Securing Industry 4.0: The Challenges and Opportunities of IT/OT Convergence

Discover how executives are securing IT/OT/IoT to leverage the benefits of emerging technologies.

A paper in partnership with Omdia

Contents

1.0 Executive summary

Context

Telstra commissioned Omdia to research the state of information technology (IT) and operational technology (OT) convergence in North Asia: China, Hong Kong SAR (the Hong Kong Special Administrative Region of China), Taiwan, Japan, and South Korea.

The research assesses the security operations (SecOps) readiness of firms to leverage emerging technologies under the Industry 4.0 revolution. It encapsulates how different sectors can leverage cloud, artificial intelligence (AI), the Internet of Things (IoT), and other advanced technologies for commercial success.

This paper gives security executives the insights they need to bolster their organisational cybersecurity resilience and support their ongoing digital transformation projects in critical infrastructure sectors, including manufacturing, healthcare, retail/wholesale, smart buildings and infrastructure, and transport, logistics & shipping.

Who did we speak to?

Field survey:

250 technology executives and managers were surveyed in September 2023.

Ten deep-dive interviews ran in parallel.

Respondent mix
(Percentage of total):

Technology or Security Executive or Manager 68%

Line of Business Director or Manager (e.g. Operations, Supply chain, Manufacturing, Quality) 32%

Sectors surveyed:

Manufacturing

Healthcare

Retail/wholesale

Smart buildings and infrastructure

Transport, logistics & shipping

Organisation size
(Percentage of total):

40% with 500-1000 employees

60% with 1000+ employees

Domains surveyed:

Information Technology and Operational Technology Converged across the NIST CSF Stack and ISA95 model

Regions surveyed:

China

Hong Kong SAR

Taiwan

Japan

Korea

IT/OT convergence, also called cyber-physical integration, is gathering pace across critical sectors in the region

Our research concluded that security preparedness is relatively low in North Asia, and firms face complex challenges. Nearly 40% of OT systems across many industries now connect to IT systems, and this proportion will increase to over 50% within a year.

Organisations are eager to exploit the benefits of emerging technologies for Industry 4.0, including IoT, AI, big data, cloud computing, hyperconnectivity, and encompassing 5G networks, enterprise mobility, and edge computing.

Industry 4.0 encapsulates strategically leveraging advanced technologies and new business models in harmony with legacy systems to optimise scale, resilience, and efficiency in critical infrastructure sectors at levels beyond historical precedents.

85% of firms expect business benefits from IT/OT convergence, including innovation, reliability, integrity, and revenue growth improvements. Across the region, many organisations are well progressed in digitalising physical systems with IT capabilities.

However, cybersecurity challenges are growing as integration progresses, and the negative impacts are multiplying. 88% of organisations have recently dealt with a security incident that directly affected OT production environments, an alarming statistic.

Leaders invest in IT/OT/IoT-enabled cybersecurity platforms and solutions to overcome increasing incidents and breaches. However, this can result in more complexity of sprawling tool sets that generate a higher volume of alerts and false positives, not to mention prohibitive management overheads. Leaders across the region emphasised the unmet need and the necessity of a “single pane of glass” to help protect against, identify, and respond to cybersecurity threats.

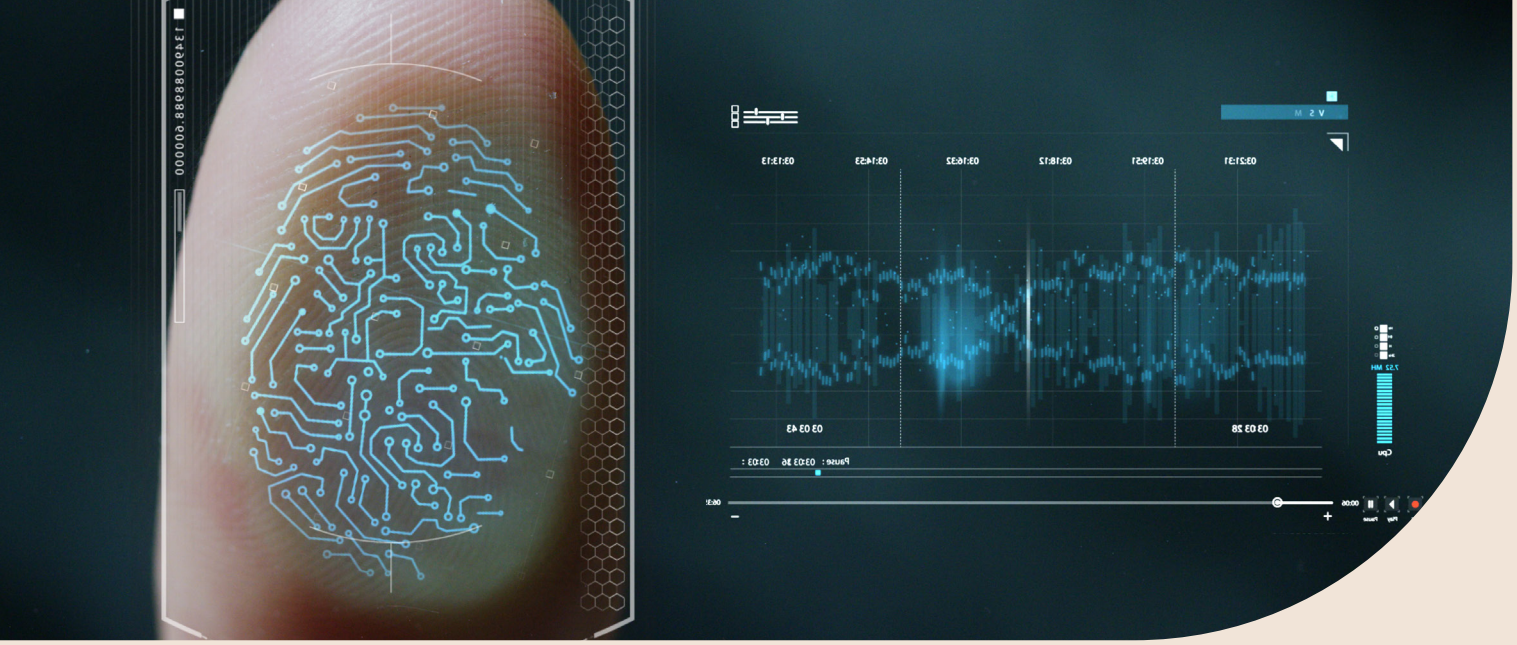
Finding people with the skills and expertise to understand the complexities of IT/OT environments and secure cyber and physical systems is a growing challenge.

China and Japan are more prepared to address IT/OT/IoT challenges than other North Asian locations. From an industry point of view, manufacturing, transport, and logistics are the least prepared.

This paper provides analysis, insights, and recommendations to help executives harness the nascent potential of emerging advanced technologies while minimising cybersecurity risks and improving resiliency.

> “The management team decided the IT team was now to handle both the IT security and the OT security. It’s better to be on the same team, because in the OT part there are several things that are very closely related. The benefits should be cost reduction and improved security.”
>
> Security executive at a manufacturer, Japan

> “Connecting IT with OT has already helped reduce development and product costs, but our SCADA, MES, PLC, and HMI are largely separate. In the future, we want to expand integration with SaaS to remove local systems and improve customisation, but this will take at least three years. Our biggest challenges are upgrading PLC, moving to 5G, and using IoT.”
>
> COO for OT at a large transport company in China



Key findings

54% of firms believe Industry 4.0-related digital transformation and leveraging advanced technologies have been the most significant factors accelerating recent IT/OT convergence.

More than 50% of firms recognise IoT, cloud computing, and enterprise mobility as essential technologies for driving digital change.

85% of firms expect business benefits from IT/OT convergence. Most firms that have completed some level of IT/OT integration are satisfied with progress across innovation, reliability, and system integrity.

More than 50% of OT systems will be connected to IT networks in the next year, up from 38% today. 76% of regional firms have digitised physical or manual processes to achieve business outcomes.

88% of organisations have recently dealt with a security incident that directly affected OT production environments.

Of those firms that suffered an incident or breach, nearly 50% experienced a significant attack on Level 3.5 DMZ systems, challenging the sufficiency of a historical, air-gapped approach to cybersecurity.

64% of security incidents in IT/OT environments were from fraud (including ransomware), 59% also experienced distributed denial-of-service (DDoS) attacks, and 58% saw malware intrusions.

74% of attacks that affected critical infrastructure operations started from IT systems and networks.

Despite the criticality to the core business, only 13% of all firms surveyed are “advanced” in securing IT/OT/IoT. 60% are only at basic or developing levels of securing OT.

In 50% of firms, the CISO is directly responsible for understanding and implementing an IT/OT converged cybersecurity program. In a slightly smaller proportion of firms that role is taken by a chief security officer or CTO.

Good visibility of all industrial IoT and OT assets is essential for 96% of organisations.

To address these challenges, 42% of firms outsource IT, OT and IoT Security to a third-party managed service provider.

