FinTech Cybersecurity: An ASEAN Outlook 2021
## INDEX

**Executive Summary**  
01

**Introduction**  
06

**FinTech in ASEAN**  
08

› FinTech: Improving financial inclusion in ASEAN  
10

› Digitalization and access to finance for SMEs  
11

› Innovations for the region and the world  
13

› FinTech and cybersecurity: A relationship worth understanding  
13

**Cybersecurity Ecosystem in ASEAN**  
16

**ASEAN FinTech Cybersecurity Matrix**  
19

**Findings of the PayPal ASEAN Cybersecurity Survey**  
26

**Recommendations**  
33

**Appendix: Country Cybersecurity FinTech Ecosystem Snapshots**  
43

**References**  
63
Southeast Asia's FinTech sector is growing at an exponential rate. In 2019 alone, digital financial services in the region generated USD 11 billion of annual revenue – a figure that is expected to more than triple to reach USD 38 billion by 2025.\(^1\)

The FinTech sector offers immense benefits for ASEAN. Primary amongst these is the potential for enhanced financial inclusion offered by innovative technological solutions. According to a 2016 KPMG report, reaching the unbanked population in Southeast Asia could result in an increase of economic contribution of USD 35 billion by 2030.\(^2\) In the aftermath of COVID-19, the ASEAN region, like the rest of the world, is focusing on economic recovery.\(^3\) The ASEAN economies’ dependence on trade with other economies that have also been badly affected; collapse in oil prices that have impacted the regional oil and gas economy; decline in tourism; and plummeting domestic demand have led to negative growth rates in economies across the region.\(^4\) As a result, the role of digitalization and technology solution providers in sustaining the regional economy is more important than ever.

The small and medium enterprise (SME) sector, that accounts for between 89% and 99% of total establishments and between 52% and 97% of total employment in the ten ASEAN Member States, is the backbone of the regional economy.\(^5\) FinTechs provide numerous technology-enabled solutions to the region’s booming SME sector in the form of innovative payment mechanisms, credit products, fraud protection systems, and data-enabled financial risk assessment solutions. Global payment service providers like PayPal enable SMEs in the region to expand their reach and sell to customers around the world.

Moreover, FinTechs in the region are catalysts for innovation across the financial, technological, and SME ecosystems. Interest in these FinTechs from global players also creates global networks for collaboration and partnership.

As ASEAN focuses on recovery from COVID-19, there is increased impetus for investments in digital transformation to nurture the regional entrepreneurial ecosystem, as well as to connect government, business, and citizens real-time. FinTechs are an important part of this chain and consumer trust in them is paramount to the success of these efforts. Consumer trust, however, can be swiftly eroded by the actions of cybercriminals and malicious actors who target vulnerable users globally, predominantly with the aim of financial gain. Globally, cybercrime causes trillions of dollars in losses each year.

As the FinTech sector becomes a vital contributor to the ASEAN regional economy, its growth as well as the newly digitalized populations of the region render it an attractive target for cybercriminals. According to the 2020 ASEAN Cyberthreat Assessment Report by Interpol, “No country or organization in the ASEAN region is spared the threat of fast-evolving cybercrime. Given their position among the fastest-growing digital economies in the world, member countries in ASEAN have become a prime target for cyberattacks.”\(^6\)
“No country or organization in the ASEAN region is spared the threat of fast-evolving cybercrime. Given their position among the fastest-growing digital economies in the world, member countries in ASEAN have become a prime target for cyberattacks.”

Source: 2020 ASEAN Cyberthreat Assessment Report by Interpol

In the absence of cyber resiliency and adequate defenses, innovative products and services can be the very medium through which malicious actors succeed in defrauding their victims. Additionally, the newly digitalized and the recently financially included are especially vulnerable to their attacks - a stark truth that was underscored by online scams perpetrated during the COVID-19 pandemic.

As a result, regulators in the region have placed great emphasis on cybersecurity and in recent years, we have seen several efforts by ASEAN as a union as well as by its member states to build up resiliency. However, as many of these measures follow a one-size-fits-all approach across sectors, the burgeoning FinTech ecosystem in the region often finds that well-meaning regulations may place rather tall hurdles in their race towards innovation and growth.

Recognizing the challenges in reconciling regulatory flexibility with prioritizing cyber hygiene for enhanced cyber resiliency in the regional fintech ecosystem, PayPal has collaborated with a boutique consulting firm, TRPC, to share this ASEAN FinTech Cybersecurity Study. Through this study, we seek to better understand the impact of cybersecurity regulations on FinTech firms in the region and to provide a balanced perspective on ways to achieve sustainable growth in the ASEAN FinTech sector without compromising safety and security of customers and their finances.

In order to do so, the study draws on the following original sources in addition to an extensive literature review:

- The 2019 PayPal ASEAN FinTech Cybersecurity Survey which was conducted amongst 44 FinTech firms across ASEAN
- The PayPal ASEAN FinTech Cybersecurity Matrix which assesses the cybersecurity regulatory ecosystem in the region

Through our survey, we found that FinTech firms in the region are diverse in size and scope. While these firms care deeply about cybersecurity, they are spending disproportionately on cybersecurity compliance — without necessarily receiving commensurate returns in terms of cyber resilience. We also found that there is an immediate need for enhanced public private engagement forums where FinTech firms and governments can collaborate on issues pertaining to cybersecurity and financial risk in order to nurture and maintain trust in the ecosystem.
THE MATRIX ASSESSES THE ASEAN MEMBER STATES UNDER FIVE KEY PILLARS:

The ASEAN nations are at varying stages of cyber readiness with a diverse regulatory environment across the region, varying levels of national engagement in capacity building for the FinTech industry, as well as an ASEAN wide cybersecurity skill gap challenge faced by FinTech firms. An encouraging result, however, is the presence of numerous bilateral and multilateral agreements across the region, many of which indicate the commitment to collaborate on resolving these issues.

KEY RECOMMENDATIONS:

*Develop principles-based cybersecurity regulations and frameworks driven by outcomes and evolving risks*

Over two-thirds of the respondent firms in our survey reported that compliance requirements are the key drivers for their investments in cybersecurity. At the same time, it is an oft-quoted truism amongst cybersecurity professionals that compliance does not equal security. ASEAN needs to move away from a rigid box-ticking approach towards cybersecurity to one that incentivizes investments in cyber resilience. We recommend risk-based requirements that can help ease undue regulatory burden while also ensuring that compliance boosts customer safety.
Enable adoption of strong cyber hygiene through ASEAN-level compatibility as well as alignment with global security standards

ASEAN FinTech has the opportunity to reap the benefits of regional economies of scale. However, this can only be made possible if cybersecurity regulations and norms across the region are standardized.

Cyberthreats are cross-border in nature and defending against them requires a collaborative approach. ASEAN should create an evolving regional cybersecurity framework that is aligned with global standards and practices. Such a framework would enable exchange of innovative cyber defense measures and expertise and ensure the retirement of legacy processes that hinder technology adoption.

Establish comprehensive programs for training and awareness on fraud and security best practices for general public and businesses

Even the most sophisticated defense systems, the most advanced infrastructure, and the most rigorous cybersecurity laws cannot protect an ill-informed end-user. Newly-digitalized consumers are especially vulnerable to cyberthreats and scams. As a result, there must be a concerted effort between governments, businesses, and academic institutions to educate the public about cyberthreats and the means to protect themselves against them. We recommend the establishment of a region-wide repository of cyber scams and threats for information sharing.

Promote a multilateral regulatory sandbox for knowledge sharing and risk management in the FinTech ecosystem

Sandboxes enable regulators to foster innovation in the FinTech ecosystem while also understanding potential risks of new products and the ways to protect their citizens and financial systems against such risks. Each ASEAN nation should host its own national sandbox in order to fully realize the benefits and the potential of the FinTech sector while also identifying country-specific risks and challenges.

Furthermore, ASEAN governments can implement and encourage internationally recognized best practices on anti-virus, patching, and anti-phishing standards.

Invest in developing a strong cybersecurity workforce to support a resilient ecosystem

Even as the cyberthreat landscape continues to expand, about 3.5 million cybersecurity positions globally are expected to go unfilled in 2021. In our survey, we found that more than a quarter of FinTech firms do not have a dedicated cybersecurity expert in their organization. We recommend ASEAN governments to work closely with the private sector to boost talent development and support the needs of the growing financial services industry. An important first step towards planning for the future would be the introduction of cybercrime mitigation, data analytics, automation technologies and cybersecurity skills in the primary and secondary
Encourage public-private partnerships in research, hiring and information sharing

Multi-stakeholder consultative processes must become the norm in the creation of new cybersecurity regulations and policies. We encourage the creation of public private forums for stakeholders from a diverse range of institutions to consult with each other on new regulations, training needs, and to share best practices. Additionally, we encourage improved collaboration on research efforts that bring together experts across the public, private, and academic sectors to create innovative solutions in cyber defense.
INTRODUCTION

Technology advancements are enabling financial service providers to serve more customers at a lower cost, provide broader reach, and with greater efficiency. The digitalization of financial services has resulted in the development of new types of products, services, and platforms. It is also creating new sources of economic growth, particularly for Micro Small and Medium Sized Enterprises (MSMEs), by providing access to global capital and markets.

From mobile digital wallets to automated insurance advisors and the provision of microloans to small and medium enterprises (SMEs), the prevalence of FinTech is rapidly growing in economies that were predominantly cash-based just a few years ago. According to the World Bank, digital financial services such as mobile payment services and digital saving accounts are reaching significant scale in both emerging and mature economies.

In ASEAN, the FinTech sector has seen tremendous growth. Southeast Asian FinTechs such as GoJek and Grab rose from humble beginnings to become digital economy juggernauts. Inspired by their success and attracted by the region’s market potential, new players regularly enter the fray. As of 2019, there were more than 490 FinTech startups registered in Singapore alone.

In 2019, there were more than 490 FinTech startups registered in Singapore alone.

In ASEAN, the FinTech sector has seen tremendous growth. Southeast Asian FinTechs such as GoJek and Grab rose from humble beginnings to become digital economy juggernauts. Inspired by their success and attracted by the region’s market potential, new players regularly enter the fray. As of 2019, there were more than 490 FinTech startups registered in Singapore alone.

The Southeast Asian FinTech story is distinguished by interest from investors all over the world. FinTech companies in Southeast Asia raised over USD 8.9 billion across 475 deals between 2015 and 2019. In 2019 alone, FinTech investment in ASEAN reached a record USD 4.1 billion across 130 deals. In the same year, digital financial services generated USD 11 billion of annual revenue across Southeast Asia – a figure that is expected to more than triple to reach USD 38 billion by 2025.

This burgeoning FinTech scene has immense potential. More than half of the adult population in the ASEAN region is still unbanked, with large segments of the population living in remote rural areas. In 2016, a regionwide KPMG study found that only 27% of the population across Southeast Asia had a bank account. While this is expected to have risen to 47% in 2018, millions of people remain unbanked or underserved in the region. Therefore, the region has some way to go in ensuring financial inclusion. Many of the access issues caused by the geographic fragmentation of the region can be overcome through technology.

**COVID-19 has been a catalyst for digitalization as businesses are rapidly adapting their strategies to evolve with changing consumer behaviors.**

COVID-19 has been a catalyst for digitalization as businesses are rapidly adapting their strategies to evolve with changing consumer behaviors. We have witnessed a tremendous shift in commerce and financial services and the global pandemic has revealed gaps in business continuity plans and IT operations. The rapid pace of digitalization globally has also spurred on governments across the world to explore emerging possibilities in FinTech such as the need for nationalized instant payment systems, dissemination of government subsidies through digital payments, and development of central-bank issued digital currencies for cross-border trade. The pandemic has also led to the emergence of new cyberthreats and attacks created around the themes of COVID-19 government subsidies and remote working.
Maintaining robust cybersecurity and resiliency against cybercrime are key for businesses to scale and thrive in the ASEAN digital economy. Without the assurance that their money and data are safe, customers will not be able to place their trust in the digital economy. At the same time, cybercriminals increasingly use sophisticated and complex attack vectors to target individuals, businesses, and even nation states.

ABOUT THE STUDY

In response to new financial service offerings across the region, ASEAN government agencies and regulators have introduced or considered new regulations and frameworks for the FinTech industry. The aim of this ASEAN FinTech Cybersecurity Study (“the study”) is to understand the implications of regulations on the growth, strategy, and resource allocation of FinTech firms in this region. This report is commissioned by PayPal and authored by PayPal and TRPC, a boutique consulting firm specializing in telecommunications and information technology with an emphasis on the Asia Pacific region. The purpose of this study is to assess cyber readiness, with an emphasis on cyber regulations and other regulatory efforts within each of the ASEAN nations, and to provide an objective perspective on efforts to balance the growth of FinTechs in the region with the safety and security of customers and their finances.

In order to do so, this study examines various aspects of ASEAN’s cybersecurity ecosystem as it relates to FinTech companies in the region. The foundation of this study is a survey that was conducted among ASEAN fintech firms in late 2019. The PayPal ASEAN FinTech Cybersecurity Survey was launched to gauge ASEAN FinTech firms’ views on cybersecurity-related challenges and opportunities as well as the rapidly evolving cybersecurity regulatory landscape in the region. Over 40 firms responded to the survey.

Based on the results of the survey, and complemented by open source research, we created the PayPal FinTech Cybersecurity Matrix (“the matrix”) to assess and analyze the cybersecurity regulatory ecosystem in the region for FinTech companies in the ASEAN member states.

The matrix consists of 12 questions grouped under five pillars:
- Legal and Policy
- Knowledge and Skills
- Investment and Spending
- Cyber Hygiene and Financial Literacy
- Stakeholder Communication and Collaboration

The matrix is designed as a standalone reference in alignment with similar efforts such as ITU’s Global Cybersecurity Index.⁶

Additionally, the findings of the survey and the matrix are supplemented by extensive literature review and insights drawn from PayPal’s own experience, both globally and regionally. Drawing from these four sources (the survey, the matrix, literature review, and PayPal’s experience), we conclude this study with recommendations for consideration by key decision makers in the region.
FINTECH IN ASEAN

The FinTech industry is at the forefront of ASEAN’s economic growth, with estimates for the region’s digital economy showing a rise from USD 100 billion in 2019 to USD 300 billion in 2025. Even amidst a general downturn in startup funding due to the COVID-19 pandemic in 2020, Southeast Asian FinTech startups raised $1.25 billion in aggregate across 125 deals. For the purposes of this study, we define FinTech companies as "organizations combining innovative business models and technology to enable, enhance, and deliver financial services." FinTech companies have played an important, if not leading role in the digitalization of the Financial Services Industry (FSI) in Asia.

One of the fastest growing segments of FinTech is digital payments, especially in ASEAN where there has been rising adoption of digital payments. Figure 1 represents the growth of digital financial services in the region and the steady increase of digital payments from 2014 to 2017 across the region. According to the 2019 Temasek-Google-Bain e-economy SEA report, the adoption of digital payments in ASEAN is expected to cross USD 1 trillion by 2025.

Figure 1:
Proportion of adult population that had made or received a digital payment in the past year

<table>
<thead>
<tr>
<th>Country</th>
<th>2014</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indonesia</td>
<td>22%</td>
<td>35%</td>
</tr>
<tr>
<td>Cambodia</td>
<td>18%</td>
<td>16%</td>
</tr>
<tr>
<td>Myanmar</td>
<td>4%</td>
<td>8%</td>
</tr>
<tr>
<td>Malaysia</td>
<td>58%</td>
<td>70%</td>
</tr>
<tr>
<td>Philippines</td>
<td>20%</td>
<td>25%</td>
</tr>
<tr>
<td>Singapore</td>
<td>87%</td>
<td>90%</td>
</tr>
<tr>
<td>Thailand</td>
<td>33%</td>
<td>62%</td>
</tr>
<tr>
<td>Vietnam</td>
<td>18%</td>
<td>23%</td>
</tr>
</tbody>
</table>

Note: No data available for Brunei Darussalam. Data unavailable for Laos PDR for 2014. In 2017, the figure was 13%. Source: The World Bank Global Findex Database 2017
While the FinTech ecosystem in ASEAN is dominated by payments and mobile wallets, constituting nearly half of the industry by some estimates, there are players offering other services and products such as lending, financial comparison and retail investment.\textsuperscript{20}

The rise of FinTech solutions in ASEAN is underpinned by the rapid adoption of technology, high mobile and internet penetration, and an increasingly educated young and urbanized population.

