and share intelligence within and across countries. Businesses have also underestimated the value-at-risk, resulting in a lack of adequate spending on cybersecurity.

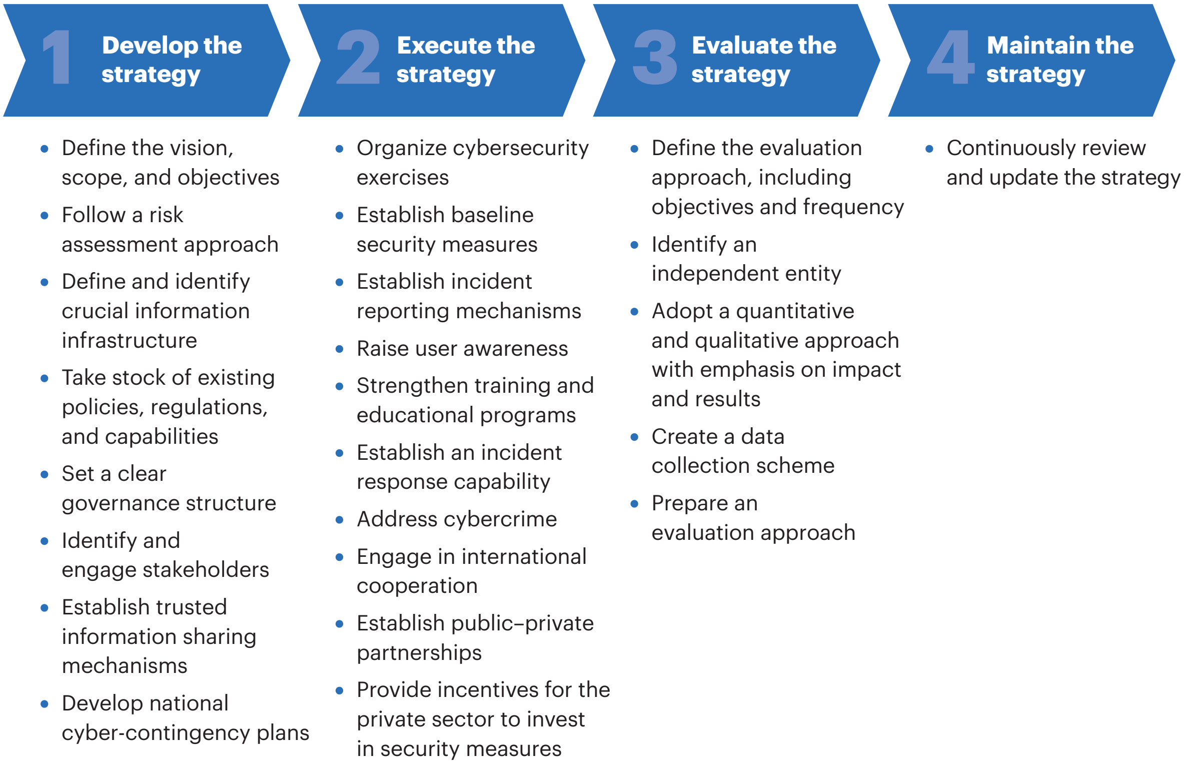
1.2.1 Varying levels of cyber readiness, with some countries lacking a strategic mindset about cybersecurity policy and governance

The Good Practice Guide from the European Network Information Security Agency (ENISA) cites four steps in defining and implementing a sound national cybersecurity strategy (see figure 4).

A look at the regional cybersecurity policy landscape reveals varying levels of cyber readiness, particularly around strategy definition and implementation, legislation, and governance (see figure 5 on page 7).[9] See the appendix for more about the current situation.

Figure 4

Four-phased approach to national cybersecurity strategy development



1 Develop the strategy

- Define the vision, scope, and objectives
- Follow a risk assessment approach
- Define and identify crucial information infrastructure
- Take stock of existing policies, regulations, and capabilities
- Set a clear governance structure
- Identify and engage stakeholders
- Establish trusted information sharing mechanisms
- Develop national cyber-contingency plans

2 Execute the strategy

- Organize cybersecurity exercises
- Establish baseline security measures
- Establish incident reporting mechanisms
- Raise user awareness
- Strengthen training and educational programs
- Establish an incident response capability
- Address cybercrime
- Engage in international cooperation
- Establish public–private partnerships
- Provide incentives for the private sector to invest in security measures

3 Evaluate the strategy

- Define the evaluation approach, including objectives and frequency
- Identify an independent entity
- Adopt a quantitative and qualitative approach with emphasis on impact and results
- Create a data collection scheme
- Prepare an evaluation approach

4 Maintain the strategy

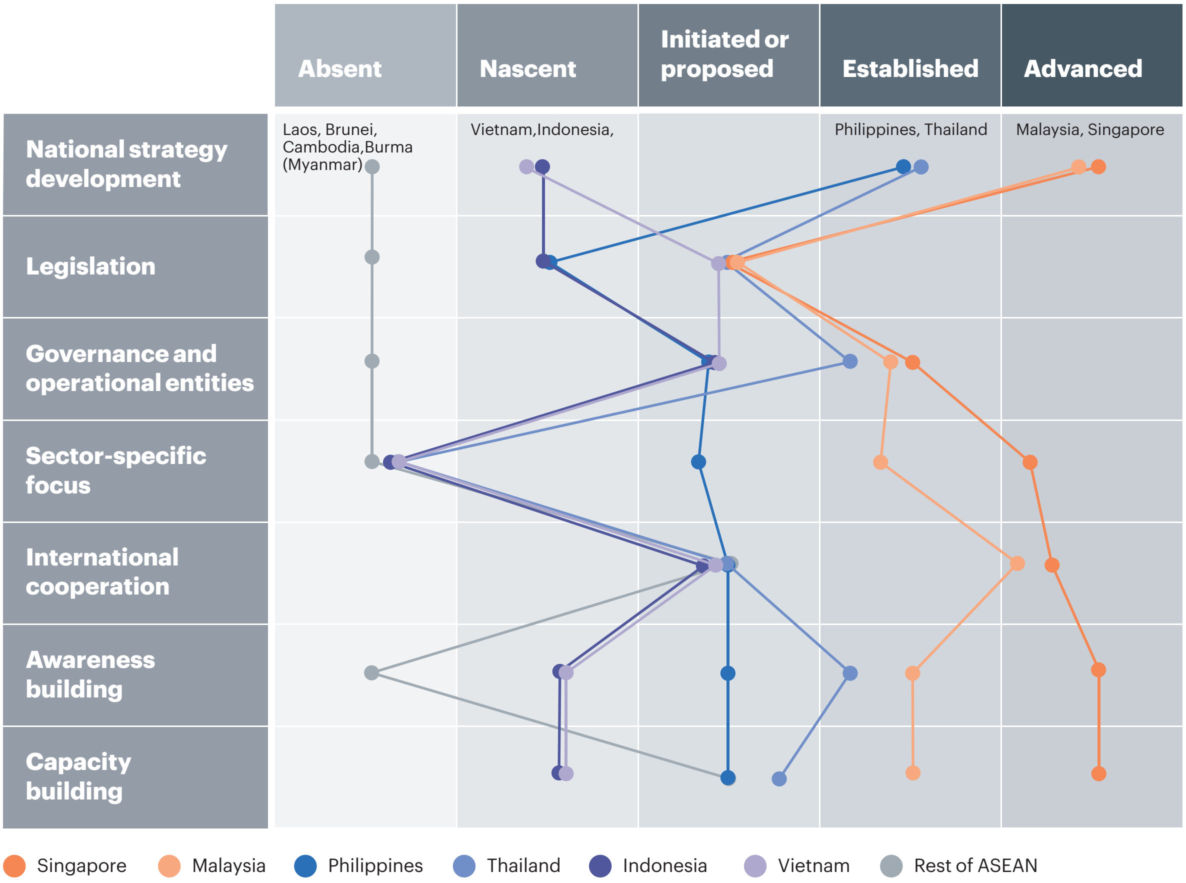
- Continuously review and update the strategy

Sources: European Union Agency for Network and Information Security; A.T. Kearney analysis

[9] Based on available information in the public domain

Figure 5

Cybersecurity policies vary widely across the ASEAN region



Sources: government websites, press clippings; A.T. Kearney analysis

Cybersecurity governance and policies are undeveloped in the region. National cybersecurity strategies have been laid out by Singapore, Malaysia, Thailand, and the Philippines. A few countries have set up national agencies to consolidate and coordinate cybersecurity agendas. These include Singapore (Cyber Security Agency of Singapore), Malaysia (CyberSecurity Malaysia), and the Philippines (Department of Information and Communications Technology). Indonesia has established a national cyber and encryption agency, Badan Siber dan Sandi Negara (the Cyber Body and National Encryption Agency), and Thailand has proposed a national cybersecurity committee. Although other countries do not have dedicated agencies, their national computer emergency response teams (CERTs) or computer security incident response teams (CSIRTs) currently play the role of national cybersecurity agencies.

The lack of sector-specific governance and policies is a region-wide issue, resulting in limited transparency and a lack of sharing of threat intelligence. One exception is the Monetary Authority of Singapore and the global Financial Services Information Sharing and Analysis Center, which have announced plans to set up the Asia Pacific Regional Intelligence and Analysis Center. This platform aims to provide deeper capabilities in cyber intelligence gathering and analysis for enhanced in-region support, specifically for financial services.

Although Singapore, Malaysia, Thailand, and Vietnam drafted cybersecurity bills in 2017, limited progress has been made across the rest of ASEAN. Cybercrime laws have also been passed in

Singapore, Malaysia, Thailand, the Philippines, and Brunei. Five of the ASEAN-6 countries have enacted data protection or privacy laws, with Vietnam being the exception.[10] Vietnam does not have a unified law regarding privacy; instead, it is informed by different laws and decrees.

Apart from Singapore and Malaysia, few ASEAN countries have made progress in all areas. However, national agencies that are working on their cybersecurity strategies and policies have rich experiences to draw upon both from their regional counterparts and from other parts of the world.

1.2.2 Absence of a unifying framework at the ASEAN level

The challenge is exacerbated by the absence of an overarching governance or legal framework that member states adhere to or a regional regulatory body to enforce policies. Unified strategy development, readiness assessments, and incident reporting are missing, limiting the collective preparedness of the region and its ability to capitalize on shared knowledge. Effective prevention and combatting cybercrime requires international cooperation because of its non-physical, cross-border nature. Without a structured ASEAN cooperative framework to address cybercrime, the region remains vulnerable.

ASEAN faces challenges in pulling together a unifying framework, largely because of the inherent absence of a power to legislate or veto budgets and appointments. The ASEAN Inter-Parliamentary Assembly has only the power of moral suasion. In contrast, the European Union, with a strong legislative framework and a powerful secretariat has placed cyber resilience very high on its agenda and has developed a cohesive regional cybersecurity strategy (see sidebar: The EU Approach to Cybersecurity on page 9). The General Data Protection Regulation (GDPR), which becomes enforceable in 2018 across the EU, requires a personal data breach[11] to be reported to the competent national supervisory authority and, in certain cases, to be communicated to the individuals whose personal data has been affected by the breach. The GDPR also provides for stringent penalties for enterprises that fail to comply.

In the past year, cybersecurity was a highlight on the ASEAN agenda, beginning with a focus on capacity building. Singapore is taking a leading role in coordinating cybersecurity cooperation by organizing the annual ASEAN Ministerial Conference on Cybersecurity, the second of which was held in September 2017 in conjunction with Singapore's International Cyber Week. Singapore has also codeveloped the ASEAN Cyber Capacity Program, an initiative to build capabilities across the region through tailored training programs, public–private partnerships, and discussions on policy and legislation.

1.2.3 Businesses underestimate value-at-risk, leading to underinvestment in cybersecurity

Adopting a value-at-risk mindset is crucial for effective threat mitigation because it drives senior-level decision-making and ensures more efficient resource allocation and mobilization. Assessing value-at-risk involves identifying high-value assets that may be at risk from a cyberattack and assessing the potential impact of a breach. Current assessments are based on historical average data, which do not account for complex, powerful attacks such as those seen recently with Target, Yahoo!, and Equifax.[12]

[10] ASEAN-6 refers to the region's top six economies: Singapore, Malaysia, Indonesia, Thailand, the Philippines, and Vietnam.

[11] Defined under Article 4(12) of the GDPR as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed

[12] The financial cost of cyberattacks considers the following parameters: the number of top companies segmented by sector and country (2,700) and the value-at-risk (grown by GDP contribution growth by sector and by country), the cost per cyberattack segmented by sector, the likelihood of a specific company being attacked, and the frequency of cyberattacks. Data sources include Ponemon Institute's *Cost of Cybercrime* and *Cost of Data Breach* studies, the World Bank, the Economist Intelligence Unit, and security analyst reports.

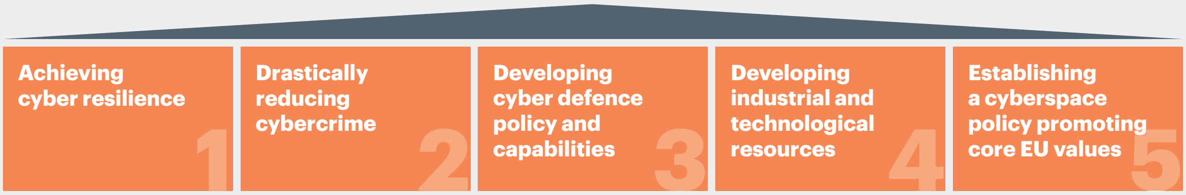
The EU Approach to Cybersecurity

The European Union (EU) developed a region-wide cybersecurity strategy in 2013 to "enhance the EU's overall performance" and to "safeguard an online environment providing the highest possible freedom and security for the benefit of everyone." This was augmented by the Cybersecurity Package announced in 2017. The figure below highlights the pillars of EU's cybersecurity strategy (see figure).

Facing similar complexities as ASEAN, such as fragmented regulation, the EU also saw the need for a unifying framework, giving rise to the Directive on Security of Network and Information Systems (NIS Directive) as part of its overall cybersecurity strategy, which entered into force in August 2016. Member states were given 21 months to adopt the directive into their national legislation. Some crucial elements of the directive include:

- A requirement for member states to be appropriately equipped, such as having a national CSIRT and a national NIS body. The CSIRTs would form a collaborative CSIRT network that would cooperate on incidents and share risk-related information.
- A cooperation group involving all member states, allowing for strategic cooperation and information sharing
- Security measures across critical information infrastructure sectors and key digital service providers, such as the mandatory reporting of serious incidents by organizations to the national authorities

Figure
Cybersecurity Strategy of the European Union


Achieving cyber resilience
1
Drastically reducing cybercrime
2
Developing cyber defence policy and capabilities
3
Developing industrial and technological resources
4
Establishing a cyberspace policy promoting core EU values
5

Sources: *Joint Communication to the European Parliament and The Council*, The European Economic and Social Committee, the Committee of the Regions, Cybersecurity Strategy of the European Union; A.T. Kearney analysis

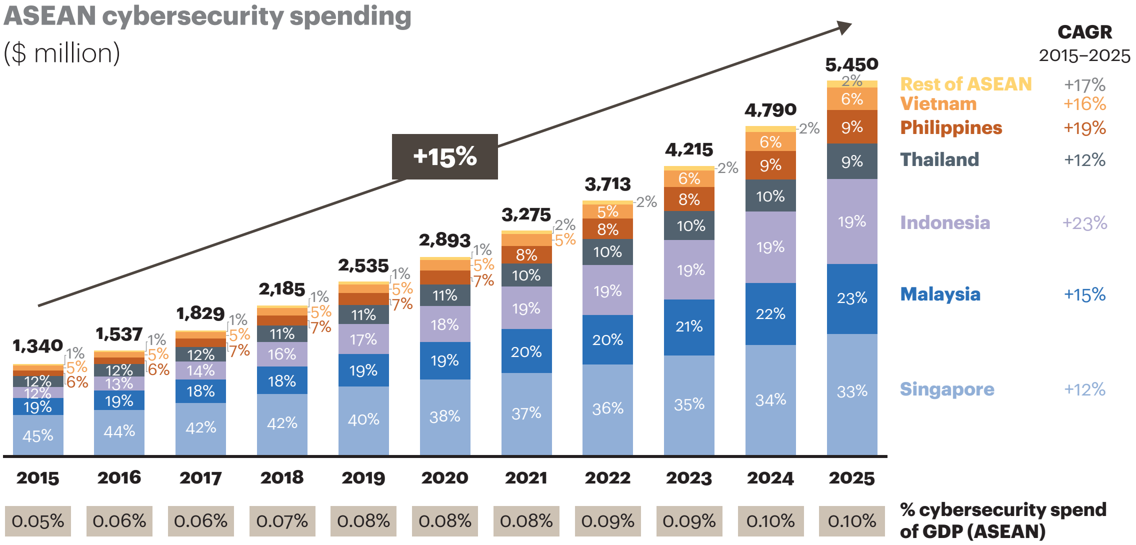
Quantifying the value-at-risk from cybercrime is challenging, and organizations around the world lack competencies in this area. One of the biggest challenges is understanding the nature of the threat to high-value assets and appropriately prioritizing and focusing mitigating resources. No organization can afford to use every defense mechanism in its arsenal, nor is it practical. However, resources must be allocated according to the magnitude of the threat and the value-at-risk.

Based on a sector-wide perspective, most ASEAN countries are at risk of cyberattacks because of the significant contribution of information and communications technology (ICT) in the sectors that are most at risk. The IBM X-Force Threat Intelligence Index has cited the following as the most cyberattacked sectors in recent years: healthcare, manufacturing, financial services, government, transportation, and retail.[13] Across the ASEAN-6, these sectors account for the majority of GDP contribution (on average of 70 percent). In the case of Singapore, the share of these sectors is even higher at 94 percent of GDP.

[13] "Monitored security is superior security," *IBM X-Force Threat Intelligence Index 2017*

ASEAN's cybersecurity spend was estimated to be $1.9 billion in 2017, representing 0.06 percent of the region's GDP. ASEAN's spending on cybersecurity is forecasted to grow at 15 percent CAGR from 2015 to 2025 (see figure 6). The top three economies—Singapore, Malaysia, and Indonesia—are likely to drive a significant portion of this growth, accounting for 75 percent of the market by 2025. Indonesia, the Philippines, Vietnam, and Malaysia are expected to see the highest growth as they address gaps in infrastructure and as the managed service landscape evolves.

Figure 6
ASEAN cybersecurity spending is expected to show double-digit growth up to 2025



Notes: Cybersecurity spend includes both private and public sector spend on the following: identity and access management, infrastructure protection (including content and endpoint), and network security.

Sources: International Data Corporation, Gartner; A.T. Kearney analysis

However, when benchmarking national cybersecurity spending as a percentage of GDP, most ASEAN countries fall below the global average and well below best-in-class, creating a potential risk of insufficient spend relative to a rapidly escalating threat landscape (see figure 7 on page 11).[14]

1.3 A nascent local cybersecurity industry with shortages of home-grown capabilities and expertise

The cybersecurity industry in the ASEAN region faces structural challenges because of its highly fragmented nature. In addition, the shortage of skilled talent impacts the competitiveness of the local industry.