2.0 IT/OT convergence is accelerating in North Asia

Industry 4.0 will drive continued IT/OT integration

North Asian organisations are eager to exploit the benefits of Industry 4.0 emerging technologies

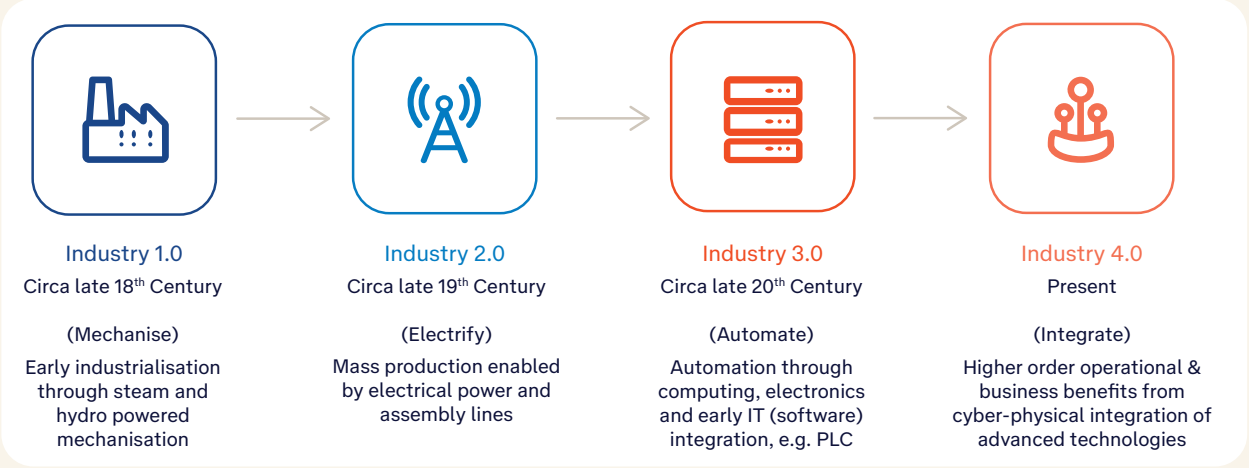
Industry 4.0 (the Fourth Industrial Revolution) refers to advancements and applications of recent digital technologies across sectors (see Figure 1).

Industry 4.0 encompasses Internet of Things (IoT), AI and machine learning (ML), cloud computing, and cybersecurity across all sectors where cyber-physical systems are essential.

Industry 4.0: A modern definition

Strategically leveraging advanced technology, including cloud, AI, and IoT, with new business models, harmonised with legacy systems to optimise scale, resilience, and efficiency in critical infrastructure sectors at levels beyond historical industry precedents.

Figure 1: The significant technological and process advancements driving industry change over time



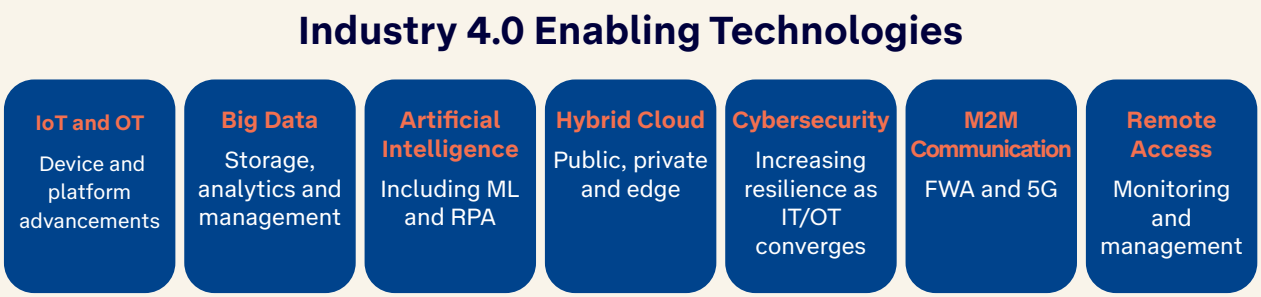
Source: Omdia

Industry 4.0 transforms data into intelligent insights and delivers commercial and human benefits. These include increasing equipment efficiency and resilience, automating functions (e.g. inventory management and maintenance schedules), improving quality, lowering energy usage, and reducing waste.

In contrast to the first, second, or third industrial revolutions, Industry 4.0 is driven by the IoT, automation, massive amounts of data, cloud computing, analytics enabled by AI/ML, and hyperconnectivity from 5G technology, technologies that did not exist or were not readily available until recently.

More recently, global multinational corporations with Asian operations and interests are making concerted efforts to redesign and optimise supply chains and manufacturing capabilities.

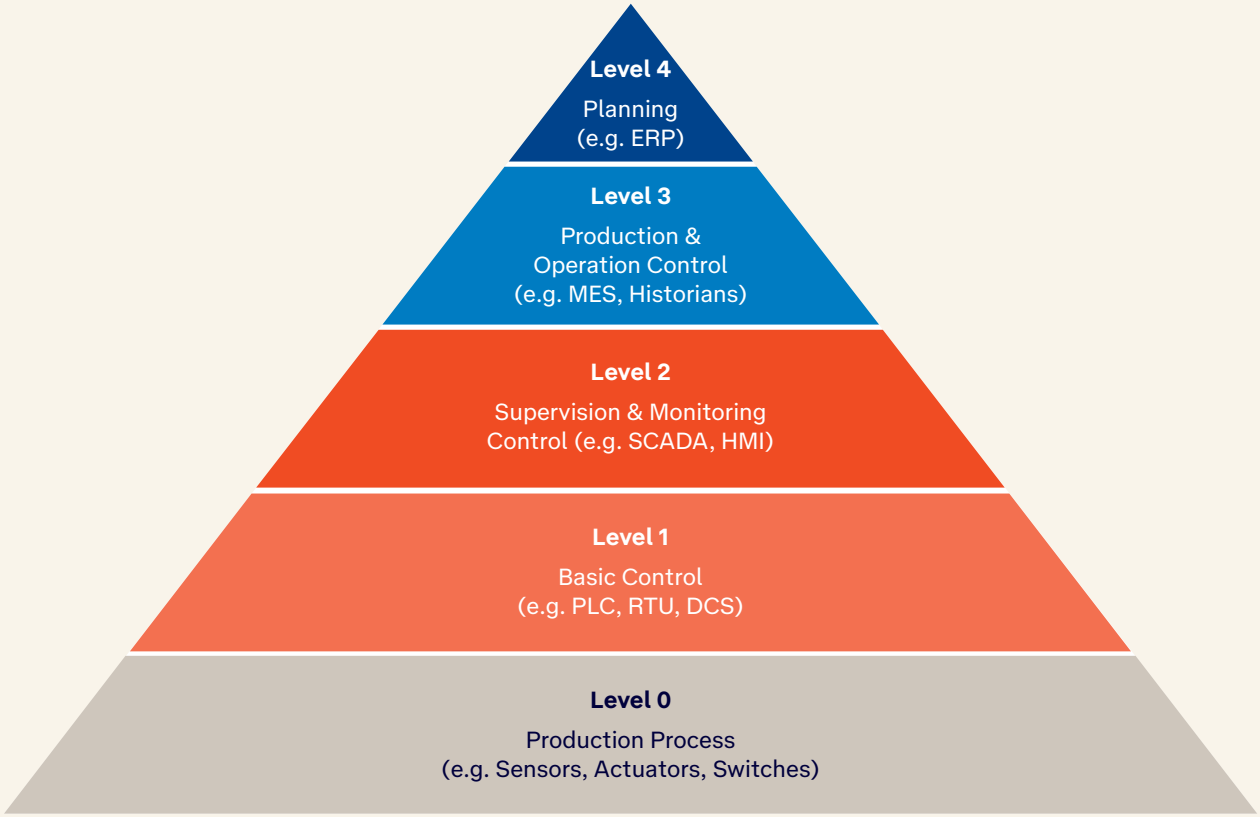
Figure 2: Essential technologies underpinning the Industry 4.0 revolution



Source: Omdia

It is essential to establish a view of the connectivity and layers of OT. The Purdue model (Purdue Enterprise Reference Architecture) influenced the now popular ISA-95 model (ANSI/ISA-95) (see Figure 3).

Figure 3: The ISA-95 (Purdue) pyramid model is a reference framework to conceptualise OT



Source: Omdia

Both terms are often used interchangeably and present a conceptual framework commonly applied to describe, analyse, and optimise industrial networks in manufacturing, utilities, industrial processes, and other service industries.

ISA-95, much like ISO/OSI in the IP data world, presents a foundational architecture; it shows the flow of data across corporate (IT) and physical (OT) networks.