The rise of FinTech solutions in ASEAN is underpinned by the rapid adoption of technology, high mobile and internet penetration, and an increasingly educated young and urbanized population. The region has been underserved by traditional financial institutions, and increasing digital connectivity and upward income mobility in the region are leading customers towards the adoption of FinTech solutions. As a result, ASEAN now boasts numerous homegrown FinTech service providers whose first-hand understanding of the gaps in the ASEAN FinTech ecosystem enable them to provide targeted solutions to fill these gaps.

In addition, with the recognized growth potential of ASEAN economies, an increasing number of investors and innovators are attracted to the region.

Table 1:
Factors driving FinTech growth, and economic impact of FinTech on ASEAN

<table>
<thead>
<tr>
<th>FACTORS DRIVING FINTECH GROWTH</th>
<th>IMPACT OF FINTECH INNOVATION ON ASEAN ECONOMIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rapid adoption of technology</td>
<td>Catalyst for increased economic activity from financial inclusion, and new services, e.g. reaching the unbanked, increasing youth banking</td>
</tr>
<tr>
<td>High internet and mobile penetration</td>
<td>Improved access to credit and finance for SMEs</td>
</tr>
<tr>
<td>Increasingly urbanized, tech savvy population</td>
<td>Data and analytics provide SMEs with information on consumer behaviors to improve profitability</td>
</tr>
<tr>
<td>Financial inclusion policies targeting traditionally underserved populations - e.g. young, rural, unbanked and underbanked</td>
<td>Innovative business ideas and the possibility of being the &quot;next unicorn&quot; inject venture capital and drive entrepreneurial spirit</td>
</tr>
</tbody>
</table>
FinTech companies have the potential to accelerate financial inclusion in the region, resulting in increased economic activity. It is estimated that leveraging digital technology to increase financial inclusion could boost GDP by 2% to 3% in markets such as Indonesia and the Philippines, and as much as 6% in Cambodia. According to a 2016 KPMG report, reaching the unbanked population in Southeast Asia could result in an increase of economic contribution of USD 35 billion by 2030.

Traditional financial services are unable to bridge this gap for a number of reasons. First, as ASEAN is a geographically diverse region, traditional banking models face challenges in reaching customers in remote areas. Underbanked communities often make small, frequent transactions which are encumbered by traditional transaction fees and inefficiency in the commercial banking system. Additionally, financial needs differ from entity to entity and are determined by multiple socio-economic and even geographic factors. Traditional providers are ill-equipped to offer bespoke products that can cater to such individualized needs.

However, FinTech can address many of these challenges. It is estimated, for instance, that globally, two-thirds of unbanked individuals have access to a mobile phone. The right FinTech solutions can enable these individuals to join the financial system with the aid of their mobile devices.

FinTech companies have focused on payments and mobile wallet solutions as a first step towards financial inclusion. The results have been impressive. In 2019, 61% of consumers in Vietnam used some form of mobile payment (up from 37% in 2018), while most consumers in Indonesia, Malaysia, the Philippines, Singapore, and Thailand have made purchases through social media platforms like Instagram and Facebook.

Additionally, homegrown FinTech players in the region are also leveraging their deep understanding of local contexts and country-specific challenges to provide innovative and highly tailored solutions to the unbanked and underbanked. For example, Julo, an Indonesian FinTech provides tailor-made Peer-to-Peer (P2P) lending solutions targeted at the unbanked population.

FinTechs in the region, with their can-do spirit and out-of-the-box thinking have identified the market opportunity that lies in serving the needs of the bottom-of-the-pyramid income segments that are often overlooked by traditional financial institutions. They recognize that the underbanked and unbanked require services that go beyond deposit and products. In Malaysia, for instance, mobile app HelloGold makes investing in gold accessible to the masses by allowing its customers to buy and sell gold in any amount from RM1 (USD 0.23) – providing the opportunity for customers from all walks of life to invest in a commodity that was previously restricted to the middle and upper income groups.

Therefore, FinTechs have the power to expand beyond “financial inclusion” and encompass the broader goal of universal financial health – which goes beyond mere account ownership to ensuring that these accounts are useful, versatile, and appropriate to individualized needs.

**FinTechs have the power to expand beyond “financial inclusion” and encompass the broader goal of universal financial health – which goes beyond mere account ownership to ensuring that these accounts are useful, versatile, and appropriate to individualized needs.**
At the same time, realizing these goals will also require a concerted effort across all ecosystem players. Liquidity and timely access to funds is of great importance to the financially underserved. FinTech’s ability to service them is therefore heavily reliant on technology adoption and the availability of digital infrastructure.

Additionally, continuous regulatory oversight is required to ensure that any operational or systemic risks, especially around cybercrime, are managed effectively. According to S&P Global, the recent suspension of services of a payment services provider affected vulnerable groups such as migrant workers and people relying on charities for welfare assistance during the COVID-19 crisis. Disruptions in access to services or products could have devastating effects on customers’ livelihoods – thereby eroding trust in the ecosystem.

DIGITALIZATION AND ACCESS TO FINANCE FOR SMALL AND MEDIUM ENTERPRISES

SMEs are the backbone of Southeast Asian economies; but the ASEAN SME sector continues to face funding and credit challenges. The SME loan to GDP ratio is low in most ASEAN nations, with figures ranging from 3% to 34%. Banks in the region have hesitated to finance SMEs as traditional credit risk assessments often put in place stringent requirements that SMEs are unable to meet, especially in the early stages of their growth.

For first-time entrepreneurs, startup capital can be especially difficult to obtain. Most traditional financial institutions rely on long-established models of credit risk assessment which require extensive financial history data or proof of collateral. Particularly in developing countries, there are many “thin-file” customers who cannot furnish such data records. The limited availability of traditional data for credit risk assessment impacts banks’ lending decisions, driving higher interest rates for SMEs or limiting financing outright.

Technology can also enable the collection and use of alternative data that can enhance credit analysis methods to provide a more holistic understanding of small businesses that might otherwise be disadvantaged by limited credit history. FinTech companies can address this funding gap in many ways. Some FinTechs can play the role of intermediaries connecting emerging SMEs and startups with interested investors. For instance, Amartha is a P2P lending marketplace in Indonesia which directly connects micro entrepreneurs seeking working capital with investors. Singapore-grown FinTech InvoiceInterchange provides working capital solutions for business growth through the provision of an invoice financing marketplace - enabling businesses to overcome cash flow fluctuations by selling their outstanding invoices to a network of investors.

FinTechs also enable SMEs to obtain better access to loans by providing alternatives to traditional credit risk-assessment by using digital payment platforms and analytics to provide a more holistic picture of an enterprise’s financial health and prospects. Innovation in SME financing facilitated by FinTechs has several long-term benefits including enhancing resiliency and agility during times of crisis or volatility.

Innovation in SME financing facilitated by FinTechs has several long-term benefits including enhancing resiliency and agility during times of crisis or volatility.
The ability to participate in global trade enables merchants on global platforms like PayPal to outperform their counterparts who may be focused on domestic markets alone. In Vietnam, between 2013-2017, exports by Vietnamese small businesses on the PayPal platform grew ninefold.

Additionally, they provide an avenue for new enterprises to build credit history that can unlock the doors to more substantive loans to support their long-term growth.29

Global payment service providers like PayPal enable SMEs in the region to sell to customers around the world.

Additionally, global payment service providers like PayPal enable SMEs in the region to sell to customers around the world. PayPal operates a two-sided global technology platform that facilitates the processing of payment transactions for over 361 million30 active account holders globally. PayPal enables consumers to safely exchange funds with merchants using a variety of funding sources. PayPal also offers merchants an end-to-end payments solution that provides authorization and settlement capabilities, and fast access to funds. PayPal’s consumers engage in cross-border shopping and merchants extend their global reach while reducing the friction in cross-border trade. Through the PayPal platform, merchants in ASEAN are able to sell to customers in more than 200 markets.

The number of export destinations reached by PayPal small businesses in Vietnam increased from 132 in 2013 to 169 in 2017, a 28% increase. In fact, SMEs on PayPal had more trade partners than their offline counterparts in 2015 and 2016, reaching consumers in 14 and 18 more markets, respectively.31

From 2013 to 2017, exports by Vietnamese small businesses on the PayPal platform grew by 9 times
Apart from creating an inclusive financial ecosystem, FinTech companies are catalysts for innovation in ASEAN. With fresh ideas and solutions on how financial services can operate outside legacy infrastructures, they can address a range of issues.

For example, unicorns like Grab and Gojek are leading access to financial services, at a scale that traditional banking has never been able to achieve. It is estimated that half of Gojek’s 100 million monthly transactions are processed through their e-wallet, GoPay. GrabPay now allows low-cost money transfer services, enabling users to remit money securely in another country at far lower costs than using traditional banking.

In addition to this, FinTechs that have proven themselves in the complex and competitive arena of the Southeast Asian digital economy attract investments from global players who can support them in their aspirations to extend beyond the region. In June 2020, for instance, PayPal announced a commercial partnership with Gojek through which PayPal’s payment capabilities will be integrated into Gojek’s services in order to allow customers of GoPay, Gojek’s digital wallet, to gain access to PayPal’s network of more than 25 million merchants around the world.

Establishing a conducive regulatory environment is important to support the growth of these FinTech businesses, which offer opportunities for catalyzing and accelerating more innovation and economic development in the ASEAN region.

**FINTECH AND CYBERSECURITY: A RELATIONSHIP WORTH UNDERSTANDING**

It is estimated that on average, about USD 608 billion – nearly 1% of global GDP – could be lost to cybercrime each year. The Asia-Pacific region alone accounts for close to a third (32.9%) of that amount. Cyberattacks could end up costing the top 1,000 companies in Southeast Asia as much as USD 750 billion in market capitalization.

The COVID-19 outbreak has increased reliance on internet for essential services, giving fraudsters the opportunity to perpetrate cybercrime through phishing attacks and social media scams. According to McAfee, as the pandemic began to spread across the world, malicious actors used phishing emails leveraging terms such as “COVID-19” and “Coronavirus” to entice users to click on links or attachments that would then steal their personal data. Scammers also impersonated organizations such as the US Governments Small Business Administration (SBA) to target small businesses by purportedly offering guidance on applying for SBA loans while in fact infecting their devices with...
Malware and trojans. McAfee also found that over the first 13 weeks of the pandemic, the number of COVID-19 related bogus websites increased from 1,600 to over 39,000. These websites explicitly targeted customers seeking to purchase medical supplies and personal protective equipment. According to a report from Google, there was a 350% increase in active phishing websites from January to March in 2020. PayPal observed an increase of more than 250% in the number of phishing attempts between Q1 and Q2 of 2020.

Firms in the financial sector are particularly vulnerable due to the value of the financial data they handle. A 2019 BCG study found that financial services firms are 300 times more likely to face a cyberattack than other companies. Additionally, the Identity Theft Resource Center concluded that “Payment card and account information are highly targeted and often the most common information obtained in a data breach.”

Emerging economies in the region are being targeted by malicious actors across the globe in cyberattacks. Malicious actors target vulnerable groups with low levels of cyber and financial literacy to plan their attacks. Taking advantage of users’ who are not knowledgeable about strong cyber hygiene practices, they are able to obtain financial account information – with dire consequences on the victim’s financial health. For the recently financially included, this can mean the loss of their entire life savings and a permanent loss of trust in the financial system, which could have a ripple effect as the lack of trust in financial institutions has been recorded as a key obstacle to financial inclusion globally.

In the book Inclusive Growth, authors Thomas and Hedrick-Wong write, “Interviews and focus groups among different strata of the society in Ho Chi Minh City revealed consistent evidence, often transmitted through ‘word of mouth’, that past bad experiences may play a significant role in influencing individual behavior...[T]he bad experience may not be purely personal but arise from stories or reports from acquaintances or individuals.”
In other words, successful cyberattacks to a FinTech solution provider can not only wreak havoc on the lives of its customers but also set back progress made in the direction of financial inclusion.

The MSME sector is also susceptible to and often ill-prepared for cyberattacks. The Chubb report on Malaysia SME Cyber Preparedness has highlighted that SMEs, which form 98% of all businesses in Malaysia, will be hit hardest without good risk mitigation and incident response planning. The report also found that 84% of Malaysian SMEs had been victims of cyber incidents in the past year.41 Due to the MSME sector’s importance to the ASEAN regional economy - MSMEs account for between 89% to 99.9% of the region’s total enterprises and between 52 to 97% of all jobs – this is worrisome. Many FinTechs in the region are themselves MSMEs or service the MSME sector. Therefore, understanding how FinTechs interact with the cybersecurity ecosystem is vital to the economic health and robustness of the region.

Furthermore, the threat of cybercrime is preventing the ASEAN FinTech sector from realizing its full potential. Low levels of both financial and digital literacy and the resultant fear of scams and cybercrime are suppressing the adoption of e-payments and other FinTech solutions in the region.

While digital payments and other digital business solutions have great potential to foster financial inclusion and expand economic opportunity, concerns regarding risks associated with payments hold back both individuals and enterprises from making the shift online.

Looking beyond the loss of revenue for companies and individuals, cybercrime can have sweeping consequences on the financial system and even wider security implications in the physical world. For example, in 2016, cybercriminals stole close to USD 1 billion from a Federal Reserve Bank of New York account belonging to the central bank of Bangladesh. These attacks, which were carried out by the subversion of the SWIFT system, set alarm bells ringing globally with experts cautioning that similar attacks could be used to initiate money transfers for terrorist financing.42

As a result, governments in the region are now increasingly cognizant of and focused on developing or refining legislative and regulatory responses that can help alleviate these threats. Since, many FinTech startups in ASEAN tend to be MSMEs – they are both attractive targets for malicious actors and may be less equipped to deal with cyberattacks.

At the same time, however, FinTechs and SMEs are also agile and open to adopt new technological solutions. In the presence of a conducive regulatory ecosystem, FinTechs would be able to choose innovative and efficient solutions to defend themselves and thereby better navigate the changing threat landscape.
While digitalization yields many benefits for the region, increased global connectivity also exposes the ASEAN region to various cybersecurity threats including data theft, data breach, cybercrime, cyber fraud, and ransomware, among others. The growth of the ASEAN economies, rising income levels of ASEAN citizens and the rising digitalization of financial services have all attracted the attention of bad actors to the region and ASEAN has become a lucrative target for cybercriminals worldwide.

Since 2016, the World Economic Forum (WEF) has highlighted data theft or fraud and cyberattacks in the top 10 global risks in terms of likelihood and impact in their annual Global Risk reports. The 2019 Cybercrime study by Accenture and Ponemon institute reports a surge in the number of security breaches globally – a 67% increase since 2015. In 2019, the average annual cost of cybercrime was USD 18.4 million for the banking industry, a 40% higher than average cost across other industries.

The Accenture-Ponemon report also found that the main threat vectors globally are malware, web-based attacks, phishing and other social engineering attacks, in addition to botnets, ransomware, and malicious code. Additionally, malware, web-based attacks, and denial-of-service attacks have caused significant revenue losses.

When we zoom in on the cyberthreat landscape in ASEAN region, we see similar challenges and threats. As we move into the next decade, we see an evolving cyberthreat landscape, with bad actors seeking higher financial gains by adopting new-age attack methods like mobile malware, machine learning based automated attacks, and by exploiting vulnerabilities in emerging technologies such as the Internet of Things (IoT), collaboration platforms and cloud-based tools.

The Interpol report on ASEAN Cyberthreat Assessment 2020 finds that global trends in cybercrime are reflected in the region. While scams targeting the vulnerable are increasingly commonplace, the region has also seen some truly devastating attacks and breaches targeting large organizations and businesses. Bad actors across the world frequently coordinate complex and sophisticated cyberattacks causing damage to critical infrastructure in the region. In 2017, a data breach targeting 12 Malaysian mobile operators led to the exposure of the personal data of 46 million Malaysian residents.

In 2018, a data leak at Thailand’s telecom operator True, resulted in the breach of the personal information of 46,000 customers. In the same year, Singapore Health Services (SingHealth) suffered a massive cyberattack in which an attacker successfully exfiltrated 1.5 million patient records. In 2019, a series of data breaches targeting Toyota Motor Corporation led to the unauthorized access of data on its servers at its subsidiaries in Thailand and Vietnam. That same year, more than 900,000 clients of Cebuana Lhuillier a Philippines-based pawnshop and remittance company were affected by a data breach incident.

Additionally, COVID-19 has shown an unprecedented acceleration of digitalization of products and services globally and the ASEAN region has been no exception. The increased adoption of e-payments and e-commerce has provided more targets for cybercriminals and the region, along with the rest of the world, saw a significant rise in cyberattacks during the pandemic.