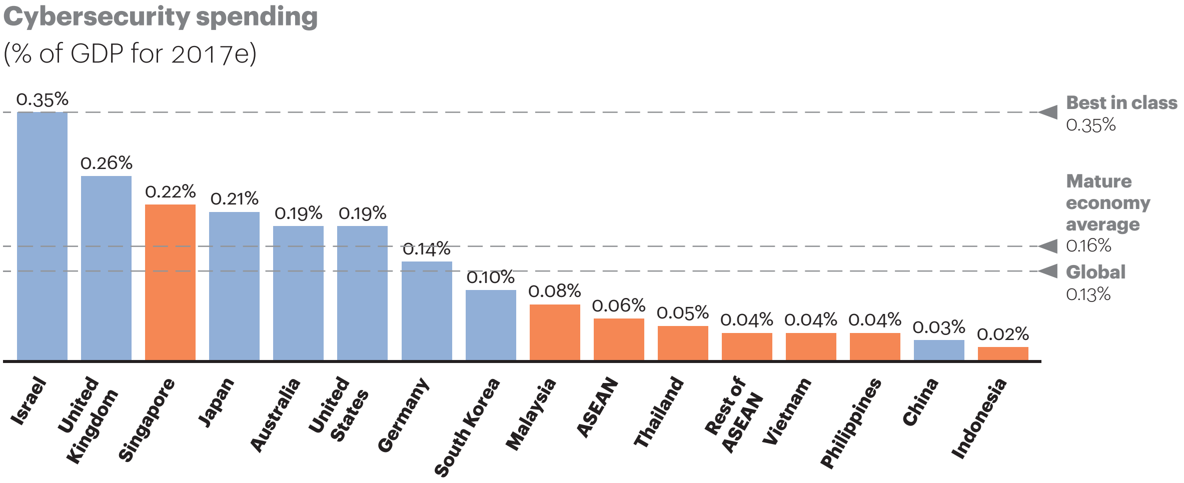
1.3.1 Fragmentation of products offerings with lack of end-to-end solution providers

The cybersecurity industry globally and in the region, is characterized by numerous products and solutions (see figure 8 on page 11). Vendor product portfolios are varied, and few offer solutions that cover the entire capability value chain. End users face the challenge of navigating through a complex web of vendor relationships to design their cybersecurity programs. Despite

[14] Based on cybersecurity as a percentage of spend for select global markets

Figure 7

Benchmarking cybersecurity spend as percent of GDP

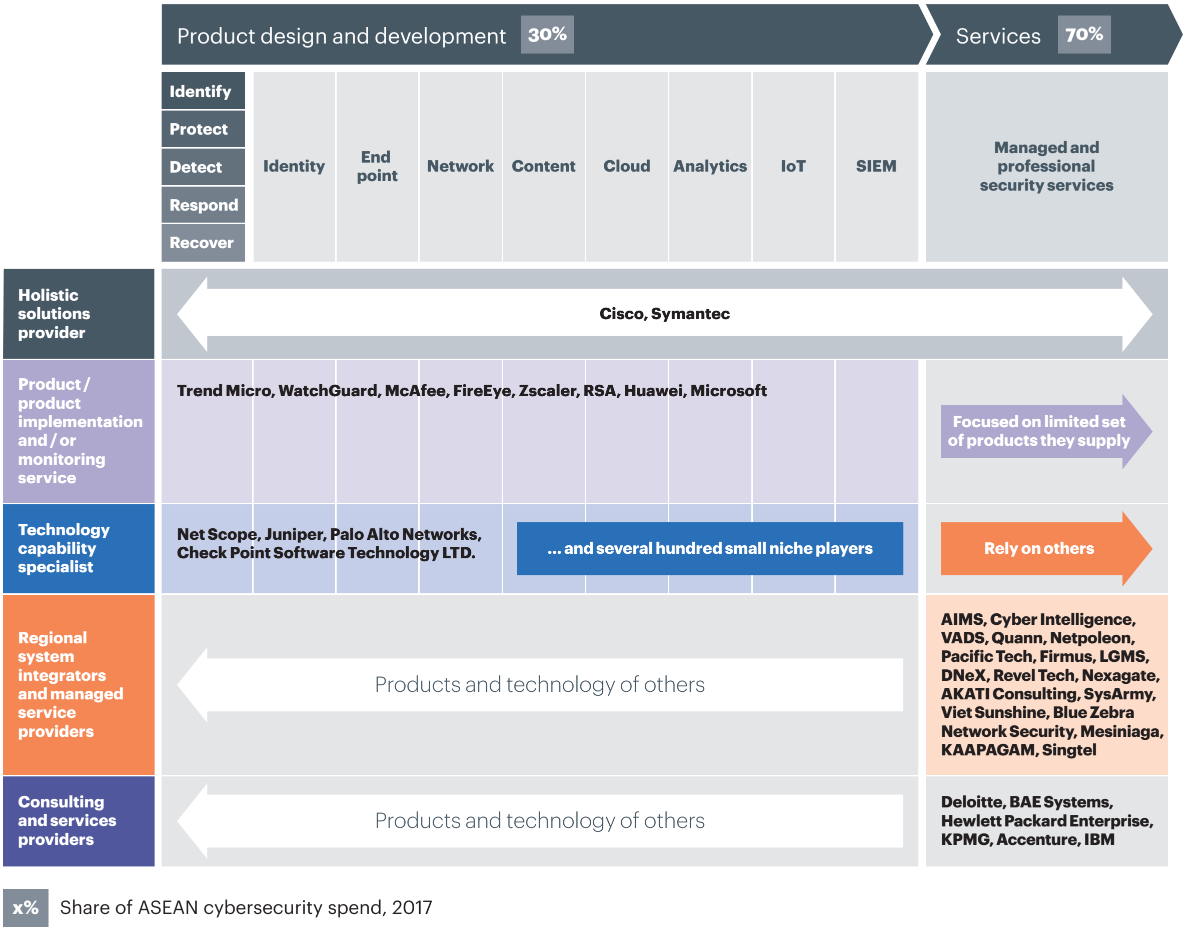


Note: Israel's cybersecurity spend benchmark is based on 2015 spend per capita.

Sources: Gartner; A.T. Kearney analysis

Figure 8

Vendors' product and service positioning across the value chain (non-exhaustive)



Product design and development 30%

Services 70%

Identify

Protect

Detect

Respond

Recover

Identity

End point

Network

Content

Cloud

Analytics

IoT

SIEM

Managed and professional security services

Holistic solutions provider

Cisco, Symantec

Product / product implementation and / or monitoring service

Trend Micro, WatchGuard, McAfee, FireEye, Zscaler, RSA, Huawei, Microsoft

Focused on limited set of products they supply

Technology capability specialist

Net Scope, Juniper, Palo Alto Networks, Check Point Software Technology LTD.

... and several hundred small niche players

Rely on others

Regional system integrators and managed service providers

Products and technology of others

AIMS, Cyber Intelligence, VADS, Quann, Netpoleon, Pacific Tech, Firmus, LGMS, DNeX, Revel Tech, Nexagate, AKATI Consulting, SysArmy, Viet Sunshine, Blue Zebra Network Security, Mesiniaga, KAAPAGAM, Singtel

Consulting and services providers

Products and technology of others

Deloitte, BAE Systems, Hewlett Packard Enterprise, KPMG, Accenture, IBM

x% Share of ASEAN cybersecurity spend, 2017

Note: SIEM is security information and event management.

Sources: interviews, industry experts; A.T. Kearney analysis access to a multitude of product vendors and service providers, security solutions are often not tailored to specific industry needs.

Although the service landscape is also highly fragmented, vendors tend to be more localized. Very few service providers have a regional presence, and most operate only in their country of origin. As one of the fastest-growing segments in the ICT landscape, cybersecurity could be a significant economic opportunity for ASEAN countries. Encouraging innovation in cybersecurity through partnerships with global vendors and greater mobility of talent could generate significant gains for the region (see sidebar: CyberSecurity Malaysia as a Vendor Certification Authority). Other countries such as the United Kingdom and Israel are leveraging cybersecurity as a source of competitive advantage.

1.3.2 Paucity of skilled talent magnifies the challenge

Even with a comprehensive cybersecurity strategy and budget, security leaders are likely to face a shortage of skilled and qualified cybersecurity professionals to implement their cybersecurity agenda. Challenges exist in both capacity and capabilities. The shortage of skilled cybersecurity talent represents a global challenge, with the US Information Systems Audit and Controls Association (ISACA) citing a global shortage of more than 2 million professionals by 2019 (see figure 9 on page 13). In ASEAN, Malaysia, for instance, currently has 6,000 cybersecurity professionals but requires 10,000 by 2020.[15]

From a capability perspective, certain specific skill sets such as systems architecture design, behavioral analytics, and digital forensics are acutely in short supply, and there is a large and growing demand for industry-specific cybersecurity talent. Executives we interviewed cite subtle nuances related to a compliance mindset needed in the financial services industry as opposed to the recognition of real risk of physical damage to life and assets applicable in the manufacturing or oil and gas industry. There is also inadequate expertise in cybersecurity support sectors, such as cyber insurance, where both effective frameworks and sufficient knowledge are needed to accurately assess the value-at-risk.

To address this, some ASEAN countries are undertaking capacity building initiatives with a strategic view. Malaysia and Singapore have comprehensive strategies to develop cybersecurity professionals. The Philippines has also outlined its approach in the recently released National Cybersecurity Plan 2022, while Thailand is working with Japan's government to develop

CyberSecurity Malaysia as a Vendor Certification Authority

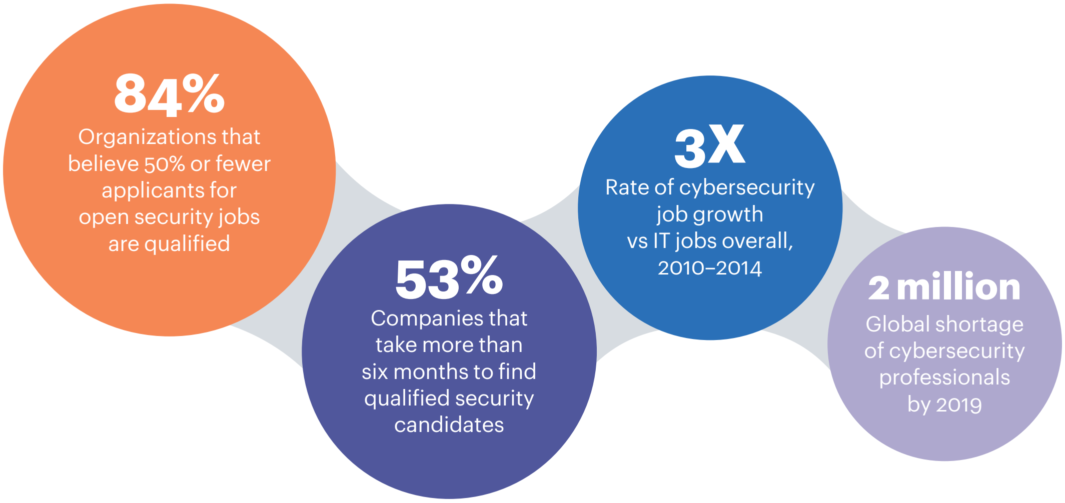
As the national cybersecurity agency of Malaysia, CyberSecurity Malaysia consolidates potential vendors and solutions, then offers recommendations to public and private bodies based on the National Institute of Standards and Technology (NIST) framework and end-user needs, ensuring a well-balanced cybersecurity approach (see section 1.4).

Even more recently, CyberSecurity Malaysia has developed a stringent certification process for local vendors, including a comprehensive evaluation methodology. This is complemented with various training initiatives to improve capabilities and ensure compliance with global standards as part of ongoing efforts to recommend world-class, comprehensive solutions whilst supporting the development of the local cybersecurity ecosystem.

[15] Malaysia Digital Economy Corporation, October 2017

Figure 9

State of global cybersecurity talent



Source: A.T. Kearney analysis

cybersecurity training programs for ASEAN. Efforts are currently under way across other markets, largely driven by the private sector and with a focus on addressing short-term skills gaps.

Earlier this year, Singapore announced plans to set up a new cyber defense vocation that will create a force of approximately 2,600 cyber defenders, consisting of mostly civilians but also leveraging National Service personnel. The vocation will fall under the Singapore Armed Forces, adding military support to the capacity-building efforts.

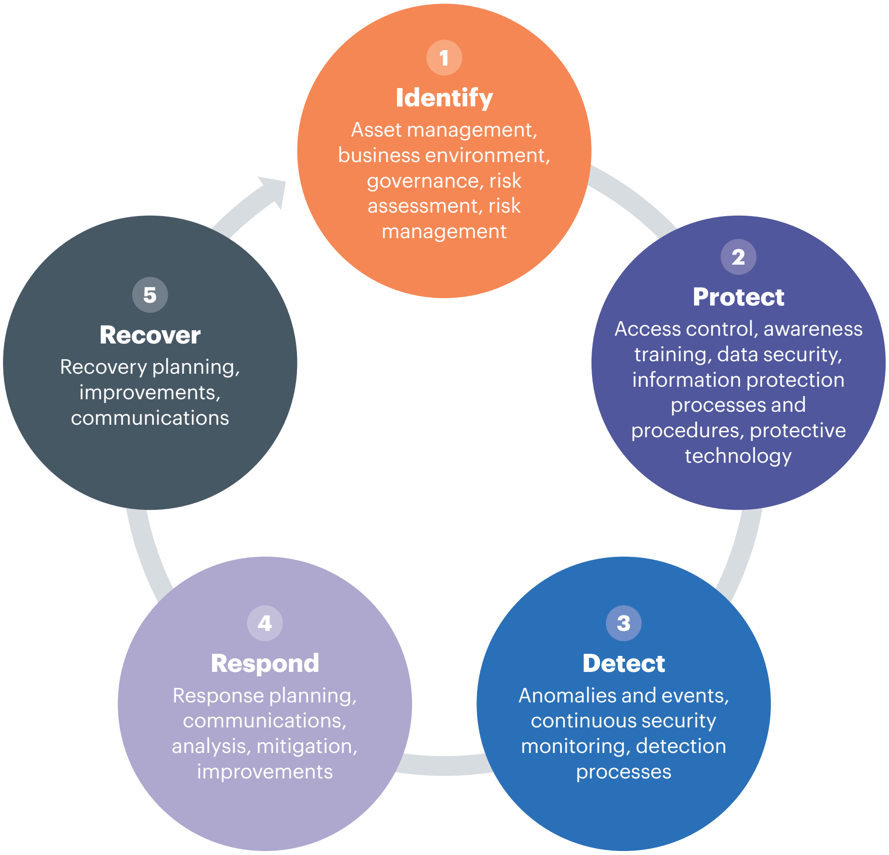
Building capacity is a long-term effort. With the majority of ASEAN member states lacking a structured and long-term approach to developing competent cybersecurity professionals, the emerging member states must rapidly adopt best practices from countries that have implemented capacity-building frameworks.

Companies across the region are also looking at other avenues to address the challenge. Select corporations in the telecom, manufacturing, and oil and gas industries have been considering strategic moves into the cybersecurity domain, either organically or through acquisitions. These companies have been actively scouting for innovative cybersecurity companies to strengthen their in-house capabilities. Because of the experience built over the years, cybersecurity is seen as part of a wider growth agenda, potentially driving new revenue streams while securing critical infrastructure. Efficiency can be gained by placing inexperienced personnel in event and incident management and leaving experienced, highly trained cyber personnel focused on the system use case engineering, tuning, and review.

1.4 Perception that cyber risk is an IT risk results in the absence of a holistic approach to cyber resilience

Corporate stakeholders often have a myopic view of cyber risk, seeing it as an IT issue and not a business risk. As a result, technology investment is perceived as the key to mitigating cyber risk. Systems architecture, people, processes, and organizational culture are the greatest assets organizations can employ to shrink the attack surface. Many organizations either underestimate

Figure 10
NIST Framework for Improving Critical Infrastructure Cybersecurity


1
Identify
Asset management, business environment, governance, risk assessment, risk management
2
Protect
Access control, awareness training, data security, information protection processes and procedures, protective technology
3
Detect
Anomalies and events, continuous security monitoring, detection processes
4
Respond
Response planning, communications, analysis, mitigation, improvements
5
Recover
Recovery planning, improvements, communications

Note: NIST is National Institute of Standards and Technology.
Sources: National Institute of Standards and Technology; A.T. Kearney analysis

or overestimate their cybersecurity requirements in the absence of a strong vision for cyber risk management. A structured approach optimizes finite resources to deliver exceptional protection appropriate to the risk they represent if the assets are strategically prioritized and apportioned. Otherwise, as is often the case, there is little thought given to how systems are designed or deployed, and the entire organization must undergo costly remediation to protect select assets.

The National Institute of Standards and Technology (NIST) framework[16] recommends five functional capabilities for achieving comprehensive, cybersecurity defense: identify, protect, detect, respond, and recover. While businesses in the region are largely focused on the identify, protect, and detect functions of the cybersecurity life cycle, we are seeing the need for greater awareness and investment around recover and respond (see figure 10).

> "There is a lot of movement in the recovery and respond parts of the life cycle but still a lot of emphasis on protect."
> **—global director of cybersecurity solutions, global energy management and automation company**

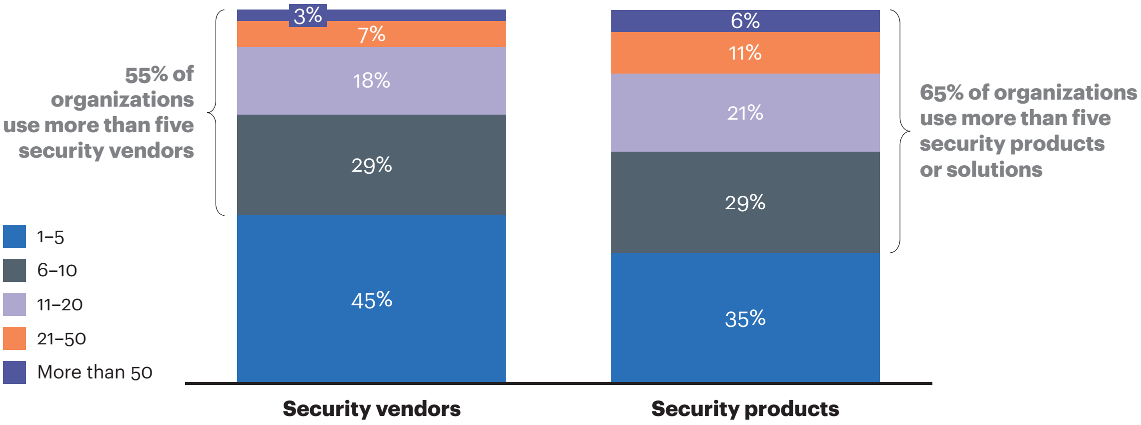
[16] The NIST Framework for Improving Critical Infrastructure Cybersecurity is a set of industry standards and best practices to help organizations manage cybersecurity risks.

In addition, our interviews reveal that most small and medium-size enterprises[17] (SMEs) generally do not see cybersecurity as a top priority. Although these firms are not usually the main target, many cyber criminals leverage supply chain linkages or shared data to infiltrate partnerships smaller companies have established with larger organizations. Verizon's 2017 Data Breach Investigations Report shows that large companies are attacked more frequently than small companies, but small companies have a significantly higher breach-to-incident ratio: 1:1.4 for small companies compared to 1:80 for large companies. Because SMEs account for between 88 to 99 percent of the region's establishments and between 52 to 97 percent of all jobs,[18] their susceptibility to breaches is a major cause for concern.

1.5 Multiple vendor relationships and product deployments result in operational complexity

Given the breadth of the security product landscape and the level of fragmentation of vendor solutions, best of breed has emerged as a preferred vendor selection model. Cisco's Annual Cybersecurity Report 2017 has highlighted the complexity of the cybersecurity landscape in terms of end-user reliance on multiple vendors and products. More than a quarter of companies in the sample use more than 10 vendors, and 36 percent deploy more than 10 cybersecurity solutions (see figure 11).

