Secure manufacturing: The challenges of IT/OT convergence

Discover how executives are securing Industry 4.0 across the US, Latin America, Europe, and Asia & Oceania

A paper in partnership with Omdia

Contents

1.0 Executive summary

Operational technology (OT) risks intensify as digitization accelerates

The convergence rate between operational technology (OT) and information technology (IT) in global manufacturing firms continues to accelerate. Across the US, Latin America, and Europe, 70% of OT systems in manufacturing firms will soon be connected to corporate IT networks, up from 50%. In Asia & Oceania, IT/OT integration is progressing at a similar pace, starting from a lower base of 40% this year, which is predicted to reach 60% soon.

This integration is primarily driven by continuous innovation. Examples include predictive maintenance, autonomous systems, real-time inventory management, improved quality control, safety monitoring, risk management, and sustainable manufacturing. Increased resiliency in manufacturing is also a key contributing factor as supply chain disruptions, geopolitical tensions, environmental impact, and industry economics continue to compress profit margins.

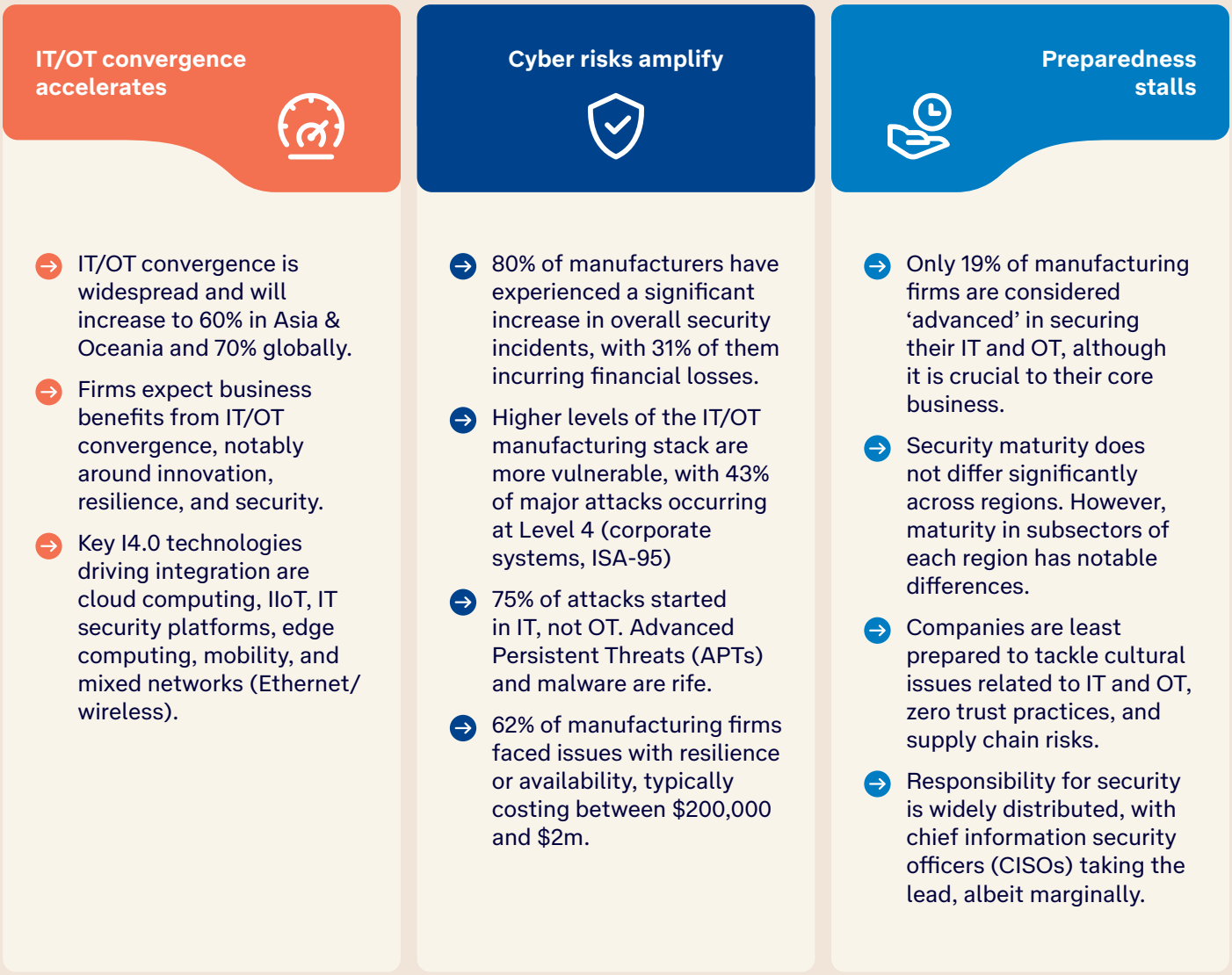
From a technical standpoint, Industry 4.0 (I4.0) technologies are essential. These include cloud computing, Industrial Internet of Things (IIoT), edge computing, artificial intelligence (AI), wireless technology (e.g., 5G), third-party OT, advanced networks (e.g., fixed wireless access [FWA]), and cybersecurity.