Indonesia, with its newly digitalized population and thriving e-commerce and FinTech sectors was particularly targeted. According to the Indonesian Ministry of Communication and Information, the pandemic raised user traffic to online marketplaces by 30 percent, while also doubling e-payment adoption. The data of newly digitalized Indonesian users thus became more lucrative than ever before. Devastating cyberattacks targeting Indonesians during the pandemic included the breach of the data on more than two million voters and as well as the breach of data on 91 million accounts of the Indonesian e-commerce giant Tokopedia. News of both attacks emerged within a span of weeks in May 2020 and both attacks targeted information that could be used to commit financial fraud and identity theft. Other sensitive personal information directly related to the pandemic also seems to have been targeted by malicious actors as a month later, there...
This mandates a forward-looking balanced regulatory regime which not only focuses on safeguarding the interests of the end users, but also provides enough space for FinTech firms to innovate and flourish.

Along with regulatory changes, it is important to have sufficient manpower with the right skillset to protect the ecosystem from various cyberthreats. Capacity building and upskilling of cyber professionals is recognized as one of the most important priorities for all governments across the region. End user education and ability to influence safe online behavior will play a big role in establishing trust in the digital ecosystem and go a long way to help grow the FinTech industry.

Even in hyper-connected Singapore where the majority of the population is tech-savvy, there were increasing reports of successful cyberattacks – including those targeting remote learning resources used in the country’s education sector. Singapore’s Cybersecurity Agency reported on its websites that, “Cybercriminals are adapting their methods as COVID-19 concerns increasingly affect aspects of everyday life,” and that the delivery methods of such actors included emails; instant messaging and SMS platforms; as well as spurious coronavirus-related websites that were used to host malware attacks or to commit financial fraud. In line with global trends, Singapore observed over 1,500 malicious phishing URLs targeting Singapore from March to May 2020. This was more than double the number from the preceding three months.

Most pandemic-related cyberattacks in the region were in the form of phishing attacks that utilized COVID-related keywords to extract sensitive information from their victims. Countries in Southeast Asia, including Singapore and Thailand, also reported scammers impersonating government officials to obtain private data such as national identity numbers or financial information from victims. The pandemic has also catalyzed the adoption of emerging technologies like Artificial Intelligence (AI) and Internet of Things (IoT), which in turn, is expected to result in a rise of these technologies being leveraged in the evolving cyberthreat landscape. Safeguarding the FinTech ecosystem against current and emerging threats will require close collaboration among all stakeholders. Regulators and FinTech firms in the region will have to work together closely to address these threats.
Phishing

Phishing is a cyberthreat wherein malicious actors use fraudulent messages to lure users into disclosing personal and sensitive information. Email has become the most prevalent medium for the delivery of phishing attacks. Phishing attacks in the region are increasingly sophisticated and employ advanced social engineering techniques. As per Kaspersky’s 2019 report on phishing, Philippines (17%), Malaysia (16%) and Indonesia (14%) have the highest number of phishing victims in the ASEAN region.52

Ransomware

Ransomware is a specialized type of malware that infects a device and then prevents the user from accessing certain files by encrypting them unless a ransom is paid. Ransomware attacks continue to evolve and have reportedly targeted many major organizations globally. Cerber, an evolved ransomware technology recently topped the number of detected ransomwares in the ASEAN region.

Botnet

Botnets are networks of compromised computers and devices controlled by cyber criminals, which can be used to target financial institutions and their customers. Amongst the most prominent botnet threats detected in the ASEAN region are Andromeda.Botnet and Conficker.Botnet.

Cryptojacking

The unauthorized use of victim’s computer to secretly mine cryptocurrency has emerged as a new threat. According to Interpol, hacked routers in the Southeast Asia region account for 18% of those cryptojacking infections globally.53 Cryptojacking as a growing threat motivated by gains in cryptocurrency places both businesses and individual users at risk.

Malware

Malware is any malicious piece of software disguised as legitimate, which once installed on the user’s computing device causes harm to the user. Malware is constantly evolving. For example, Emotet, which had originally focused on the theft of banking credentials, now aims to distribute other malware. Other banking malware like LokiBot and Xloader have also been seen to target the ASEAN region.

Web and Mobile Application Attack

Configuration weakness or vulnerabilities in web and mobile application allow cybercriminals to exploit them for exfiltrating data and for other nefarious activities. As organizations use more varied technology stacks, the number of vulnerabilities that need to be managed increase. As a result, web and mobile application attacks gain prominence as digital transformation continues around the region and across the world.
While cybersecurity has been a key area of focus for all ASEAN nations in recent years, the approach, progress and results so far vary widely across the region. The PayPal ASEAN FinTech Cybersecurity matrix ("the matrix") is an attempt to provide one perspective of the current state of cybersecurity laws, awareness and practices in the FinTech ecosystem.

Driven primarily by survey responses and open source research, the matrix could serve as a helpful reference for governments, industry associations and business owners to get a high-level view of cyber readiness in each market.

The matrix applies 12 questions across the following five pillars:

- Legal and Policy
- Knowledge and Skills
- Investment and Spending
- Cyber Hygiene and Financial Literacy
- Stakeholder Communication and Collaboration

The traffic light rating is used in the matrix as a visual indicator to track progress especially where attention is needed. Table 2 provides the questions that were used to assess each ASEAN member state, categorized by the pillars mentioned to assess key aspects of their cybersecurity regulatory environment for the FinTech sector.

<table>
<thead>
<tr>
<th>LEGAL AND POLICY</th>
<th>Is there a cybersecurity law, regulation, or policy in place, either standalone or as part of a wider digital security framework?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Is there a national body/agency specifically responsible for cybersecurity (beyond the national CERT)?</td>
</tr>
<tr>
<td></td>
<td>Is there a regulatory sandbox for the FinTech sector run by the financial regulator/central bank?</td>
</tr>
<tr>
<td>KNOWLEDGE AND SKILLS</td>
<td>Is there a government–run national framework/program specifically devoted to developing cybersecurity skills (for SMEs, students, professionals, retirees, etc.)?</td>
</tr>
<tr>
<td></td>
<td>Is there a government–run national certification/accreditation framework for cybersecurity professionals?</td>
</tr>
<tr>
<td></td>
<td>Are there any government mechanisms to encourage skills and capacity-building in the field of cybersecurity – specifically for FinTech companies?</td>
</tr>
<tr>
<td>INVESTMENT AND SPENDING</td>
<td>Is there a national budget specifically devoted to cybersecurity?</td>
</tr>
<tr>
<td></td>
<td>Are there government–run funding programs devoted to helping FinTech companies strengthen their cybersecurity capabilities?</td>
</tr>
</tbody>
</table>
Based on the survey results and open-source research, we developed the PayPal ASEAN FinTech Cybersecurity Matrix ("the Matrix") to assess and analyze the cybersecurity regulatory ecosystem in the region for FinTech companies in the ASEAN member states. The Matrix provides a snapshot of the landscape at the time of the writing of this report, as analyzed from publicly available information.

<table>
<thead>
<tr>
<th>PayPal ASEAN FinTech Cybersecurity Matrix 2020</th>
<th>Brunei</th>
<th>Cambodia</th>
<th>Indonesia</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LEGAL AND POLICY</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there a cybersecurity law, regulation, or policy in place, either standalone or as part of a wider digital security framework?</td>
<td>⚫️</td>
<td>⚫️</td>
<td>⚫️</td>
</tr>
<tr>
<td>Is there a national body/agency specifically responsible for cybersecurity (beyond the national CERT)?</td>
<td>⚫️</td>
<td>⚫️</td>
<td>⚫️</td>
</tr>
<tr>
<td>Is there a regulatory sandbox for the FinTech sector run by the financial regulator/central bank?</td>
<td>⚫️</td>
<td>⚫️</td>
<td>⚫️</td>
</tr>
<tr>
<td><strong>KNOWLEDGE AND SKILLS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there a government-run national framework/program specifically devoted to developing cybersecurity skills (for SMEs, students, professionals, retirees, etc.)?</td>
<td>⚫️</td>
<td>⚫️</td>
<td>⚫️</td>
</tr>
<tr>
<td>Is there a government-run national certification/ accreditation framework for cybersecurity professionals?</td>
<td>⚫️</td>
<td>⚫️</td>
<td>⚫️</td>
</tr>
<tr>
<td>Are there any government mechanisms to encourage skills and capacity-building in the field of cybersecurity – specifically for FinTech companies?</td>
<td>⚫️</td>
<td>⚫️</td>
<td>⚫️</td>
</tr>
<tr>
<td><strong>INVESTMENT AND SPENDING</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there a national budget specifically devoted to cybersecurity?</td>
<td>⚫️</td>
<td>⚫️</td>
<td>⚫️</td>
</tr>
<tr>
<td>Are there government-run funding programs devoted to helping FinTech companies strengthen their cybersecurity capabilities?</td>
<td>⚫️</td>
<td>⚫️</td>
<td>⚫️</td>
</tr>
<tr>
<td><strong>CYBER HYGIENE AND FINANCIAL LITERACY</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are there government-run public awareness campaigns developed and implemented specifically for cybersecurity?</td>
<td>⚫️</td>
<td>⚫️</td>
<td>⚫️</td>
</tr>
<tr>
<td>Are there any government-run campaigns specifically devoted to strengthening consumers’ digital and financial literacy?</td>
<td>⚫️</td>
<td>⚫️</td>
<td>⚫️</td>
</tr>
<tr>
<td><strong>STAKEHOLDER COMMUNICATION AND COLLABORATION</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there a government-led (semi-) formalized collaboration framework between the cybersecurity industry and the FinTech sector?</td>
<td>⚫️</td>
<td>⚫️</td>
<td>⚫️</td>
</tr>
<tr>
<td>Are there any intergovernmental bilateral or multilateral agreements on growing, strengthening, or improving domestic FinTech sectors?</td>
<td>⚫️</td>
<td>⚫️</td>
<td>⚫️</td>
</tr>
</tbody>
</table>

- Present
- In progress (includes instances where plans have been laid out but information about implementation is not publicly available)
- Absent / Information not publicly available
<table>
<thead>
<tr>
<th>PayPal ASEAN FinTech Cybersecurity Matrix 2020</th>
<th>Laos</th>
<th>Malaysia</th>
<th>Myanmar</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LEGAL AND POLICY</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there a cybersecurity law, regulation, or policy in place, either standalone or as part of a wider digital security framework?</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Is there a national body/agency specifically responsible for cybersecurity (beyond the national CERT)?</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Is there a regulatory sandbox for the FinTech sector run by the financial regulator/central bank?</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td><strong>KNOWLEDGE AND SKILLS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there a government-run national framework/program specifically devoted to developing cybersecurity skills (for SMEs, students, professionals, retirees, etc.)?</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Is there a government-run national certification/ accreditation framework for cybersecurity professionals?</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Are there any government mechanisms to encourage skills and capacity-building in the field of cybersecurity – specifically for FinTech companies?</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td><strong>INVESTMENT AND SPENDING</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there a national budget specifically devoted to cybersecurity?</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Are there government-run funding programs devoted to helping FinTech companies strengthen their cybersecurity capabilities?</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td><strong>CYBER HYGIENE AND FINANCIAL LITERACY</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are there government-run public awareness campaigns developed and implemented specifically for cybersecurity?</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Are there any government-run campaigns specifically devoted to strengthening consumers’ digital and financial literacy?</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td><strong>STAKEHOLDER COMMUNICATION AND COLLABORATION</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there a government-led (semi-) formalized collaboration framework between the cybersecurity industry and the FinTech sector?</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Are there any intergovernmental bilateral or multilateral agreements on growing, strengthening, or improving domestic FinTech sectors?</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
</tbody>
</table>

- ✅: Present
- ✅: In progress (includes instances where plans have been laid out but information about implementation is not publicly available)
- ✅: Absent / Information not publicly available
## PayPal ASEAN FinTech Cybersecurity Matrix 2020

<table>
<thead>
<tr>
<th>Category</th>
<th>Philippines</th>
<th>Singapore</th>
<th>Thailand</th>
<th>Vietnam</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LEGAL AND POLICY</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there a cybersecurity law, regulation, or policy in place, either standalone or as part of a wider digital security framework?</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>Is there a national body/agency specifically responsible for cybersecurity (beyond the national CERT)?</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>Is there a regulatory sandbox for the FinTech sector run by the financial regulator/central bank?</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td><strong>KNOWLEDGE AND SKILLS</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there a government-run national framework/program specifically devoted to developing cybersecurity skills (for SMEs, students, professionals, retirees, etc.)?</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>Is there a government-run national certification/accreditation framework for cybersecurity professionals?</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>Are there any government mechanisms to encourage skills and capacity-building in the field of cybersecurity – specifically for FinTech companies?</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td><strong>INVESTMENT AND SPENDING</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there a national budget specifically devoted to cybersecurity?</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>Are there government-run funding programs devoted to helping FinTech companies strengthen their cybersecurity capabilities?</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td><strong>CYBER HYGIENE AND FINANCIAL LITERACY</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are there government-run public awareness campaigns developed and implemented specifically for cybersecurity?</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>Are there any government-run campaigns specifically devoted to strengthening consumers’ digital and financial literacy?</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td><strong>STAKEHOLDER COMMUNICATION AND COLLABORATION</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there a government-led (semi-) formalized collaboration framework between the cybersecurity industry and the FinTech sector?</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>Are there any intergovernmental bilateral or multilateral agreements on growing, strengthening, or improving domestic FinTech sectors?</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
</tbody>
</table>

- ⬤ Present
- ⬤ In progress (includes instances where plans have been laid out but information about implementation is not publicly available)
- ⬤ Absent / Information not publicly available
**OBSERVATIONS**

**Legal and Policy**

Results from the matrix reveal a positive (mostly green) trend in ASEAN’s legal and policy support for the FinTech cybersecurity ecosystem. Most ASEAN nations already have national cybersecurity laws or frameworks in place or have drafted their own laws, which is an important requirement for business clarity.

The matrix shows that a number of ASEAN countries such as Singapore, Thailand and Vietnam have defined their national cybersecurity laws, albeit at various stages of implementation (e.g. Singapore’s Cybersecurity Act 2018, and Vietnam’s Cybersecurity Law). Others who do not have national cybersecurity laws have made legislative amendments or changes by enacting fragmented cybersecurity initiatives such as the announcement of the establishment of the National Cybersecurity Agency by Brunei. Others have established national agencies to coordinate cybersecurity agendas, such as Malaysia, which is reviewing the feasibility of implementing a cybersecurity law.

While it is not the sole determining factor for a conducive FinTech ecosystem, a national cybersecurity framework is foundational to providing legal and policy clarity for FinTech businesses to function.

Financial regulators like the Monetary Authority of Singapore (MAS) and Bank Negara Malaysia (BNM) have also published specific technology and cybersecurity risk management requirements for their constituents to follow, which are more stringent than current national laws. Eight of ten ASEAN member states (AMS) have established national cybersecurity agencies. Cambodia and Laos, have yet to complete this step. However, both countries have national computer emergency response teams (CERTs) in place to help protect national security and critical infrastructure. In fact, when it comes to national CERTs, ASEAN nations have made considerable progress in collaborating across the region to establish multiple centers of excellence in cybersecurity such as Thailand, Vietnam and Singapore.

ASEAN is also doing well in its support of establishing and operating financial regulatory sandboxes, with six out of ten AMS having already done so. For example, Malaysia established the Financial Technology Regulatory Sandbox Framework in October 2016, Singapore launched the FinTech Regulatory Sandbox in November 2016, while Myanmar and Vietnam are making plans to announce their sandboxes soon. The sandbox construct has proven to be quite useful in helping bootstrap innovative concepts in the market while also assisting FinTech firms to become more familiar with regulatory requirements without compromising their time to market objectives.

Also, national priorities and stages of market maturity have resulted in cybersecurity approaches differing significantly across the region. This challenge is exacerbated by the lack of a governance or legal framework at the regional level, or a regional body responsible for standard setting and enforcement. According to the Center for Strategic International Studies (CSIS), regional policymakers and regulators are narrowly focused on cyber risks affecting their specific jurisdictions, making it hard for FinTech and startups to adequately prepare for and respond to growing transnational, cross-jurisdictional cyberthreats. Hence, the diverse cybersecurity landscape in the region could pose a risk for local and foreign financial institutions.
Knowledge and Skills

ASEAN member states are at different stages of maturity in establishing government-led initiatives to support the growth and development of cybersecurity knowledge and skillsets. Around half of them have created and are running such manpower initiatives, some like Indonesia have been doing so for quite some time, and a few like Thailand, while in early stages, have started programs focused on cybersecurity in the FinTech sector.

