The state of IT and OT convergence in China

The way that businesses use technology is evolving at a rapid pace. Tech-driven innovation is a key battleground for competitive differentiation across industries and markets, as organisations embrace the Internet of Things (IoT), big data, Artificial Intelligence (AI), cloud, and modern network technology as part of a push towards Industry 4.0.

Building interconnected digital value chains requires organisations to unify traditionally separate processes across Information Technology (IT) and Operational Technology (OT). This convergence of IT and OT helps businesses achieve new levels of growth and operational scale, although it raises critical security challenges that can be difficult to address.

Telstra commissioned technology research company Omdia to investigate the state of IT and OT convergence in North Asia, including China, Hong Kong, South Korea, Japan and Taiwan. While 85% of firms expect business benefits from convergence, many find it difficult to manage cybersecurity challenges.

Despite some common hurdles, each market shows interesting distinctions. Here are some key barriers and enablers for IT/OT convergence in China.
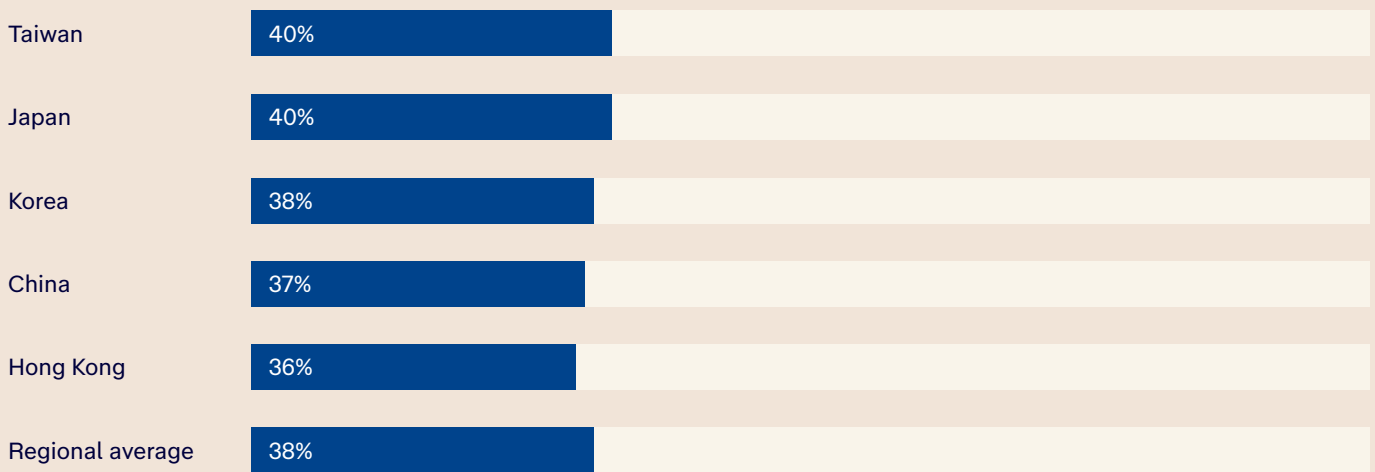
IT/OT maturity in China

China has the second-lowest levels of IT/OT system integration in North Asia, with 37% of IT and OT systems integrated across industrial settings, compared to a regional average of 38% (see Figure 1).

In China, 46% of firms have completed some level of digitisation to connect IT and OT systems, much higher than the regional average of 34%. Across the region, 44% of firms have integration activities in progress and only 8% are at the beginning stages of this work.