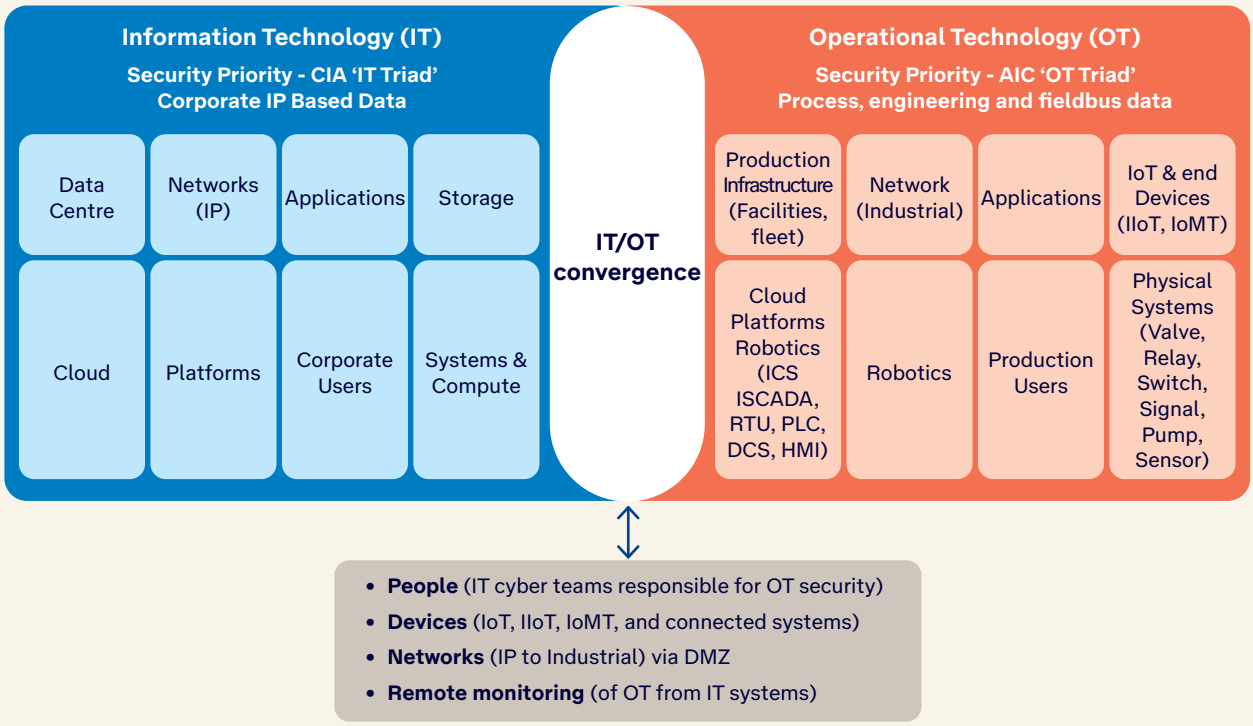
Each model layer represents different degrees of data flow from east to west (within each layer) and north to south (across layers), including from IT access down to OT.

IoT devices are increasingly common at Level 0 and are part of OT. IoT includes connected devices communicating and transferring data autonomously between other devices, the cloud, and more complex systems. IoT spans consumer (e.g. home automation, connected cars) through business and commercial use, including in industrial settings to complement industrial control systems (ICS) by augmenting data flow and control when attached or embedded.

Where and why IT and OT (including IoT) are converging

As shown in Figure 4, convergence is pervasive across a wide array of IT and OT domains, including IoT and IIoT.

Figure 4: IT and OT convergence spans people, devices, networks and remote monitoring



Source: Omdia

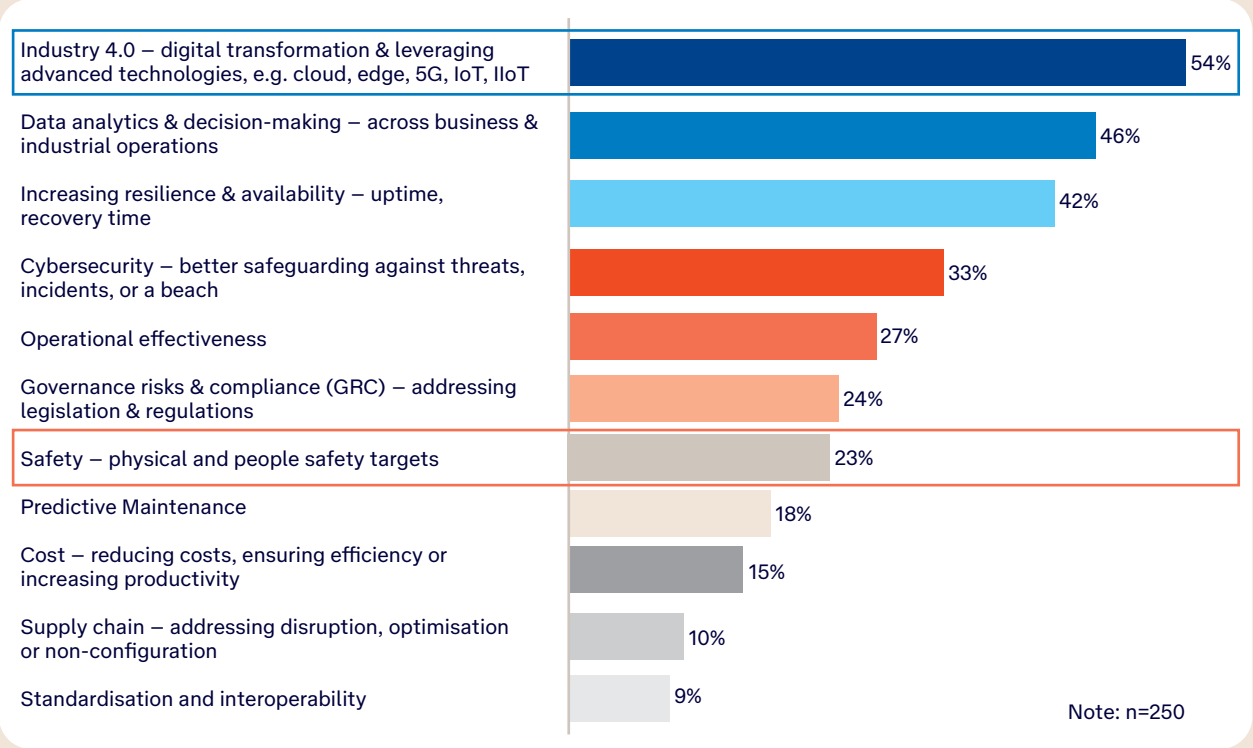
Across the region, the most crucial factors accelerating the convergence between IT and OT systems in the past 18-24 months have been Industry 4.0, data analytics, increasing operational resilience, and addressing cybersecurity (see Figure 5).

In OT environments, the most important goals are typically safety, integrity, and availability (the SIA triad), while in IT cybersecurity, the focus is on confidentiality, integrity, and availability (the CIA triad).

The survey responses indicate that safety is essential but not a primary driver of advanced technologies. In most cases, Industry 4.0 technologies can greatly improve safety outcomes in industrial environments.

Figure 5: Industry 4.0 is a key driver of IT integration with OT

Q. What have been the most crucial factors accelerating the convergence between IT and OT systems in the past 18-24 months?



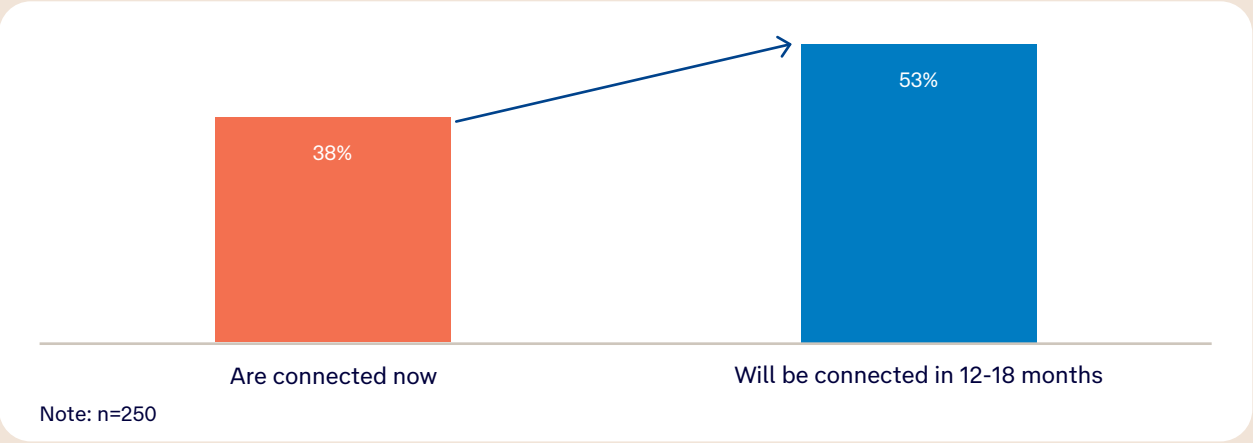
Source: Omdia

IT/OT integration will drive industry-changing benefits

Cyber-physical integration continues to grow across industries (see Figure 6).

Figure 6: Cyber-physical integration is rapidly increasing as IoT devices proliferate across industries

Q: What percentage of your OT systems or physical operational systems are/will be connected to IT systems?



Source: Omdia

The percentage of OT systems and IoT devices connected to IT networks is constantly growing (see Figure 5). Moreover, 48% of executives state that better connecting IT with OT is “very important” to achieving their business outcomes (see Figure 7).

Figure 7: Innovative industry model changes are made possible through technology

Smart Manufacturing

Advanced robotics and computer-controlled, self-optimising manufacturing plant leveraging AI autonomous sensors to improve production (horizontally) across industrial environments and (vertically) up into quality assurance and research development.

Intelligent buildings

Leveraging connectivity, sensors, and automation through building management systems, IoT, and big data to drive sustainability and energy optimisation, safety, and monitoring improvements that will increase the standard of living.

Retail and wholesale

Harnessing automation across inventory management and ordering, predicting customer demands through advanced analytics, and increasing sales and service through digital channels.

Healthcare

Significantly improving health outcomes through electronic health records, telemedicine, health device additive manufacturing using 3D Printing, robotic-assisted surgery, and the Internet of Medical Things (IoMT).

Supply chain & logistics

IoT, robotics, AI, and big data to monitor, analyse, and predict demand for advanced planning, resilient supply chains to meet shifting market demands, and autonomous robots in handling and distribution centres.

