creates the potential risk of many of these devices being weaponized and used across businesses, industries, and even countries.

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

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

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

The proliferation of consumer IoT devices

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

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

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

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

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