For example, Malaysia’s Digital Economy Corporation (MDEC) has established a number of cybersecurity training programs, such as NxFORCE, a four-week long cybersecurity capacity-building program. It has also started the Skill-Up Program, in collaboration with the Protection Group International UK and Asia Pacific University of Technology and Innovation, to run accreditation courses for cybersecurity. The Philippines released an initial request for information (RFI) in June 2019 to develop a Cyber Training Facility Project under the Department of Information and Communications Technology (DICT), although no further information was available on this RFI as of May 2020. However, as shown in the matrix, more attention is required in developing national frameworks for cybersecurity training and skills accreditation, especially in Brunei, Cambodia, Laos, Myanmar, and Vietnam.

More attention is required in developing national frameworks for cybersecurity training and skills accreditation.

The cybersecurity skills gap is a crucial area for growth in the region. While this impacts all sectors, the urgency on enhanced data privacy and management, regulatory requirements and rapid growth of digitalization exacerbates the impact on the FinTech sector.

Investment and Spending

The matrix illustrates that six out of ten countries in ASEAN had identifiable budget items or spending announcements on cybersecurity. Brunei’s Autoriti Monetari Brunei Darussalam (AMBD) Financial Sector Blueprint 2016-2025 makes mention of increasing investment in FinTech; however, this is not specific to cybersecurity capabilities.

Over the last few years, an ASEAN-wide approach to security has resulted in major investments towards cybersecurity in the form of centers of excellence and capacity building programs. While these are critical investments at the regional level and will benefit all ASEAN nations, our focus in the matrix has been on country-level programs run by regulators or other government agencies that are aimed at improving cybersecurity capabilities in the FinTech ecosystem. Government-run funding programs devoted to helping FinTech companies strengthen their cybersecurity capabilities demonstrate a national commitment to the development of cyber resilience capability. At the moment, it appears that most countries do not have such initiatives, apart from Singapore.
Cyber Hygiene and Financial Literacy

ASEAN countries are doing relatively well in establishing and running public awareness campaigns for both cybersecurity and financial literacy. Most AMS have some form of public education programs in place, which bodes well for the future of a healthy FinTech ecosystem, particularly if end-users maintain good cyber hygiene while using FinTech products and services.

Stakeholder Communication and Collaboration

A balanced approach towards creating a strong FinTech cybersecurity ecosystem should take into account the needs of the business community while still ensuring robust cybersecurity protections. At the time of writing, Brunei and Singapore have established government-led collaborations between the cybersecurity and FinTech sector through the Singapore’s Cybersecurity Advisory Panel\(^9\) and through Brunei’s Digital Payment Roadmap 2025.\(^{10}\)

It is encouraging to see that all AMS have established some form of bilateral or multilateral cooperation agreement with other countries to grow their domestic FinTech sectors. As leading examples, Singapore and Malaysia have established multiple international FinTech partnerships. Singapore and China have formed a number of FinTech cooperation initiatives.\(^{71}\) Additionally, Singapore and India established a Joint Working Group on FinTech.\(^{72}\) Malaysia’s Securities Commission has inked innovation cooperation agreements known as “FinTech bridges” with regulators in major financial centers from Hong Kong, Dubai and Singapore. Partnerships with leading FinTech hubs will not only grow the anchoring countries’ domestic FinTech sectors, they could also benefit other ASEAN countries who can capture downstream economic benefits such as provision of IT and engineering manpower.

Within ASEAN, Bank of Thailand’s MOU initiatives with Cambodia, Laos, Myanmar and Vietnam to expand cross-border currency settlement\(^{73}\) promote the development and interoperability of a unified QR code for use across the ASEAN borders.\(^{74}\) On the cybersecurity front, Singapore launched a new center in 2020 for ASEAN member states to collaborate and conduct research, share knowledge and train to respond to cyberthreats.\(^{75}\) The center serves an important role in coordinating and strengthening ASEAN’s cybersecurity efforts. This bodes well for the future of FinTech growth in ASEAN, indicating that ASEAN regulators and governments are gearing up for collaborative international growth in this sector.
FINDINGS OF THE PAYPAL ASEAN CYBERSECURITY SURVEY

The ASEAN FinTech Ecosystem Cybersecurity Readiness Survey asked FinTech companies across Southeast Asia about their perspectives on cybersecurity and its value proposition to their business, such as the impact of cybersecurity regulations on their growth, resource allocation and investment decisions. A total of 44 FinTech companies across the spectrum responded to the survey – from financial service activities such as money changing and remittance to financial leasing and credit granting firms.

Table 3:
Main service provided by respondent company

<table>
<thead>
<tr>
<th>RESPONSES</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking</td>
<td>18.2%</td>
</tr>
<tr>
<td>Financial Leasing and Credit-Granting</td>
<td>15.9%</td>
</tr>
<tr>
<td>Financial Service Activities</td>
<td>20.5%</td>
</tr>
<tr>
<td>Insurance and Reinsurance, intermediaries and brokers, and related Auxiliary Services</td>
<td>2.3%</td>
</tr>
<tr>
<td>Trusts and Funds and Similar Financial Entities and Fund Management Activities, and Related Auxiliary Activities</td>
<td>2.3%</td>
</tr>
<tr>
<td>Securities and commodities exchanges and brokerage</td>
<td>2.3%</td>
</tr>
<tr>
<td>Auxiliary technology support of financial services</td>
<td>13.6%</td>
</tr>
<tr>
<td>Other (please specify): Advisory, Mortgage valuation, lending, Gold trading, Blockchain company, Social commerce</td>
<td>25%</td>
</tr>
</tbody>
</table>

The majority of the responses (62%) came from young FinTech companies in the region (less than five years), while more than one-third (34%) respondents from companies which had been established for more than 10 years.

Our sample also included responses from both small and large FinTechs in the region. While nearly one-third of the respondents have 10 or fewer employees on their payroll (30%), a little over a quarter of respondents were from companies with 11-50 employees (27%) and over one-third (36%) came from larger companies with more than 200 employees.
Respondent firms were also geographically diverse, with roots in various markets both within and outside ASEAN, and with many serving multiple markets in the region, as seen in Tables 4 and 5.

Through our survey, we also sought to understand how FinTechs in the region are responding to the cybersecurity regulatory ecosystem in Southeast Asia. We were especially interested in understanding how FinTechs learn about regulations, how emerging cybersecurity regulations impact their businesses, and what the ecosystem-wide effects are.

The 2018 ASEAN FinTech Census by Ernst & Young concluded that nearly half (41%) of all FinTechs in the region are yet to break even.76 As a result, FinTechs in Southeast Asia often have to make difficult choices regarding resource allocation. While most FinTech firms in Southeast Asia have prioritized cybersecurity while making budgetary and personnel decisions, some face challenges. In our survey, we found that 64% of all respondent firms have allocated two or more employees to deal with cybersecurity and information security requirements. However, there is still a large proportion of FinTech companies – 27.3% who have dedicated less than one person to cybersecurity. This means that there could be more than a quarter of ASEAN FinTech companies who have
employees with multiple roles - dealing with cybersecurity as a secondary responsibility along with their other full-time role.

Similarly, the survey results show that FinTechs in the region are often unable or unwilling to allocate resources for cybersecurity-personnel and infrastructure. A significant share of the firms surveyed (43.2%) indicated that they spend less than 3% of their operating budget on cybersecurity. Considering how expensive and detrimental potential data breaches can be – to the firms themselves as well as to their customers – this low figure provides cause for concern.

In determining the allocation of these resources, FinTech companies in the region identified a diverse range of cybersecurity needs that they seek to meet. When asked to name key priority areas shaping their hiring and investment decisions in cybersecurity, 72.7% of the respondent firms identified data security and loss protection as key. The second-most frequently cited driver was regulatory compliance, with 63.6% of firms highlighting this as a priority area, followed by network security and end-point protection cited as key by 45.5% of respondents.

Authentication and authorization (36.4%) and incident management (31.8%) round out the top five priority areas, shaping hiring and investments in cybersecurity - followed by third party management (18.2%), threat management (15.9%), and security assurance (13.6%).
Regulators are working to ensure strong cybersecurity fundamentals are in place to keep consumers safe online and to ensure the financial system is stable and secure from cyberthreats and cybercrime. This is particularly challenging in the face of improved connectivity, rising mobile penetration, and a dynamic FinTech start-up ecosystem that is a prime target for cyberattacks. One-third of respondent firms said that they had experienced a cybersecurity incident in the 12 months preceding the survey.

Policymakers in the region therefore face a complex optimization problem in drafting cybersecurity regulations. On the one hand, the regulatory ecosystem must be flexible enough to support innovation and entrepreneurship in FinTech. On the other hand, FinTech players need to be incentivized to place customer protection and trust at the core of their business. A conducive regulatory environment is one that can balance both needs.

As seen in Figure 10, the regulatory environment has a significant impact on decisions to allocate cybersecurity resources. The survey results also indicate that compliance requirements drive most FinTech companies’ (70.5%) investment in cybersecurity, demonstrating the importance of instituting regulations that help protect against cybercrime while supporting firms to appropriately manage risks.

At the same time, our survey found that there is increased customer demand for cybersecurity – with nearly one-fifth (18.2%) of respondents citing this as their key driver for investments in cybersecurity. Other drivers of investment include protection against hacks and other industrial attacks (7%), and competitive pressure from cybersecurity efforts undertaken by peers (4.6%).
Even as regulatory requirements drive increased investments in cybersecurity, FinTechs in the region are facing significant challenges in ensuring compliance. The majority (59%) of survey respondents said that complying with cybersecurity regulations was a challenge, due to factors such as a lack of resources. Nearly 90% of them cited resource and budgetary constraints; 60.7% said that unavailability of talent with the required skillsets was a problem; and more than half (53.6%) the respondents indicated that management was not placing enough priority on compliance to cybersecurity regulations.

The results show that FinTech companies may need assistance messaging the importance of cybersecurity from a management priority and budget perspective. Research has shown that corporate stakeholders often have a myopic view of cyber risk, thinking that investing in new technologies will suffice to combat or mitigate risk. The Hewlett Foundation highlights the disconnect between technical practitioners and policy professionals as a major, persistent obstacle to the emergence of effective cybersecurity frameworks.

At the same time, there are other systemic factors which hinder firms from fully complying with regulations. Through our survey we found what seems to be a significant communication gap between regulators and FinTech companies, who are not receiving timely communications and support in order to stay abreast with the latest regulatory developments. When asked how they learn about new cybersecurity regulations, FinTech companies
responded that they hear about them through the media or press (36.4%), through the regulators’ websites (13.6%), find out about them from their professional networks (13.6%), or industry associations (15.9%), or that they have no way of finding out (4.6%). Only 15.9% of all respondents have some form of direct contact with the government regulators who inform them about new cybersecurity regulations.

**Figure 12:**
Source of information about new cybersecurity regulations
Share of participants

![Graph showing sources of information about new cybersecurity regulations](image)

Firms that had to divert resources stated that increased compliance burdens led to them spending less on several other key areas of business. Funds were reallocated from areas including internal systems and processes as well as product innovation and plans for market expansion, among others.

**Figure 13:**
Areas from which resources were diverted
Share of participants

![Graph showing areas from which resources were diverted](image)

Note: Other includes staff bonus

The survey also sought to understand how compliance was affecting resource allocation within companies. Nearly half of all respondent firms said they have had to divert resources from other areas of business to comply with cybersecurity regulations. This result highlights the urgent need to balance the FinTech ecosystem’s business needs and the need for cybersecurity protection, to ensure continued economic growth and business innovation in the region.
The increased adoption of new technologies such as the Internet of Things (IoT), virtual currencies, and artificial intelligence (AI) increase cybersecurity threats from unknown vectors (e.g. new devices), in addition to putting new types of assets at risk (e.g. cryptocurrencies). For example, NTT Security’s 2017 Global Threat Intelligence Report identified that 60% of all IoT-based attacks in 2016 originated from Asia. In June 2020, the release of the Ripple20 group of vulnerabilities is estimated to affect millions of IoT devices globally and further extended to traditional infrastructure through supply chain networks. These contribute to the ever-evolving cybersecurity regulatory environment.

While this presents a resourcing challenge for FinTech companies (as observed earlier), FinTechs themselves recognize that cybersecurity is crucial to the success of their business – even beyond the compliance requirements.

6 out of 10 FinTech firms believe that cybersecurity is a business differentiator for their business offerings.

Six out of ten FinTech firms (61.4%) believe that cybersecurity is a business differentiator for their business offerings. Considering how important trust and security are to any financial transaction, this is not surprising. It is therefore important that these firms are able to invest in the right cybersecurity tools for themselves while remaining compliant to the requirements set by regulators.

Unfortunately, the current regulatory environment does not seem to be inspiring confidence amongst FinTechs as the majority of FinTech companies felt that either investing in cybersecurity compliance would not yield better results (10%) or remained unsure about its impact on their business (52%).

However, more than one-third (38.6%) of FinTech companies found that investing in cybersecurity compliance yielded better business results. These benefits were mostly seen in increased brand awareness (60%), better customer engagement (55%), increased sales (10%), and better relationships with the regulator and reduced fraud cases (10%). Expanding these benefits across firms in the region will require a concerted effort between multiple stakeholders.

In the next section, we provide recommendations on how these benefits could be further extended to firms in the region.
ASEAN is an incredibly diverse region and this diversity is reflected in the financial service needs of its people. Archipelagoes like Indonesia and the Philippines provide opportunities for innovative products that can transcend geographic limitations. Newly emerging economies such as Cambodia, Myanmar and Laos serve up the possibility of technological leapfrogging. Highly connected economies with tech-savvy populations and a thriving SME sector such as Singapore, Thailand, Vietnam, and Malaysia offer the opportunity to cater to sophisticated customers who are ready to embrace new and innovative solutions.

However, throughout the region, exciting opportunities for innovation and growth co-exist with elevated risks from bad actors.

These risks not only place stumbling blocks to the growth of the FinTech industry in the region, they also pose complex regulatory challenges to policymakers who have to balance the creation of an enabling environment for a burgeoning FinTech sector while protecting the customers that FinTech firms seek to serve.

In order to develop and update policies to balance the need for ensuring cybersecurity while supporting business innovation, we provide six main recommendations based on our research and analysis.

**Develop principle-based frameworks for cybersecurity regulations driven by outcomes and evolving risks**

Over two-thirds of the respondent firms in our survey said that compliance requirements are the key driver for their investments in cybersecurity. This implies, that for many firms, the focus of their cyber defense efforts is not on security or risk mitigation.

**Compliance does not equal security.**

Compliance does not equal security. The cyberthreat landscape is constantly evolving. Attackers are quick to exploit vulnerabilities in new and emerging products and technologies. As threats become increasingly sophisticated, a compliant FinTech can no longer be considered inherently safe or secure. A defensive approach that prioritizes compliance as a tick-box exercise limits companies’ ability to direct resources where they are most useful, making threat monitoring and mitigation difficult against new sophisticated attack techniques.

An approach that refocuses FinTech firms towards resilience will help them identify weaknesses and shore up their defenses. A regulatory approach that urges such refocusing would be outcome-based. It would set out performance-focused security principles that companies and FinTechs should strive towards. This also encourages innovation around achieve optimal results aligned with risk tolerance and key business objectives.

From a regulator’s perspective, checklist-based point in time compliance should not be the ultimate goal of any cyber regulation. Instead, a principle-based regulatory ecosystem that moves away from a rigid box ticking approach and incentivizes investments in foundational controls, cyber risk mitigation, and threat management with customer safety as its key outcome is vital.

An important aspect of this shift is the recognition that there is immense diversity in both size and scale of FinTech firms and services in the region and hence, a prescriptive one-size-fits-all cybersecurity regulations cannot meet these firms’ or their customers’ needs. The FinTech marketplace has a variety of needs and risk categories, with ‘FinTech’ businesses running the gamut from virtual banks, to insurance companies, to companies that provide data services. This has resulted in a FinTech ecosystem which is subject to myriad cybersecurity regulations, that can be challenging to comply with, since many existing policies and regulations are not...
Risk-based requirements that are contingent on services rendered as well as the scale of the FinTech can help ease undue regulatory burden and ensure that compliance bolsters resilience.

Enable adoption of strong cyber hygiene through ASEAN-level compatibility as well as alignment with global security standards

With an estimated 125,000 new users in ASEAN going online every day, the ASEAN digital economy is projected to grow exponentially, amounting to USD 300 billion by 2025. However, such growth is contingent on increased convergence across ASEAN markets. As former ASEAN Secretary-General Mr. Le Luong Minh observed in 2015, “While the region is diverse and varied, the growing middle classes in ASEAN share similar demands and consumption patterns. This should allow companies to build broader regional platforms and take advantage of economies of scale.” For companies to serve ASEAN as a single market and to benefit from the resultant economies of scale, ASEAN countries will have to implement “cohesive and interoperable legislation” in all areas, including cybersecurity.