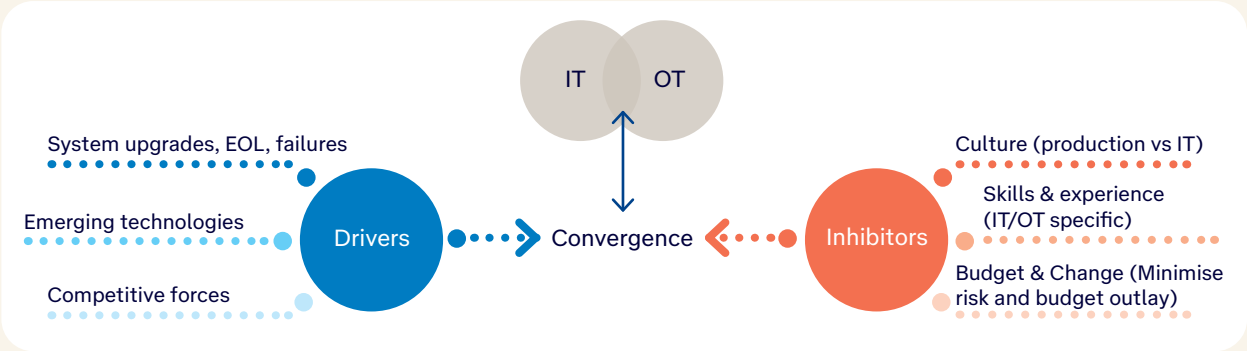
Source: Omdia

There are many current and emerging examples of where integration will deliver transformative innovations. The emergence of advanced technologies, microservices architecture, and hypercompetitive global markets will see a new era of digital transformation across industries.

Understanding the drivers and inhibitors of convergence

Figure 5 revealed that Industry 4.0 is an important IT/OT convergence driver across sectors. Interviews with executives and experts across the region surfaced other critical factors that will foster and hinder IT/OT integration, captured in Figure 8.

Figure 8: Primary factors identified by regional leaders that will encourage or hinder IT/OT integration



Source: Omdia

Drivers

End of life (EOL): Systems with complex upgrade cycles are reaching EOL across Level 0 (production) through Level 4 (ERP/mainframes), including IoT and IIoT.

Solution availability: There is readiness for and access to new architectures (Azure AKS for IoT), industry solutions (SAP, Oracle), and specialist firms (Siemens, Emerson, Honeywell, Schneider Electric).

Market forces: As new entrants (e.g. Chinese manufacturers) harness new technologies to dramatically lower the cost of entry into established markets, established firms must leverage similar technologies into their IT/OT estate to drive efficiency, scale, and cost/quality.

Inhibitors

"Us versus them": Responsibilities for IT (corporate) and OT (production/ industrial) systems are typically divided between teams at sites (e.g. manufacturing) because of the physical nature of operations.

Insufficient skills: This includes skills in IT/OT security as Industry 4.0 technologies rapidly evolve.

Investments: Challenging macroeconomic conditions mean many firms in mature sectors face flat or reducing IT and security budgets (e.g. they allocate most investment to "run", not "innovate").

Legacy systems: Aging ICS and supervisory control and data acquisition (SCADA) are potentially too expensive to rip and replace with specialised OT solutions.

> In China, we are trying to make a modern community based on building automation systems. These are connected to a control centre, so you know what's really happening in a building, and you can make near real-time decisions around temperature, lighting, and security."
>
> Technology director at a smart building provider in China

Overcoming integration challenges is becoming increasingly possible

As highlighted in the previous section, the technology industry continues to innovate and offer various solutions to address convergence issues, for example, Microsoft Azure AKS for IoT.

Omdia also notes that applying convergence and Industry 4.0 technologies to established legacy infrastructure does not mean having to adopt traditional specialist OT solutions. Many vendors are playing catch-up with supporting the modern IoT-enabled paradigm (the ENISA-revised Purdue model is an example).

A more cost-effective approach for established sectors with tight budgets is to start with modern cloud infrastructure and IoT frameworks (MQTT, Azure AKS for IoT) and build support for Industry 4.0 alongside operational technologies to meet tactical outcomes (e.g. cost reductions) and strategic benefits (e.g. product innovation).

Further, as OT security shifts increasingly to IT groups and corporate security executives, Omdia expects rapid adoption of OT-specific security platforms that tightly integrate with existing security information and event management (SIEM) and security orchestration, automation, and response (SOAR) capabilities.

3.0 The state of IT/OT/IoT integration with cybersecurity in North Asia

Cybersecurity is a critical issue when leveraging advanced technologies

Understanding the core challenges and incident rates

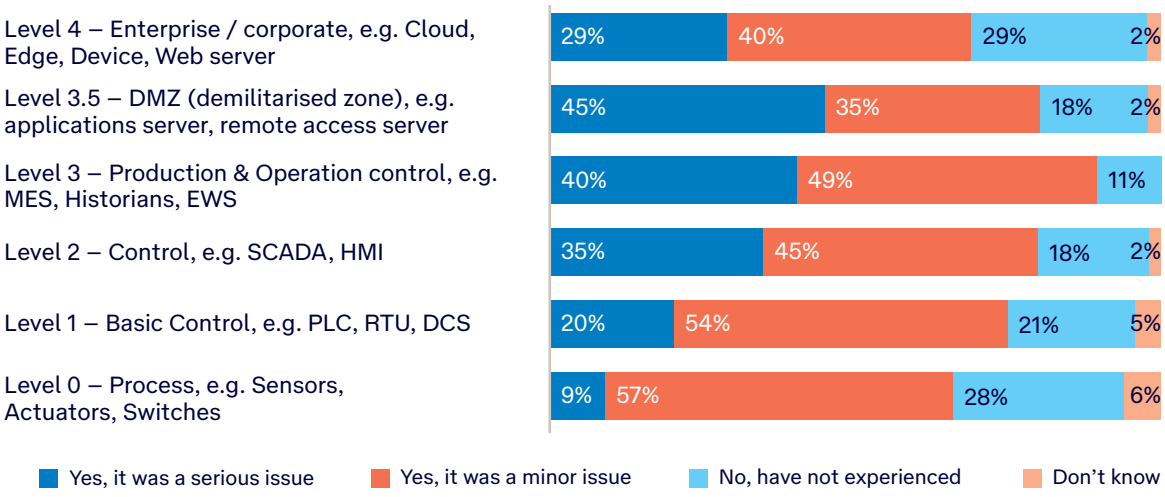
Cybersecurity is both an expected outcome of IT/OT convergence, including IoT and IIoT, and a challenge as integration progresses.

More than 30% of executives ranked security as one of the most extensive improvement areas expected from future IT/OT convergence, alongside revenue growth (35% of respondents), integrity improvement (42%), reliability (47%), and innovation (52%).

However, security is a challenge for the 38% of firms that have already integrated. In the past year, 88% of organisations have dealt with a security incident that had a direct impact on OT production environments (see Figure 9).

Figure 9: Every firm with OT has faced a recent security incident across each level of industrial environments

Q: Has your organisation experienced a significant increase in overall security incidents or breaches in any of these areas in the last 12 months?



Note: n=250

Source: Omdia

Fraud, DDoS, and malware are the most prevalent attacks on OT systems

Factors driving OT risks include economic and geopolitical damage from successful attacks, fraud crimes through ransomware, extortion and operational disruption threats, and common attacks targeting IoT (see Figure 10).

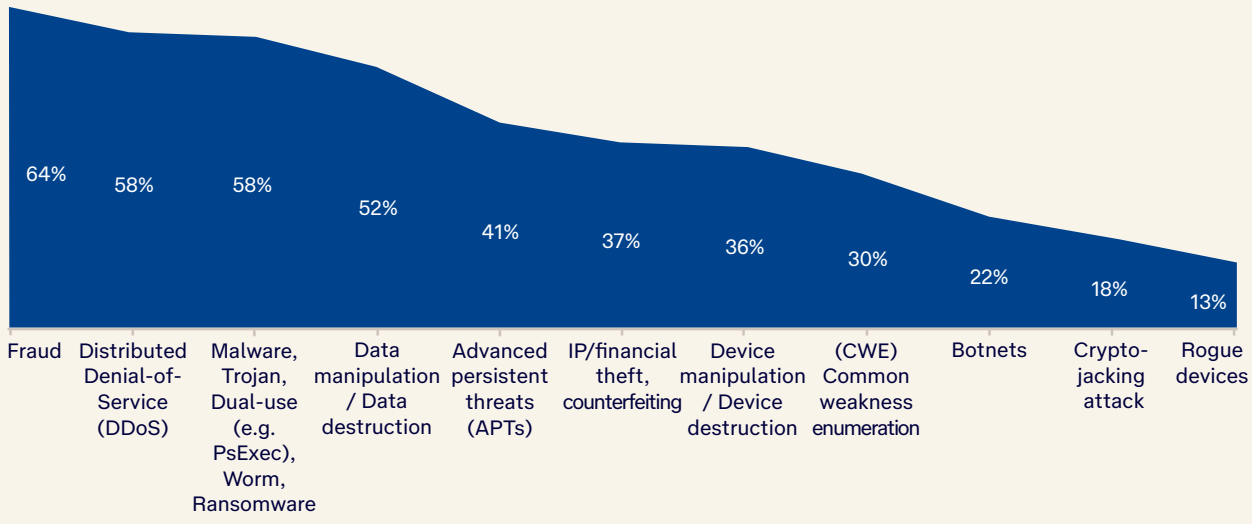
Attackers are becoming more sophisticated in accessing unencrypted or unsecured connected IoT systems to access, extract, and exploit commercially sensitive data or traverse across devices into other systems. Common goals of attacks are to disrupt operations for cyber-extortion gains and steal proprietary and confidential data.