Figure 11
Number of security vendors and products used by organizations



Sources: Cisco 2017 Annual Cybersecurity Report; A.T. Kearney analysis

A complicated vendor landscape with security products that do not work well together can lengthen the time to identify and contain a breach, thereby increasing vulnerability.

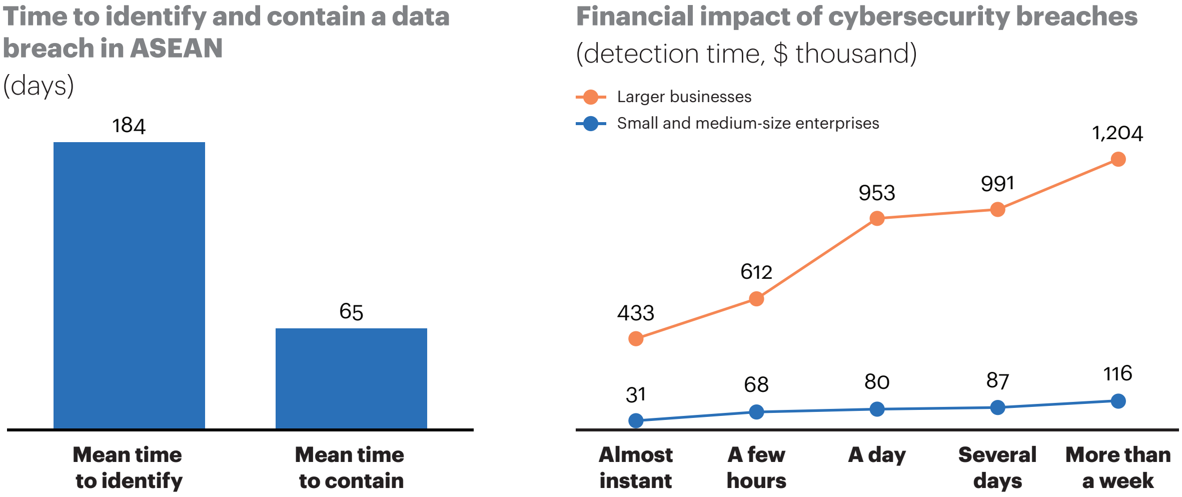
In the ASEAN region, data published by the Ponemon Institute suggests that it takes on average 184 days to identify a data breach and close to 65 days to contain it (see figure 12 on page 16). Cyber dwell time, defined as the number of days a threat actor remains undetected within a given environment until remediation, is reported to be 65 percent higher in the Asia Pacific

[17] Using the Malaysian definition: establishments with fewer than 200 employees in manufacturing or 75 employees in services and other areas

[18] ASEAN Economic Community, Small and Medium Enterprises Overview

Figure 12

Costs escalate the longer a cyberattack remains uncontained



Time to identify and contain a data breach in ASEAN
(days)

Financial impact of cybersecurity breaches
(detection time, $ thousand)

Sources: Ponemon Institute, European Political Strategy Centre; A.T. Kearney analysis

region as compared to the Americas.[19] These metrics can have a significant impact on the financial outcome of a breach as detailed in figure 12. Executives recognize this as an opportunity to trim their security product portfolio to drive ease of management, enhance interoperability, and improve operational effectiveness.

> "You cannot be married to a single vendor. We are vendor agnostic. We test many different platforms, most of which are in the top percentile, then we decide. We recommend that the vendor base should not exceed five."
>
> **—global energy management and automation company**

When mapping their cybersecurity portfolios, organizations can benefit from a cyber defense matrix (see figure 13 on page 17).

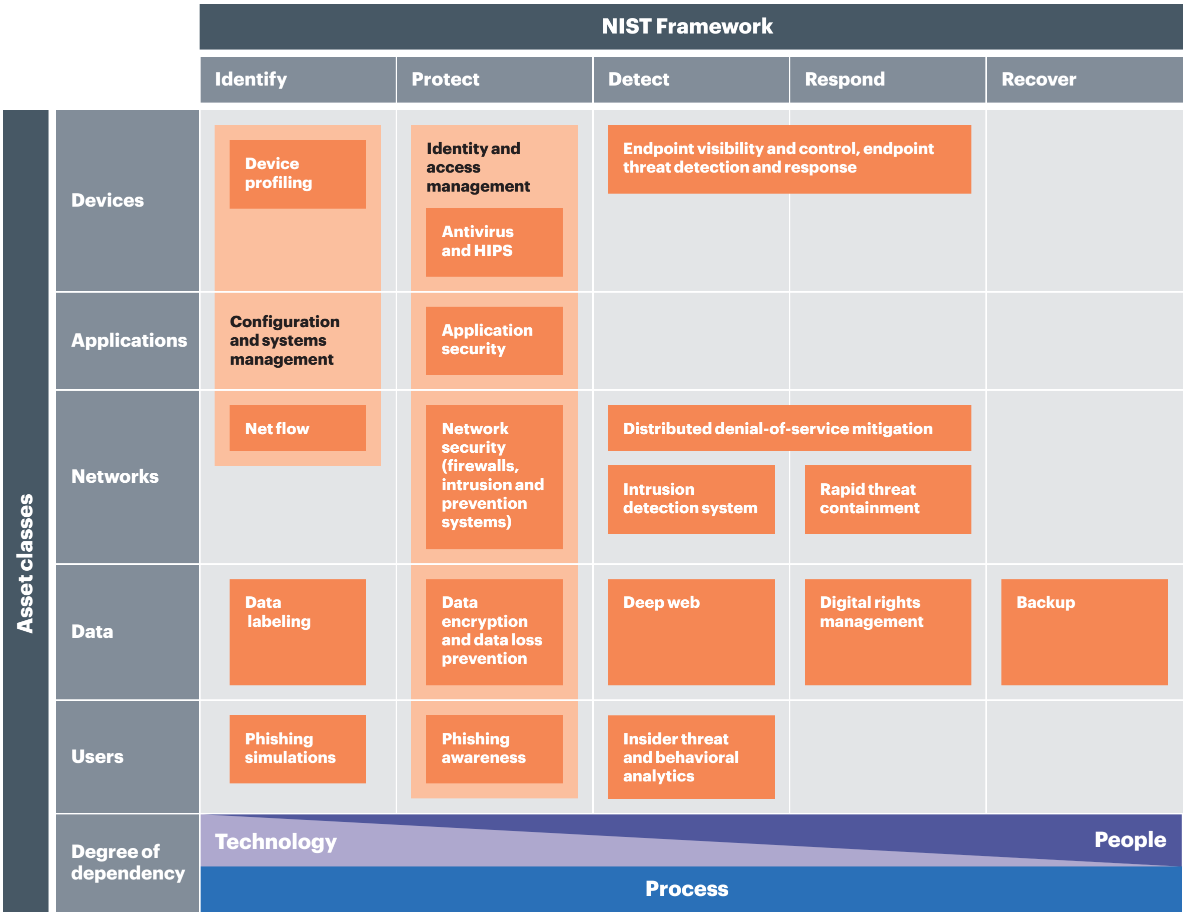
Mapping asset classes against the NIST framework will help identify gaps in the portfolio and could help trim the security and vendor portfolio by identifying duplication and focusing attention on fewer, more comprehensive providers.

Enterprises can benefit from a platform that is simple, open, and automated—enabling better integration between products from the same vendor and the ability to share data with other third-party technologies. Security product integration frameworks (SPIF) facilitate the sharing of security-related metadata, help standalone security products and services to interoperate effectively, and ultimately improve the efficacy of enterprises' unique security architectures. SPIFs enable pre-integration of standalone third-party security products, eventually enabling enterprises to construct a customized, more effective enterprise security solution architecture.

[19] *M-Trends 2017: Trends from the Year's Breaches and Cyber Attacks*, M-Trends Reports

Figure 13

A cyber-defense matrix can help optimize the cybersecurity portfolio



	NIST Framework				
Asset classes	Identify	Protect	Detect	Respond	Recover
Devices	Device profiling	Identity and access management Antivirus and HIPS	Endpoint visibility and control, endpoint threat detection and response		
Applications	Configuration and systems management	Application security			
Networks	Net flow	Network security (firewalls, intrusion and prevention systems)	Distributed denial-of-service mitigation Intrusion detection system	Rapid threat containment	
Data	Data labeling	Data encryption and data loss prevention	Deep web	Digital rights management	Backup
Users	Phishing simulations	Phishing awareness	Insider threat and behavioral analytics		

Note: HIPS is host-based intrusion prevention system. NIST is National Institute of Standards and Technology.
Sources: RSA, National Institute of Standards and Technology; A.T. Kearney analysis

2 The Cybersecurity Challenge is Escalating

In section 1, we highlighted that ASEAN countries are a prime target for cyberattacks, and a low level of preparedness makes the region particularly vulnerable. There is a need for urgency in addressing the problem as the threat landscape will escalate.

In the rapidly evolving cyber landscape, four issues must be addressed:

- The growing interconnectedness across the region and geographical dispersion of the physical supply chain will intensify systemic risk, making the region only as strong as its weakest link.
- Diverging national priorities and varying paces of digital evolution will continue to foster a sustained pattern of underinvestment.
- Limited sharing of threat intelligence, often because of mistrust and a lack of transparency, will lead to even more porous cyber defense mechanisms.

- Technological evolution will render threat monitoring and response more complex, particularly given the rise of encryption, multi-cloud operations, proliferation of IoT, and convergence of OT and IT environments.

These four issues will aggravate the current, unprepared situation in the region. If the region fails to address these issues, the value-at-risk for ASEAN is significant: The region's top listed companies could be exposed to a $750 billion erosion in current market capitalization. In addition, cybersecurity concerns have the potential to derail the region's digital innovation agenda, one of the core pillars for its success in the digital economy.

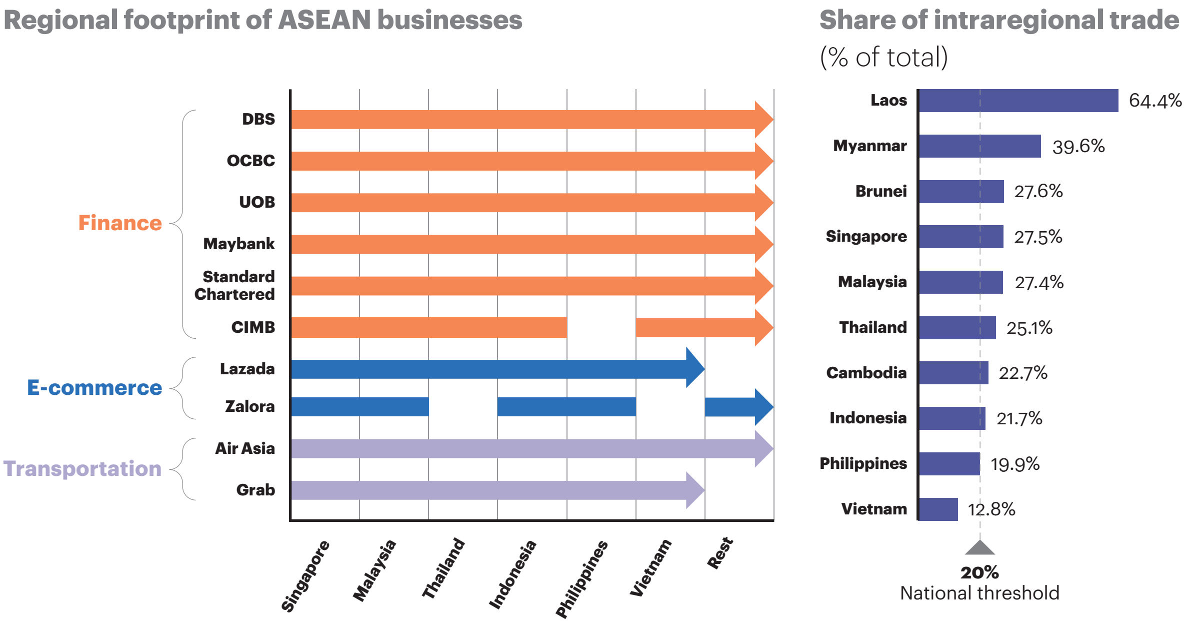
2.1 The cybersecurity challenge is likely to get more complex

2.1.1 Systemic risk will make the region only as strong as its weakest cyber link

With growing intraregional trade and business linkages across ASEAN countries, the risk of contagion in the event of cyberattacks across the region is high. Figure 14 highlights the extensive footprint that banks, e-commerce companies, and transportation companies have across the region. For eight out of the 10 ASEAN countries, intra-regional trade accounts from more than 20 percent of total trade. Intra-ASEAN investment has also been steadily increasing over the years and in 2016 accounted for a quarter of the total foreign direct investment (FDI) flows of $96 billion into the region.[20] Sectors with the highest proportion of intra-regional investment include manufacturing, financial services, and real estate.

Factors that have contributed to the rise in intraregional investment are the growing financial strength and significant cash holdings of ASEAN firms and their drive to internationalize for greater competitiveness and to access markets, natural resources, and strategic assets.

Figure 14
Regional footprint of ASEAN businesses and member states' share of intraregional trade



Regional footprint of ASEAN businesses

Share of intraregional trade (% of total)

Source: A.T. Kearney analysis

[20] ASEAN Secretariat, ASEAN FDI database

With economic interconnectedness, the region faces more systemic risk, a concept traditionally applied to financial services. Systemic risk is defined as the risk that a cyber event cascades into related ecosystem components, creating adverse effects in public health, safety, the economy, or national security.[21] Recent cyber heists are game changing in their implications on regional systemic risk, demonstrating that threat actors need not attack a core system to exploit its weaknesses. Systemic risk took center stage with the hacking of banks in Bangladesh, Vietnam, and Ecuador—exposing the entire SWIFT network of more than 11,000 banks (see sidebar: Systemic Attack on SWIFT).

Further, as discussed, supply chain partners have the potential to be the weak links in any company's business operation. Even if companies can ensure the robustness of their own cybersecurity operations, there is often limited visibility into the business partner ecosystem, creating blind spots in data security. The challenges are twofold in the region: First, supply chain partners are at varying levels of IT and security readiness, requiring significant foundation-setting and training. Second, the adoption of security standards is as yet nascent, and companies with a regional footprint as well as market entrants face the risk of differing regulations by country, leading to inefficiencies in intraregional trade.

2.1.2 Diverging national priorities because of varying paces of digital evolution will foster a pattern of sustained underinvestment

Despite the region's interconnectedness, the networked readiness and pace of digital evolution across ASEAN countries has been and is likely to continue to be much different (see figure 15 on page 20).

As the region becomes increasingly digital, there will be a greater need to spend more on cybersecurity. There is a strong correlation between the share of the digital economy and spend

Systemic Attack on SWIFT

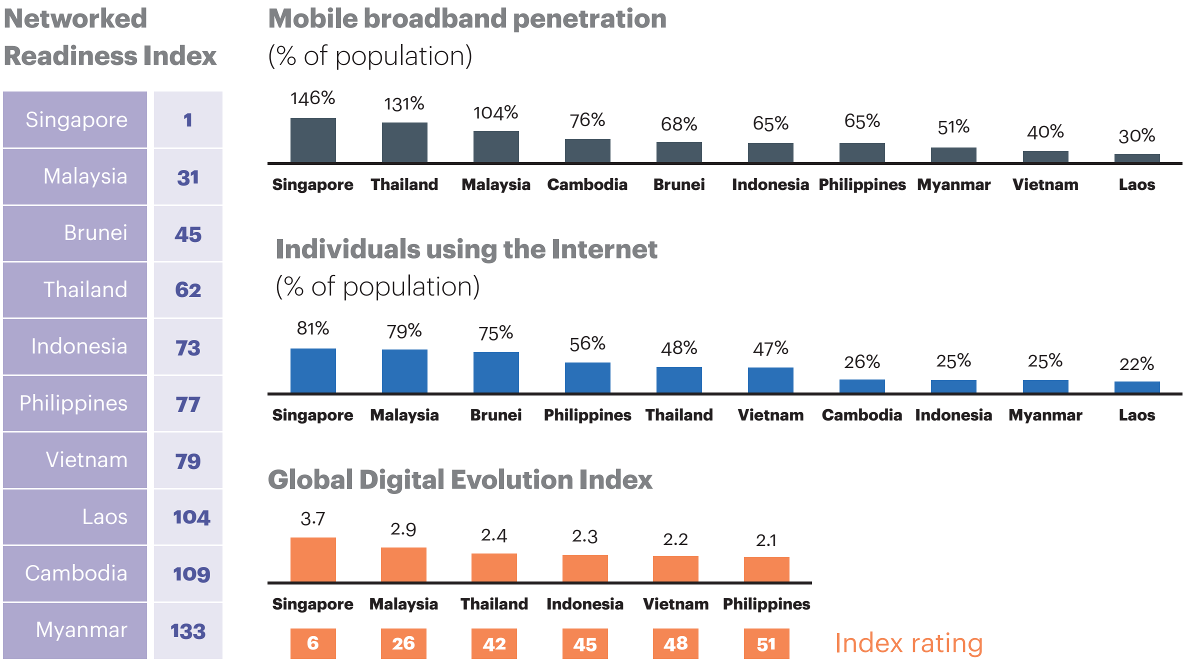
Systemic cyber risk recently came under scrutiny with the discovery of three separate hacking incidents against member institutions connected to the SWIFT network at banks in Bangladesh, Vietnam, and Ecuador, accounting for more than $90 million in stolen funds. The attacks demonstrated that the applications that enable the financial messaging traffic between member banks can be manipulated and misused when member institutions do not strictly adhere to the security standards. Previously, accessing the SWIFT network required being physically present at a dedicated terminal.

However, as banking requirements and technologies have changed, the ability for financial institutions to connect to this network has changed as well. Banks now leverage multiple applications, resident on various user endpoints, to interface with the SWIFT network. Each connected endpoint presents an avenue of attack for threat actors to fraudulently create and send financial messages. The Bangladesh Central Bank hack is a prime example of this situation; a threat actor infiltrated a poorly secured network and used an unsecured endpoint to carry out one of the largest bank heists in history. Approximately 11,000 institutions enjoy access to SWIFT, and the ability of the network to withstand a cyberattack is only as good as the weakest link in the network.

[21] *Understanding Systemic Cyber Risk*, World Economic Forum

Figure 15

The ASEAN region has a significant digital divide



Note: Brunei was not ranked in 2016; ranking based on 2014 report.
Sources: World Economic Forum, World Bank, GSMA; A.T. Kearney analysis

on cybersecurity (see figure 16 on page 21). The Digital Evolution Index (DEI) 2017[22] rankings for the ASEAN cohort suggest that some ASEAN countries are exhibiting significant digital momentum with strong headroom for growth. But the digital divide is likely to result in differing national investment priorities that can lead to friction when determining investment commitments for national and regional cybersecurity defense.