Across the world, regulatory divergence has been identified as a drain on resources and an impediment to the growth of businesses. A 2018 OECD study on the subject, which surveyed 250 compliance or risk management officers and leaders from financial institutions discovered that regulatory divergence leads to steep increases in operating cost globally. The same study found that 51% of financial institutions had to divert resources (including senior management time and capital) away from investment in risk management activities as a result of regulatory divergence.

In ASEAN, efforts towards harmonizing policies and regulations on cybersecurity across the region are imperative, as FinTech companies struggle to comprehend, fulfill, and implement cross-cutting, and at times contradictory, regulatory requirements. National initiatives providing clear guidance to FinTech companies – including how to design cybersecurity policies to address the organizations’ unique risks – will help alleviate this challenge to an extent. Additionally, increased focus should be placed on standardizing these efforts at a regional level. A common regulatory stance for cybersecurity can be further accelerated by adopting international standards, the promotion of passporting measures, and the development of pan-ASEAN industry platforms for stakeholders to coordinate and share
Innovation in financial services is transforming the economies of ASEAN and the lives of its citizens. New products balancing the need to foster innovation with that of protecting customers and the financial system against risks.

A popular approach that has been used by regulatory agencies around the world is a sandbox. The intent of a sandbox has been conducting ASEAN Incident Cyber Drills (ACID) exercises for the last decade, with the most recent 14th iteration being hosted by the Cybersecurity Agency of Singapore (CSA) in September 2019. At the Fourth ASEAN Ministerial Conference on Cybersecurity (AMCC) in Singapore in 2019, ASEAN Ministers stated their commitment to fulfill the need for a formal mechanism to coordinate ASEAN cybersecurity efforts.

Building on these efforts, ASEAN should create an evolving regional cybersecurity framework that is aligned with global standards and practices. Such a framework would enable exchange of innovative cyber defense measures and expertise and ensure the retirement of legacy processes that hold back technology adoption. Placing internationally recognized security standards such as ISO 27000:2013 and the NIST Cybersecurity Framework as guiding factors in the development of a regional cybersecurity framework would also facilitate regional policy coherence as well as improved strategic alignment and information sharing.

Cyberthreats are cross-border in nature and countering them requires a concerted international effort. Increased harmonization and adherence to international standards not only provides opportunities for FinTech to grow, but reduced regulatory complexity is also instrumental in driving down implementation errors and in enabling better comprehension and compliance. A harmonized regional approach would encourage continuing and consistent dialogue towards improving the framework and increased agility in responding to emerging threats.

At the regional level, ASEAN has announced concerted efforts on cybersecurity coordination, with Singapore drafting the ASEAN cybersecurity framework under its 2018 ASEAN chairmanship, and the establishment of the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE). However, more needs to be done. ASEAN could consider developing a regional initiative to improve policy interoperability so that compliance to the cybersecurity standards in one ASEAN country would be sufficient for a FinTech firm to offer these same services in another country. Regional cooperation efforts can lead to collective security and further enhancement of national cyber security measures. At the same time, improved policy interoperability would strengthen the regional ICT infrastructure and enable member states with developing infrastructure or incipient cybersecurity regulations to leverage regional best practices.

There is already a rich history of cybersecurity coordination in the region. For example, the ASEAN Computer Emergency Response Teams (CERTs) have been conducting ASEAN Incident Cyber Drills (ACID) exercises for the last decade, with the most recent 14th iteration being hosted by the Cybersecurity Agency of Singapore (CSA) in September 2019. At the Fourth ASEAN Ministerial Conference on Cybersecurity (AMCC) in Singapore in 2019, ASEAN Ministers stated their commitment to fulfill the need for a formal mechanism to coordinate ASEAN cybersecurity efforts.

Building on these efforts, ASEAN should create an evolving regional cybersecurity framework that is aligned with global standards and practices. Such a framework would enable exchange of innovative cyber defense measures and expertise and ensure the retirement of legacy processes that hold back technology adoption. Placing internationally recognized security standards such as ISO 27000:2013 and the NIST Cybersecurity Framework as guiding factors in the development of a regional cybersecurity framework would also facilitate regional policy coherence as well as improved strategic alignment and information sharing.

Cyberthreats are cross-border in nature and countering them requires a concerted international effort. Increased harmonization and adherence to international standards not only provides opportunities for FinTech to grow, but reduced regulatory complexity is also instrumental in driving down implementation errors and in enabling better comprehension and compliance. A harmonized regional approach would encourage continuing and consistent dialogue towards improving the framework and increased agility in responding to emerging threats.

At the regional level, ASEAN has announced concerted efforts on cybersecurity coordination, with Singapore drafting the ASEAN cybersecurity framework under its 2018 ASEAN chairmanship, and the establishment of the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE). However, more needs to be done. ASEAN could consider developing a regional initiative to improve policy interoperability so that compliance to the cybersecurity standards in one ASEAN country would be sufficient for a FinTech firm to offer these same services in another country. Regional cooperation efforts can lead to collective security and further enhancement of national cyber security measures. At the same time, improved policy interoperability would strengthen the regional ICT infrastructure and enable member states with developing infrastructure or incipient cybersecurity regulations to leverage regional best practices.

There is already a rich history of cybersecurity coordination in the region. For example, the ASEAN Computer Emergency Response Teams (CERTs) have been conducting ASEAN Incident Cyber Drills (ACID) exercises for the last decade, with the most recent 14th iteration being hosted by the Cybersecurity Agency of Singapore (CSA) in September 2019. At the Fourth ASEAN Ministerial Conference on Cybersecurity (AMCC) in Singapore in 2019, ASEAN Ministers stated their commitment to fulfill the need for a formal mechanism to coordinate ASEAN cybersecurity efforts.

Building on these efforts, ASEAN should create an evolving regional cybersecurity framework that is aligned with global standards and practices. Such a framework would enable exchange of innovative cyber defense measures and expertise and ensure the retirement of legacy processes that hold back technology adoption. Placing internationally recognized security standards such as ISO 27000:2013 and the NIST Cybersecurity Framework as guiding factors in the development of a regional cybersecurity framework would also facilitate regional policy coherence as well as improved strategic alignment and information sharing.

Cyberthreats are cross-border in nature and countering them requires a concerted international effort. Increased harmonization and adherence to international standards not only provides opportunities for FinTech to grow, but reduced regulatory complexity is also instrumental in driving down implementation errors and in enabling better comprehension and compliance. A harmonized regional approach would encourage continuing and consistent dialogue towards improving the framework and increased agility in responding to emerging threats.

Promote a multilateral regulatory sandbox for knowledge sharing and risk management in the FinTech ecosystem

Innovation in financial services is transforming the economies of ASEAN and the lives of its citizens. New products and services are leveraging data, mobile technology, and new business models to deliver unique financial offerings. At the same time, however, many of these innovations come with risks. Regulators have the difficult task of balancing the need to foster innovation with that of protecting customers and the financial system against risks. A popular approach that has been used by regulatory agencies around the world is a sandbox. The intent of a
Sandboxes provide regulators with a front row seat to emerging technologies and business models, which in turn, enables them to formulate laws and regulations that factor in these developments.

Sandboxes can catalyze product development, enhance opportunity for investment, and facilitate the formation of policies that keep pace with innovation. Sandboxes also help to level the playing field for new and smaller players to enter the market, thereby providing increased scope for competition and innovation. Sandboxes also help ensure that any problems are identified and fixed in the development stage where the impact is minimal.

In ASEAN, as seen in the matrix, sandboxes are a popular regulatory instrument to encourage the development of the FinTech sector. However, some countries continue to lag behind. To fully realize the benefits and the potential of the ASEAN FinTech sector, each ASEAN nation should host its own sandbox.

To enable FinTechs in the region to benefit from each other’s experiences and collaborate on innovations, we recommend the establishment of formalized channels of collaboration and knowledge-sharing between national sandboxes in ASEAN. Sharing lessons learned across the region can also help regulators ensure that policymaking in their jurisdictions remain up to date on emerging technologies and business models.

The long-term goal of these endeavors should be the creation of an ASEAN-wide sandbox – one that can help FinTechs test out their products designed with an ASEAN regional consumer base in mind. Extending the pilot scope across ASEAN, while clearly not without challenges, could leap-frog typical growth timelines and help regional companies to compete with established businesses and multinationals that enter the region with vast resources.

The ASEAN Secretariat and central banks in the region should work closely with the private sector to begin laying the foundation for such a regional sandbox. Additionally, closely aligning an ASEAN-wide sandbox with existing cyber resiliency initiatives such as the ASEAN-Singapore Cybersecurity Centre of Excellence would facilitate the growth of region-wide FinTechs while also ensuring that customers and their data are protected.
Invest in developing a strong cybersecurity workforce to support a resilient ecosystem

The expanding cyberthreat landscape has caused a global shortage of cybersecurity professionals. Across the world, some 3.5 million cybersecurity positions are expected to go unfilled in 2021, demonstrating a major disconnect between cybersecurity needs (the overwhelming rise of cybercrime) and cybersecurity experts (qualified, specialized, and experienced professionals).91

Countries in ASEAN are similarly affected by the cybersecurity skills gap. For example, there were 6,000 cybersecurity professionals in Malaysia in 2018, but it was anticipated that more than 10,000 would be needed by 2020 to meet the demands of a rapidly growing digital economy.92 Even Singapore, often seen as a model for digital economies in the region, is bracing for a potential talent shortage of up to 3,400 cybersecurity professionals in 2020.93 In the survey, we found that more than a quarter of FinTech companies who responded - 27.3% - do not have a dedicated cybersecurity personnel on their roster. Considering the rising tide of cybercrime, this shortage is particularly worrisome.

At the same time, cybersecurity for FinTechs requires an additional level of specialized skill sets. In our survey, more than half the respondent firms (61%) stated that a lack of requisite skillsets in their workforce had made it difficult for them to comply with cybersecurity regulations. Additionally, more than a quarter of the respondent firms (27.3%) said that their cybersecurity capabilities rested in the hands of one person who manages these responsibilities alongside other roles. Government agencies must urgently work with the private sector to increase talent development and access in order to adequately service the needs of the financial services industry.

Government agencies must urgently work with the private sector to increase talent development and access in order to adequately service the needs of the financial services industry.

Fortunately, ASEAN has been cognizant of the skills gap and have already begun initiatives to bridge it. The ASEAN-Japan Cybersecurity Capacity Building Centre was launched in June 2018 in Thailand, giving the Thai business ecosystem an opportunity to be trained in cybersecurity skills.94 Singapore has also set up the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) in October 2019, which will devote USD21 million on policy and technical training programs over five years.95 The MAS has also established the Cybersecurity Capability Grant (CCG) of up to 50% to deepen cybersecurity capabilities and develop cybersecurity talent in Singapore’s financial services sector.96 Furthermore, ASEAN governments have been working on setting up undergraduate programs for cybersecurity and otherwise integrating cybersecurity into the formal educational system, be it at university or more formative levels, when dealing with the talent shortages.

The FinTech sector can also play an important role collaborating with institutes of secondary and tertiary education to train students in vital cyber defense and technological skills. The PayPal FinTech Program for institutes of vocational learning in Singapore is an example of such an initiative. Through a curriculum specially designed for students at these institutes, the program grooms FinTech talent to be future-ready and equips polytechnic students with the foundation of e-payments and cybersecurity in FinTech transactions. The students can then use this knowledge to integrate PayPal solutions into their school or industry projects. They can also work with MSMEs to integrate these solutions into their websites, thereby earning supplementary income while also enabling MSME digitalization in Singapore and beyond. As of 2019, 1200 students had benefitted from this curated training material. In addition, PayPal also conducted an AI workshop series for the instructors at these institutes to further strengthen academia-industry linkages in this space. Outside ASEAN, the Hong Kong Institute of Technology and the international cybersecurity certification organization EC-Council have come together to create training & certification programs.
that will meet the market demand for skilled cybersecurity professionals and ensure industry-oriented training and education.⁹⁷

An important first step towards planning for the future would be the introduction of cybercrime mitigation, data analytics, automation technologies and cybersecurity skills in early-learning stages of the schooling systems in ASEAN, with educational pathways drawn through to university. Skills introduced into the curriculum should go beyond programming to also include training in allied topics such as data science, cryptography and cybersecurity. By introducing these topics at a young age, students become more aware of the diversity of options and opportunities available in the sector and discover specific roles that fit their aptitudes and interests.

Additionally, as countries in ASEAN begin looking at ways to equip their populations for the future of work, there is an opportunity to train mid-career workers who seek to attain new skills to become cybersecurity professionals. Such training should focus both on short-term programs to fulfil immediate needs⁹⁸ as well as long-term guidance to help workers specialize and acquire expertise.

Increasingly important, is the need for dedicated focus on supporting entry and growth of women into the field of cybersecurity. Women are currently severely underrepresented in the field, with estimates stating that they make up only about 11% of cybersecurity professionals globally.⁹⁹

A future-ready training plan should also be established beyond ensuring the workforce for technical cybersecurity knowledge. This should include training a new type of worker who has hybrid skillsets – one who understands that the cybersphere is constantly evolving, and knows how to evolve with it, and knows how to use emerging technology such as data and artificial intelligence to enforce cybersecurity and understand cyber risk, and cybercrime management. It would require reimagining and going beyond conventional internship programs and require extensive collaboration between academia, public agencies and the private sector.

Focusing resources and attention on skills training for women yields multiple benefits, even beyond the obvious and important goal of equal representation for women in the cybersecurity workforce. In the present situation of acute talent shortage, bridging the gender gap will be impossible unless women view cybersecurity as a viable vocation. Secondly, as in any other field, the absence of diversity reduces the range and scope of ideas brought to the table. As Priscilla Moriuchi, Director of Strategic Threat Development at Recorded Future, said to Forbes in 2018, "We need people with disparate backgrounds because the people we are pursuing (threat actors, hackers, ‘bad guys’) also have a wide variety of backgrounds and experiences. The wider variety of people and experience we have defending our networks, the better our chances of success."¹⁰⁰

A future-ready training plan should also be established beyond ensuring the workforce for technical cybersecurity knowledge. This should include training a new type of worker who has hybrid skillsets – one who understands that the cybersphere is constantly evolving, and knows how to evolve with it, and knows how to use emerging technology such as data and artificial intelligence to enforce cybersecurity and understand cyber risk, and cybercrime management. It would require reimagining and going beyond conventional internship programs and require extensive collaboration between academia, public agencies and the private sector.

**ASEAN can see immense benefits from exploring innovative schemes like credential passporting across the region to enable easier movement of talent across Southeast Asia.**

At the regional level, ASEAN can see immense benefits from exploring innovative schemes like credential passporting across the region to enable easier movement of talent across Southeast Asia. ASEAN already has a regulatory template for such arrangements in the form of Mutual Recognition Arrangements (MRAs) which aim to facilitate mobility of professionals or skilled labor in ASEAN and are currently in place for specific sectors including engineering, nursing, and medicine. Regional passporting has been introduced in the European Union through the Cybersecurity Act which has introduced EU-wide rules for cybersecurity certification. As a result, companies in the EU benefit from having to certify their products, processes and services only once and see their certificates recognized across the Union.
A collaborative initiative along with such MRAs could be an ASEAN-wide program for workforce development in the cybersecurity sector. Due to the specialized needs of the financial sector, ASEAN governments could partner with FinTechs and traditional financial institutions to formulate the curriculum as well as the delivery of training modules under such a program. By providing live online training to students at varying levels of cybersecurity expertise, such an initiative could also facilitate real-time exchange of experiences and ideas across ASEAN. Such an initiative would especially benefit emerging enterprises in the FinTech space and beyond due to reduced training costs as well as increased availability of trained cybersecurity professionals while also providing new income earning opportunities for newly developed professionals.

**Establish comprehensive programs for training and awareness on fraud and security best practices for general public and businesses**

The cybersecurity ecosystem is only as strong as its weakest link. Even the most sophisticated defense systems, the most advanced infrastructure, and the most rigorous cybersecurity laws cannot protect an ill-informed end-user. With the increasing adoption of FinTech solutions by citizens of ASEAN, cybersecurity is no longer a concern that rests solely with experts and regulators. Every user needs to be better educated about the technologies they use and how malicious actors can target them.

Users who are taking their first steps towards digitalizing their finances should be educated about ways to protect themselves online.