Following this convergence, most manufacturing firms have recently experienced a significant increase in security breaches and incidents involving OT systems. Notably, most of these incidents originated in IT (cyber) rather than OT and caused expensive and significant disruption.

There is a rising tension between integration and cybersecurity. Greater connectivity between IT and OT increases the risks of a breach. However, it is necessary to harness advanced technology for manufacturing innovation. Interestingly, our research found that improving both cyber and physical security is the second-highest factor driving convergence and does not impede connectivity.

However, very few firms are mature in protecting and defending against cyber risks associated with IT/OT. The responsibility for security often lacks consistency and clarity. People and cultural issues hinder security posture readiness, which amplifies the technical challenges.

Figure 1: Growing risks amid accelerated integration and lagging preparation



Source: Omdia

To evaluate and provide guidance on the effects of IT/OT integration on digital infrastructure, Telstra commissioned Omdia to research the challenges faced by leading manufacturers and provide recommendations. This paper presents findings from the global study of n=513 spanning the US, Europe, Latin America, and Asia & Oceania.

The manufacturing subsectors covered include smart manufacturing; equipment and other discrete manufacturing; industrial process manufacturing; construction (e.g., mineral and metal mining); and agriculture (e.g., food and other consumer product manufacturing).

Who did we speak to?

In partnership with Omdia, the study gathered 513 total unique global quantitative responses from manufacturing firms at a pivotal time in the market.

Figure 2: Details of the survey

Field survey n=513

Over five hundred technology executives responsible for IT or OT security were surveyed in September 2024

Respondent mix (percentage of total)

- 51% are executives from technology or security roles (e.g., chief information officer [CIO])
- 49% are line-of-business (LOB) directors

Sectors surveyed

- Equipment and other discrete manufacturing
- Automotive and vehicle manufacturing
- Industrial process manufacturing
- Construction (mineral and metal mining)
- Agriculture (food and other consumer product manufacturing)

Organization size (percentage of total)

- 45% with 500–999 employees
- 55% with over 1,000 employees

Domains surveyed

Converged IT/OT across the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and the ISA-95 standards

Regions surveyed

- Global (total n=513)
- US: 72
- Latin America: 30
- Europe: 156
- Asia & Oceania: 255

Source: Omdia

Key findings

Figure 3: Increased cybersecurity risks with IT/OT convergence

The convergence of IT and OT in manufacturing is set to accelerate

- 86% of firms indicated that IT/OT integration is important for business outcomes.
- Innovation, availability, and security are the most important business goals of IT/OT integration.
- Integration is already widespread and will increase further, with anticipated levels reaching 60% in Asia & Oceania and 70% across Europe, Latin America, and the US.
- I4.0, cybersecurity, and increasing resilience are the main factors driving integration, to offset resulting security threats.
- Ethernet and industrial protocols are the most important network types for integration. Private 5G is fast growing.

Cybersecurity impact on manufacturing

- Last year, 80% of manufacturing firms experienced a significant increase in overall security incidents or breaches. Higher levels of the IT/OT stack are particularly vulnerable.
- Of these breaches or incidents, 31% resulted in financial losses and/or operational downtime.
- An overwhelming majority (75%) of attack trajectories originated from IT targeting OT, highlighting that converging IT and OT comes at a significant cyber risk.
- 54% of security incidents in IT/OT environments were from advanced persistent threats (APTs), 45% from malware, and 39% from distributed denial of service (DDoS) attacks.
- Additionally, 62% of manufacturing firms faced issues related to resilience or availability, with costs typically ranging from $200,000 to $2m.

