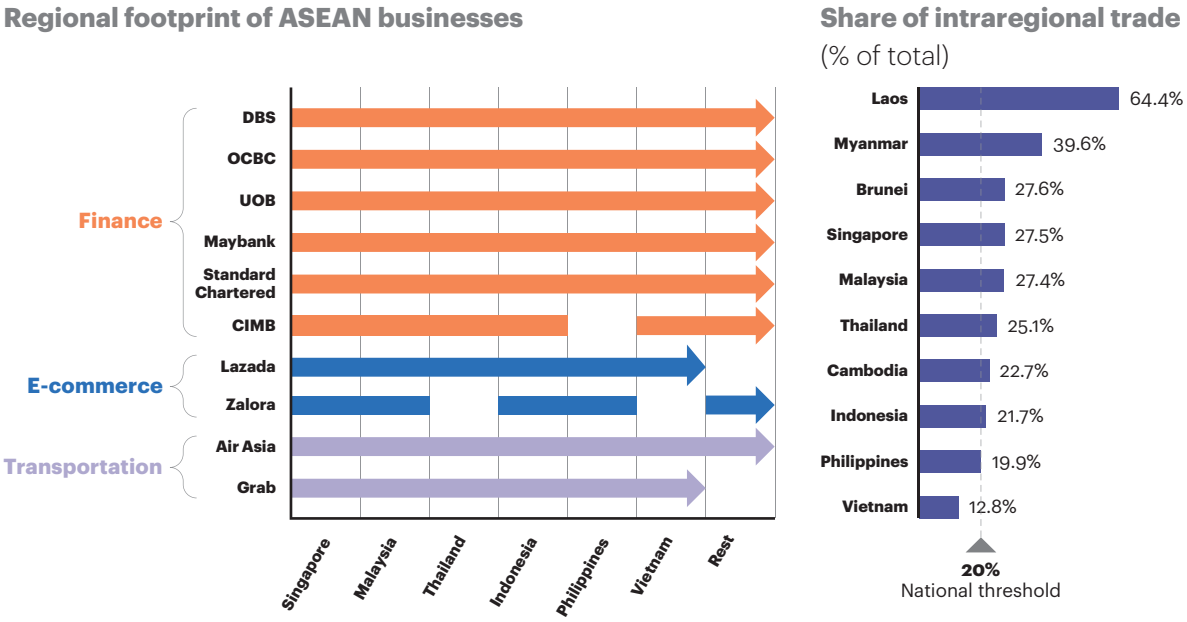
2.1 The cybersecurity challenge is likely to get more complex

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



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

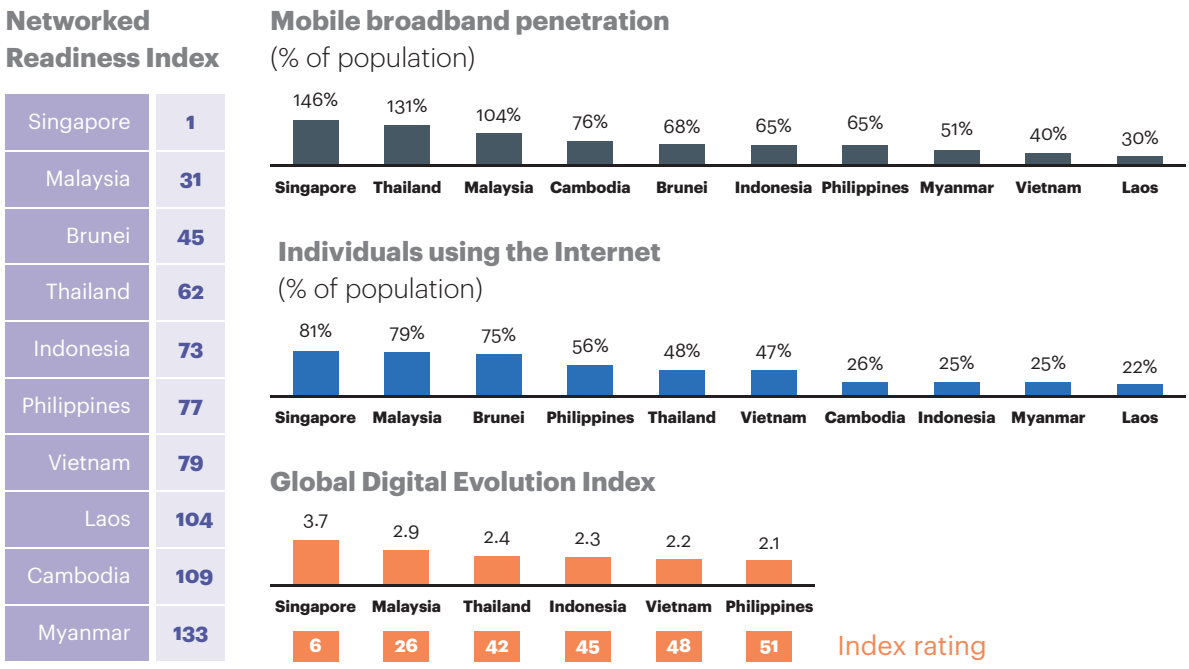
Systemic cyber risk recently came under scrutiny with the discovery of three separate hacking incidents against member institutions connected to the SWIFT network at banks in Bangladesh, Vietnam, and Ecuador, accounting for more than $90 million in stolen funds. The attacks demonstrated that the applications 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.