Users who are taking their first steps towards digitalizing their finances should be educated about ways to protect themselves online. Financial information is explicitly targeted in cyberattacks. Many of these attacks rely on social engineering and fraudulent emails and they take advantage of users’ inexperience of good cyber hygiene. For instance, phishing attacks explicitly seek financial account information such as online banking credentials. A successful attack of this nature can be devastating for a customer’s financial life. At the same time, perceived risk and trust have been identified as important factors in determining attitudes towards e-payment adoption. Therefore, the threat of cybercrime and lack of information about ways to protect themselves can dissuade people from adopting financial solutions designed to improve their lives through technology. To counter these attacks, consumers must be educated enough to identify threats and protect themselves against them so that they have the confidence to navigate their financial lives online.

Such cyber literacy efforts should be tailored to the technical and financial literacy levels of various sections of the population. Additionally, it is also important to ensure that victims of cyberattacks are emboldened to report their experience. Studies have found that victims of fraud often feel ashamed that they “fell for it” or worry that they will be seen as unintelligent. As a result, they do not report the scam due to feelings of embarrassment. This can be dangerous and counterproductive. After all, neither policymakers nor cybersecurity experts can address a threat without becoming aware of it. Empowering victims to speak up ensures that decision makers can help mitigate the spread of such scams.

ASEAN should also consider establishing an easily accessible region-wide repository of cyber scams and threats which would serve as an important step towards both information sharing between various stakeholders in the region as well as a database for users to gain information about prevalent threats and the means to counter them. The private sector also has an important role to play in this endeavor. In Singapore, the National Crime Prevention Council(NPC), which is a collaboration between the Singapore Policy Force and other government agencies as well as commercial and industry players,
launched a website (www.scamalert.sg) in 2014 that has since become a single destination for Singaporean residents to report and stay updated on online scams.

Governments and private companies can work together to ensure that information about cyber hygiene and cyber protection is accessible to all, especially in times of crisis. The COVID-19 crisis, which has led to educational institutions and workplaces moving online and relying increasingly on online learning, video conferencing, and other remote working technologies, has also led to a corresponding increase in cybercrime targeted at these systems. In Singapore, in April 2020 during the initial stages of the pandemic, the government banned the use of popular video-conferencing application Zoom in home-based school education after instances of hackers breaching e-learning sessions. Subsequently, cybersecurity professionals from private sector firms including PayPal provided pro-bono workshops and training to teachers in the country to help them safeguard against such intrusions.

By working together on such initiatives, ASEAN as a region can develop mechanisms to educate end users across ASEAN markets with consistent, pertinent, and up-to-date messaging on cyber hygiene and protecting themselves online.

Governments in the region can also support businesses by educating end-users on the shared responsibility of cybersecurity. This would support the FinTech ecosystem by aligning their business risks and priorities with customers and end-users. For instance, the Bankers Association of the Philippines, upon the encouragement of Bangko Sentral ng Pilipinas (BSP), ran a campaign, “Be Aware, Be Cybersafe” in 2019 to increase public awareness of cybersecurity. Brunei’s BruCERT also developed videos in 2018 to increase the public awareness of cybersecurity. In Singapore, there are eye-catching public service advisories in public transportation vehicles, bus stops, and train stations that provide public information about common cyberattacks, ways to prevent them, and contact details of law enforcement agencies to turn to for help.

Furthermore, ASEAN governments can implement and encourage internationally recognized best practices on anti-virus, patching, and anti-phishing standards. ASEAN can come together to adopt the use of internationally recognized email and domain authentication standards (DMARC) to protect users from attacks perpetrated through fraudulent email. Over 90% of all cyberattacks globally start with a phishing email and phishing has been recognized as the most likely first step in attacks by cyberterrorists. Anti-phishing measures that can be promoted by governments include authentication standards which validate that the domain contained in an email “From” header is authentic by crosschecking against Domain Name System (DNS) records. Email servers can then accept, reject, or warn against incoming emails based on this information. Financial institutions and payments providers are often used as bait in phishing attacks and have therefore developed expertise in countering them. By working closely with the private sector, ASEAN governments can ensure that their constituents are better informed and protected against such attacks.

Governments in the region can also support businesses by educating end-users on the shared responsibility of cybersecurity. This would support the FinTech ecosystem by aligning their business risks and priorities with customers and end-users. For instance, the Bankers Association of the Philippines, upon the encouragement of Bangko Sentral ng Pilipinas (BSP), ran a campaign, “Be Aware, Be Cybersafe” in 2019 to increase public awareness of cybersecurity. Subsequently, cybersecurity professionals from private sector firms including PayPal provided pro-bono workshops and training to teachers in the country to help them safeguard against such intrusions.

By working together on such initiatives, ASEAN as a region can develop mechanisms to educate end users across ASEAN markets with consistent, pertinent, and up-to-date messaging on cyber hygiene and protecting themselves online.

Governments in the region can also support businesses by educating end-users on the shared responsibility of cybersecurity.

Encourage public-private partnerships in research, hiring and information sharing

From the results of our survey, we see that there is an urgent need to boost regular-industry engagement, as well as strengthen public-private collaboration in cybersecurity. FinTech companies appear to be proactively seeking out information on cybersecurity regulations by themselves, but there are opportunities to establish stronger information sharing and collaboration mechanisms.

A consistent two-way engagement between policymakers and the FinTech industry yields benefits to both. Policymakers are kept updated about emerging threats in the space and can keep a finger on the pulse of the FinTech industry to understand its cybersecurity needs. Policymakers can also plan for measures to counter emerging threats without stifling innovation by taking the perspectives of FinTech institutions into account.
Just as global standards are developed through multi-stakeholder and transparent processes, involving non-government stakeholders in the process of developing cybersecurity frameworks will help enhance security through the sharing of best practices.

An example of such an approach was seen in Malaysia, where, the Internet Banking Task Force was set up in 2004 by the Bank Negara Malaysia (BNM) and the banking industry to develop a comprehensive regulatory response to cybersecurity threats. Financial institutions can share intelligence and discuss issues related to Internet banking, including cybersecurity. Through the Task Force, the BNM, industry and other government agencies, including the Malaysian Communications and Multimedia Commission (MCMC), CyberSecurity Malaysia and the Royal Malaysia Police, effectively engage with each other. Enhanced engagements can bring tangible results. BNM reports that the Task Force was instrumental in mitigating the threat of SMS-based scams in the country.

Another successful example, from outside the region, is the Australian FinTel Alliance, which was the world's first private-public partnership that brought together government and private sector members (including PayPal) from Australia and beyond to counter malicious actors and crime in the financial sector. Together, members of the Australian FinTel Alliance work together with law enforcement agencies to counter complex financial crimes, including those perpetrated online.

The private sector should also explore ways in which they can proactively reach out to government bodies.

Other similar groups are the World Economic Forum’s ASEAN e-Payments Coalition, which is a voluntary grouping of FinTech and financial sector industry companies working on supporting the development of an integrated and harmonized digital payment framework across ASEAN with the goal of supporting the growth of cross-border e-commerce.

Another important measure that governments in the region can take is to ensure that new regulations and cyber norms are introduced after a process of public consultation with diverse stakeholders. Such consultations can help take into account the latest developments in both FinTech and cybersecurity while also ensuring that there are no unintended externalities that hinder innovation or onerous compliance burdens.

Ensure that new regulations and cyber norms are introduced after a process of public consultation with diverse stakeholders

The private sector should also explore ways in which they can proactively reach out to government bodies. One method is to establish industry groups which engage with regulators, carrying messages from the private sector before regulations are created. For example, the ASEAN FinTech Innovation Network (AFIN) was established as a not-for-profit membership organization created by MAS, International Finance Corporation (IFC), and ASEAN Banker’s Association (ABA) to promote FinTech-Financial Institution (FI) collaboration and support financial inclusion.

Given the speed of the evolution of cyberthreats, and the rapid development of business opportunities in the FinTech space, a conducive FinTech environment must include mechanisms and channels for strong stakeholder communications, consultation, and engagement. These could include a variety of engagement mechanisms including light-touch communication channels such as email lists, working group meetings, as well as formal consultations during the drafting of regulations.

Information-sharing and cooperation is critical and should be fostered. We especially encourage the
creation of public private forums for stakeholders from a diverse range of institutions to consult with each other on new regulations, training needs, and to share best practices. In Singapore, the Joint Cybersecurity Working Group (JCSWG) that is co-organized by the US and Singapore governments has been effective in enabling conversations between governments and the private sector in order to identify their respective priorities, to coordinate capacity building measures, as well as to create cyber policies that are productive and consistent. Meetings of the Working Group focus on a wide variety of issues at the national and regional level including emerging regulatory trends, challenges and resource gaps, cyber hygiene and cyber norms, among others. Similar working groups that include regulators from central banks and other financial regulators as well as cybersecurity agencies and which seek to provide a platform for engagement between these regulators and the private sector can help facilitate business-sensitive policymaking while ensuring preparedness for new threats.

Additionally, governments and financial institutions can also collaborate to establish a trusted platform for the sharing of threat intelligence, breaches, or new attack vectors to support timely response including disbursement of advisories for SMEs and the ecosystem. Information sharing on threats and responses using a regional clearinghouse can help organizations in the region enhance their security levels by leveraging each other’s knowledge and experience.  

As NIST states in its Guide to Cyber Threat Information Sharing, “Using [shared] knowledge, an organization can make threat-informed decisions regarding defensive capabilities, threat detection techniques, and mitigation strategies. By correlating and analyzing cyberthreat information from multiple sources, an organization can also enrich existing information and make it more actionable. This enrichment may be achieved by independently confirming the observations of other community members, and by improving the overall quality of the threat information through the reduction of ambiguity and errors. Organizations that receive threat information and subsequently use this information to remediate a threat confer a degree of protection to other organizations by impeding the threat’s ability to spread. Sharing of cyberthreat information allows organizations to better detect campaigns that target particular industry sectors, business entities, or institutions.”

By implementing research grants that incentivize collaborative intellectual property creation and research between academia and private organizations, governments in the region can help promote research and development in the area of cyber defense.

Cybercrime, like the internet, is borderless. Countering it will also require a borderless multi-stakeholder approach that can only be facilitated through communication and collaboration.

Additionally, cyber protection mechanisms need to become increasingly innovative as cybercriminals think of newer niftier ways to perpetuate attacks. By implementing research grants that incentivize collaborative intellectual property creation and research between academia and private organizations, governments in the region can help promote research and development in the area of cyber defense.
LEGAL AND POLICY

Is there a cybersecurity law, regulation, or policy in place, either standalone or as part of a wider digital security framework?
No, but a Data Security Law is being planned.\textsuperscript{112}

Is there a national body/agency specifically responsible for cybersecurity (beyond the national CERT)?
Yes, the Cybersecurity Working Committee (CSWC)\textsuperscript{113} which supports the National Security Committee (NSC) at the Prime Minister’s Office, and also the Brunei Computer Emergency Response Team (BruCERT).\textsuperscript{114} In March 2019, the government also announced plans to set up a National Cybersecurity Centre, but this has yet to materialize.\textsuperscript{115}

Is there a regulatory sandbox for the FinTech sector, run by the financial regulator/central bank?
Yes, this is run by AMBD.\textsuperscript{116}

KNOWLEDGE AND SKILLS

Is there a government-run national framework/program specifically devoted to developing cybersecurity skills (for SMES, students, professionals, retirees, etc.)?
Yes, there are ad hoc programs such as the ones organized by the Authority for Info-communications Technology Industry of Brunei Darussalam (AITI) which conduct digital skills and cybersecurity programs, including for senior citizens.\textsuperscript{117}

Is there a government-run national certification/accreditation framework for cybersecurity professionals?
No.
Are there any government mechanisms to encourage skills and capacity-building in the field of cybersecurity - specifically for FinTech companies?
No.

INVESTMENT AND SPENDING

Is there a national budget specifically devoted to cybersecurity?
Yes, but it is not clearly earmarked. Security is one of the pillars of the Brunei Digital Government Strategy, and the Ministry of Transport and Infocommunications (MTIC) has alluded to its budget including cybersecurity, and the Financial Sector Blueprint to 2025 mentions increasing investment in FinTech, but there are no specific budget figures earmarking developments in cybersecurity.

Are there government-run funding programs (grants, accelerators, etc.) devoted to helping FinTech companies strengthen their cybersecurity capabilities?
No.

CYBER HYGIENE

Are there government-run public awareness campaigns developed and implemented specifically for cybersecurity?
Yes, run by the IT Protective Security Services Sdn Bhd (ITPSS) in its role as BruCERT, and also cybersecurity awareness initiatives run by the Authority of Info-Communications Technology Industry (AITI) Brunei.

Are there any government-run campaigns specifically devoted to strengthening consumers’ digital and financial literacy?
Yes, run by AMBD under the Financial Sector Blueprint.

STAKEHOLDER COLLABORATION

Is there a government-led (semi-) formalized collaboration framework between the cybersecurity industry and the FinTech sector?
Yes, the Brunei Digital Payment Roadmap 2025, formalizes cybersecurity concerns with FinTech development.

Are there any intergovernmental bilateral or multilateral market agreements on growing, strengthening, or improving the domestic FinTech sector?
Yes, AMBD has signed MOUs with fellow regulators and authorities, including in Cambodia and Thailand, as well as the Singapore-Brunei cooperation on FinTech.
LEGAL AND POLICY

Is there a cybersecurity law, regulation, or policy in place, either standalone or as part of a wider digital security framework?
No, but there is a draft Cybercrime Law.¹²⁷

Is there a national body/agency specifically responsible for cybersecurity (beyond the national CERT)?
No, but there is the Cambodia Computer Emergency Response Team (CamCERT).¹²⁸

Is there a regulatory sandbox for the FinTech sector, run by the financial regulator/central bank?
No.

KNOWLEDGE AND SKILLS

Is there a government-run national framework/program specifically devoted to developing cybersecurity skills (for SMES, students, professionals, retirees, etc.)?
No.

Is there a government-run national certification/accreditation framework for cybersecurity professionals?
No.

Are there any government mechanisms to encourage skills and capacity-building in the field of cybersecurity - specifically for FinTech companies?
No.
INVESTMENT AND SPENDING

Is there a national budget specifically devoted to cybersecurity?
No.

Are there government-run funding programs (grants, accelerators, etc.) devoted to helping FinTech companies strengthen their cybersecurity capabilities?
No.

CYBER HYGIENE

Are there government-run public awareness campaigns developed and implemented specifically for cybersecurity?
No.

Are there any government-run campaigns specifically devoted to strengthening consumers’ digital and financial literacy?
Yes, the National Bank of Cambodia runs National Financial Literacy Day to boost Cambodians’ financial literacy.

STAKEHOLDER COLLABORATION

Is there a government-led (semi-) formalized collaboration framework between the cybersecurity industry and the FinTech sector?
No.

Are there any intergovernmental bilateral or multilateral market agreements on growing, strengthening, or improving the domestic FinTech sector?
Yes, there is an MOU to strengthen cooperation in FinTech innovation between the MAS and National Bank of Cambodia. Also, there is a cross-border fund transfer scheme using QR codes, established by the BOT with Cambodia, Laos, Myanmar, and Vietnam (CLMV).
LEGAL AND POLICY

**Is there a cybersecurity law, regulation, or policy in place, either standalone or as part of a wider digital security framework?**

No, but there is a draft Cybersecurity Law (RUU KSS).\(^{132}\)

**Is there a national body/agency specifically responsible for cybersecurity (beyond the national CERT)?**

Yes, the National Cyber and Encryption Agency (Badan Siber dan Sandi Negara or BSSN),\(^ {133}\) and the Indonesia Security Incident Response Team on Internet Infrastructure / Coordination Center (ID-SIRTII/CC).\(^ {134}\)

**Is there a regulatory sandbox for the FinTech sector, run by the financial regulator/central bank?**

Yes, under the financial regulator Financial Services Authority (Otoritas Jasa Keuangan or OJK),\(^ {135}\) as well as with the Bank Indonesia (BI).\(^ {136}\) The Financial Services Authority (OJK) has also launched the Electronic Gateway for Digital Finance Information Systems (Gesit), which is an online registration system for FinTech startups wanting to grow its business through the OJK Infinity, an innovation hub, business incubator and education center for FinTech.\(^ {137}\)

KNOWLEDGE AND SKILLS

**Is there a government-run national framework/program specifically devoted to developing cybersecurity skills (for SMES, students, professionals, retirees, etc.)?**

No.