Manufacturers cyber readiness stalls

- Only 19% of all firms surveyed are ‘advanced’ in securing their IT/OT environments based on the NIST CSF, despite its critical importance to core manufacturing processes.
- Firms demonstrated higher confidence (operational and advanced) in their security measures based on the NIST CSF (69%) than the Purdue model (60%).
- In 20% of firms, the CISO is responsible for understanding and implementing a converged IT/OT cybersecurity program, followed closely by the chief risk officer (CRO) (14%) and chief technology officer (CTO) (13%).
- Having good visibility of all industrial IoT and OT assets within the organization is essential for 70% of organizations.

Source: Omdia

2.0 The convergence of IT/OT in manufacturing is accelerating

I4.0 is enabling digital transformation in manufacturing

Manufacturing is a complex sector, having undergone significant advancements over the past 200 years. These changes can be broadly categorized into technological and process advancements, recognized as four critical revolutions. Historically, Industry 1.0 (I1.0) marked early industrialization through mechanization, followed by electrification (I2.0), and then automation (I3.0).

Omdia sees I4.0 in manufacturing as key to enabling efficiency, innovation, mass production, automation, and other advances that leverage technology advancements to create new use cases across various industries.

Industry 4.0 (I4.0) manufacturing

Optimize scale, resilience, and efficiency in manufacturing by strategically leveraging advanced technologies, including cloud computing, AI, and IoT, with new business models, harmonized with legacy systems at levels beyond historical industry precedents.

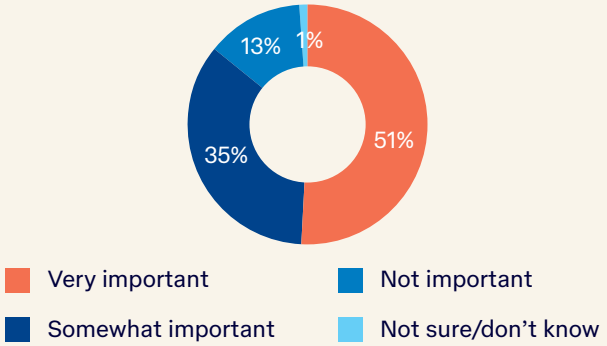
Industry innovation enabled by convergent technologies

Globally, manufacturing executives agree IT/OT convergence is important, largely driven by Industry 4.0, to achieve greater innovation among other strategic and tactical goals (**Figure 4**).

Figure 4: I4.0 is driving IT/OT convergence in manufacturing to foster innovation, reliability, and security

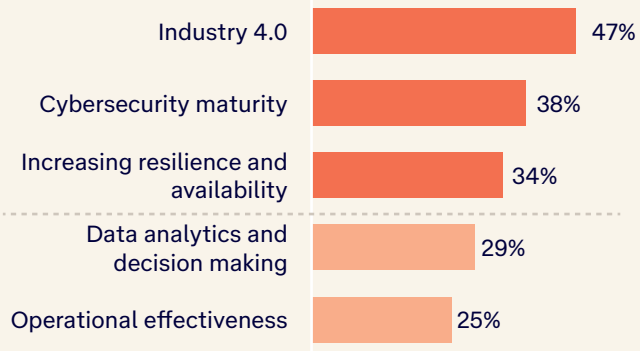
86% of manufacturing executives agree IT/OT convergence is important

Q. How important is connecting IT with OT (or other means of controlling physical and operational components) to achieve your business outcomes?