DDoS attacks are dominant as more IoT (including IIoT and IoMT) devices come on net through fixed, virtual (SD-WAN), and mobile (5G) networks connected to hybrid cloud and edge computing.

> “Across IT and OT, we have over 200 security incidents a month to investigate. There are lots of people trying to hack into our system with brute force attacks and port scanning, especially of our DMZ. We will lose HK$10m per day if our OT production system goes down.”
>
> Security executive at a manufacturing company in Taiwan

Figure 10: Cyber extortion and fraud are common problems among critical infrastructure sectors

Q: What were the most significant IoT or OT-specific cybersecurity-triggered incidents, events, or threats you encountered in the past 12 months?



Source: Omdia

Dispelling the “air-gapped security is enough” myth

Historically, manufacturing and other industrial sectors have relied on air gapping for security. Air gapping – sometimes called security by obscurity – is where OT systems, including IoT and IIoT, are typically physically, logically, or virtually segregated from corporate IT systems, and this has been relied on to insulate ICS from external threats.

This approach requires LAN segmentation (physical or virtual) to segregate industrial networks from corporate systems with tight control over remote access.

The challenge with this mindset is the inevitability of IT/OT convergence across the different OT levels over time and the ensuing risks where cybersecurity implications are not pinpointed or addressed.

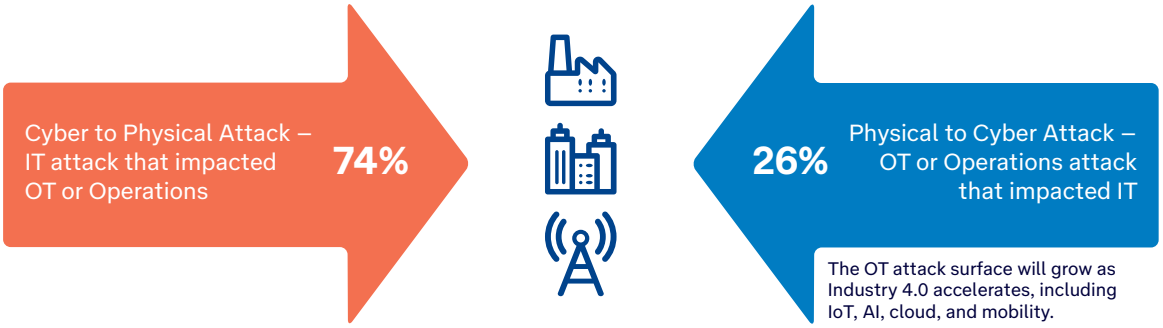
Omdia’s research revealed that 80% of organisations have experienced a recent significant increase in security incidents in their Level 3.5 DMZ environment, with most attacks that affected critical infrastructure sectors originating in IT, not OT (see Figure 11).

The upshot is that firms must assume OT can be affected either directly through or independently of IT, but regardless, any major security incident will cause significant disruption to core operations, representing a material risk to the business.

> “The Asia region is a massive growth engine for us. But OT security is a challenge as IT teams often overlay a conventional IT solution to OT problems with a hardware format. Also, conventional manufacturers are often at a disadvantage as they have embedded systems. This results in a time-consuming process and significant changes that need to be made.”
>
> Japan operations director of a US car manufacturer expanding into connected cars

Executives must be prepared for the worst as cybercriminals become more emboldened with successful attacks and extortions and the attack surface increases with adoption of Industry 4.0 technology (especially IoT).

Figure 11: Most attacks that affect the OT environment originate in IT and corporate systems



Expensive cost of being offline
A direct attack on OT, or the threat of direct interference with the monitoring or control of OT, is sufficient to take operations offline while investigation or remediation takes place.

Harder for attackers to execute, but still a risk
Unencrypted, unsecured, and misconfigured physical devices, including sensors, PLC, and SCADA, are less common. However, as these devices age, failures become a challenge.

Source: Omdia

4.0 IT/OT security preparedness in North Asia

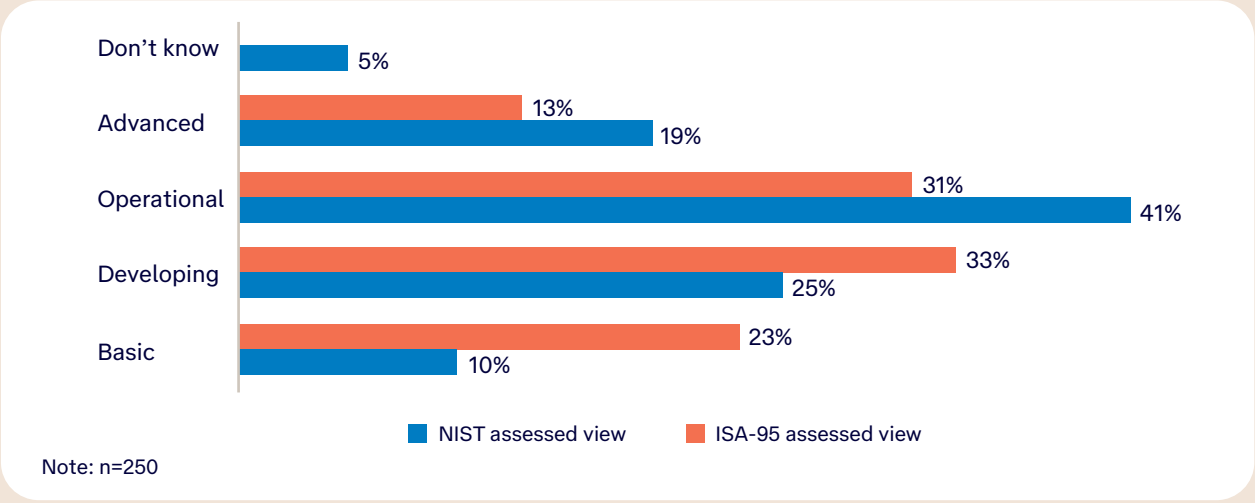
This white paper is intended to help IT and OT security executives across sectors and throughout the region understand the challenges and consider their firms' readiness. Our research reveals that most firms are unprepared for OT security challenges as cybersecurity executives become increasingly responsible for OT environments.

IT/OT security readiness is challenged and seems riskier through the lens of devices and systems (ISA-95)

Figure 12 shows many firms are still at only the fundamental levels of basic or developing maturity in securing IT/OT convergence, including IoT (IIoT), and the readiness is higher when they are assessed through a threat lifecycle lens (NIST CSF) than when we look at the OT stack (ISA-95). IIoT refers to the industrial use of IoT technologies, platforms, and capabilities for sector-specific outcomes and is crucial for North Asia.

Figure 12: Firms are far less prepared for OT security when assessed through the ISA-95 (Purdue) model than through NIST CSF

Q: How mature is your organisation in securing IT/OT convergence from 1 to 4? (Comparing NIST with ISA95/ Purdue framework perspectives)



Note: n=250

Source: Omdia

The NIST CSF framework assessment assumes that asset visibility, cross-team security integration, tools, platforms, and architectures are in place across the industrial and IT/corporate zones. Conversations with executives reveal that most cybersecurity executives are increasingly responsible for OT security, including IoT and IIoT but have limited visibility of what they are expected to secure.

Physical isolation (factory floor, isolated production environments, and raised floor), aging un-agentable systems, and organisational structures (e.g. operations versus IT management) exacerbate this challenge despite the risks.

> “I have responsibility for the OT devices at our manufacturing plant, but I don’t actually have physical access to them.”
>
> IT security director at a manufacturing firm in Korea

OT security preparedness differs across locations and sectors

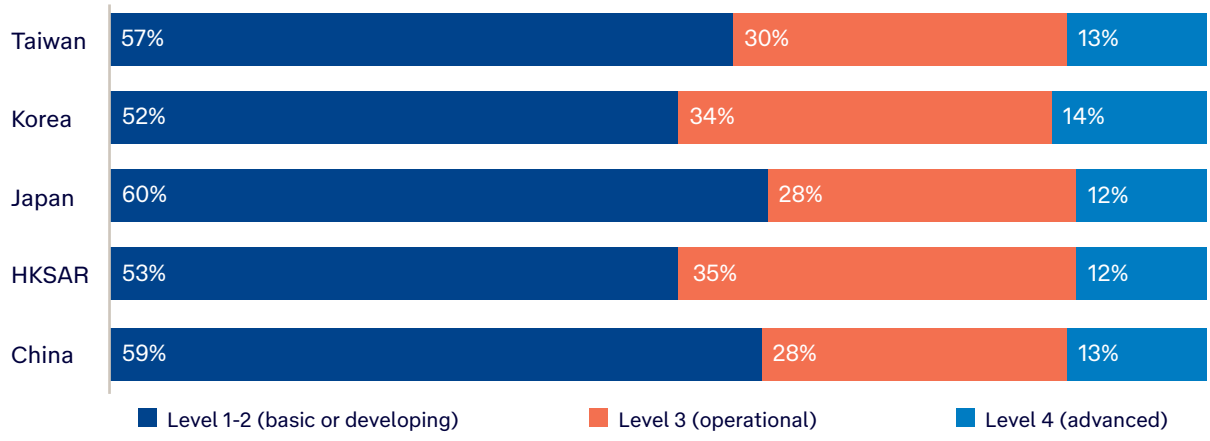
Figure 12 shows that most firms (56%) are only at basic or developing maturity levels in securing OT, including IoT and IIoT. Alarmingly, only 13% of firms in critical infrastructure sectors are advanced in security-connected OT systems, despite the absolute dependence on SCADA, ICS, and IoT for core business operations in these heavily industrialised sectors.