**Is there a government-run national certification/accreditation framework for cybersecurity professionals?**

Yes, a framework has been launched by the National Cyber and Encryption Agency and National Professional Certification Body.\(^ {138}\)

**Are there any government mechanisms to encourage skills and capacity-building in the field of cybersecurity - specifically for FinTech companies?**

Yes, but these mechanisms are not used regularly. The National Cyber and Encryption Agency often hosts ad-hoc
“technical workshops” for electronic service providers and FinTech companies to improve regulatory compliance.139

INVESTMENT AND SPENDING

_Is there a national budget specifically devoted to cybersecurity?_
Yes, IDR2.2 trillion (USD130 million) has been allocated to the BSSN.140

_Are there government-run funding programs (grants, accelerators, etc.) devoted to helping FinTech companies strengthen their cybersecurity capabilities?_
No, but there are some support programs such as in 2016, President Joko Widodo announced a focus on e-commerce policy package (also known as the E-Commerce Roadmap) to create 1,000 “technopreneurs” by 2020.141

CYBER HYGIENE

_Are there government-run public awareness campaigns developed and implemented specifically for cybersecurity?_
Yes, BSSN and the Indonesia Security Incident Response Team on Internet Infrastructure/ Coordination Center (ID-SIRTII) conduct cybersecurity awareness, including seminars and courses.142

_Are there any government-run campaigns specifically devoted to strengthening consumers’ digital and financial literacy?_
Yes, there is a campaign run by Bank Indonesia.143

STAKEHOLDER COLLABORATION

_Is there a government-led (semi-) formalized collaboration framework between the cybersecurity industry and the FinTech sector?_
No.

_Are there any intergovernmental bilateral or multilateral market agreements on growing, strengthening, or improving the domestic FinTech sector?_
Yes, an MOU has been signed between the MAS and OJK,144 and there is also a FinTech Indonesia collaboration agreement with FinTech Australia.145
LAOS

LEGAL AND POLICY

Is there a cybersecurity law, regulation, or policy in place, either standalone or as part of a wider digital security framework?
No.

Is there a national body/agency specifically responsible for cybersecurity (beyond the national CERT)?
No, but there is the Lao Computer Emergency Response Team (LaoCERT).

Is there a regulatory sandbox for the FinTech sector, run by the financial regulator/central bank?
No.

KNOWLEDGE AND SKILLS

Is there a government-run national framework/program specifically devoted to developing cybersecurity skills (for SMES, students, professionals, retirees, etc.)?
No.

Is there a government-run national certification/accreditation framework for cybersecurity professionals?
No.
Are there any government mechanisms to encourage skills and capacity-building in the field of cybersecurity - specifically for FinTech companies?
No.

INVESTMENT AND SPENDING

Is there a national budget specifically devoted to cybersecurity?
No.

Are there government-run funding programs (grants, accelerators, etc.) devoted to helping FinTech companies strengthen their cybersecurity capabilities?
No.

CYBER HYGIENE

Are there government-run public awareness campaigns developed and implemented specifically for cybersecurity?
No.

Are there any government-run campaigns specifically devoted to strengthening consumers’ digital and financial literacy?
No, but the Bank of Lao PDR has started cooperation with OECD, ADBI, and GIZ as partners in financial inclusion and financial education.147

STAKEHOLDER COLLABORATION

Is there a government-led (semi-) formalized collaboration framework between the cybersecurity industry and the FinTech sector?
No.

Are there any intergovernmental bilateral or multilateral market agreements on growing, strengthening, or improving the domestic FinTech sector?
Yes, there is a cross-border fund transfer scheme using QR codes, established by the BOT with Cambodia, Laos, Myanmar, and Vietnam.148
MALAYSIA

LEGAL AND POLICY

Is there a cybersecurity law, regulation, or policy in place, either standalone or as part of a wider digital security framework?
Yes, the National Cyber Security Policy.149

Is there a national body/agency specifically responsible for cybersecurity (beyond the national CERT)?
Yes, the National Cyber Security Agency (Agensi Keselamatan Siber Negara or NACSA).150

Is there a regulatory sandbox for the FinTech sector, run by the financial regulator/central bank?
Yes, the BNM manages a regulatory sandbox.151

KNOWLEDGE AND SKILLS

Is there a government-run national framework/program specifically devoted to developing cybersecurity skills (for SMES, students, professionals, retirees, etc.)?
Yes, NACSA conducts periodic training and awareness programs for professionals in the private sector.152 Also, the Malaysia Digital Economy Corporation (MDEC) conducts training programs, which include NxFORCE, a four-week long cybersecurity skills and capacity-building program for undergraduates, and CSI:MY, which targets pre-university youths.153

Is there a government-run national certification/accreditation framework for cybersecurity professionals?
Yes, through the CyberGuru Cyber Security Professional Development (CSPD) program run by CyberSecurity Malaysia.154
Are there any government mechanisms to encourage skills and capacity-building in the field of cybersecurity - specifically for FinTech companies?

There are some co-partnered initiatives such as the BNM-AFI training on cybersecurity for financial inclusion.155

INVESTMENT AND SPENDING

Is there a national budget specifically devoted to cybersecurity?

Yes.156

Are there government-run funding programs (grants, accelerators, etc.) devoted to helping FinTech companies strengthen their cybersecurity capabilities?

Yes, there are but indirectly, under the MDEC sandbox and other entrepreneurship programs157 which fintech companies may also apply for.

Are there any government mechanisms to encourage skills and capacity-building in the field of cybersecurity - specifically for FinTech companies?

There are some co-partnered initiatives such as the BNM-AFI training on cybersecurity for financial inclusion.155

CYBER HYGIENE

Are there government-run public awareness campaigns developed and implemented specifically for cybersecurity?

Yes, such as CyberSAFE run by CyberSecurity Malaysia,158 and also Cyber999159 which is a help center run by Cybersecurity Malaysia to assist Malaysia internet users in dealing with cybersecurity incidents.

Are there any government-run campaigns specifically devoted to strengthening consumers’ digital and financial literacy?

Yes, through the Financial Education Network (FEN), which is implementing the Malaysia National Strategy for Financial Literacy 2019-2023.160

STAKEHOLDER COLLABORATION

Is there a government-led (semi-) formalized collaboration framework between the cybersecurity industry and the FinTech sector?

Yes, through mentorship programs and other initiatives to boost the digital economy’s cyber resilience through MDEC and CyberSecurity Malaysia. For example, there are collaborative mechanisms established through the CyberSecurity Malaysia Collaboration Programme (CCP),161 a public-private partnership that targets Malaysian registered companies that provide cybersecurity products and services, banding them to work together to deliver improved cybersecurity measures in the country. In addition, the Coordinated Malware Eradication and Remediation Platform (CMERP) was developed locally through public-private collaboration.162

Are there any intergovernmental bilateral or multilateral market agreements on growing, strengthening, or improving the domestic FinTech sector?

Yes, the Securities Commission (SC) Malaysia has inked a number of innovation cooperation agreements, also known as “FinTech bridges” with a number of regulators in major financial centers, including Hong Kong Securities and Futures Commission (SFC), the Dubai Financial Services Authority (DFSA) and the MAS.163
**MYANMAR**

**LEGAL AND POLICY**

*Is there a cybersecurity law, regulation, or policy in place, either standalone or as part of a wider digital security framework?*

No, but the Ministry of Transport and Communications (MOTC) is drafting a cybersecurity law.\(^{164}\)

*Is there a national body/agency specifically responsible for cybersecurity (beyond the national CERT)?*

Yes, the National Cyber Security Centre (NCSC), together with the Myanmar Computer Emergency Response Team (mmCERT),\(^{165}\) under the aegis of the Ministry of Transport and Communications.\(^{166}\)

*Is there a regulatory sandbox for the FinTech sector, run by the financial regulator/central bank?*

No.

**KNOWLEDGE AND SKILLS**

*Is there a government-run national framework/program specifically devoted to developing cybersecurity skills (for SMES, students, professionals, retirees, etc.)?*

No.

*Is there a government-run national certification/accreditation framework for cybersecurity professionals?*

No.
Are there any government mechanisms to encourage skills and capacity-building in the field of cybersecurity - specifically for FinTech companies?
No.

INVESTMENT AND SPENDING

Is there a national budget specifically devoted to cybersecurity?
Yes, insofar as the MOTC is drafting the cybersecurity law, and where mmCERT falls under its purview.167

Are there government-run funding programs (grants, accelerators, etc.) devoted to helping FinTech companies strengthen their cybersecurity capabilities?
No.

CYBER HYGIENE

Are there government-run public awareness campaigns developed and implemented specifically for cybersecurity?
Yes, such as the National Cybersecurity Awareness Month run as a collaboration between the Information Technology and Cyber Security Department of the Ministry of Transport and Communications, Myanmar Computer Federation, Myanmar Information Security Association and the US ICT Council for Myanmar.168

Are there any government-run campaigns specifically devoted to strengthening consumers’ digital and financial literacy?
Yes, Myanmar has a number of partnerships with private sector companies to increase consumer digital and financial literacy, such the Financial Inclusion Roadmap, also known as Making Access Possible (MAP). A partnership between the Myanmar Ministry of Planning and Finance, in partnership with UK-funded DaNa Facility, and the United Nations Capital Development Fund (UNCDF) Myanmar, it includes programs which support the development of quality and affordable financial services, and aid development of financial literacy.169

STAKEHOLDER COLLABORATION

Is there a government-led (semi-) formalized collaboration framework between the cybersecurity industry and the FinTech sector?
No.

Are there any intergovernmental bilateral or multilateral market agreements on growing, strengthening, or improving the domestic FinTech sector?
Yes, there is a cross-border fund transfer scheme using QR codes, established by the BOT with Cambodia, Laos, Myanmar, and Vietnam.170
PHILIPPINES

LEGAL AND POLICY

Is there a cybersecurity law, regulation, or policy in place, either standalone or as part of a wider digital security framework?

Yes, the National Cybersecurity Plan 2022,\textsuperscript{171} as well as the Republic Act No. 10175: Cybercrime Prevention Act of 2012 (CPA).\textsuperscript{172}

Is there a national body/agency specifically responsible for cybersecurity (beyond the national CERT)?

Yes, the Cybercrime Investigation and Coordination Center (CICC), which is attached to the Department of Information and Communications Technology (DICT),\textsuperscript{173} as well as the National Cybersecurity Inter-Agency Committee (NCIAC).\textsuperscript{174}

Is there a regulatory sandbox for the FinTech sector, run by the financial regulator/central bank?

Yes, established in 2019 by the BSP.\textsuperscript{175}

KNOWLEDGE AND SKILLS

Is there a government-run national framework/program specifically devoted to developing cybersecurity skills (for SMES, students, professionals, retirees, etc.)?

Yes, there is a partnership between the Department of Information Communications Technology (DICT) with the AMA Computer University to promote cybersecurity education.\textsuperscript{176} DICT has also worked in tandem with the Commission of Higher Education (CHED) to create a bachelor’s degree on Cybersecurity,\textsuperscript{177} as well as with the Department of Education (DepEd) to integrate Cybersecurity into the Senior High School curriculum.\textsuperscript{178}

Is there a government-run national certification/accreditation framework for cybersecurity professionals?

Yes, the ICT Specialist Proficiency Examination, run by the DICT.\textsuperscript{179}
Are there any government mechanisms to encourage skills and capacity-building in the field of cybersecurity - specifically for FinTech companies?

Yes, the BSP Circular 808\textsuperscript{180} and Circular 982\textsuperscript{181} provide parameters and best practices to help financial institutions, including FinTech companies, to identify, prevent, detect, respond to, and recover from cyberattacks. In 2018, Central Bank adopted RegTech (regulatory technology) and SupTech (supervisory technology) for existing regulatory and supervisory tools to tackle cyberthreats in FinTech.

INVESTMENT AND SPENDING

*Is there a national budget specifically devoted to cybersecurity?*

Yes, DICT announced in 2017 that it would be spending PHP2 billion/USD39m to the nation’s cyber defenses.\textsuperscript{382}

*Are there government-run funding programs (grants, accelerators, etc.) devoted to helping FinTech companies strengthen their cybersecurity capabilities?*

Somewhat, there are innovation and incubator hubs developed in partnership with the government to grow entrepreneurs, some of which we may assume to be FinTech companies.\textsuperscript{183}

CYBER HYGIENE

*Are there government-run public awareness campaigns developed and implemented specifically for cybersecurity?*

Yes, such as the IT Security Awareness campaign run by the Integrated Government Philippines (iGovPhil) Program.\textsuperscript{184}

*Are there any government-run campaigns specifically devoted to strengthening consumers’ digital and financial literacy?*

Yes, there is the Financial Literacy Campaign run by the BSP,\textsuperscript{185} as well as the BSP Economic and Financial Learning Program (BSP EFLP),\textsuperscript{186} and other awareness campaigns.

STAKEHOLDER COLLABORATION

*Is there a government-led (semi-) formalized collaboration framework between the cybersecurity industry and the FinTech sector?*

Somewhat. While the information of an official framework is not publicly available, there are some initiatives planned, such as in 2018, the BSO announced a new unit under its Financial Supervision Sector for cybersecurity called the Financial Technology Sub-Sector (FTSS). FTSS is composed of the Payments and Settlements Oversight Department and the Core Information Technology Specialist Group.\textsuperscript{187}

*Are there any intergovernmental bilateral or multilateral market agreements on growing, strengthening, or improving the domestic FinTech sector?*

Yes, there is a FinTech Cooperation Agreement signed between the BSP and MAS in 2017,\textsuperscript{188} and another MOU signed with Hong Kong’s Alliance for Financial Stability with Information Technology (AFS-IT).\textsuperscript{189}
**SINGAPORE**

---

**LEGAL AND POLICY**

*Is there a cybersecurity law, regulation, or policy in place, either standalone or as part of a wider digital security framework?*

Yes, the Singapore Cybersecurity Act 2018.\(^{190}\)

*Is there a national body/agency specifically responsible for cybersecurity (beyond the national CERT)?*

Yes, the Cyber Security Agency of Singapore (CSA),\(^{191}\) supported by SingCert and other related agencies.

*Is there a regulatory sandbox for the FinTech sector, run by the financial regulator/central bank?*

Yes, the FinTech Regulatory Sandbox launched in 2017 by the MAS.\(^{192}\)

---

**KNOWLEDGE AND SKILLS**

*Is there a government-run national framework/program specifically devoted to developing cybersecurity skills (for SMES, students, professionals, retirees, etc.)?*

Yes, CSA has a partnership with the Info-communications Media Development Authority (IMDA) to offer the Cyber Security Associates and Technologists Program.\(^{193}\) The government also provides funding for skills development, including cybersecurity, in the SkillsFuture program.\(^{194}\) The National Research Foundation (NRF) provides grants for research and development into cybersecurity.\(^{195}\)

*Is there a government-run national certification/accreditation framework for cybersecurity professionals?*

Yes, the CSA runs the Cyber Security Associates and Technologists (CSAT) Program.\(^{196}\)
Are there any government mechanisms to encourage skills and capacity-building in the field of cybersecurity - specifically for FinTech companies?
Yes, USD15 million has been set aside by the government to boost banks’ cybersecurity capabilities.197

INVESTMENT AND SPENDING

Is there a national budget specifically devoted to cybersecurity?
Yes, USD15 million has been set aside by the government to boost banks’ cybersecurity capabilities.

Are there government-run funding programs (grants, accelerators, etc.) devoted to helping FinTech companies strengthen their cybersecurity capabilities?
Yes, the abovementioned USD15 million has been set aside by the government to boost banks’ cybersecurity capabilities,198 which will include FinTech companies. In addition, FinTech companies are also able to tap on the grants from the National Research Foundation (NRF), to conduct research and development into cybersecurity.199

CYBER HYGIENE

Are there government-run public awareness campaigns developed and implemented specifically for cybersecurity?
Yes, CSA runs regular cybersecurity government-run public awareness campaigns such as the annual National Cybersecurity Awareness Campaign.200

Are there any government-run campaigns specifically devoted to strengthening consumers’ digital and financial literacy?
Yes, such as the MoneySense initiatives, run by the MAS and Ministry of Manpower (MOM) to improve financial health of Singaporeans.201

STAKEHOLDER COLLABORATION

Is there a government-led (semi-) formalized collaboration framework between the cybersecurity industry and the FinTech sector?
Yes - MAS established a high-level industry Cyber Security Advisory Panel (CSAP) in 2017, composed of leading cybersecurity experts and thought leaders from the financial services private sector.202

Are there any intergovernmental bilateral or multilateral market agreements on growing, strengthening, or improving the domestic FinTech sector?
Yes, there are many partnerships which Singapore has established, such as Singapore and China FinTech cooperation,203 and the Singapore and India Joint Working Group (JWG) on FinTech,204 as well as numerous other partnerships to build and extend FinTech collaboration with other markets.
THAILAND

LEGAL AND POLICY

Is there a cybersecurity law, regulation, or policy in place, either standalone or as part of a wider digital security framework?
Yes, the Thailand Cybersecurity Act, B.E. 2562 (2019).205

Is there a national body/agency specifically responsible for cybersecurity (beyond the national CERT)?
Yes, under the Ministry of Digital Economy and Society (MDES),206 the Electronic Transactions Development Agency of Thailand (ETDA) is the current Acting National Cybersecurity Agency,207 along with the Thai Computer Emergency Response Team (ThaiCERT) and the Digital Forensics Centre.208

Is there a regulatory sandbox for the FinTech sector, run by the financial regulator/central bank?
Yes, it was established by the BOT.209

KNOWLEDGE AND SKILLS

Is there a government-run national framework/program specifically devoted to developing cybersecurity skills (for SMES, students, professionals, retirees, etc.)?
Yes, under the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC), where training workshops will be run every two months.210

Is there a government-run national certification/accreditation framework for cybersecurity professionals?
Yes, the ETDA and the Thailand Information Security Association (TISA) have created the Information Security Expert Certification (ISEC), a cybersecurity course for Thais in 2013,211 and are also offering training courses for the Certified Information Systems Security Professional (CISSP) examination.212

Are there any government mechanisms to encourage skills and capacity-building in the field of cybersecurity - specifically for FinTech companies?
Somewhat. Thailand and Japan have jointly developed an ASEAN Centre of Excellence (COE) for cybersecurity capacity building, and one initiative is exclusively by Ministry of Digital Economy and Society (MDES) with the
help of electronic transactions agency. While not specific to FinTech companies, they are able to benefit from it.

