The convergence of IT and OT

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

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

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

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

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

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