From a location perspective, Hong Kong SAR and South Korea are relatively more mature in OT cybersecurity than China, Taiwan, and Japan (see Figure 13).

More firms across the region have optimised supply chains to overcome COVID-19 and other geopolitical disruptions by diversifying production and distribution across North Asian locations. However, the similarities between locations underscores an overall lack of preparedness that cybersecurity executives must address at a corporate level: not one country has mastered this.

Figure 13: Regional view: All regional locations are at low OT cybersecurity readiness levels

Q: How mature is your organisation in securing connected IT/OT at each level of the Purdue model?



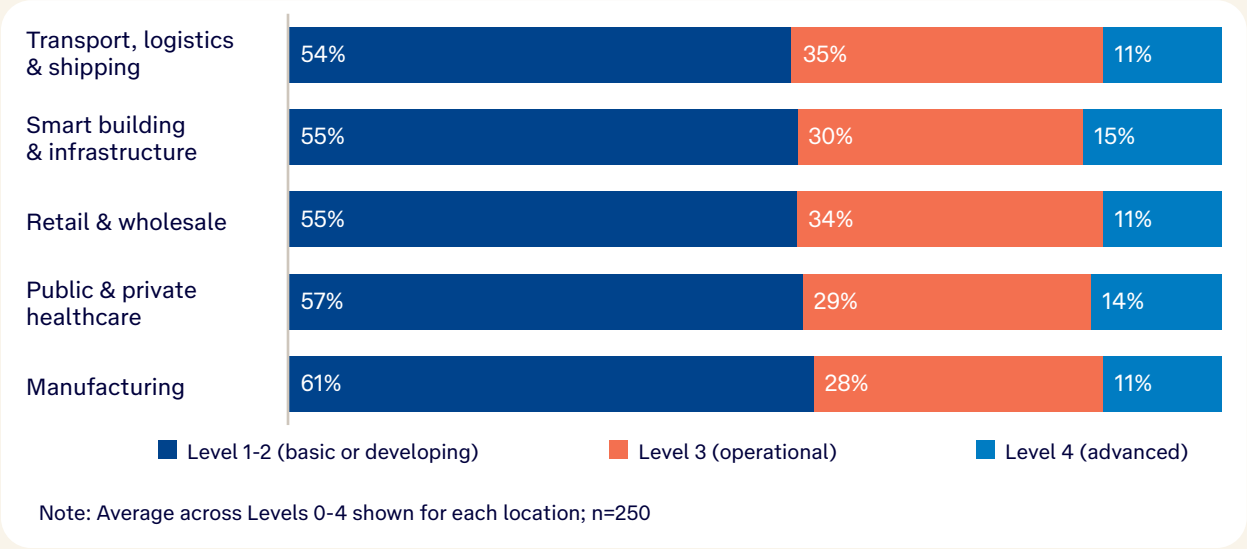
Note: Average across Levels 0-4 shown for each location; n=250

Source: Omdia

Figure 14 shows the industry comparisons for OT cybersecurity maturity across North Asia, highlighting comparable levels of low advancement across all sectors.

Figure 14: Industry view: Manufacturing is comparatively less mature in OT cybersecurity

Q: How mature is your organisation in securing connected IT/OT at each level of the Purdue model?



Note: Average across Levels 0-4 shown for each location; n=250

Source: Omdia

From a sector perspective, transport, logistics, and shipping have undergone large-scale automation projects to streamline processes and improve resilience. Firms in this sector are least prepared to secure Level 2, including SCADA and HMI.

Smart buildings and infrastructure are experiencing high growth, spread across greenfield deployments in commercial and retail sectors, and driven by smart city funding and public interest. The industry is predicated on leveraging IoT, and the sectors have matured relatively quickly in OT security, but challenges remain in addressing Level 3 (production and operational control, e.g. BMS) and 3.5 (DMZ).

The retail and wholesale sector has also undergone major transformative efforts due to external market forces, and it often relies on transport and logistics for success. However, slim margins and lower cost of entry from international imports/exports have constrained budgets for further OT security enhancements. This sector is least advanced in Levels 2, 3, and 3.5 across the ISA-95 model.

Healthcare presents a mix of public and private firms, challenged with tight budgets and pressure from regulatory burdens and patient outcomes. This sector is least prepared for Level 3 (production and operation control challenges).

In manufacturing, operations are often years or decades old and highly resistant to change, with minimal transformation budgets because of competitive pressures. Firms in this sector are most advanced in securing Level 0 (e.g. sensors and actuators) but are least prepared for Level 3.5 (DMZ).

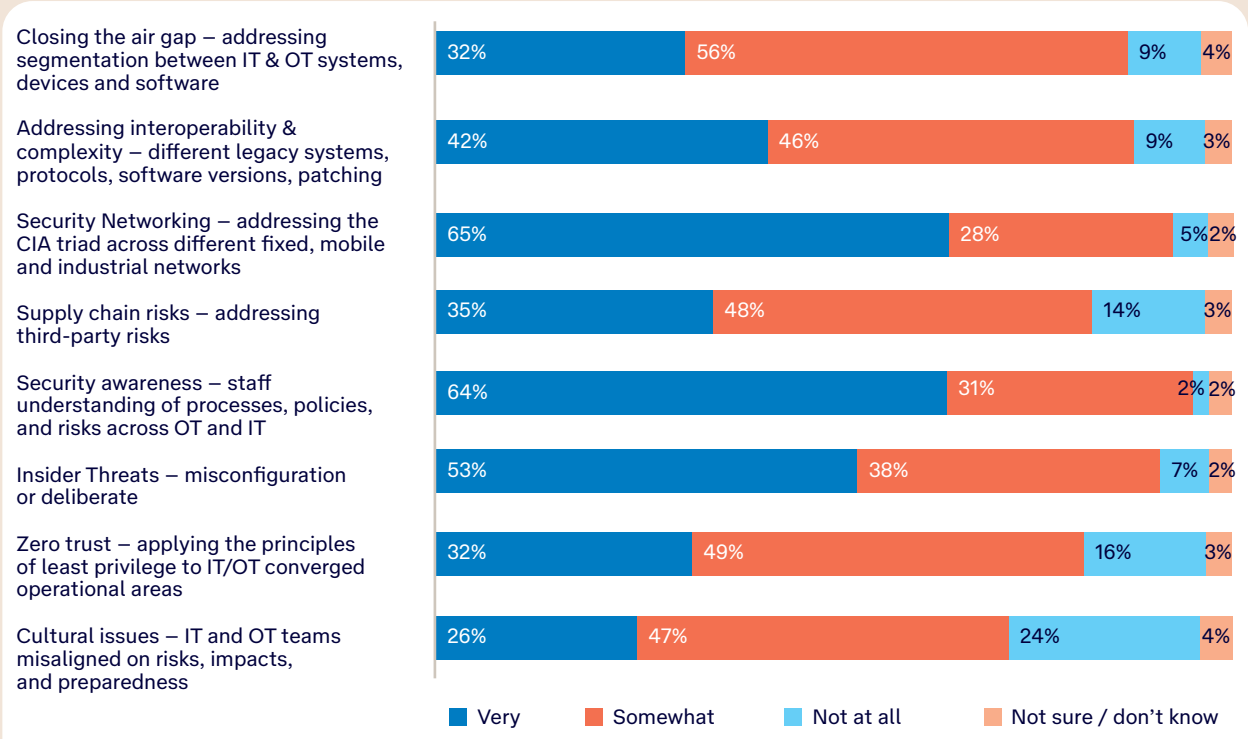
> “We have IT people managing the security and production of SCADA on the factory floor and at our sites, but they don’t understand OT, so the responsibility falls back to the CTO. We’re thinking about hiring a CISO for both (IT and OT), but they are hard to find.”
>
> Security executive at large wholesale and retail company in Taiwan

The importance of pinpointing challenges in threat types across OT environments

Firms seem well prepared to address networking, security awareness, and insider threats. Moreover, the notable areas in which firms are only somewhat prepared include “closing the air gap”, “zero trust”, and “supply chain (including third-party) risks”. Any one of these issues is sufficient to not just stall the primary goal of innovation but to undermine the operational integrity of ICS environments.

Figure 15: To address OT cybersecurity challenges, address the weakest areas first

Q: How prepared is your organisation in the following corporate IT/OT converged security areas?



Note: Response average across all sectors; n=250

Source: Omdia

Cybersecurity executives are increasingly responsible for managing OT security

Historically, engineering-led production managers were directly responsible for production and operations. This model made excellent sense because of the physical nature of the task and plant segregation from corporate locations and systems.

As IT and OT increasingly converge, responsibility and accountability (action and ownership) lines between IT leaders and their OT counterparts blur.