INVESTMENT AND SPENDING

Is there a national budget specifically devoted to cybersecurity?
Yes, it will likely fall under the National Cybersecurity Agency.

Are there government-run funding programs (grants, accelerators, etc.) devoted to helping FinTech companies strengthen their cybersecurity capabilities?
Somewhat. The BOT has signed an agreement with the Hong Kong Applied Science and Technology Research Institute (ASTRI) to help enhance cybersecurity and developing FinTech, particularly the efficiency and security of Thailand’s electronic transactions, as well as the resilience of its financial system against cyberthreats.

CYBER HYGIENE

Are there government-run public awareness campaigns developed and implemented specifically for cybersecurity?
Yes, the ETDA runs Thailand Cybersecurity Week, for example.

Are there any government-run campaigns specifically devoted to strengthening consumers’ digital and financial literacy?
Yes, financial literacy campaigns are run under the Financial Consumer Protection Centre (FCPC) under the BOT.

STAKEHOLDER COLLABORATION

Is there a government-led (semi-) formalized collaboration framework between the cybersecurity industry and the FinTech sector?
Yes. The BoT, in partnership with ETDA, supported the Thai Bankers’ Association (TBA) in establishing the Thailand Banking Sector Computer Emergency Response Team (TB-CERT) in 2017. TB-CERT aims to strengthen cybersecurity cooperation among financial institutions by sharing information, alerting about risks, and providing guidelines to combat cyberthreats. In addition, there is also the SPARK Accelerator is established by National Innovation Agency (NIA) from Ministry of Science and Technology with the cooperation of AGW Group. The program covers the following sectors: FinTech, cybersecurity, e-commerce, IoT, Big Data, and Healthcare.

Are there any intergovernmental bilateral or multilateral market agreements on growing, strengthening, or improving the domestic FinTech sector?
Yes, amongst other agreements, the BOT and the Central Bank of the Russian Federation for cybersecurity and FinTech innovation cooperation, and also with the People’s Bank of China (PBOC) have an agreement for FinTech cooperation.
VIETNAM

LEGAL AND POLICY

Is there a cybersecurity law, regulation, or policy in place, either standalone or as part of a wider digital security framework?
Yes, the Cybersecurity Law (Decree 72).222

Is there a national body/agency specifically responsible for cybersecurity (beyond the national CERT)?
Yes, the Ministry of Public Security,223 along with the Authority of Information Security (AIS) under the Ministry of Information and Communications,224 and also the Vietnam Computer Emergency Response Team/Coordination Centre (VNCERT/CC),225 and the National Electronic Authentication Center.226

Is there a regulatory sandbox for the FinTech sector, run by the financial regulator/central bank?
No, but there have been developments in policy which suggest that this may be in the works.227

KNOWLEDGE AND SKILLS

Is there a government-run national framework/program specifically devoted to developing cybersecurity skills (for SMES, students, professionals, retirees, etc.)?
Yes, Decision 99 released in 2014 by the Prime Minister was a plan to train and develop human resources for the country’s information security by 2020, including 2000 workers with university and postgraduate education in information security.228

Is there a government-run national certification/accreditation framework for cybersecurity professionals?
No.

Are there any government mechanisms to encourage skills and capacity-building in the field of cybersecurity - specifically for FinTech companies?
No.

INVESTMENT AND SPENDING

Is there a national budget specifically devoted to cybersecurity?
No.

Are there government-run funding programs (grants, accelerators, etc.) devoted to helping FinTech companies strengthen their cybersecurity capabilities?
No, but there are growing spaces for FinTech companies to expand in Vietnam, driven by the private sector.²²⁹

CYBER HYGIENE

Are there government-run public awareness campaigns developed and implemented specifically for cybersecurity?
No.

Are there any government-run campaigns specifically devoted to strengthening consumers’ digital and financial literacy?
Yes, some run by government or in partnership such as the Vietnam Bank for Social Policies co-funded with Citi, and Home Credit (2013) co-funded with large shopping centers, as well as the Aflatoun financial education program for children from 6-14 years old, in cooperation with Hue City and the Vietnam Association for the Protection of Children’s Rights (VAPCR).²³⁰ Further, the SBV has also been put in charge of the National Financial Inclusion Strategy (FI Strategy).²³¹

STAKEHOLDER COLLABORATION

Is there a government-led (semi-) formalized collaboration framework between the cybersecurity industry and the FinTech sector?
No.

Are there any intergovernmental bilateral or multilateral market agreements on growing, strengthening, or improving the domestic FinTech sector?
Yes, there is a cross-border fund transfer scheme using QR codes, established by the BOT with Cambodia, Laos, Myanmar, and Vietnam.²³² There is also an agreement between the SBV and MAS.²³⁴
REFERENCES

7. https://cybersecurityventures.com/jobs/
11. Ibid.
30. As of November 2020
REFERENCES

32 https://asia.nikkei.com/Spotlight/Cover-Story/Go-jek-sparks-an-Indonesian-banking-revolution
34 https://theaseanpost.com/article/southeast-asias-cybersecurity-emerging-concern
36 https://transparencymap.google.com/safe-browsing/overview
39 https://medium.com/@SustainableDFS/the-critical-role-of-trust-in-financial-inclusion-144fd935e1e1
42 https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/
43 https://asia.nikkei.com/News/Asia-Pac/ASEAN-remains-prime-target-for-cyberattacks
44 https://www.weforum.org/reports/the-global-risks-report-2019
52 As cited in https://securitybrief.asia/story/asean-a-hotbed-for-phishing-attacks
54 Due to the dynamic nature of the industry, the status captured may not reflect the latest updates in each area but should still provide the reader an overall assessment of the environment and more importantly act as a tool to help continue to determine the progress in each area.
59 https://www.mas.gov.sg/development/FinTech/regulatory-sandbox
62 https://www.csis.org/analysis/financial-sector-cybersecurity-requirements-asia-pacific-region
63 https://mdec.my/digital-economy-initiatives/for-the-industry/entrepreneurs/cybersecurity/
68 https://www.nrf.gov.sg/programmes/national-cybersecurity-r-d-programme
72 Ibid.
78 https://hewlett.org/building-capable-cyber-policy-field
80 https://www.jsot-tech.com/ripple20/
86 https://asean.org/chairmans-statement-3rd-asean-ministerial-conference-cybersecurity
91 https://cybersecurityventures.com/jobs
94 https://iotbusiness-platform.com/blog/asean-japan-cybersecurity-capacity-building-centre-to-be-launched-

https://www.mas.gov.sg/schemes-and-initiatives/fsti-cybersecurity-capability-grant


https://techbeacon.com/security/why-we-need-more-women-cybersecurity


Ibid.


https://www.brucert.org.bn/


https://borneobulletin.com.bn/over-bnd53m-budget-for-mtic/


126 https://www.straitstimes.com/politics/spore-brunei-to-boost-economic-cooperation
132 https://gallery.mailchimp.com/3952d41620b893439c9090d05/files/b2646429-bdd0-415d-9ee5-dcb6f88ae422/190528_RUU_Keamanan_dan_Ketahanan_Siber_ENG_.pdf
133 https://bssn.go.id/
134 https://www.idsirtii.or.id/
142 https://idsirtii.or.id/en/page/training.html
146 https://www.laocert.gov.la/en/Page-1-
147 http://www.oecd.org/finance/financial-education/Lao%20PDR%202018%20Summary%20Record.pdf
149 https://www.nacsa.gov.my/ncsp.php
150 https://www.nacsa.gov.my/
154 https://www.cyberguru.my
155 https://www.afi-global.org/events/bnm-afi-member-training-cybersecurity-financial-inclusion
157 https://www.go-ecommerce.my/campaign/perkhidmatan-edagang-setempat
158 https://www.cybersafe.my/cyber999.html
163 https://www.sc.com.my/resources/media-releases-and-announcements/sc-establishes-FinTech-cooperation-
agreements-with-major-financial-centres
165 https://www.mmcert.org.mm/about-us.html
166 https://www.motc.gov.mm/my/%E1%80%9E%E1%80%90%E1%80%84%E1%80-%
BA%E1%80%B8%E1%80%A1%E1%80%81%E1%80%BB%E1%80%80%E1%80%BA%E1%80%A1%E1%80%9C%E1%80%80%E1%80%BA%E1%80%A1%E1%80%94%E1%80%84%E1%80%BA%E1%80%B8%E1%80%8E%E1%80%95%E1%80%8A%E1%80%AC%E1%80%94%E1%80%BE%E1%80%84%E1%80%B7%E1%80%BA-%E1%80%86%E1%80%AD%E1%80%AF%E1%80%80%E1%80%BA%E1%80%A0%E1%80%98%E1%80%AC%E1%80%9C%E1%80%AF%E1%80%B6%E1%80%81%E1%80%BC%E1%80%AF%E1%80%B6%E1%80%9B%E1%80%B1%E1%80%B8%E1%80%A6%E1%80%B8%E1%80%85%E1%80%AE%E1%80%B8%E1%80%AC%E1%80%94
security-plan-2022
176 https://dict.gov.ph/dict-ama-forges-partnership-to-promote-cybersecurity-education/
177 https://pia.gov.ph/news/articles/1014934
sia.com/cybersecurity-in-the-philippine-academe-to-bridge-skills-gap/
179 https://dict.gov.ph/wp-content/uploads/2017/05/2017-ICT-Specialist-Proﬁciency-Examination-FAQ.pdf and
180 http://www.bsp.gov.ph/ regulations/regulations.asp?id=3174
182 https://cnnphilippines.com/business/2017/05/04/Govt-to-invest-P2B-for-national-cybersecurity.html
184 http://i.gov.ph/cyber-security/
186 http://www.bsp.gov.ph/about/advocacies_fin.asp
curing-the-future-of-financial-technology-against-cybercrime
https://www.kapronasia.com/asia-banking-research-category/vietnam-fintech-regulatory-sandbox.html
https://www.opengovasia.com/vietnam-strengthens-human-resources-for-information-security-tasks/
https://fintechnews.sg/30318/vietnam/key-takeaways-from-vietnam-startup-ecosystem/
ACKNOWLEDGEMENTS

Research Team
PayPal
Usman Ahmed, Director, Head of Global Public Policy
Mathilde Bonneau, Lead Manager, Government Relations
Steven Xavier Chan, Senior Director and Regional Head of Government Relations, Asia Pacific
Lim Siew Hoon, Infosec Research and Outreach Global Program Manager
Phoram Mehta, Senior Director, Chief Information Security Officer for Asia Pacific
Amrita V. Nair, Associate, Government Affairs
Mangesh Samant, Business Information Security Officer for Southeast Asia

Special thanks to our fellow colleagues, Sophia Ho, Head of Communications, Southeast Asia; Jerry Tso, Head of Singapore Development Center and the PayPal Innovation Lab team for their contribution and support to the report.

TRPC
Peter Lovelock, CEO and Founder, TRPC Pte Ltd
Lim May-Ann, Managing Director
Hiromi Oka, Research Analyst
Faiza Saleem, Research Analyst
Cheryl Tan, Research Analyst

We would like to thank all the FinTech companies for their participation in the PayPal ASEAN cybersecurity survey. We are also extremely grateful to the following contributors for their support to the report: - American Chamber of Commerce in Singapore, Singapore Economic Development Board, and Singapore FinTech Association.

About PayPal
Fueled by a fundamental belief that having access to financial services creates opportunity, PayPal is committed to democratizing financial services and empowering people and businesses to join and thrive in the global economy. PayPal has remained at the forefront of the digital payment revolution for more than 20 years. Our open digital payments platform gives PayPal's over 375 million active account holders the confidence to connect and transact in new and powerful ways, whether they are online, on a mobile device, in an app, or in person. Through a combination of technological innovation and strategic partnerships, PayPal creates better ways to manage and move money, and offers choice and flexibility when sending payments, paying or getting paid. Available in more than 200 markets around the world, the PayPal platform enables consumers and merchants to receive money in more than 100 currencies, withdraw funds in 56 currencies and hold balances in their PayPal accounts in 25 currencies.

At PayPal, we regard fighting cybercrime as a strategic business priority, and we invest heavily in trying to keep our sites and services as safe and secure as possible. PayPal's philosophy on cybersecurity has a heavy focus on customer data protection. Everything we do around security is living up to our commitment as the "secure way to pay and be paid."

For more information on PayPal, visit https://www.paypal.com/about.
About TRPC

TRPC is a specialist think-tank and research consultancy focused on ICT, telecommunications and digital industries and services in the Asia Pacific. With over 30 years' experience working with multinational firms, industry associations, government bodies, and international organisations, TRPC’s research-driven, evidence-based work highlights the economic impact of the emergence of new business models and the developments in telecommunications and information technologies, as well as the impact of the policy and regulatory issues associated with the digital economy at large. TRPC serves as secretariat for the Asia Cloud Computing Association (ACCA) and runs the Asia Chapter of the International Institute of Communications (IIC), both platforms where policymakers and industry stakeholders interact on a regular basis over pertinent and current digital economy issues in the Asia Pacific region. TRPC is headquartered in Singapore with regional offices in Hong Kong, and Melbourne, Australia. Contact them at https://www.trpc.biz
DISCLAIMER STATEMENT

This report has been prepared and issued by PayPal Pte. Ltd.

This report presents an analysis of the Fintech cybersecurity landscape in ASEAN at time of writing. Information in this document is based on a review of existing publicly available information available to PayPal at the time of preparation, internally developed data and other sources that are believed to be reliable and was guided by expert input and advice throughout its preparation.

This document and the information provided herein, which may include recommendations, are released to inform interested parties of research and to encourage collaboration of FinTechs towards a cyber resilient FinTech ecosystem in the ASEAN region. It should not be construed in any manner whatsoever as tailored advice.

While reasonable care has been taken in the preparation of the document to ensure that its contents are accurate, complete and up-to-date as at the date of publication, PayPal does not make any warranty or representation (expressly or impliedly) to that effect. PayPal does not guarantee and is not responsible for the quality, currency, propriety, accuracy, completeness or reasonableness of any statements, information or conclusions contained in the report or the source documentation. PayPal is not responsible for any errors or omissions or injury, loss or damage arising from or relating to the use (or misuse) of any information, statements or conclusions contained in or implied by the information in this report or in any of the source documentation.

This document may contain links to other information available on the websites of third parties on the Internet. PayPal does not have control over the content of such sites. Use of third-party sites is governed by the terms and conditions set out for such sites. PayPal does not make any guarantee with respect to any information contained on such third-party sites and PayPal is not responsible for any injury, loss or damage suffered as a result of using such third-party sites.

Opinions contained in this report represent those of PayPal at the time of publication. Forward-looking information or statements in this report contain information that is based on assumptions, forecasts of future results, estimates of amounts not yet determinable, and therefore involve known and unknown risks, uncertainties and other factors which may cause the actual results, performance or achievements of their subject matter to be materially different from current expectations.

To the fullest extent allowed by law, PayPal accepts no liability whatsoever for any direct, indirect or consequential losses, loss of profits, damages, costs or expenses arising out of or in connection with the use of all or any of the data or information in this report.

This legal disclaimer and any questions or matter of any nature arising from or relating to the content or use (or misuse) of this document will be governed by and interpreted in accordance with the laws of Singapore, and all proceedings shall be subject to the exclusive jurisdiction of the courts of Singapore.

Copyright © 1999-2021 PayPal. All rights reserved.