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

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

2.1.4 Technological evolution is increasing complexity

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

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

The convergence of IT and OT

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

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

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