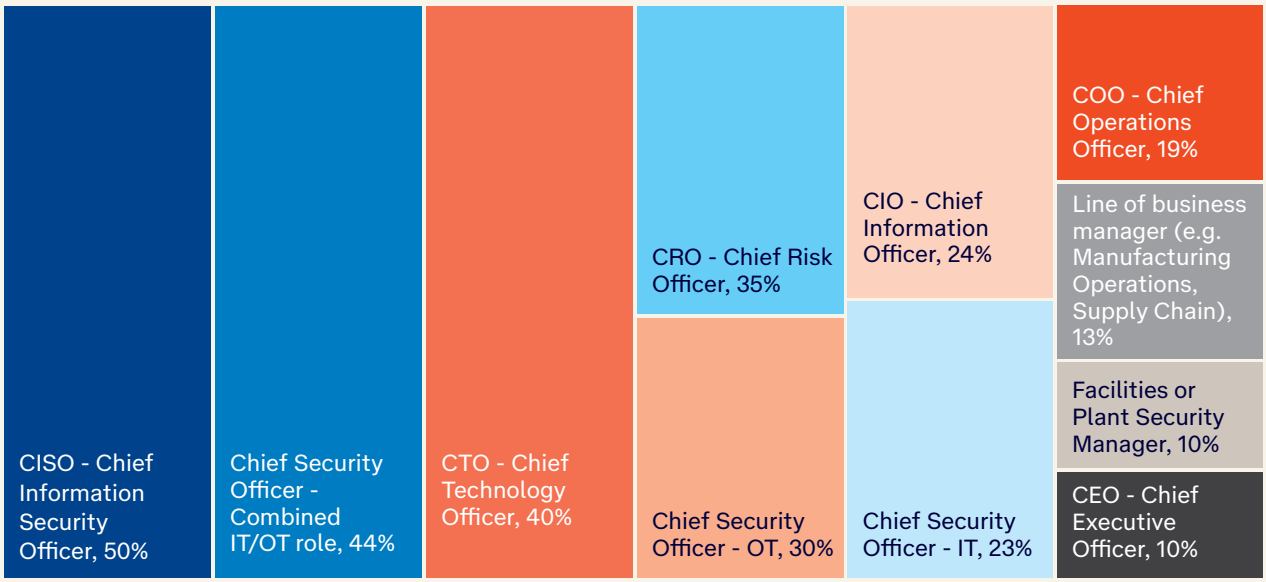
Omdia observes that the heightened risk of attack and reliance on CISO and IT security executives for the more visible part of a firm's security means the balance of responsibility is shifting. However, the power is not moving at a commensurate rate: operations offices' line-of-business managers (e.g. production, logistics, hospital, or management facilities) are the gatekeepers and custodians of Level 0-3 systems by reason of proximity.

Figure 16 highlights that IT security executives need the resources, tools, and support to meet their mandate and expectations to secure IT/OT convergence.

> "Bringing IT and OT together is very important to the business as it supports monitoring of hardware and fundamental systems, e.g. sequencer and temperature monitoring systems. But our networks are highly segregated as we worry about security."
>
> CTO at a large healthcare device manufacturer in Hong Kong

Figure 16: Cybersecurity executives are increasingly responsible for managing OT security, more so than COOs and line-of-business (production) managers

Q: Who is responsible for understanding and implementing IT/OT converged security in your organisation?



Note: n=250

Source: Omdia

Firms will engage third parties to expedite IT/OT security readiness

Under the pressure of increasing risks and complexity, most firms will engage a third party under an outsourcing agreement or with in-house teams (see Figure 17) to bolster IT/OT/IoT-specific security services.

Executives in the region speak of the challenges of finding skilled and experienced staff that understand both IT and OT from a security perspective, especially in their industry context.

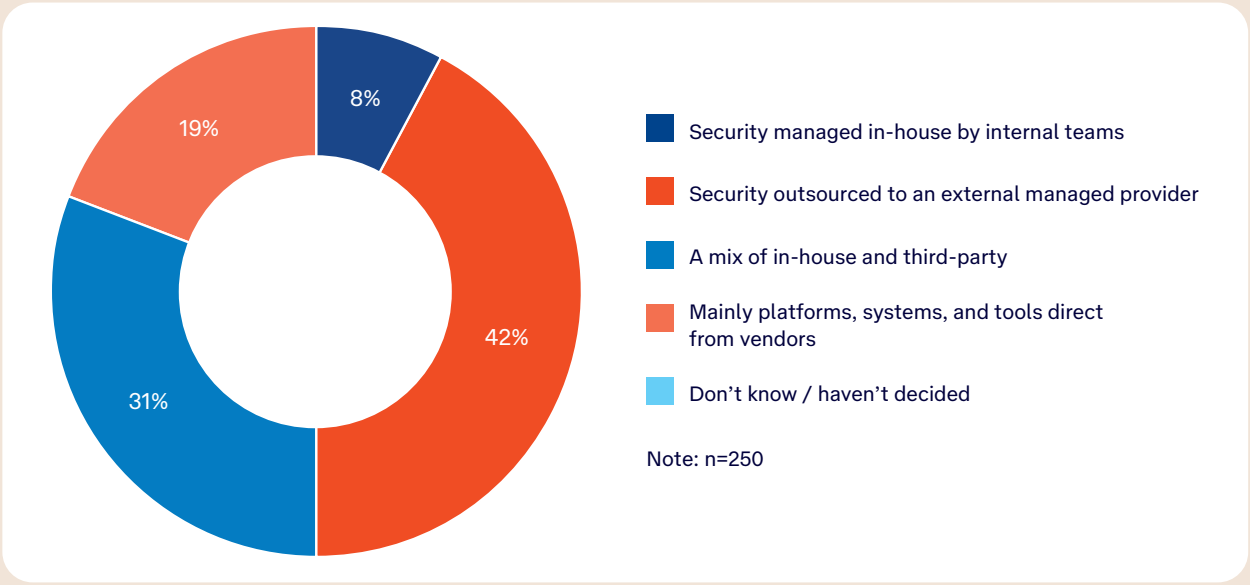
Vendor options for security include managed security service providers (MSSPs), OEMs and OT system providers, IT security platforms with IoT/OT capabilities, and niche/specialised IoT/OT security firms.

A recent and relentless spate of attacks on critical infrastructure sectors and tightening regulations and mandates will turn up the heat on cybersecurity executives. However, they face skills challenges, complex systems to manage, and equally challenging (but capable) IoT and OT cybersecurity platforms.

> “Our chosen IT/OT security partner will need to have modular solutions suited to our region and help us use AI and big data to analyse traffic and better understand attack behaviours; this will help improve safety and reduce warnings in our systems.”
>
> COO for OT at a large transport company in China

Figure 17: More than 70% of firms will engage a third-party service provider to address OT security challenges

Q: How will your organisation likely manage IT and OT security (across IT and OT convergence) 18 months from now?



Source: Omdia

5.0 A path forward

Conclusion

While the benefits of convergence are high, the risk of a breach originating in either the cyber or physical environment with material impacts on production, operations, revenue, and health and safety outcomes is similarly elevated.

This research confirms that the IT and OT stacks are siloed at many companies and embody different disciplines and expertise, including complex mechanical and electrical engineering and bifurcated information technology practices.

As digital capabilities take on a more strategic role in organisations, there will be growing motivation to break down those silos and converge IT/OT stacks. Subsequently, the ability to manage the cybersecurity risks across these interconnected systems will become a defining factor for operational resilience, customer experience, and competitive sustainability.

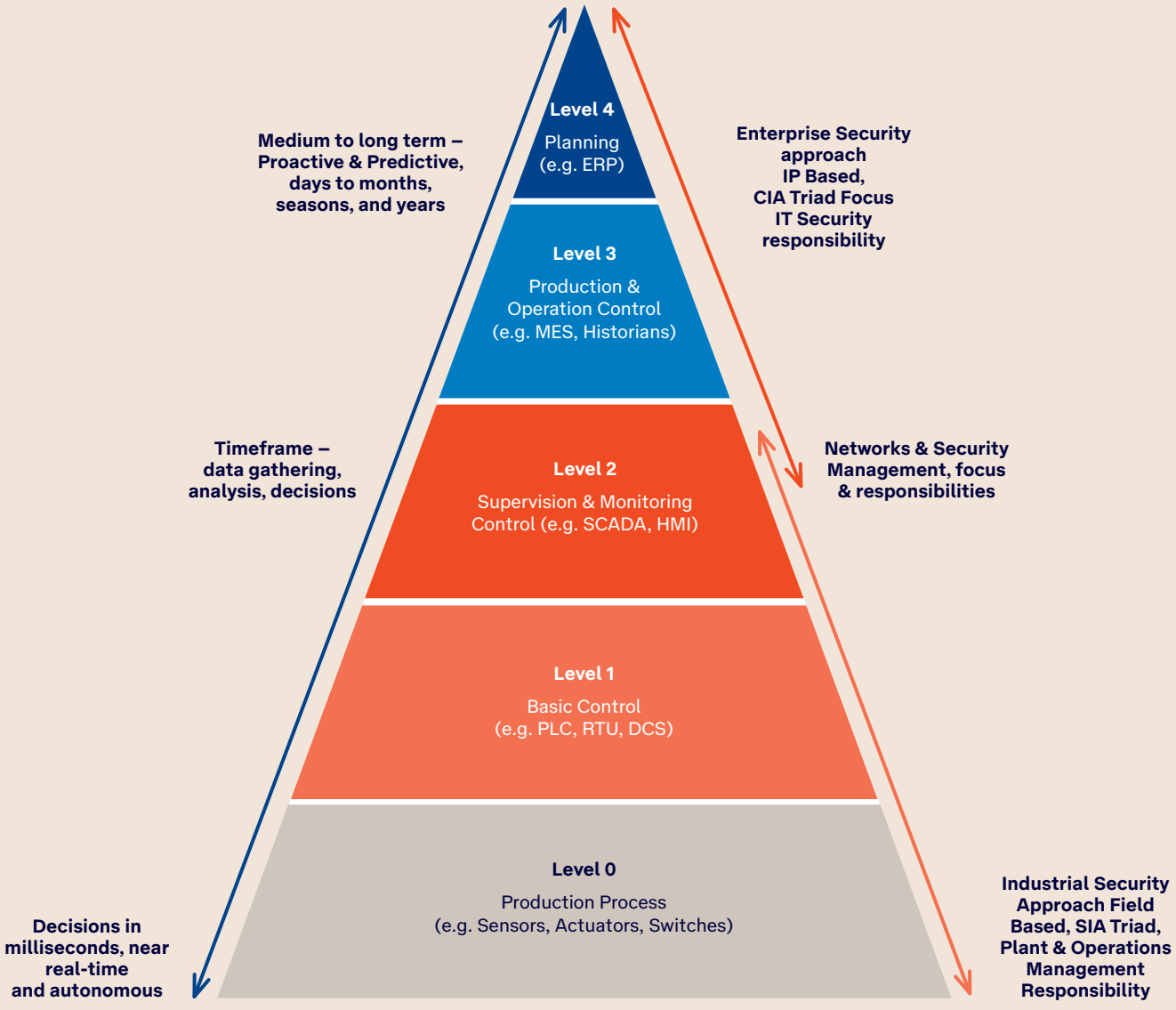
Figure 18: Extending the ISA-95 pyramid model under Industry 4.0 to consider key cybersecurity impacts