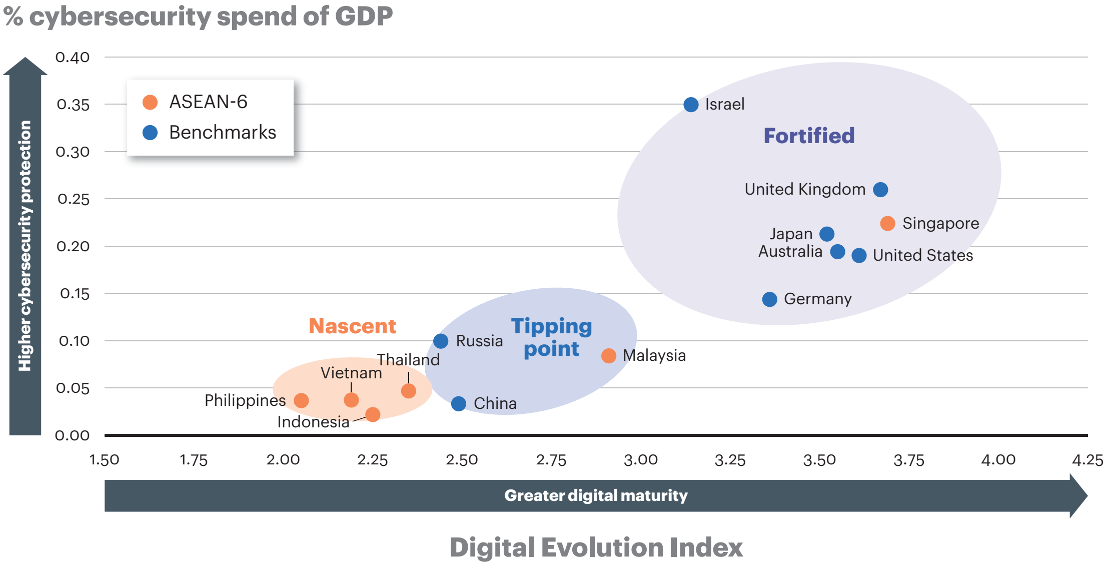
Benchmarking the region's cybersecurity spend as a percentage of GDP shows that most economies are on a strong digital growth trajectory, but without a commensurate increase in cybersecurity spend. The region currently spends an average 0.06 percent of its collective GDP on cybersecurity, while the world's top countries spend at least five times the relative proportion of their GDP.

The region's lower level of investment can be attributed to several factors. First, there is a lack of policy-level guidance and clarity on prudent practices in terms of cybersecurity spend. Second, as highlighted earlier, cybersecurity is considered to be an IT issue and not a business risk, thereby underestimating the value-at-risk. Third, a defense only approach focused on protection capabilities results in detection, recovery, and response being under developed. Finally, reporting mechanisms for breaches and their associated financial impact remain limited, making it difficult to calculate the risk.

As such, there is a need to establish a clear cybersecurity investment path for respective ASEAN countries based on the pace of digital evolution, risk levels, and the current level of

[22] The Digital Evolution Index is calculated from 108 digitalization indicators across four areas: supply conditions, demand conditions, the institutional environment, and innovation and change, including smartphone adoption; digital payment adoption; R&D spend; communication, financial, and logistics infrastructure; transparency and the rule of law; the business environment, and financing options.

Figure 16
Correlation between digital evolution and cybersecurity spend



Sources: World Bank, Tufts University *Digital Planet 2017*, analyst reports; A.T. Kearney analysis

preparedness. Providing transparent guidance that informs cybersecurity investment decisions can accelerate each country's transition from awareness to action.

2.1.3 Limited threat intelligence sharing because of a lack of trust and transparency will lead to even more porous cyber defense mechanisms

Most ASEAN governments and businesses are reluctant to share incident information or threat intelligence, which is crucial for forensic investigation and prevention. With the growing sophistication and faster pace of cyberattacks (for example, zero-day exploits and advanced persistent threats), sharing intelligence, and best practices along with a joint incident response can help mitigate the region's cyber risk (see sidebar: Cisco and Interpol Collaborate to Combat Cybercrime).

The lack of intelligence sharing is a global issue, stemming from limited mandates to share specific cyber incident information across intelligence agencies. Furthermore, ASEAN lacks a governing framework to introduce incident reviews on a regional level. Efforts are under way in

Cisco and Interpol Collaborate to Combat Cybercrime

Cisco and the International Criminal Police Organization (Interpol) announced an agreement to share threat intelligence as the first step in jointly fighting cybercrime. The alliance will see the two organizations develop a coordinated and focused approach to data sharing. This not only will allow for quick threat detection around the world, but also pave the way for potential collaboration on training and knowledge sharing.

Cisco's agreement with Interpol supports the organization's programs targeting both pure cybercrime and cyber-enabled crimes to assist member countries with identifying cyberattacks and their perpetrators.

the financial sector to collaborate among key partners, but this is not replicated in other critical information infrastructure sectors.

> "The tendency for corporates is to keep quiet. No one wants to be the next Target or Yahoo! Revealing too much could be damaging to a company's brand. It is very difficult, particularly in ASEAN, to expect companies to openly share without changes at the policy level."
>
> **—regional automation and industrial security provider**

2.1.4 Technological evolution is increasing complexity

The evolution of technology is adding complexity to the effective monitoring of and response to cyber incidents for an array of reasons:

- The convergence of IT and OT
- The proliferation of consumer IoT devices
- The accelerated adoption of multi-cloud computing
- The growing share of encrypted traffic
- The increasing uptake of virtual currency

The convergence of IT and OT

The global market for the industrial IoT is projected to grow at a CAGR of 21 percent from 2016 to 2021, reaching $123.8 billion by 2021. This will give rise to security concerns as the newly connected operational endpoints become new access points to insert malware into the wider network or the endpoints themselves become targets to incapacitate, destabilize, or even weaponize the network.

With industrial control system cybersecurity breaches on the rise, inadequate protection has become a critical issue. Historically, OT and IT have been two distinct functions. While IT is responsible for the systems that collect, transport, and process data for the business, OT generally comprises the systems that handle the monitoring and automation of industrial control systems through supervisory control and data acquisition systems attached to distributed control systems, programmable logic controllers, remote terminal units, and field devices. OT is focused on the automation of machines, processes, and systems within a plant, while IT focuses on the enterprise information systems required to support business operations. Business objectives are not the only difference between OT and IT functions. Employees in these respective functions also have distinct roles, reporting structures, and departmental cultures, while the technology platforms are frequently logically or physically separated. Most notably, risk evaluation and tolerances differ significantly.

Vast differences exist between OT and IT, but replacing legacy OT systems with IP-enabled devices has lessened the isolation these systems once relied on and has expanded the attack surface. Deployed IoT devices have very limited computational sophistication in terms of cyber risk mitigation capabilities beyond isolation techniques. This makes them vulnerable and creates the potential risk of many of these devices being weaponized and used across businesses, industries, and even countries.

Industry stakeholders have concerns about the lack of standards and guidelines, limited sharing of knowledge, and insufficient talent in relation to cybersecurity, particularly in OT.

> “There are no global standards on how to deal with the convergence of OT and IT, and everyone has a differing view on the approach.”
>
> **—regional manufacturing player**

> “Within the industry, we do not share information on the best way to deal with the convergence of IT and OT; these are considered trade secrets. We do not talk to other industries either, but everyone is facing the same problem.”
>
> **—regional manufacturing player**

The proliferation of consumer IoT devices

The regional consumer IoT market is expected to grow at 35 percent CAGR between 2015 and 2020, reaching $7.53 billion in 2020.[23] This growth is driven by factors such as rapid urbanization, the growth of the middle class, and technology and device proliferation.

In ASEAN, several member states have also launched programs to increase their use of IoT, particularly in urban environments. Malaysia’s MIMOS, the national ICT R&D center under the Ministry of Science, Technology, and Innovation, released its National IoT Strategic Roadmap in 2015. Singapore’s Smart Nation, launched in 2014, includes a range of ongoing initiatives that utilize a countrywide IoT platform to improve citizens’ quality of life and accelerate innovation. Bangkok, Jakarta, and Ho Chi Minh have also launched smart city programs.

> “In the last few years, the transportation sector has seen the proliferation of IoT and connected cars, which have the potential to be ubiquitously connected and form a far larger attack surface for DDoS—multiple times larger than what we have seen in the Mirai worm example.”
>
> **—land transport authority in an ASEAN country**

IoT endpoints tend to be unsophisticated devices, representing low-hanging fruit for attackers who will identify the weakest link in a connected network. The network, or the edge that connects the endpoints to the platforms, is also vulnerable. IoT attacks are already extremely

[23] *Analysis of the Asia Pacific Internet of Things Market*, Frost & Sullivan

prevalent in Asia. According to NTT Security's *2017 Global Threat Intelligence Report*, 60 percent of all IoT-based attacks in 2016 originated from Asia, most likely because of the historically vulnerable profile of products in Asian markets.

In this context, a secure access policy and software-defined segmentation is vital. The network can be a security sensor, giving visibility of network traffic from these proliferating devices and ensuring access is granted and usage enforced using software defined segmentation. To implement effective and efficient application segmentation, it is critical to understand how application components are communicating with each other, what infrastructure services they are dependent on, and how the component clusters are grouped together. Rich telemetry and unsupervised machine learning can be used to achieve this. This application insight and dependency form the basis of the segmentation policy, helping to contain a breach by ensuring that attacks do not move laterally.

The accelerated adoption of multi-cloud computing

Enterprise IT operations are also shifting to a new operating paradigm with multi-cloud computing, where each unique cloud environment introduces new vulnerabilities. Not only are there multiple access and authentication nodes to manage securely, cloud platforms themselves represent attractive, well-connected targets for malicious hackers. Since the end of 2016, more hackers have been targeting cloud systems, with attacks ranging in sophistication, as they work relentlessly to breach corporate cloud environments.[24] Security professionals also identify cloud infrastructure and mobile devices to be among the most challenging to defend against attacks.

Segregating and protecting memory spaces prevents applications in cloud environments from accidentally interfering with one another's data or malicious software from being able to see and modify it at will. Recent news releases have highlighted two related vulnerabilities—Meltdown and Spectre—that allow a malicious application running on a computer to peek into the memory of another application on the same computer and interfere with it. Meltdown makes the segregation and protection process unreliable, while Spectre essentially tricks applications into accidentally disclosing information that would normally be inaccessible, safe inside their protected memory area. These vulnerabilities are most devastating in public cloud environments where applications from different customers often end up running on the same physical computer. End-to-end encryption, a security technique where data is encrypted before it even gets to the cloud and is then decrypted by clients when it is received from the cloud, offers a solution to the challenge. As a result, it no longer matters whether data is accessed by attackers in the cloud—because even if it is, it is not useful. It is encrypted and cannot be decrypted by the attacker without the keys, which are not present in the cloud that was attacked.

The growing share of encrypted traffic

An additional complexity is the increasing opaqueness of the data flow itself as the use of encryption grows. A growing share of enterprise network traffic is now being encrypted, creating gaps in security effectiveness that companies cannot afford to ignore. Gartner predicts that by 2019, 80 percent of Internet traffic will be encrypted. Encryption technology has enabled much greater privacy and security for enterprises that use the Internet to communicate and transact business online. Mobile, cloud, and Web applications rely on well-implemented encryption mechanisms, using keys and certificates to ensure security and trust. However, businesses are not the only ones to benefit from encryption. Threat actors have leveraged these same benefits to

[24] *Cisco 2017 Annual Cybersecurity Report*

evade detection and to secure their malicious activities. The overall increases in encrypted traffic and attacks render threat recognition difficult and create gaps in traditional, layered-defense systems because intrusion prevention fails to occur.

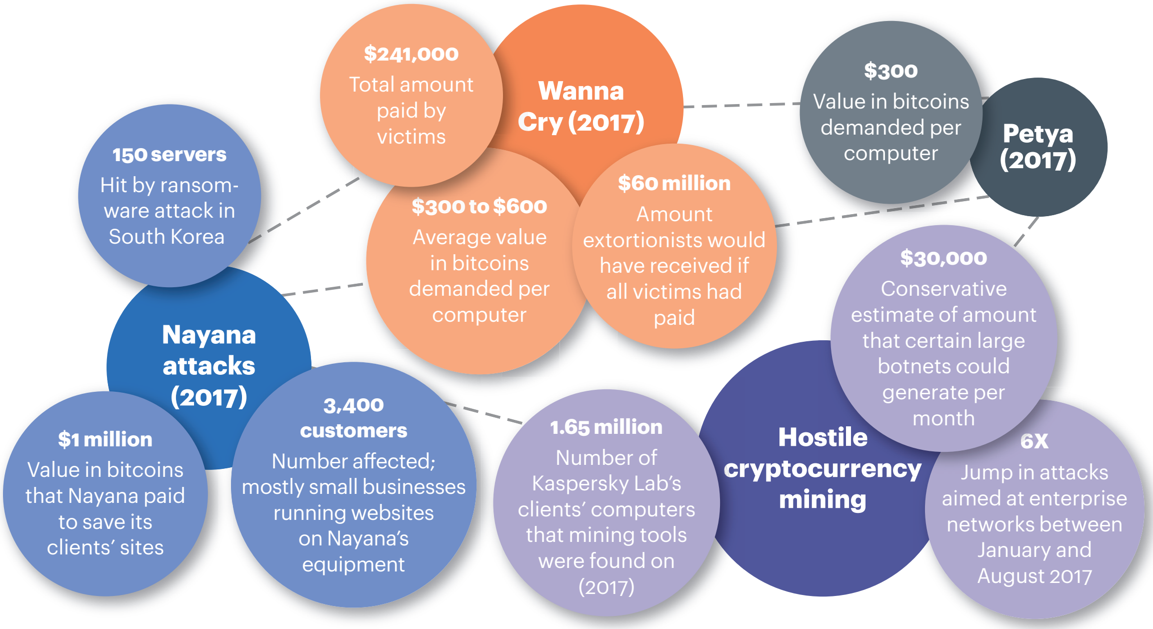
Encrypted traffic analytics provide insight into threats in encrypted traffic using network analytics.[25] The focus is on identifying malware communications in encrypted traffic through passive monitoring, the extraction of relevant data elements and supervised machine learning with cloud-based global visibility.

The increasing uptake of virtual currency

Since Bitcoin, the first decentralized cryptocurrency, was released in early 2009, similar digital currencies have crept into the worldwide market, including a spin-off called Bitcoin Cash. Abuse of virtual currencies is on the rise (see figure 17).

Figure 17

Virtual currency is increasingly a target for cyberattacks



Wanna Cry (2017)
$241,000 Total amount paid by victims
$300 to $600 Average value in bitcoins demanded per computer
$60 million Amount extortionists would have received if all victims had paid
$300 Value in bitcoins demanded per computer
Petya (2017)
150 servers Hit by ransom-ware attack in South Korea
Nayana attacks (2017)
$1 million Value in bitcoins that Nayana paid to save its clients' sites
3,400 customers Number affected; mostly small businesses running websites on Nayana's equipment
1.65 million Number of Kaspersky Lab's clients' computers that mining tools were found on (2017)
Hostile cryptocurrency mining
$30,000 Conservative estimate of amount that certain large botnets could generate per month
6X Jump in attacks aimed at enterprise networks between January and August 2017

Source: A.T. Kearney analysis

Security experts have seen a spike in attacks over the past year, aimed at stealing computer power for cryptocurrency mining operations.[26] Researchers have detected several large botnets set up to profit from cryptocurrency mining along with a growing number of attempts to install mining tools on organizations' servers.

Illegal mining operations set up by insiders, which can be much more difficult to detect, are on the rise. These are often carried out by employees with high-level network privileges and the technical skills needed to turn their company's computing infrastructure into a currency mint.

[25] *Encrypted Analytics Traffic*, Cisco

[26] "Hijacking Computers to Mine Cryptocurrency Is All the Rage," *MIT Technology Review*, 5 October 2017

In this context, policy alignment across the region is vital to reduce the opportunities for criminals to benefit from unregulated areas. In September 2017, the European Commission proposed a directive to expand the scope of cyber offenses such as fraud to include all monetary transactions, including those involving cryptocurrency, strengthening the ability of law enforcement authorities to tackle this form of crime. The law will also introduce common rules about penalties and clarify the scope of member states' jurisdiction in such offenses. In the ASEAN region, the recognition of the threat posed by virtual currencies is nascent with almost no policy alignment across member states.

2.2 The exposure for ASEAN's top companies is $750 billion and is likely to increase

Assessing the cost of data breaches is challenging because of the lack of transparent reporting. Analysts estimate the fiscal impact of such breaches based on surveys conducted globally and in the ASEAN region. The impact depends on how many records are lost in the breach and what percentage of the customer base has churned after the breach. The average total organizational cost of a data breach in ASEAN in 2016 was $2.36 million, according to Ponemon Institute's *2017 Cost of Data Breach Study*. The largest component of this cost was detection and escalation, which accounted for 41 percent of the total cost while lost business accounted for 30 percent. The average cost ranges from $1.8 million for less than 10,000 records to $3.4 million for more than 50,000 records. Extrapolating the data for the top 1,000 listed companies suggests a cumulative exposure for the region of $180 billion to $365 billion in the period from 2017 to 2025.

However, this estimated cost does not apply to catastrophic or mega data breaches because there is limited research or data available about their impact. Erosion in market capitalization has ranged from 10 to 35 percent for exceptional attacks such as Target, Yahoo!, and Equifax.[27] This represents the financial impact of such attacks on the companies themselves and does not consider the wider economic repercussions related to lost productivity or the indirect impact on other sectors. In these cases, the number of records breached ranged from 41 million to 3 billion. Applying the extreme market capitalization loss scenario to the market capitalization of ASEAN's top 1,000 listed corporations places the exposure at $750 billion in current market capitalization, significantly higher than estimates of the impact of "business as usual" breaches.

In addition to the financial impact, the opportunity cost of poor cyber resilience is that it can impact a company's growth and innovation agenda. In Cisco's *Cybersecurity as a Growth Advantage* report, 71 percent of executives say concerns over cybersecurity are impeding innovation in their organizations. Thirty-nine percent say they halted mission-critical initiatives because of cybersecurity issues. Among industries, the perceived threat to innovation was highest in technology products, business services, retail, and banking.

To stimulate innovation while managing the associated cybersecurity risks, some countries have developed safe environments through regulatory sandboxes. For example, the Monetary Authority of Singapore's initiative to sandbox emerging financial technology provides a safe space for experimenting, making it easier to protect, detect, respond, and recover within a small area (the sandbox). Vulnerabilities can then be identified and fixed before the technology is widely used across an industry or multiple industries where intrusions would be much harder to contain. This approach promotes innovation while minimizing potential risk. The Malaysian banking regulator, Bank Negara, has initiated a similar approach.

[27] Period of analysis ranges from two weeks to three months.

3 Call to Action: The Need for an Active Defense Mindset

Trust and resilience are the cornerstones of growth in a digital economy. This section provides an agenda for policy makers and the private sector to work together to heighten awareness about cybersecurity and adopt a stance of active defense. The US Department of Defense defines active defense as the employment of limited offensive action and counterattacks to deny a contested area or position to the enemy. For cybersecurity, active defense is about flipping the asymmetry between defenders and attackers via cooperation among defenders. Cybersecurity programs often defend infrastructure in silos, even though vulnerabilities extend across peer companies and vendors. Meanwhile, adversaries plan and execute sophisticated attacks across several targets at once. Active defense means working together to defend and take advantage of the region's collective resources. Following this active defense mindset, an urgent four-point agenda is needed as part of the region's cybersecurity defense playbook (see figure 18).

3.1 Elevate cybersecurity on the regional policy agenda

The region's policy makers have agreed on the importance of closer coordination. However, given the varying levels of preparedness and vastly differing national priorities, there is a need to elevate cybersecurity on the regional and national policy agenda through the following actions:

- Steer the implementation of a Rapid Action Cybersecurity Framework.
- Elevate cybersecurity to the top of the agenda in regional economic dialogue.

