address the investment gap, ASEAN countries need to spend[3] between 0.35 and 0.61 percent of their GDP—or $171 billion collectively—on cybersecurity in the period spanning 2017 to 2025. This is a small price to pay considering the value-at-risk and the fact that ASEAN governments spend up to 3.4 percent of GDP[4] on other items, including defense.

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

1 The ASEAN Region: A Prime Target for Cyberattacks

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

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

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

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

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

[4] World Bank

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

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