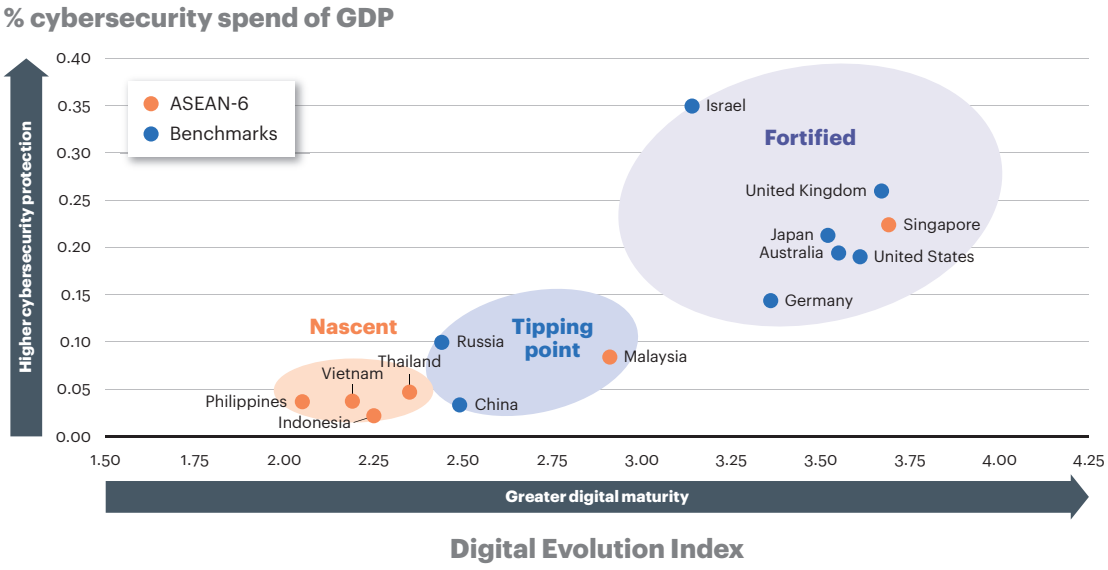
The region's lower level of investment can be attributed to several factors. First, there is a lack of policy-level guidance and clarity on prudent practices in terms of cybersecurity spend. Second, as highlighted earlier, cybersecurity is considered to be an IT issue and not a business risk, thereby 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*

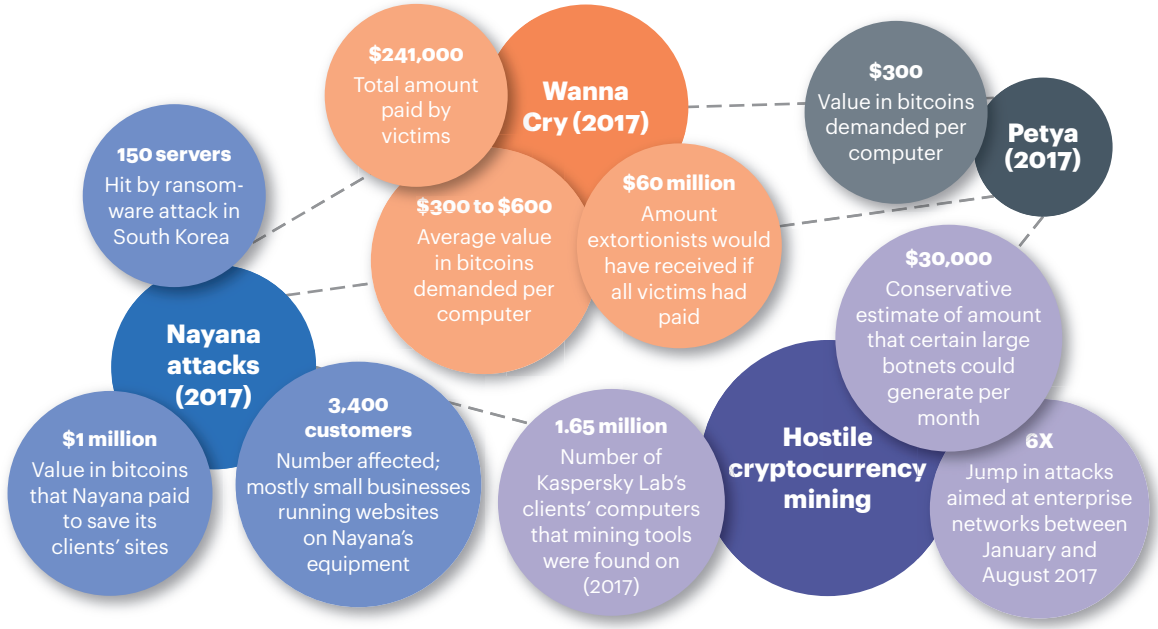
evade detection and to secure their malicious activities. The overall increases in encrypted traffic and attacks render threat recognition difficult and create gaps in traditional, layered-defense systems because intrusion prevention fails to occur.

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



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.