Figure 18
Regional cybersecurity defense playbook

Elevate cybersecurity on the regional policy agenda	• Concerted coordination to steer the implementation of a Rapid Action Cybersecurity (RAC) Framework • Elevate cybersecurity to the top of the agenda in economic dialogue (for example, establish a regional coordination platform and multilateral agreement to have "cybersafe" trading partners)
Secure a sustained commitment to cybersecurity	• Pursue a commitment to address the regional cybersecurity spending gap • Define and track cybersecurity metrics through a cyber-hygiene dashboard
Fortify the ecosystem	• Foster a risk-centric mindset in the corporate sector • Instill a culture around sharing threat intelligence • Extend cyber resilience across the supply chain (i.e. to business partners) • Implement regional public–private partnerships and encourage industry alliances
Build the next wave of cybersecurity capability	• Develop the next generation of security professionals • Strengthen the local cybersecurity industry through deeper cooperation and collaboration with global players • Drive R&D around emerging threat vectors, including artificial intelligence and blockchain • Anchor world-class capabilities

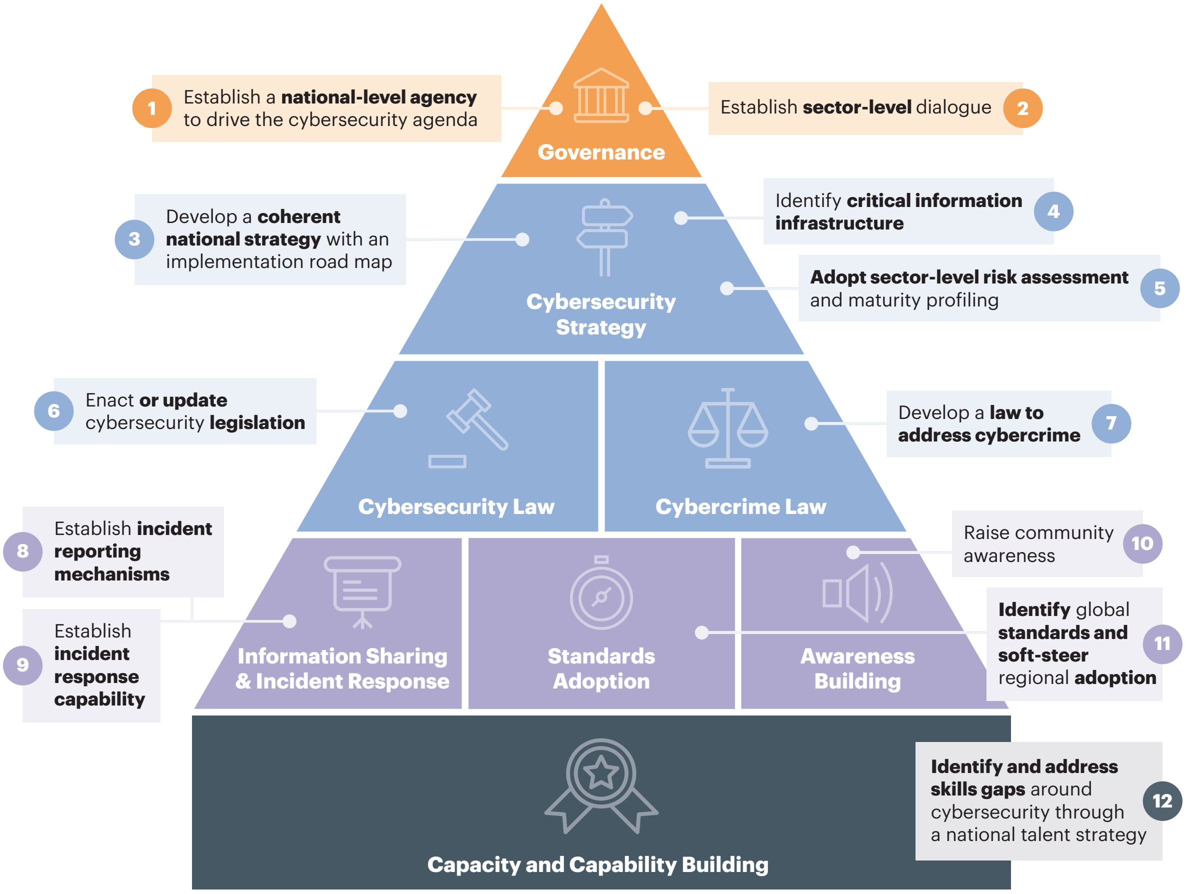
Source: A.T. Kearney analysis

3.1.1 Steer the implementation of a Rapid Action Cybersecurity Framework

As highlighted earlier, a few ASEAN countries have already defined their national strategy around cybersecurity together with an implementation road map. However, the pace, urgency, and level of harmonization of policy thrusts around cybersecurity across the rest of the region remains too slow.

The AMCC has taken steps to extend collaboration on cybersecurity across the region. However, a system based on loose collaboration of national agencies and voluntary exchanges is unlikely to go far enough to make ASEAN safe. To be effective, a tighter coordination mechanism is needed. A Rapid Action Cybersecurity Framework focused on addressing current weaknesses in cyber resilience in each country across the region is the first step in establishing some degree of harmony in terms of readiness across the region (see figure 19). This is a threshold requirement for countries such as Laos, Cambodia, and Myanmar to speedily implement the institutional frameworks needed to govern cybersecurity and interface with the rest of the region. The Rapid Action Cybersecurity Framework envisages 12 strategic imperatives, aimed at fixing the basics related to cybersecurity across the region. National governments should take the lead in implementing the Framework with support and guidance from the AMCC.

Figure 19
Rapid Action Cybersecurity Framework



1 Establish a **national-level agency** to drive the cybersecurity agenda
Establish **sector-level** dialogue 2
Governance
3 Develop a **coherent national strategy** with an implementation road map
Identify **critical information infrastructure** 4
Adopt sector-level risk assessment and maturity profiling 5
Cybersecurity Strategy
6 Enact **or update** cybersecurity **legislation**
Develop a **law to address cybercrime** 7
Cybersecurity Law
Cybercrime Law
8 Establish **incident reporting mechanisms**
9 Establish **incident response capability**
Raise community awareness 10
Identify global **standards and soft-steer** regional **adoption** 11
Information Sharing & Incident Response
Standards Adoption
Awareness Building
Identify and address skills gaps around cybersecurity through a national talent strategy 12
Capacity and Capability Building

Source: A.T. Kearney analysis

As discussed, several ASEAN countries have identified national agencies to drive their cybersecurity agenda. In others, the process is still ongoing, with CERTs serving as the de facto agency in charge of cybersecurity. It is important to define who within each country is responsible for managing and evaluating the cybersecurity strategy and ensure the v esting of sufficient authority to drive action across sectorial and government department boundaries. While centralized and decentralized models exist, establishing an **independent central national agency to define and supervise the security agenda** will foster a strong enforcement mindset.

An imperative of the Rapid Action Cybersecurity Framework is the definition of a **national cybersecurity strategy** by each country with a sharp vision, scope, objectives, and a practical road map for implementation (see sidebar: Australia's Cybersecurity Policy). In this context, an approach based on risk identification, risk analysis, and risk evaluation is crucial. **Risk assessments** should be carried out both at the national and sectorial level. **Defining and identifying critical sectors and critical information infrastructure** (CII) while engaging with CII owners at the outset is a vital part of the strategy. A clear set of sector specific risk mitigation mechanisms needs to be put in place. Assessing and prioritizing high-value assets and determining the probability of breach should be at the core of such risk assessments.

Enacting **pragmatic cybersecurity legislation or updating it** to current needs is the next step in the Rapid Action Cybersecurity Framework. While political issues could affect policy alignment at the regional level, the increasing integration of ASEAN requires a certain level of harmonization and coordination. Furthermore, because technology is rapidly advancing, the laws could quickly fall far behind. Adopting a careful approach in collaboration with the private sector, aimed at regulating human behavior and spreading a cybersecurity culture, is vital to ensure pragmatic legislation in each country.

To address **cybercrime**, each country must define cybercrime laws and strengthen local law enforcement. The only existing multilateral treaty addressing cybercrime is the Budapest

Australia's Cybersecurity Policy

The main themes of Australia's Cyber Security Strategy released in 2016 are co-leadership, strong cyber defenses, global responsibility and influence, and growth and innovation. A key tenet is the recognition of a national cybersecurity partnership that places the onus on government agencies and business leaders to set the national cybersecurity agenda. A cyber ambassador will identify opportunities for practical international cooperation and ensure Australia has a coordinated, consistent, and influential voice on international cyber issues.

The Australian Signals Directorate has developed strategies to help cybersecurity professionals mitigate cybersecurity incidents. This guidance addresses targeted cyber intrusions, ransomware, and external adversaries with destructive intent, malicious insiders, business email compromise, and industrial control systems. This policy has become standard practice for industry stakeholders as well. Areas such as escalated privilege management, 48-hour patch deployment, and application whitelisting are seen as the most effective tools for reducing cyber risk. Recent updates to this policy have added application hardening, blocking macros and daily backups. These controls were mandated via a critical review of incidents responded to by the national CERTs and were analyzed to be the most effective controls that would have prevented more than 85 percent of the breaches.

Convention on Cybercrime, proposed by the Council of Europe in 2001, which includes provisions for cross-border assistance between law enforcement agencies on cybercrime separate from the more cumbersome Mutual Legal Assistance Treaty arrangements. Despite the Philippines having committed to the Budapest Convention, none of the other ASEAN countries has signed. Adopting an ASEAN-initiated multilateral regime around cybercrime consistent with the Budapest Convention could bring about strategic and operational benefits to the region, particularly in the area of rapid law enforcement cooperation.

Information sharing among stakeholders is a powerful mechanism to better understand a constantly changing environment. Sharing views on emerging threats, risks and vulnerabilities together with aspects related to national security, provides powerful insight into how the threat landscape is evolving. In this context, it is important to properly define the information sharing mechanism and the underlying rules that govern it, including non-disclosure agreements, traffic-light protocol, antitrust rules, and law enforcement access. A sectorial approach to information sharing is a good start, but this should be extended to encourage cross-sector communication as there are many interdependencies between sectors, for example between the banking and telecom sector for mobile payments.

National cybersecurity agencies have a pivotal role to play in driving adoption and harmonization of **standards** across the region. A start could be made with standards such as ISO 27001 and the NIST Cybersecurity Framework. Collaboration at the sectorial level to share best practices around specific concerns such as IT-OT convergence and wider adoption of standard specifications for sharing threat intelligence such as STIX and TAXII can significantly benefit the region.

Raising awareness about threats and vulnerabilities and their impact on society has become vital. With greater awareness, individual and corporate users can learn how to behave in the online world and protect themselves from risks. Defining the target of awareness-raising campaigns and identifying mechanisms to address them is a joint responsibility of both the public and private sectors. Initiatives such as Safer Internet Day, International Youth Day, and ENISA's security month have helped tremendously to increase social awareness and modify online behavior.

Apart from the above, it is vital that the region adopts a forward-looking **talent strategy** aimed at addressing the capacity and capability gaps highlighted earlier. Cross-regional collaboration efforts at training together with industry can enable countries to tap into each other's strengths to quickly boost the talent level.

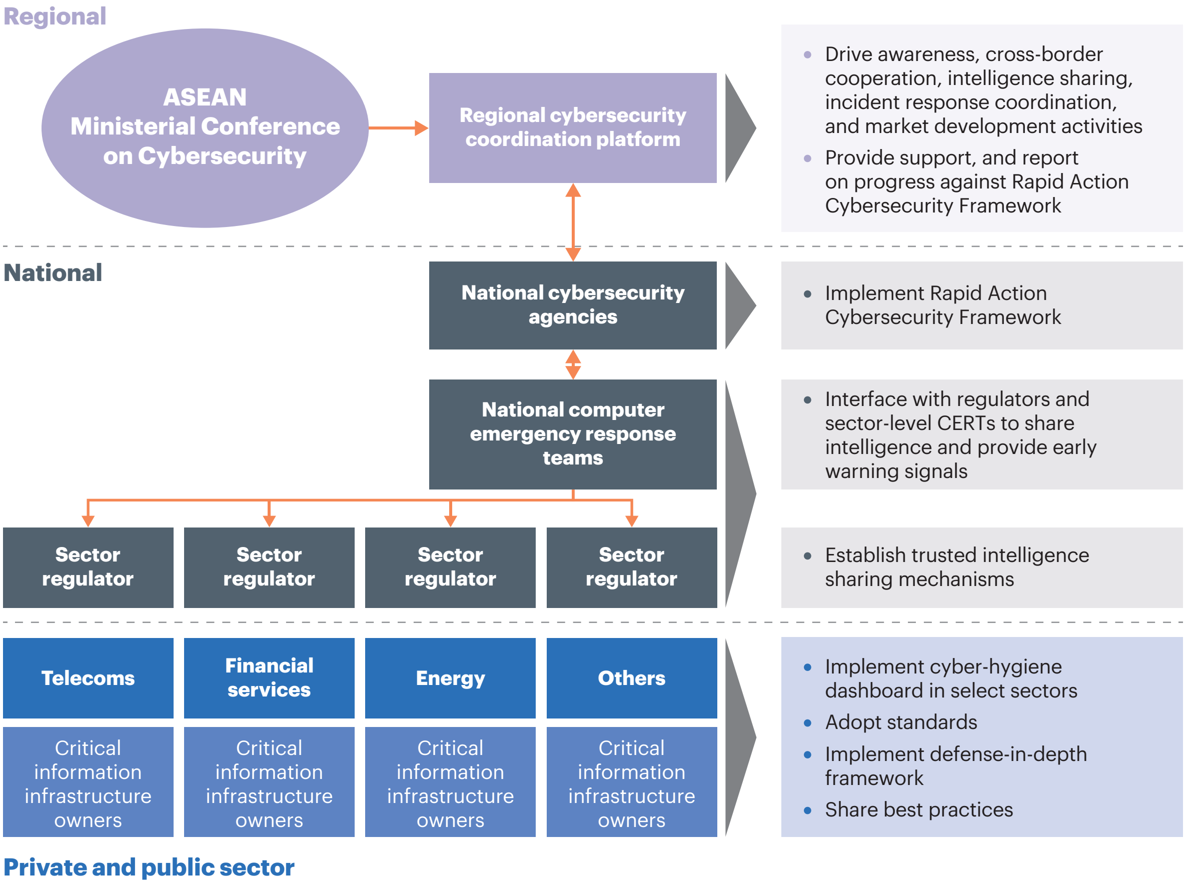
3.1.2 Elevate cybersecurity to the top of the agenda in regional economic dialogue

In addition to the Ministerial Conference, a regional operational coordination platform is needed to interface with various national agencies. This facilitates the creation of awareness, cross-border cooperation, and market development activities, including adoption and harmonization of standards (see figure 20 on page 31). A coordination platform can help improve capabilities across the cybersecurity life cycle by facilitating information sharing to improve threat detection, enable region-wide deterrence, provide counter-strategies, and enabling the development of national cybersecurity capabilities. Identification of cyber safe trading partners based on their ability to meet minimum threshold requirements in a timely manner will help to significantly elevate cybersecurity on the economic agenda.

Most importantly, the scope of the annual report provided by the ASEAN secretary-general should be expanded to include a report on the progress of each country based on the Rapid Rapid Action Cybersecurity Framework and foster attention and progress across the region.

Figure 20

Regional cybersecurity governance framework


Regional
ASEAN Ministerial Conference on Cybersecurity
Regional cybersecurity coordination platform
Drive awareness, cross-border cooperation, intelligence sharing, incident response coordination, and market development activities
Provide support, and report on progress against Rapid Action Cybersecurity Framework
National
National cybersecurity agencies
Implement Rapid Action Cybersecurity Framework
National computer emergency response teams
Interface with regulators and sector-level CERTs to share intelligence and provide early warning signals
Sector regulator
Sector regulator
Sector regulator
Sector regulator
Establish trusted intelligence sharing mechanisms
Telecoms
Financial services
Energy
Others
Critical information infrastructure owners
Critical information infrastructure owners
Critical information infrastructure owners
Critical information infrastructure owners
Implement cyber-hygiene dashboard in select sectors
Adopt standards
Implement defense-in-depth framework
Share best practices
Private and public sector

Source: A.T. Kearney analysis

3.2 Secure a sustained commitment to cybersecurity

Two initiatives can help secure sustained commitment to cybersecurity:

- Pursue a commitment to address the cybersecurity spending gap.
- Define and track cybersecurity metrics through a sector-level cyber-hygiene dashboard.

3.2.1 Pursue a commitment to address the cybersecurity spending gap

Coupled with the region's digital divide, differing national priorities and the perception about the value-at-risk results in a suboptimal allocation of funds to address cybersecurity.

Among ASEAN countries, three potential clusters of countries could emerge over time:

a. Leaders: those with strong digital momentum, established institutional frameworks, and near- benchmark levels of cybersecurity spend

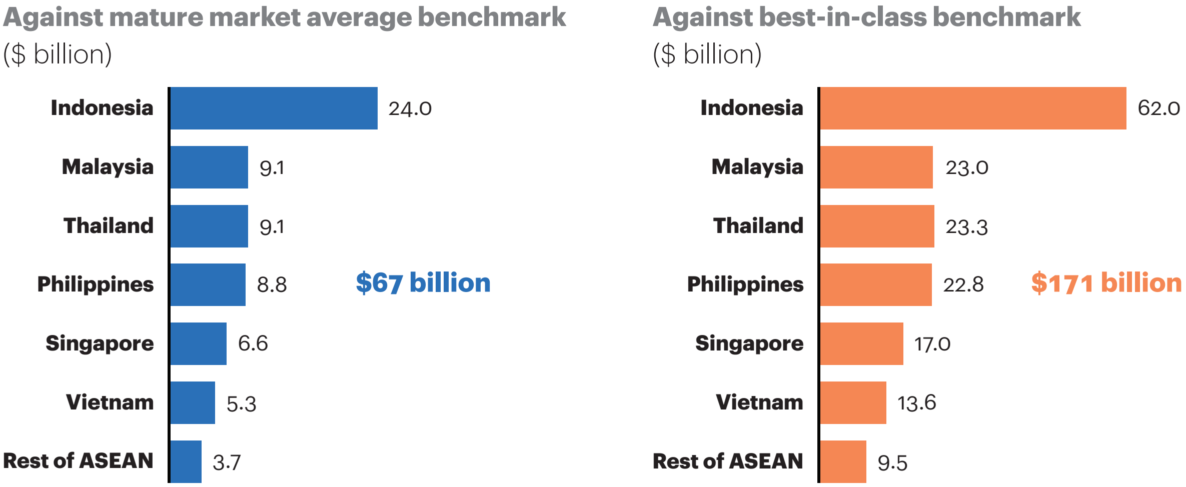
b. Steady risers: those that exhibit strong momentum around digital and are in the process of building institutional frameworks around cybersecurity

c. Breakout performers: those with the potential to leapfrog the rest of ASEAN but with no legal or institutional frameworks for cybersecurity

ASEAN countries are currently underspending on cybersecurity. A step-up in investment is needed to raise cybersecurity spending to benchmark levels (see figure 21). If each ASEAN country spends between 0.35 and 0.61 percent of GDP annually on cybersecurity between 2017 and 2025, spending would be in line with best-in-class countries. Our estimates suggest that this translates into a $171 billion collective spend for the region in the period spanning 2017 to 2025. This represents a justifiable and manageable investment, considering the value-at-risk and that individual governments spend on average 1.8 percent and up to 3.4 percent of GDP on defense.[28]

Figure 21

Target cumulative cybersecurity spend, 2017 to 2025



Notes: Mature market average includes the United States, the United Kingdom, and Germany.
Best in class is based on spend levels as a percentage of GDP for Israel. Rest of ASEAN is Laos, Brunei, Cambodia, and Myanmar.

Sources: Gartner, International Data Corporation; A.T. Kearney analysis

Indonesia stands out as potentially requiring a significant investment as the share of its digital economy is expected to grow significantly in the coming years.

3.2.2 Define and track cybersecurity metrics through a sector-level cyber-hygiene dashboard

Barriers to trust and transparency emanate partly from a lack of structured mechanisms to collect data, measure performance, and share intelligence. The lack of consistently defined and applied cybersecurity metrics and mechanisms within each country to collect and share the output data makes it difficult to assess the effectiveness of a cyber program and drive continuous improvement.