Industry 4.0 Enabling Technologies

- **Enterprise Applications** – e.g. ERP, SCM, CRM, tailored for industrial use cases
- **Hybrid Cloud** – SaaS, PaaS, IaaS, IaaC, Serverless, and flexible delivery models for scale and resilience from corporate to the factory floor or fleet
- **IoT** – including IIoT and IoMT, enabled by M2M and 3/4/5G and enterprise mobility
- **AI** – ML, RPA, GenAI, LLM, big data, data science, and data management
- **Open APIs** – and microservices architecture linking customers, suppliers, and partners
- **VNF** – SD-WAN, micro-segmentation
- **Edge computing** – digital twins, remote monitoring, and augmented reality
- **Advanced Robotics** – enhanced ICS

Industry 4.0 Security Impacts

- **Legal and regulatory** – compliance and reporting on meeting standards including ISO/IEC 27001:2022, executive order for critical infrastructure
- **Failing 'air gap'** – using NGFW to connect physical with virtual for secure data flows between levels 3-4 down to level 0
- **Zero trust** – least privilege and MFA to control IT/OT/IoT movement
- **IT/OT Tools** – leveraging non-OEM OT security platforms and tools with discovery, vulnerability management, agentless monitoring, reporting and incident management, threat detection, and configuration management
- **Physical Impacts** – compromised devices across levels 0-1 from lateral attacks, misconfiguration causing equipment failure or requiring offline remediation



Source: Omdia

Recommendations

The insights presented in this white paper serve to coalesce extensive quantitative and qualitative research across North Asia to benefit organisations.

Cybersecurity leaders across the leading firms surveyed have an integrated view of cybersecurity across IT and OT, need a single pane of glass for cyber-resilience, and should foster extensive collaboration between IT and engineering teams, leverage third parties, and actively explore IT-based OT security platforms.

To help address the IT/OT cybersecurity challenge, consider the following conceptual model to assess Industry 4.0-enabling technologies across OT levels with corresponding cyber-impacts.

OT cybersecurity is complex, and most environments are highly risk avoidant and on tight IT security budgets. Based on extensive interviews with regional experts and this in-depth survey, Omdia recommends prioritising IT/OT and IoT security across four core areas, captured in Figure 19.

Figure 19: Four priority areas in IT/OT and IoT security

1

Collaborate to bridge the cultural and skills divide

Cybersecurity leaders are tasked with securing IT and OT as the two converge, but their budgets and authority do not always match the ask.

CEOs need to foster and support efforts by the C suite and IT/cybersecurity directory to collaborate across product (engineering) and IT (corporate) operations as functions for digital resilience. Failure to do so will result in incidents or (worse) attacks on IT that affect OT and cause lost revenue, reputational damage, and operational downtime.

2

Define strategy across the five pillars of IT/OT and IoT security readiness

Omdia recommends executives responsible for OT security should assess and prioritise improvement levels, using an agile and programmatic approach level of uplift. It is important to note that change takes time, and organisations require a robust plan to succeed.

3

Unlock value from industry frameworks OT security tools

Organisations continue to invest in many IT security tools, each with unique capabilities; however, OT is a different challenge because of un-agentable systems. Security leaders need to consider extending IT security tools with OT-specific capabilities that span asset discovery, categorisation, monitoring, and SecOps (incident response to recovery). Modern cloud infrastructure and IoT frameworks (MQTT, Azure AKS for IoT) also provide a way to assess and increase readiness rapidly.

4

Leverage the right partner in converged IT/OT and IoT cybersecurity

Cybersecurity skills are expensive and in short supply across the region, even more so in IT/OT-converged security. Leading North Asian organisations increasingly plan to address security constraints by leveraging third parties to better respond to threats and become more proactive.

Executives in the region should consider partnering with security services providers and engaging professional services from in-region providers that understand their sector and IT/OT-specific challenges.

Source: Omdia

6.0 Appendix

Omdia was pleased to conduct this research in partnership with Telstra International. The insights and trends within this white paper reflect the latest experiences of organisations based on in-depth fieldwork carried out in the second and third quarter of 2023.

We trust this paper will guide security, technology, and business leaders in leveraging Industry 4.0 technologies through mature OT cybersecurity for sustainable competitive advantage.

Methodology

To better understand the reality of IT and OT converged cybersecurity in North Asia (including cyber-physical and IoT), Telstra International commissioned Omdia to conduct an independent, comprehensive, local market study focusing on China, Hong Kong SAR, Taiwan, Japan, and South Korea.

This survey focuses on the enterprise use of IT/OT and IIoT (excluding consumer-specific technology).

Throughout this survey, IT and OT convergence refers to digital connectivity, digitalisation, and digital transformation projects that link corporate and other IT networks to physical operational components, including but not limited to industrial control systems (ICS), SCADA systems, programmable logic controllers (PLC), and any other such systems controlling physical, operational components such as robotic picking, automated production lines, and smart building controls, across the Purdue model or otherwise.

Other terms in scope include IT, IoT, IIoT, OT, and industry-specific security, where information and physical systems interconnect. Please see the taxonomy section for specific definitions used in this survey.

From August through November 2023, Omdia conducted a direct primary research survey of 250 senior security decision makers at mid- and large-sized firms across manufacturing, public and private healthcare, retail and wholesale, smart buildings and infrastructure, and transport, logistics, and shipping.

Small to medium enterprises (501 - 999 employees) comprised 40% of respondents. The remaining 60% were large organisations (more than 1,000 employees). Half of respondents were IT executives (including CIO, CTO, CISO), and the other half were senior technology leaders (including technology leads and senior consultants).

Omdia also conducted in-depth interviews with 10 senior decision makers responsible for choosing cloud in their organisations to reveal detailed views of executives' aspirations, challenges, constraints, and service provider partner considerations in OT security.

Respondent roles surveyed included technology or security executive (e.g. CIO, CTO, CISO, CSO, VP/ director ICT – 32% of respondents), senior technology or security manager (e.g. infrastructure manager, associate manager, team leader – 35%), line-of-business director or executive (e.g. operations, supply chain, manufacturing, quality – 18%), and line-of-business manager (e.g. plant manager, operations manager, supply chain, manufacturing, quality – 15%).

Global counterpoints in this research draw on Omdia's global expertise in its digital enterprise services and cybersecurity intelligence services.

Author

Adam Etherington

Senior Principal Analyst, Digital Enterprise Services

adam.etherington@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision-makers thrive in the connected digital economy. We offer expert analysis and strategic insight across the IT, telecoms, and media industries through our global base of analysts.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalise on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

About Telstra

Telstra is a leading telecommunications and technology company with a proudly Australian heritage and a longstanding, growing international business. Telstra International provides services to thousands of business, government, carrier and OTT customers.

Over several decades we have established the largest wholly-owned subsea cable network in the Asia-Pacific, with a unique and diverse set of infrastructure that offers access to the most intra-Asia lit capacity. We empower businesses with innovative technology solutions including data and IP networks, and network application services such as managed networks, unified communications, cloud, industry solutions, integrated software applications and services. These services are underpinned by our subsea cable network, with licenses in Asia, Europe and the Americas and access to more than 2,000 Points of Presence (PoPs) in more than 200 countries and territories globally.

In July 2022 Telstra completed the acquisition of Digicel Pacific, the largest mobile operator in the South Pacific region.

Copyright notice and disclaimer

Contact your Telstra account representative for more details.

telstraenquiry@team.telstra.com telstrainternational.com

2024.04.14 307 PM