Over half (51%) of China-based organisations plan to have IT and OT well integrated in the next 12 to 18 months and 54% see it as important for business outcomes, which is the highest in the region (with a cross-region average of 48%).
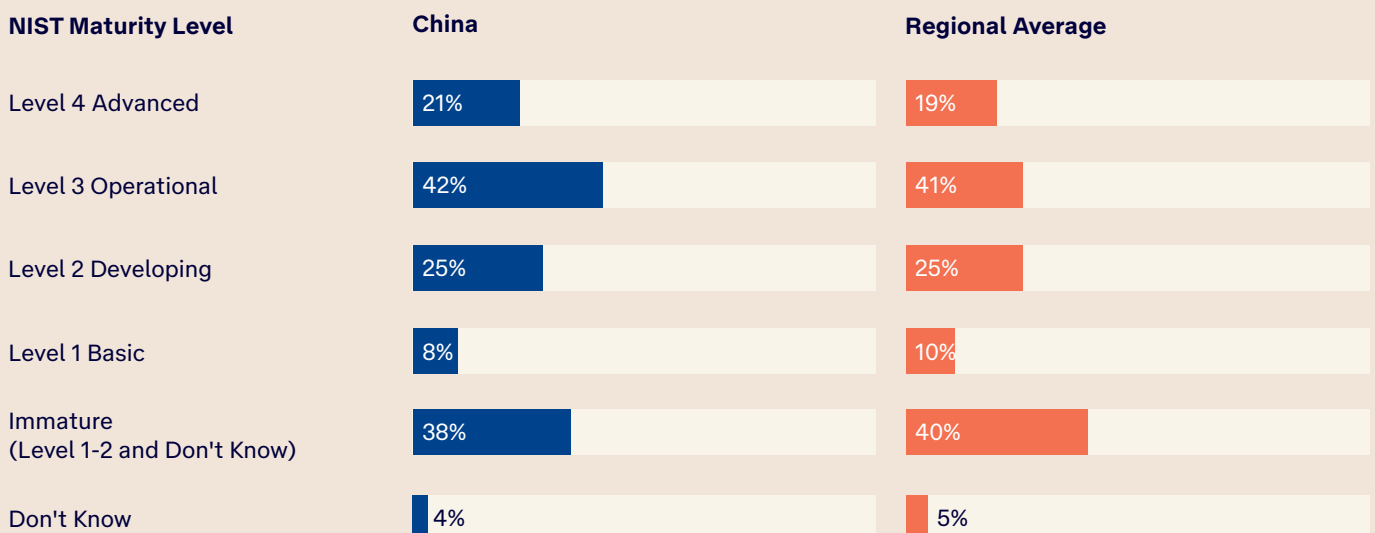
Figure 1: Percentage of IT/OT integration by market

| Market	Percentage
Taiwan	40%
Japan	40%
Korea	38%
China	37%
Hong Kong	36%
Regional average	38%

OT security maturity in China

China is the second-most mature market when it comes to OT security, with 21% of firms saying they're 'advanced' in securing OT, exceeding the cross-regional average of 19%. However, IT/OT security is still sub-optimal, with 38% of firms reporting immature levels (see Figure 2).

Figure 2: OT security maturity in China

NIST Maturity Level	China	Regional Average
Level 4 Advanced	21%	19%
Level 3 Operational	42%	41%
Level 2 Developing	25%	25%
Level 1 Basic	8%	10%
Immature (Level 1-2 and Don't Know)	38%	40%
Don't Know	4%	5%

In China, 70% of the most significant major security incidents or breaches that impacted operations started in cyber (IT), with just 30% starting in OT (see Figure 3). That's largely consistent with the rest of the region and highlights the risk of how attacks targeting IT can impact operational processes and technology as convergence progresses.