In sectors such as financial services, identifying and tracking meaningful metrics can provide an enhanced level of transparency while also improving performance on these metrics over time. A few metrics can help focus the cybersecurity agenda on the areas that matter most (see figure 22 on page 33). The onus is on regulators to identify metrics that have the most relevance to their respective sectors and ensure consistent, up-to-date definitions. Establishing metrics at a sectoral level requires a consultative approach while keeping in mind organizational constraints and different business needs.

[28] World Bank data for Malaysia, Singapore, Indonesia, Thailand, Vietnam, and the Philippines

Figure 22

Focus the cybersecurity agenda on relevant metrics

Function	Management perspective	Metrics
Incident management	How well do we detect, accurately identify, handle, and recover from security incidents?	• Mean time to incident discovery • Number of incidents • Mean time between security incidents • Mean time to incident recovery
Vulnerability management	How well do we manage the organization's exposure to vulnerabilities by identifying and mitigating known vulnerabilities?	• Vulnerability scanning coverage • Percent of systems with no known severe vulnerabilities • Mean time to mitigate vulnerabilities • Number of known vulnerabilities
Patch management	How well are we able to maintain the patch state of our systems?	• Patch policy compliance • Patch management coverage • Mean time to patch
Application security	Can we rely on the security model of business applications to operate as intended?	• Number of applications • Percent of critical applications • Risk assessment coverage • Security testing coverage
Configuration management	How do changes to system configurations affect the security of the organization?	• Mean time to complete changes • Percent of changes with security reviews • Percent of changes with security exceptions
Corporate spending	What is the level and purpose of spending on information security?	• IT security spending as percent of IT budget • IT security budget allocation

Sources: Centre for Internet Security; A.T. Kearney analysis

> "Regulators need to acknowledge that industries have different business needs and organizational constraints, and thus it would be difficult to mandate cybersecurity metrics in a one-size-fit-all approach."
>
> **—land transportation authority, ASEAN country**

A cyber-hygiene dashboard should be an integral part of the corporate performance monitoring system, tracking internal readiness on strategy, culture, technology, processes, and organization (see figure 23 on page 34).

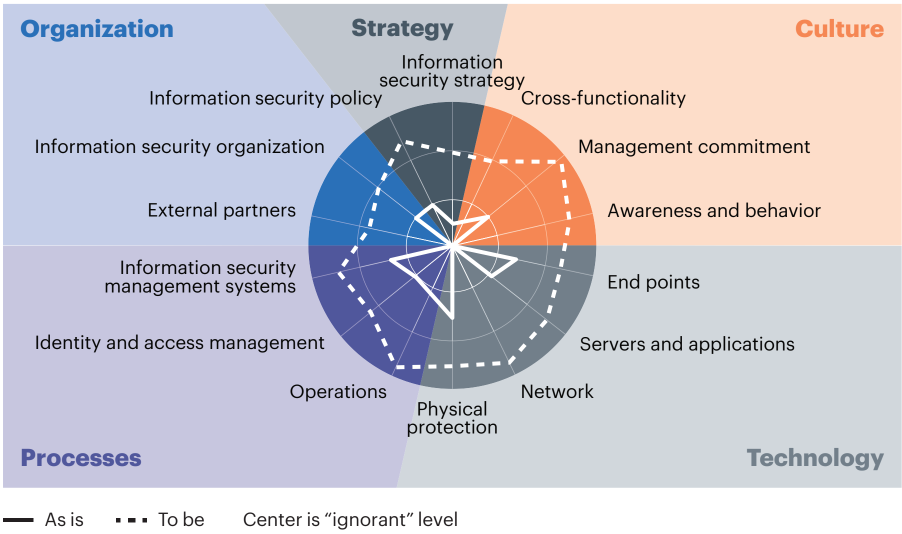
3.3 Fortify the ecosystem

The active defense mindset needs to be extended across the ecosystem in each country by not only implementing best practice guidelines in the corporate sector, but also raising cyber awareness across business partners. Four moves can help fortify the ecosystem:

- Foster a risk-centric mindset around cybersecurity for the corporate sector.
- Instill a culture of transparency in sharing threat intelligence.

Figure 23

Deploy a cyber-hygiene dashboard



Source: A.T. Kearney analysis

- Extend cyber resilience across the supply chain.
- Forge public–private partnerships and industry alliances.

3.3.1 Foster a risk-centric mindset around cybersecurity for the corporate sector

The lack of a holistic approach around strategy, governance, organization, and culture often results in organizations being highly vulnerable despite relying on the best vendors and products. A four-step approach can help companies define their cybersecurity strategy (see figure 24).

Figure 24

Define a cybersecurity strategy with a focus on four areas

1 Align on business objectives

- Identify key business drivers
- Identify security drivers that can assist in accomplishing business outcomes

2 Identify high-value assets

- Establish a working definition of high-value information system assets
- Establish a portfolio of systems to be assessed as HVAs
- Analyze potential HVA candidates to create a list of recommended HVAs for road-map planning
- Review and validate the HVA list to be used for risk assessment

3 Conduct cyber-threat probability and impact risk assessment

- Establish primary threat vectors facing HVAs
- Establish a framework for plotting the potential risk and business impact from cyber threats
- For each identified HVA:
  - Review against industry's common threats
  - Establish risk profile: probability and impact
  - Prioritize the assets into groups based on the risk profile and other criteria

4 Assess cyber capabilities to defend HVAs

- Perform a cyber health check
- Assess capabilities by HVA against NIST CF and defense-in-depth model
- Create a collective view of current and planned capability deployments for coverage and gaps
- Perform a gap analysis of planned HVA initiatives using the NIST CF

Notes: HVA is high-value asset. NIST CF is the National Institute of Standards and Technology Cybersecurity Framework.

Source: A.T. Kearney analysis

The first step is to align on business objectives and raise the profile of cybersecurity as a business risk imperative. Second, high-value assets should be identified and prioritized. Third, a cyber threat impact risk assessment should be conducted. Finally, it is imperative to identify cyber capabilities needed to defend high-value assets.

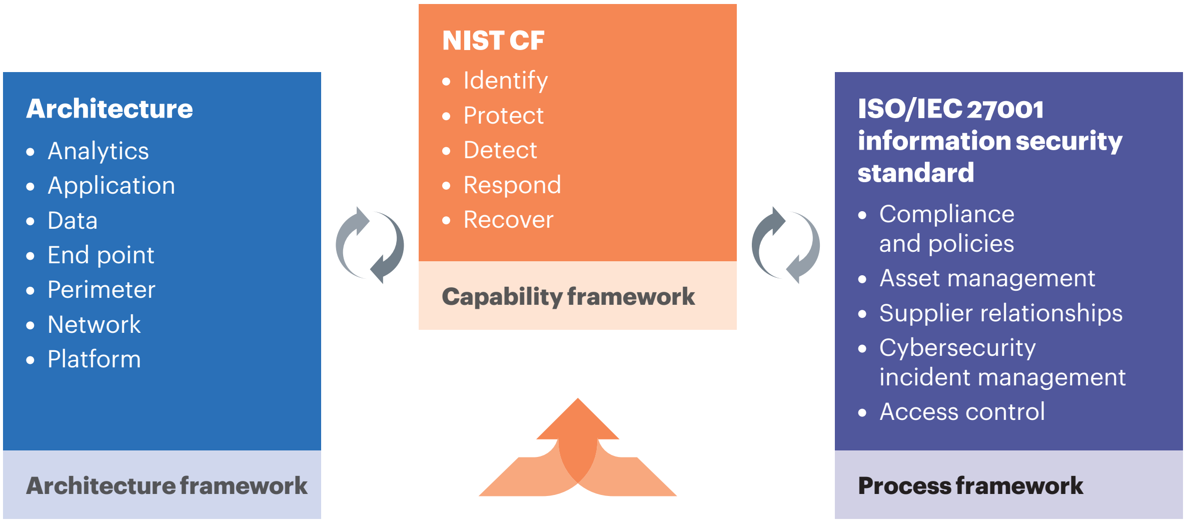
> "We are in the process of setting up the CISO function with an independent mandate to report to the board, distinct from the CIO. We have conducted cybersecurity posture assessments across our major operating companies. This has helped to build awareness, but there is a lot of work to do to build a solid governance framework."
>
> **—major regional telecoms group**

In defining their strategy to enhance cyber resilience, businesses need to consider the value-at-risk. To assess the value-at-risk, businesses could take either an asset- or liability-based view. An asset-based view involves valuing critical assets and the potential reputational damage from an attack. Alternatively, businesses could consider a liability-based approach, building scenarios and quantifying the financial and reputational loss. Building potential scenarios with a combination of historical data and judgment about the probability of a threat can create a better understanding of the value-at-risk and help allocate resources in a more judicious manner.

Businesses should leverage industry best practices and standards such as the NIST Cybersecurity Framework, ISO 27001, and an architecture framework based on risk-centric security (see figure 25).

Figure 25

Adopt a risk-centric approach to cybersecurity



Architecture

- Analytics
- Application
- Data
- End point
- Perimeter
- Network
- Platform

Architecture framework

NIST CF

- Identify
- Protect
- Detect
- Respond
- Recover

Capability framework

ISO/IEC 27001 information security standard

- Compliance and policies
- Asset management
- Supplier relationships
- Cybersecurity incident management
- Access control

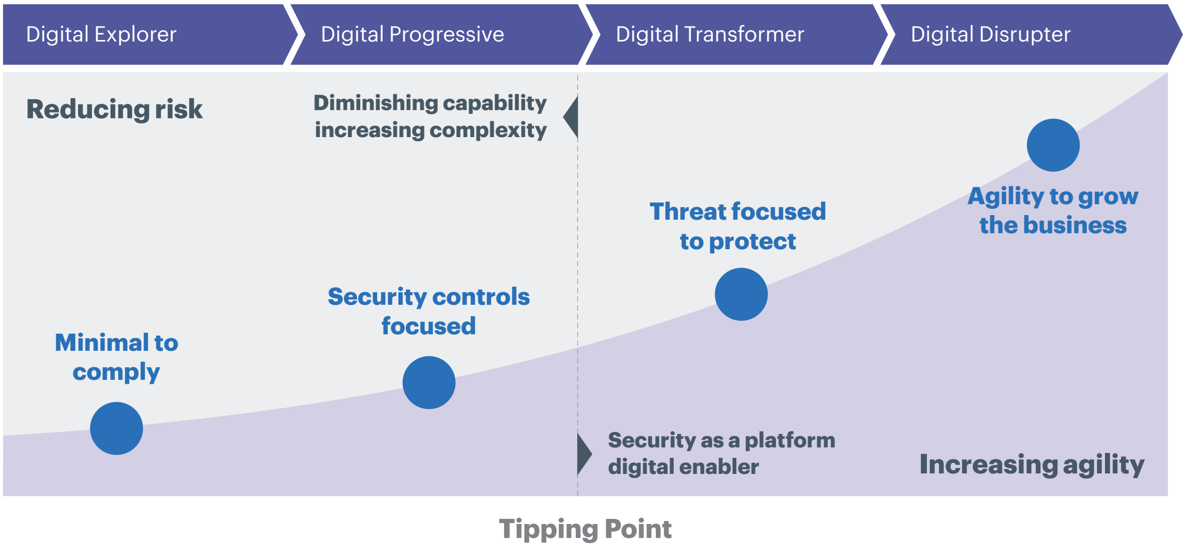
Process framework

Note: NIST CF is the National Institute of Standards and Technology Cybersecurity Framework.

Source: A.T. Kearney analysis

As digitalization grows, security must also mature (see figure 26). An organization's evolution across the various stages of cyber excellence could be measured and tracked, providing a useful measure of cyber readiness. A security maturity model can help map an organization's digital transformation journey against its security profile (see Appendix A on page 50). For smaller organizations looking to partner with large multinationals or CII owners, performance on the security maturity model should be a threshold requirement for doing business. This will raise the profile of cybersecurity among all business partners and promote resilience across the supply chain. Singapore's Cybersecurity Bill calls for regular system audits by an approved third party. For CII owners, a maturity model can help identify cybersafe business partners.

Figure 26
Security as a digital enabler


Digital Explorer
Digital Progressive
Digital Transformer
Digital Disrupter
Reducing risk
Diminishing capability increasing complexity
Agility to grow the business
Threat focused to protect
Security controls focused
Minimal to comply
Security as a platform digital enabler
Increasing agility
Tipping Point

Source: A.T. Kearney analysis

Cyber insurance companies are increasingly looking at an organization's strategy, policy, and governance while pricing cyber insurance. Depending on the sector, a vulnerability scan or a penetration test may also be carried out in addition to reviewing the size of the security budget in relation to the total IT budget. Putting in place a comprehensive, layered cybersecurity strategy can help businesses reduce their insurance spend.

3.3.2 Instill a culture of transparency in sharing threat intelligence

Defending a country's digital assets requires close cooperation across a range of stakeholders, including government agencies, the private sector, and end users. Despite general agreement about the need to do this, information-sharing remains inadequate both globally and in the region. Legal impediments—some real, some perceived—are obstacles to more robust information sharing among private-sector entities and between the private sector and the government. The US Cybersecurity Information Sharing Act aims to improve cybersecurity by giving private companies liability protection when they share relevant information with federal or private entities, allowing companies to remove information that identifies someone who is not directly related to a threat.

ENISA suggests three types of approaches to share information on cybersecurity incidents: traditional regulation, self- and co-regulation, and information and education schemes.[29]

> "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."
>
> **—Sun Tzu**

ASEAN countries must move beyond regulations and trigger education and awareness building. In the initial stages of development, an awareness-building approach focused on value-at-risk and driven by national cybersecurity agencies or national-level CERTs could help create a climate of confidence and trust to share good and bad practices and experiences and discuss preparedness measures. Keeping the sharing group small and using traffic-light protocols or other rules on how information could be shared can inculcate the right behaviors around sharing. Regular table-top exercises, cyber incident drills, and stress testing, currently carried out in Singapore and Malaysia, need to be extended to the rest of ASEAN.

There is also merit in cross-sector communication, given the convergence of sectors in the digital sphere (for example, telecoms and banking). It is also useful to develop an early-warning system for CIIs. Such systems require the cooperation of a wide range of stakeholders, both private and public, and could be the central capability for handling creeping, slow-burn, and sudden crises. Having a common language for sharing threat information enables greater standardization. For example, STIX and TAXII is an open community-driven effort and a set of free specifications that help with the automated exchange of cyber threat intelligence. One of the key benefits of STIX and TAXII is that it helps to exchange cyber threat intelligence between different systems.

Economic incentives stemming from cost savings such as quicker reaction to threats or anticipating network failures and from the quality, value, and use of shared information should be touted as the main reasons for building a sharing culture. More robust sharing of private and public network security information as well as threat information—in real time—would create a level of situational awareness that would enable operational and strategic decisions to be made about how to better protect them and respond to attackers. In Singapore, threat intelligence sharing is facilitated by three-tiered security operations centers at the national, sectorial and corporate levels that facilitate the mandated collection of data and the monitoring and analysis of cyber threats and act as an early warning system for attacks. Singapore's Ministry of Home Affairs and the Land Transport Authority have established security operations centers for their sectors, and the Cyber Security Agency (CSA) of Singapore hopes to set up similar centers in every sector. In addition, CII owners and operators in certain sectors must report cybersecurity incidents to the regulator. Depending on the nature of the incident, these may then be reported to CSA. In addition to allowing the regulator and the CSA to determine if the incident is systemic, this creates another means of sharing information that may be useful for other CII sectors. Awareness building and education on cybersecurity also takes place in a voluntary manner, as in the UK cross-sector initiative (see sidebar: Cybersecurity Information Sharing Partnership, United Kingdom on page 38).

[29] *Cybersecurity Information Sharing: An Overview of Regulatory and Non-Regulatory Approaches*, ENISA, December 2015

Cybersecurity Information Sharing Partnership, United Kingdom

The Cybersecurity Information Sharing Partnership (CiSP) is a joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential, and dynamic environment, increasing situational awareness and reducing the impact on UK businesses. The success of this approach depends on the eagerness of members to share information and to be transparent regarding their needs.

The involvement of a national agency such as CERT-UK, assures members that the information sharing platform is secure, and continuously monitored and tested. CiSP produces a wide range of products to cater for organizations at all levels of cyber maturity. These include, but are not limited to:

- **Alerts and advisories, including those from national and international partners**
- **Best practice and guidance documents on common themes**
- **Quarterly reports on threat trends**
- **Malware and phishing email analysis**

> "There are two major obstacles to sharing intelligence. First, there is the difficulty in understanding the benefits of collaborating and sharing what may be deemed as highly confidential information. Second, high volumes of raw data pose a challenge to filtering and classifying what is important."
>
> **—land transportation authority, ASEAN country**

3.3.3 Extend cyber resilience across the supply chain

As discussed, cyber criminals often use SMEs' low levels of readiness to infiltrate the partnerships these companies have with larger organizations. Because of this, the cybersecurity lens must be extended across the entire supply chain.

Building cyber resilience across the supply chain requires a consideration of supply chain, managed services, and cloud services vendor management practices. The supply chain represents a significant cybersecurity risk because there are many ways a supply chain breach could occur. For example, a software manufacturer could be breached via malware that modifies source code that is then distributed to enterprises that use the software. Another common compromise vector is the theft of a vendor's credentials that grant remote access to an enterprise the vendor works with, leading to infiltration of the enterprise network from a trusted source. High-profile breaches have included Target, Home Depot, and the US Office of Personnel Management. In addition, ICT services and support are often outsourced to reduce costs and streamline operations.

> “Sophistication of threat vectors is increasing. We are seeing supply chains of leading multinational companies (MNCs) being increasingly targeted with a view to get to the real crown jewels: the MNCs’ high-value assets.”
> **—global cyber insurance company**

Small organizations are often targeted because they are more vulnerable, represent a single point of failure, or have disproportionate access to valuable information given their size within a supply chain.

To build resilience, it is important to institutionalize a multi-stakeholder supply chain risk assessment process that engages as many members of the supply chain as possible. Critical business relationships must be graded according to the consequences of losing their services and be regularly reviewed for relevance and interactions between subsequent supply chain members identified. This is technically challenging and some of the most complex supply chains have so many external partners they may be unable to assess the risk of doing business with each one. The adoption of a security-by-design mindset can help to avoid piecemeal implementation of cybersecurity solutions and the need for costly and often ineffective retrofitting at a later stage. Additionally, aggressive monitoring of data flows across supply chain links can help reveal potential indicators of compromise and provide insight into potentially risky behavior. Businesses across ASEAN can benefit significantly by adopting a security-by-design mindset as part of their cybersecurity strategy.

Building resilience across the supply chain requires a five-step vendor management program as detailed below:

a. Identify the most significant vendors.

b. Specify the primary touch points with each vendor.

c. Establish guidelines that are consistent with a risk-centric mindset.

d. Integrate with the organization’s risk management and audit practices.

e. Aggressively monitor data flows across supply chain links.

3.3.4 Forge public–private partnerships and industry alliances

The public and private sectors can benefit from working together on cybersecurity initiatives. The private sector controls much of the critical infrastructure that is vulnerable to cyber threats. Some companies that own such infrastructure have already defined cybersecurity strategies and governance, giving them unique expertise and experience in dealing with potential threats.