Figure 3: Origin of attacks on organisations

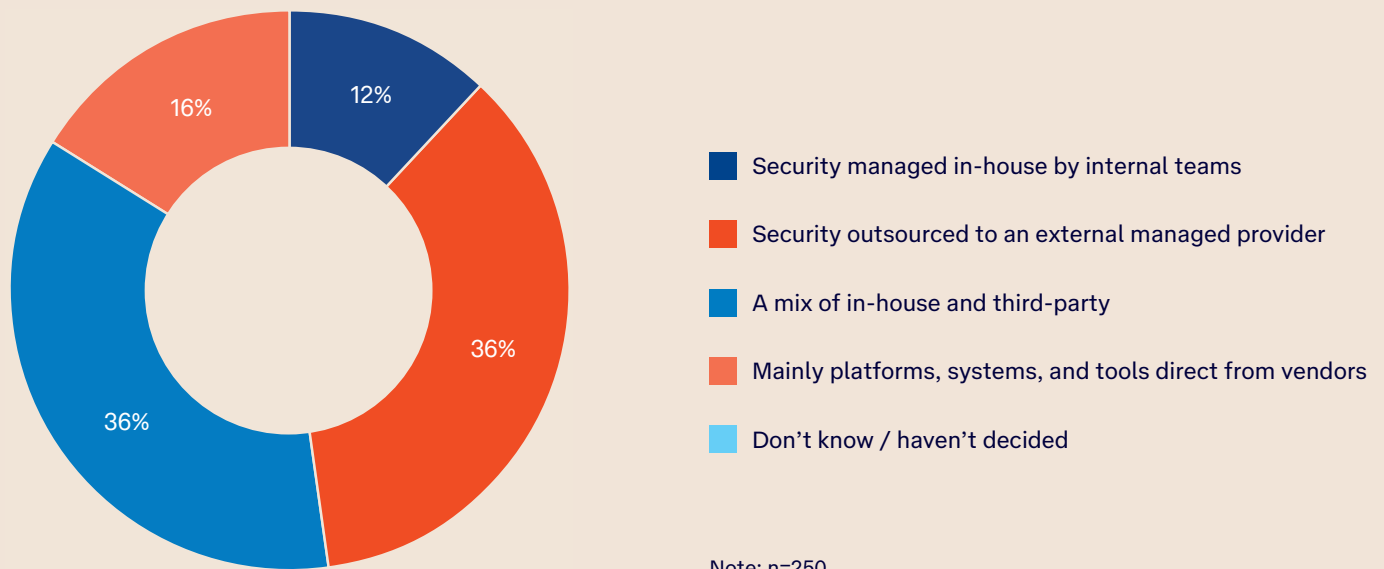|	Physical (OT) to Cyber (IT) Attack	Cyber (IT) to Physical (OT) Attack
China	30%	70%
Average	26%	74%
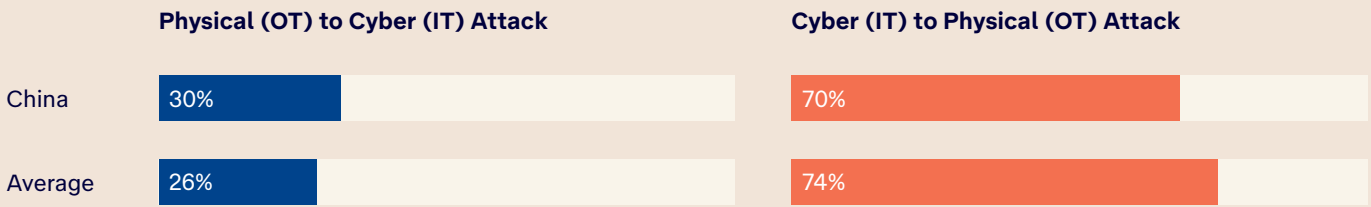
Calling in outside help

Finding the right talent to help manage the complexity of IT/OT convergence is incredibly challenging for many organisations. Risks often mount very quickly, as threats that target one previously siloed system can rapidly have a broader impact on critical business data and processes once integrated.

That's why most firms across North Asia plan to engage a third party to help them manage IT and OT security in the next 18 months, with 42% saying they'll completely outsource security to an external managed services provider.

The need for third-party help is strong in China, with 72% of firms planning to outsource to an external provider (either completely or in a mixed arrangement), while just 12% plan to go it alone and 16% say they'll rely largely on vendor platforms, systems, and tools (see Figure 4).

Figure 4: How will your organisation likely manage IT and OT security 18 months from now?

- 12% Security managed in-house by internal teams
- 36% Security outsourced to an external managed provider
- 36% A mix of in-house and third-party
- 16% Mainly platforms, systems, and tools direct from vendors
- Don't know / haven't decided

Note: n=250

With a team of trusted IT and OT security experts, Telstra is fully equipped to help North Asian organisations take the next step on their IT/OT convergence journeys. To learn more about how convergence can transform your business, get in touch with a Telstra representative or download the full white paper at telstra.com/securing-ot-it-convergence-whitepaper

Telstra

Want to learn more about how to improve IT and OT security in your organisation?

Contact your Telstra account representative for more details.

🌐 **telstrainternational.com**   ✉️ **telstraenquiry@team.telstra.com**