Cooperation between industry and governmental agencies on joint cybersecurity initiatives can leverage the unique yet complementary strengths of both sectors. According to the Intelligence and National Security Alliance, the mission of cybersecurity PPPs is threefold. First, these partnerships must identify and detect behaviors of concern. Second, PPPs must ensure that actors from both sectors comply with the standards of the partnership. Third, and most importantly, PPPs must provide a mechanism for response after a cyber threat; this entails conducting examinations of an attack and addressing any necessary shortcomings in the current defense system. Furthermore, effective PPPs should ensure that cybersecurity developments in the private sector and their policy implications are well understood by policy makers. PPP programs have supported numerous objectives including sharing of best practices and threat intelligence, harmonization of standards, greater inclusion of SMEs and research and development into emerging threat vectors. Singapore, for example, has developed several PPP programs, including the Singtel Cybersecurity Institute, the Cybersecurity Centre of Excellence, and the Cyber Risk Management Project. PPPs have tended to focus on three objectives: workforce development, research and development, and information sharing. The main private-sector parties in these partnerships generally come from institutes of higher learning, research institutes, and cybersecurity solution vendors, including cyber insurance.

Industry alliances have also emerged around niche areas such as IoT security, which regional companies could benefit from. These alliances are largely focused on solving security concerns around IoT through collaborative research and shaping of standards. ASEAN countries should look to align with these global industry alliances or explore regional alliances focused on their specific needs. Some of the key alliances that have emerged include the IoT Cybersecurity Alliance, the Industrial Internet Consortium, and the Cyber Threat Alliance. In addition, Cisco has co-founded the Trusted IoT Alliance, a consortium of 17 companies to help establish a protocol for a blockchain-based IoT. The mission of this new alliance is to set the standard for an open-source blockchain protocol in major industries worldwide.

3.4 Build the next wave of cybersecurity capability

Cybersecurity presents a significant economic opportunity for the region, given that it is one of the fastest-growing segments in the ICT space. A concerted effort at encouraging the development of the local industry will allow regional companies to take advantage of these opportunities. Countries in the region need to continue to drive the growth of ASEAN cybersecurity workforce capability and develop frameworks that ensure greater mobility across the vendor ecosystem.

Building the next wave of cybersecurity capabilities will require a focus on four areas:

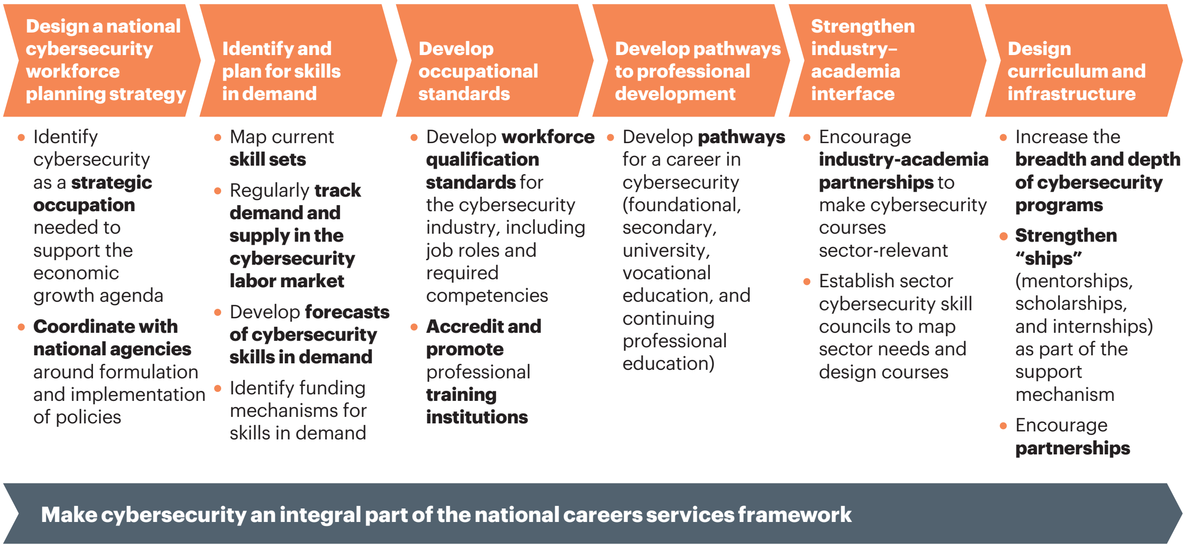
- Develop the next generation of cybersecurity professionals.
- Strengthen the local cybersecurity industry through deeper cooperation and collaboration with global players.
- Foster R&D around emerging threat vectors.
- Anchor world-class capabilities to facilitate knowledge exchange and capability building.

3.4.1 Develop the next generation of cybersecurity professionals

Because of the gap in both capacity and capabilities, the region needs more people to pursue cybersecurity careers with a tailored development of skills to meet the needs of individual industries. In this context, it is important to raise the profile of cybersecurity and develop a clear policy framework for capacity and capability development (see figure 27 on page 41). National agencies in charge of driving the cybersecurity agenda need to lay out a clear strategy around cybersecurity workforce planning aimed at elevating the occupation as a strategic occupation critical to support the digital economy. This requires closer coordination with a range of public-sector agencies, including education ministries, workforce development agencies, and economic development agencies. There is also a need to constantly monitor and track specific cybersecurity skills, such as OT security. Developing forecasts of skills that are in demand and identifying plans to address them is integral to the development of the local industry.

Figure 27

Address gaps in cybersecurity capacity and capabilities



Design a national cybersecurity workforce planning strategy

- Identify cybersecurity as a **strategic occupation** needed to support the economic growth agenda
- **Coordinate with national agencies** around formulation and implementation of policies

Identify and plan for skills in demand

- Map current **skill sets**
- Regularly **track demand and supply in the cybersecurity labor market**
- Develop **forecasts of cybersecurity skills in demand**
- Identify funding mechanisms for skills in demand

Develop occupational standards

- Develop **workforce qualification standards** for the cybersecurity industry, including job roles and required competencies
- **Accredit and promote** professional **training institutions**

Develop pathways to professional development

- Develop **pathways** for a career in cybersecurity (foundational, secondary, university, vocational education, and continuing professional education)

Strengthen industry–academia interface

- Encourage **industry-academia partnerships** to make cybersecurity courses sector-relevant
- Establish sector cybersecurity skill councils to map sector needs and design courses

Design curriculum and infrastructure

- Increase the **breadth and depth of cybersecurity programs**
- **Strengthen "ships"** (mentorships, scholarships, and internships) as part of the support mechanism
- Encourage **partnerships**

Make cybersecurity an integral part of the national careers services framework

Source: A.T. Kearney analysis

Setting up occupational standards for cybersecurity includes identifying job roles and competencies as well as accreditation of training programs and approved suppliers. A vital aspect of cybersecurity capacity is developing multiple educational pathways, ranging from classes that provide foundational skills to higher-level courses:

- **K–12.** Create awareness via outreach programs to educate the public, including children.
- **Universities.** Promote cybersecurity as a career using industry-linking programs, targeted university courses, and innovation opportunities.
- **Industries.** Scale up cybersecurity professional development via specialized skill-building and conversion programs for professionals.

Encouraging engagement between industry and academia will ensure that programs are tailored to specific industries. Setting up cybersecurity skill councils with representation from industry can be an effective way to increase engagement between industry and academia. MDEC has a three-tier capacity-building program that targets youth, university students, and the workforce (see figure 28 on page 43).

Global technology companies such as Cisco with a strong presence in the region are leading the way in developing the next wave of cybersecurity professionals (see sidebar: Cisco Networking Academy Cybersecurity Courses on page 42).

3.4.2 Strengthen the local cybersecurity industry through deeper cooperation and collaboration with global players

Our value chain analysis across select ASEAN markets revealed the presence of many global vendors in the products and solution portion of the value chain. While the services part of the value chain has seen some evidence of localization, the potential of the local industry remains largely untapped. Fragmentation of the vendor landscape and lack of regional mobility are major challenges to the local cybersecurity industry participating more fully to address cybersecurity

Cisco Networking Academy Cybersecurity Courses

Cisco Networking Academy (www.NetAcad.com) is an IT skills and career-building program for learning institutions and individuals worldwide. Networking Academy delivers classroom instruction, online teaching materials, interactive tools, and hands-on learning to students from every socioeconomic background so they can develop the knowledge and skills required to succeed in a technology-driven market.

More than 7.8 million people have joined the Networking Academy and have become a force for change in the global economy since 1997. More than 1 million students enroll each year in 180 countries. It has a network of more than 22,000 instructors and more 10,400 educational institutions use the academy's curriculum. In ASEAN alone, more than 770,000 students have been trained, with more than 500 academies and 1,400 instructors.

In support of the skills-to-jobs learning experience is an unparalleled ecosystem which provides support to the educational institutions and their students. With a focus on corporate social responsibility, Cisco provides the curriculum, learning platform, and 24/7 teaching and learning resources. There are more than 650 support and training partners throughout the world that provide services to the member educational institutions. The program also offers discounts on certification exams and equipment necessary as part of the instructional space. Global communities and local learning institutes provide instructors, students, classroom space, and lab facilities.

NetAcad.com, the global delivery platform, supports the entire program throughout the world. The Cisco Networking Academy global delivery platform is available in seven languages with some courses translated into as many as eighteen languages. One of the most powerful components of the platform is the custom assessment engine that provides detailed reports on a student's learning strengths and weaknesses with recommended course topics to help close the gaps. The platform also delivers a world-class learning management environment, which enables instructors to manage and customize their classroom and interactions with their students.

The Networking Academy portfolio learning outcomes include the following:

- Exploratory offerings emphasize exposure to new ideas and some basic conceptual understanding with a taste of the breadth of skills one might learn—with the desire to encourage students to consider a career in a particular technology area or type of technology-related business.
- Foundational offerings develop a breadth of conceptual understanding and practice of beginning and intermediate skills that form the basis for choosing one or two areas to specialize their skills.
- Career-ready offerings give students the depth of skills needed to prepare for an entry-level job or increased specialization using iterative learn-and-apply skill cycles in every lesson.
- Collaborate for Impact are checkpoint experiences within the foundational and career-ready offerings that synthesize all skills learned to date in a real-world, problem-solving context.

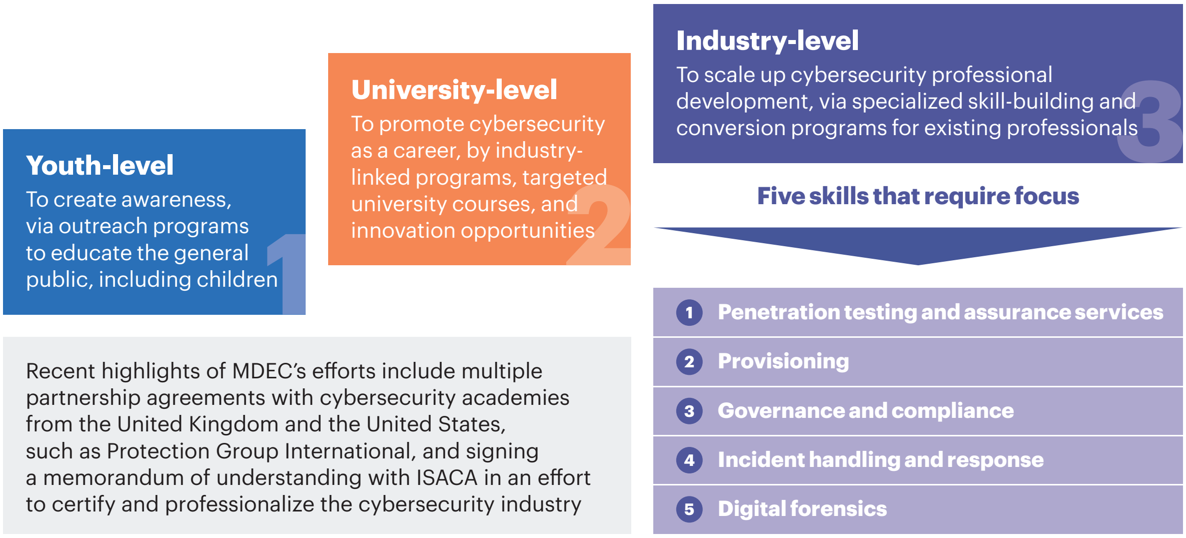
The portfolio includes a heavy emphasis on preparation for industry-recognized certifications, which lead to greater employment opportunities (see Appendix C: The Networking Academy's Learning Portfolio on page 51).

challenges. This makes it difficult for companies to compete on the national, regional, and global level and reduces the choice of viable and usable cybersecurity technologies to which citizens and businesses have access.

A tactical approach to overcome fragmentation in the local vendor landscape is the development of a certification framework for security products, consistent with the EU's security-by-design approach. The supply of ICT security products and services in ASEAN as well as in the EU has

Figure 28

MDEC's three-tier capacity-building program



Youth-level

To create awareness, via outreach programs to educate the general public, including children

University-level

To promote cybersecurity as a career, by industry-linked programs, targeted university courses, and innovation opportunities

Industry-level

To scale up cybersecurity professional development, via specialized skill-building and conversion programs for existing professionals

Five skills that require focus

1. **Penetration testing and assurance services**
2. **Provisioning**
3. **Governance and compliance**
4. **Incident handling and response**
5. **Digital forensics**

Recent highlights of MDEC's efforts include multiple partnership agreements with cybersecurity academies from the United Kingdom and the United States, such as Protection Group International, and signing a memorandum of understanding with ISACA in an effort to certify and professionalize the cybersecurity industry

Note: MDEC is Malaysia Digital Economy Corporation.

Sources: interview with Malaysia Digital Economy Corporation; A.T. Kearney analysis

remained very fragmented geographically. This makes it difficult for companies to compete on the national, regional, and global level and reduces the choice of viable and usable cybersecurity technologies that citizens and businesses have access to. Certification can play a significant role in increasing trust and security in products and services. In addition to certification, the European Commission is exploring the creation of a European, commercially oriented, voluntary labeling scheme for the security of ICT products.

3.4.3 Foster R&D around emerging threat vectors

Most R&D cybersecurity solutions focus on solving yesterday's problem without looking ahead to the next great challenge. R&D activities need to focus on products that are easy to use, intuitive, and secure. R&D should also take into consideration the lack of skilled talent. Our interviews highlight the need for efforts to be focused on three areas:

- Automation and artificial intelligence
- Tackling disinformation
- Security in the OT environment

> "Singapore has established a fund of SGD 190 million for spending on cybersecurity research over the period from 2015 to 2020. The focus is on developing products which are easy to use, intuitive as well as secure by design. Security in an IoT environment is another major area of focus."
>
> **—deputy chief executive, CSA of Singapore**

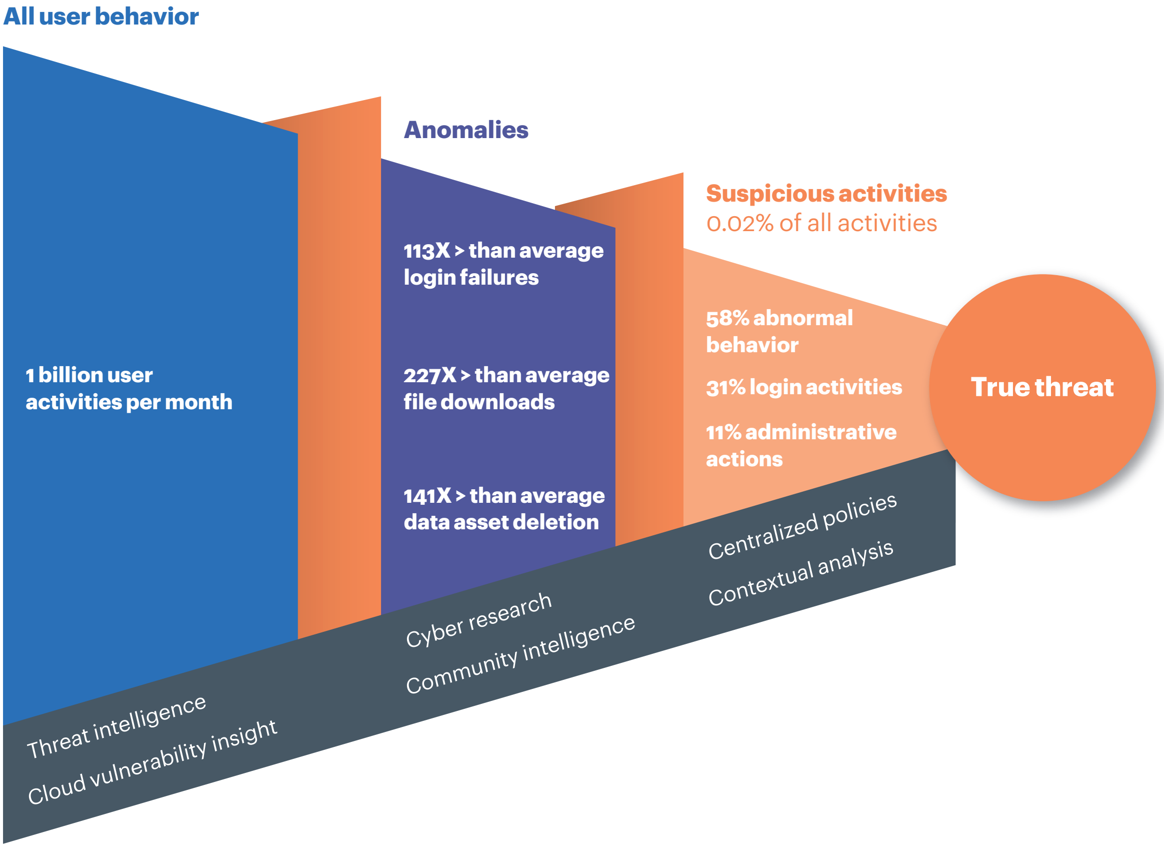
The Australian Cyber Security Research Institute (ACSRI) has been set up and funded by the Australian government. ACSRI combines private companies, public agencies, and universities with a focus on leading cyber research. ACSRI participants have committed about $90 million, and the Australian government has augmented this with an additional $50 million. ACSRI is industry led—minimizing the risk of wasting research funds on areas that are being done commercially elsewhere or where Australia does not have a competitive advantage. ACSRI aims to support about 600 postgraduate research personnel over seven years.

Automation and artificial intelligence

According to Cisco's 2017 Annual Cybersecurity Report, only one in 5,000 user activities (0.02 percent) connected with third-party cloud applications is suspicious. The challenge for security teams is to pinpoint that one instance. Only with automation can security teams cut through the noise of security alerts and focus their resources on investigating true threats. The multistage process of identifying normal and potentially suspicious user activities hinges on the use of automation, with algorithms applied at every stage (see figure 29).

AI and machine learning have the power to disrupt the industry. Security leaders should explore innovative technologies that turn defenses into learning systems. Unsupervised machine-learning approaches, such as those focused on user and entity behavior analytics, work at the intersection of human behavior and big data analytics. Solutions should focus on removing people from the

Figure 29
Identifying user patterns with automation



Source: A.T. Kearney analysis

loop as much as possible. The next area for focused, applied research should explore the most effective means to hunt within networks in real time. Research should move the industry closer to eliminating the detection gap instead of allowing threats to go undetected for months or even days. The AI capabilities should go hand in hand with research embedded within a hunt framework to automate the search, detection, and eviction of the adversary, while automating many of the processes that remain overly manual and time- and resource-intense. Given the talent shortage, AI technologies could help the ASEAN region leapfrog the rest of the world in building learning cybersecurity systems that evolve with additional data.

Tackling disinformation

Historically, when data was digitally stolen, the attacker kept it hidden. Today, this data is likely to be released along with a combination of valid and altered data to maximize the desired impact. Similarly, bots are often used to spread disinformation, especially on social media. R&D efforts to distinguish between content created by bots and humans could help tackle the rising use of disinformation, including using natural language processing aimed at the content itself or analytics on time frequency and other temporal patterns to expose bot-driven behavior. Because bots are a growing percentage of online traffic, any capability must also be able to separate disinformation from the streams of legitimate bot-driven advertising.

Security in the OT environment

The convergence of IT and OT has become a business imperative. The absence of standards or guidelines around IT and OT convergence remains a significant challenge, and the shortage of skilled professionals with an understanding of the nuances of industry-specific challenges amplifies the problem.

3.4.4 Anchor world-class capabilities to facilitate knowledge exchange and capability building

Attracting world-class companies with advanced capabilities has long been a strategy to facilitate knowledge exchange and develop the local industry. A pillar of Singapore's cybersecurity strategy is to use the country's status as an economic hub to attract world-class cybersecurity companies to base advanced operations, engineering, and R&D activities in Singapore. This increases access to cutting-edge cybersecurity capabilities and creates cybersecurity career pathways.

The Malaysia Digital Economy Corporation formalized a strategic partnership with the Protection Group International to help the country develop cybersecurity capabilities. The organization will share its expertise and set up a cybersecurity academy in Malaysia.

The region could benefit from establishing clusters for cybersecurity innovation. In other markets, these ecosystems are emerging in areas that provide the factors needed to sustain the development of the industry. Proximity to government cybersecurity functions creates a ready talent pool with access to job opportunities. Research centers and incubators and industry leadership in the form of national agencies, military cyber units, large companies, or chambers of commerce serve as catalysts for the growth of the local ecosystem. Establishing connections between military and government units and the corporate sector is an important way to attract and nurture talent. Global cybersecurity clusters such as Beersheba in Israel and Malvern in the United Kingdom exhibit similar features such as close links with government cybersecurity functions, strong leadership by the private sector, and the presence of training hubs (see sidebar: The United Kingdom's Malvern Cybersecurity Cluster on page 46).

The United Kingdom’s Malvern Cybersecurity Cluster

The United Kingdom has one of the most successful cybersecurity industries when measured in terms of economic growth. The sector alone contributed GBP 1.8 billion in exports to the UK economy in 2015 and grew from GBP 17.6 billion in 2014 to almost GBP 22 billion in 2015. Despite its relatively small size, the United Kingdom has 17 cybersecurity clusters.

In 2014, amid demand from small cybersecurity companies across the country, the UK Cyber Security Forum social enterprise was spun out of Key IQ and founded to help volunteers start cybersecurity clusters across the nation. The Forum acts as a focal point for organizations that want to engage with small, innovative companies and facilitates lobbying with the government about issues they face. The Malvern Cyber Security Cluster is now one of the clusters under the umbrella of the Forum.

The Malvern Cyber Security Cluster was founded in September 2011 by Key IQ Ltd. and today has a high concentration of active and innovative small cybersecurity companies. The area is now recognized as one of the primary locations in the United Kingdom for the research, development, and commercialization of cybersecurity products and services and is increasingly referred to as Cyber Valley.

4 Conclusion and Next Steps

The region’s response to the cybersecurity challenge needs to be comprehensive and forward-looking, engaging an array of stakeholders to deal with the threat and support the region’s leap into the vanguard of the digital economy. No country, company, or individual can surmount the cybersecurity challenge alone. Thus, every stakeholder has a role to play in creating a safe environment. The crucial shift from the failures of traditional cybersecurity to cyber resilience will require moving beyond protecting against attacks to building resilient assets and processes. The practices, procedures, and processes used to build and maintain technological systems will determine the success or failure of the next big attack.

In section 3, we highlighted that concerted actions will be required along a comprehensive four-point agenda to tackle the core of the problem:

1. Elevate cybersecurity on the regional policy agenda.
2. Secure a sustained commitment to cybersecurity.
3. Fortify the ecosystem.
4. Build the next wave of cybersecurity capability.

Immediate action is required. In figure 30 on page 47, we have outlined some of these actions. In the short term, national governments across ASEAN should speedily implement the 12-point agenda highlighted under the Rapid Action Cybersecurity Framework. The ASEAN secretary-general’s annual report should be expanded to include a review of how each country’s progress. This would increase awareness and raise the bar in terms of preparedness.

A sustained and committed approach to investing in cybersecurity is needed as the region becomes more digitally connected. From 2017 to 2025, ASEAN will need to spend $171 billion (0.35 to 0.61 percent of annual GDP) to align with international benchmarks. Given that the value-at-risk for ASEAN’s top 1,000 listed companies is roughly $750 billion in terms of current

Figure 30

Stakeholder view of the call to action

Call-to-action agenda	Regional	National
Elevate cybersecurity on the regional policy agenda	• Set up regional cybersecurity coordination platform • Track national progress via the ASEAN Secretary-general's annual report	• Implement the 12-point Rapid Action Cybersecurity Framework • Establish sector-level governance mechanism
Secure a sustained commitment to cybersecurity	• Track cybersecurity investments against the agreed commitment • Report on national cybersecurity spend	• Engage with private-sector stakeholders to stimulate cybersecurity investment • Set up a cyber-hygiene dashboard for crucial sectors to define and track key performance indicators at the sectorial level • Recommend standards for voluntary adoption
Fortify the ecosystem	• Adopt voluntary certification of vendors and develop recommended lists • Foster cross-border cybersecurity cooperation across the region and around the world • Encourage public–private partnerships across the region	• Adopt voluntary certification of vendors, and develop recommended lists • Establish and incentivize trusted sharing mechanisms • Set up security maturity assessments as a formal cyber certification for the private sector • Set-up industry alliances • Encourage public–private partnerships
Build the next wave of cybersecurity capabilities	• Develop cross-border capabilities to prevent cybercrime • Support regional start-ups to boost development of advanced solutions and address white spaces • Set up regional R&D fund for cybersecurity with contribution from member countries	• Align the cybersecurity talent strategy with the national workforce planning agenda • Identify and plan for skills in demand • Develop career pathways around cybersecurity • Foster R&D around emerging threat vectors • Anchor world-class capabilities to facilitate knowledge exchange

Source: A.T. Kearney analysis

market capitalization, this is a small price to pay, especially since other items on the fiscal budget such as defense account for up to 3.4 percent of the region's annual GDP.[30]

Corporate boards and chief information security officers (CISOs) have important roles to play in creating a defense-in-depth culture in their organizations (see figure 31 on page 48). These roles include elevating cybersecurity on the board of directors' agenda and establishing the CISO function as an independent reporting function. CISO responsibilities include establishing group-wide strategies, governance, and conducting value-at-risk assessments. In addition, cybersecurity resilience needs to be extended to business partners through a continuous process of education and inclusion in internal risk audit assessments.

Forging industry alliances and engaging with educational institutions to develop industry-relevant cybersecurity courses will help build a stronger local industry and address capacity and capability gaps.

[30] World Bank based on data for Malaysia, Singapore, Indonesia, Thailand, Vietnam, and Philippines

Figure 31
Action agenda for board and CISO stakeholders

Call-to-action agenda	Corporate board	CISO
Elevate cybersecurity on the corporate agenda	• Table cybersecurity as a crucial board of directors' agenda item • Establish the CISO as an independent function with board-level reporting	• Establish a group-wide cybersecurity strategy, governance, processes, and culture • Implement information security management system compliant with ISO 27001 • Establish working definitions for high-value assets, and identify primary threat vectors
Secure a sustained commitment to cybersecurity	• Set up a cybersecurity investment framework • Embed a value-at-risk mindset in decision making	• Benchmark and track cybersecurity spend vs. IT budget • Set up and monitor cybersecurity metrics on a regular basis • Conduct cyber risk posture assessments • Review opportunities to trim security product portfolio • Conduct regular scenario analysis of value-at-risk
Fortify the ecosystem	• Instill a risk-centric culture	• Engage with peers in and across sectors to share threat intelligence and best practices • Extend cybersecurity policies and processes across the supply chain • Participate in industry alliances with specific focus on emerging threat vectors
Build the next wave of cybersecurity capabilities	• Elevate cybersecurity capacity building as a strategic imperative	• Engage in capacity and capability building initiatives • Interface with academic institutions to design curricula and programs aligned with industry needs • Explore investments in emerging security technologies, such as artificial intelligence and blockchain

Source: A.T. Kearney analysis

Given the current level of readiness of individual ASEAN countries and the magnitude of change needed along with the inherent complexity of creating a coherent region-wide approach, a system based on loose collaboration of national authorities and voluntary exchanges is unlikely to be enough. Only a radical agenda and a stance of active defense with multi-stakeholder engagement can defend the region and capitalize on its collective resources.

Acknowledgements

Contributors to this report: Nikolai Dobberstein, Dieter Gerdemann, Clif Triplett, Gareth Pereira, Germaine Hoe, and Shaamil Azhari

For more perspectives on ASEAN cybersecurity, please contact:

Nikolai Dobberstein, partner, head of Communications, Media & Technology, Asia Pacific, Kuala Lumpur, Malaysia
nikolai.dobberstein@atkearney.com

Dieter Gerdemann, partner, Singapore
dieter.gerdemann@atkearney.com

Gareth Pereira, principal, Malaysia
gareth.pereira@atkearney.com

We would like to thank our partner, Cisco Systems, for the company's invaluable contribution and support to the development of this report.

Appendix A: Security Maturity Model

	Minimal to comply	Security controls focused	Threat focused to protect	Agility to grow the business
Digital transformation strategy	Digital transformation initiated at function or line of business level, but uncoordinated with enterprise strategy.	Digital transformation initiatives are tied to enterprise strategy but with short-term focus and tactical solutions.	Integrated, continuous enterprise wide digital transformation innovation in place.	Digital initiatives transforms market and customers by creating new business models and services.
Security business objectives Objectives, leadership, cross-function, culture	Business-level planning focused on meeting external or internal compliance and legal requirements. Cybersecurity planning is reactive and highly tactical.	Cybersecurity planning focused on protecting core business assets and processes. Security is treated as a silo function and perceived as a barrier to digital transformation initiatives.	Cybersecurity planning aligned with digital transformation objectives to prioritize cybersecurity as a business concern, leveraging accreditation to improve external confidence.	Continuously review and optimizes digital transformation initiatives in alignment with risk assessment. Processes in place for business to govern execution of security throughout business lifecycle.
Digital risk management Strategy, management, governance, compliance, data protection	Risk management seen as a legal issue for meeting external or internal compliance requirements.	Risk management framework employed to baseline risk estimation and guide the application of appropriate security controls. Risk is treated in technical terms.	Economic and external assurance framework and organizational processes applied to continuous risk management. IT risk is seen in context of business risk and a part of strategic requirements.	Data-driven performance metrics in risk estimation and cost-benefit model for use across the business and programs. Risk treated in business opportunity terms.
Security program Policy, architecture, operations, monitoring, controls, SDLC, metrics	Cybersecurity handled by IT, focusing on basic authentication, perimeter-based security, and standard threat protection mechanisms.	Cybersecurity program build around protection of users, data, and applications through application of essential security controls.	Cybersecurity program aligned with risk strategy and employs capabilities to continuously monitor for and respond to threats.	Cybersecurity program implements processes and technical architecture across enterprise. Cybersecurity capabilities enable business processes.
Digital platform Virtualization, cloud, network, mobile, IoT	Basic cybersecurity and asset management solutions for digital platforms to conform with external and internal compliance requirements.	Distinct cybersecurity controls across applied across physical, virtual, internal, and external digital platform environments.	Cybersecurity controls augmented for threat monitoring and response across digital platforms and employ risk model for external services.	Integrated, automated security controls across digital platforms based on a distributed security model that focuses on securing users, data, and applications.

Note: SDLC is systems development life cycle.

Sources: International Data Corporation; A.T. Kearney analysis

Appendix B: ASEAN Countries Cybersecurity Policy Developments

	Strategy	Legislation	Governance and operational entities	Sector-specific and international cooperation	Awareness and capacity-building
ASEAN	⬜ No overarching unifying strategy in place	⬜ No ASEAN-wide laws in place	⬜ No ASEAN-wide governing bodies; Annual ASEAN Ministerial Conference gathers key stakeholders to discuss cybersecurity	🟧 Annual ASEAN CERT Incident Drill to enhance cooperation and coordination among ASEAN CERTs; ASEAN Cybersecurity Industrial Attachment Programme	🟧 ASEAN Cyber Capacity Programme (launched 2017) to develop technical, policy and strategy building capabilities; no collaborative education strategy
Singapore	🟦 National Cybersecurity Strategy in place (2016) with definition of CII sectors	🟧 Cybersecurity Bill drafted (2017); Computer Misuse and Cybersecurity Act (1993, amended 2017); Personal Data Protection Act	🟦 Cyber Security Agency of Singapore; NCIRT in place; MAS for financial services	🟧 Singapore “soft lead” for ASEAN cooperation; multiple bilateral agreements and MoUs; MAS coordinates financial sector collaboration	🟦 Comprehensive awareness strategy part of National Cybercrime Action Plan (2016); holistic capacity-building strategy in place; professionalizing data protection officers
Malaysia	🟦 National Cybersecurity Policy launched (2016) with definition of CNII sectors	🟧 New cybersecurity law being drafted (2017); Computer Crime Act (1997); Personal Data Protection regulation	🟧 MDEC; Cybersecurity Malaysia; entities under Cybersecurity Malaysia include MyCERT, MyCC, MyCSC, etc.	🟧 Multiple international bilateral agreements and MoUs; public–private and sector-specific cooperation under NCSP	🟦 CyberSAFE (public awareness) and CyberGuru (technical knowledge); MDEC’s strategic talent development; Cybersecurity Malaysia’s local vendor development
Thailand	🟧 National cybersecurity strategy drafted	🟧 National Cybersecurity Bill proposed (2017); Computer Crimes Act (2007, amended 2017); Personal Data Protection Act	🟧 National Cybersecurity Committee (proposed), aims to protect CNII sectors; ThaiCERT	⬜ No overarching strategy in place; Digital Forensics Center coordinates international training cooperation	🟧 Digital Forensics Center provides services and training; MDES currently promotes awareness; no overarching strategy in place
Indonesia	⬜ No national cybersecurity strategy	⬜ No specific cybersecurity laws; electronic information and transactions law; data protection regulation	🟧 BSSN recently launched (2017) to consolidate activities, not yet fully formed; GOV CSIRT and ID-CERT; ID-SIRTII/CC	⬜ Part of BSSN’s agenda, no overarching strategy in place; few bilateral partnerships, for example with Japan	🟧 Part of BSSN’s agenda, no overarching strategy in place; fragmented training and awareness by ID-SIRTII/CC and ID-CERT
Philippines	🟧 National Cybersecurity Plan 2022 launched (2017) with definition of CII sectors	🟧 No cybersecurity-specific laws; Cybercrime Prevention Act (2012); Data Privacy Act (2012)	🟧 DICT is leading agency; CICC monitors cybercrime and oversees CERT	🟧 Protection and management of CII under NCP 2022; CICC to facilitate international and business-sector cooperation	🟧 Under NCP 2022 agenda, no current strategy in place; plan to establish CISO program in government agencies
Vietnam	⬜ No national cybersecurity strategy	🟧 Law on cybersecurity drafted (2017); no cybercrime or data protection laws in place	🟧 MIC leads; AIS leads activities on information security; VNCERT; VNISA investigations, trainings, and coordination	⬜ No strategy in place; VNCERT and VNISA work with private sector	🟧 No overarching strategy in place; VNISA organizes info security seminars, events; MIC coordinates awareness and training
Rest of ASEAN	⬜ No strategy in place	⬜ Largely absent; some countries such as Laos are drafting cybercrime laws	⬜ Largely no governance bodies; CERTs typically act as national cybersecurity agency: response, awareness, etc.	⬜ No public–private or sector-specific focus, except Cambodia’s emphasis on financial sector; fragmented international cooperation	⬜ No education strategy; CERTs responsible for general awareness

⬜ Absent 🟧 Initiated or proposed 🟦 Established and operational

Notes: CERT is computer emergency response team; CII is critical information infrastructure; CNII is critical national information infrastructure; CICC is the Cybercrime Investigation and Coordinating Center; VNISA is the Vietnam Information Security Association; NCIRT is National Cyber Incident Response Teams; MAS is Monetary Authority of Singapore; MOUs are memorandums of understanding; BSSN is Badan Siber dan Sandi Negara; MIC is Ministry of Information and Communications; AIS is American International School.

Source: A.T. Kearney analysis

Appendix C: The Networking Academy's Learning Portfolio

🟠 Aligns to certification

🔵 Instructor training required

🟣 Self-paced

Collaborate for impact				
Introduction to packet tracer	Packet tracer	Hackathons	Prototyping lab	Internships

	Exploratory	Foundational	Career-ready
Networking		🔵 **Networking Essentials** 🟣 **Mobility Fundamentals**	🔵🟠 **CCNA R&S:** Introduction to Networks, R&S Essentials, Scaling Networks, Connecting Networks 🔵🟠 **CCNP R&S:** Switch, Route, TShoot **Emerging Tech Workshop:** Network Programmability Using Cisco APIC-EM*
Security	🟣 **Introduction to Cybersecurity**	🟣 **Cybersecurity Essentials** **IoT Security***	🔵🟠 **CCNA Security** 🔵🟠 **CCNA Cyber Ops***
IoT and analytics	🟣 **Introduction to IoT**	🔵 **IoT Fundamentals:** Connecting Things, Big Data and Analytics Hackathon Playbook	
OS and IT	🟣 **NDG Linux Unhatched**	🟠🟠 **NDG Linux Essentials** 🔵🟠 **IT Essentials**	🟠 **NDG Linux I** 🟠 **NDG Linux II**
Programming		🟠 **CLA: Programming Essentials in C** 🟠 **CPA: Programming Essentials in C++** 🟠 **PCA: Programming Essentials in Python*** **Emerging Tech Workshop:** Experimenting with REST APIs Using Cisco Spark*	🟠 **CLP: Advanced Programming in C*** 🟠 **CPP: Advanced Programming in C++**
Business	🟣 **Be Your Own Boss**	🟣 **Entrepreneurship**	
Digital literacy	🟣 **Get Connected**		

Note: CCNA R&S is Cisco Certified Network Associate Routing and Switching.

Sources: Cisco; A.T. Kearney analysis

Table of Figures

ATKearney

A.T. Kearney is a leading global management consulting firm with offices in more than 40 countries. Since 1926, we have been trusted advisors to the world's foremost organizations. A.T. Kearney is a partner-owned firm, committed to helping clients achieve immediate impact and growing advantage on their most mission-critical issues. For more information, visit www.atkearney.com.

Americas

Atlanta
Bogotá
Boston
Calgary
Chicago
Dallas
Detroit
Houston
Mexico City
New York
San Francisco
São Paulo
Toronto
Washington, D.C.

Asia Pacific

Bangkok
Beijing
Brisbane
Hong Kong
Jakarta
Kuala Lumpur
Melbourne
Mumbai
New Delhi
Perth
Seoul
Shanghai
Singapore
Sydney
Tokyo

Europe

Amsterdam
Berlin
Brussels
Bucharest
Copenhagen
Düsseldorf
Istanbul
Lisbon
Ljubljana
London
Madrid
Milan
Moscow
Munich
Oslo
Paris
Prague
Rome
Stockholm
Vienna
Warsaw
Zurich

Middle East and Africa

Abu Dhabi
Doha
Dubai
Johannesburg
Riyadh

For more information, permission to reprint or translate this work, and all other correspondence, please email: insight@atkearney.com.

The signature of our namesake and founder, Andrew Thomas Kearney, on the cover of this document represents our pledge to live the values he instilled in our firm and uphold his commitment to ensuring "essential rightness" in all that we do.

A.T. Kearney Korea LLC is a separate and independent legal entity operating under the A.T. Kearney name in Korea.

A.T. Kearney operates in India as A.T. Kearney Limited (Branch Office), a branch office of A.T. Kearney Limited, a company organized under the laws of England and Wales.