I4.0 is the biggest driver of this convergence

Q. What have been the top three factors accelerating the convergence between IT and OT systems in the past 24 months?



With the goal of increasing innovation, reliability, and security

Q. Rank the top three areas in which you expect the biggest improvements in future IT/OT convergence (top rank results)

Notes: n=513, global

Source: Omdia

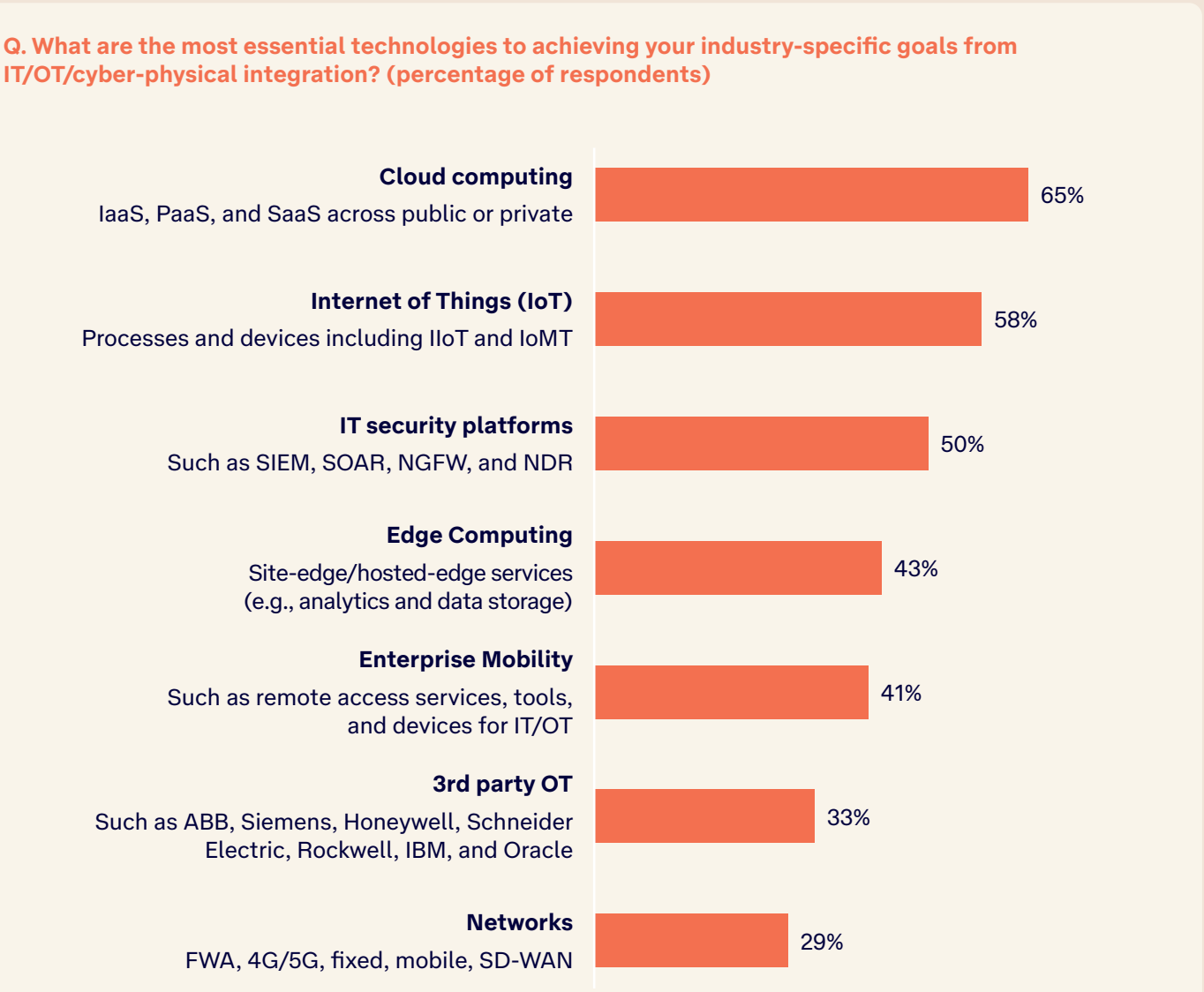
This shift is unanimous. Across different decision-maker roles, 54% of lines of business (LOB) and 50% of executives rated this convergence as 'very important'. The reason for this trend is the capability of IT to make OT smarter, ultimately driving commercial impact in both discrete and process manufacturing. IT plays a vital, complementary role to traditional OT (physical systems).

A conceptualized view of IT/OT integration is provided in **Appendix 1**.

Cloud computing, IoT, and cyber platforms are essential I4.0 technologies

Omdia has identified several key I4.0 technologies for the manufacturing sector. These include cloud computing, IIoT, security platforms, and edge computing (**Figure 5**).

Figure 5: Essential I4.0 technologies in manufacturing



Source: Omdia

These technologies complement each other and can contribute to industrial settings. However, they are part of a broader ecosystem that must align physically with virtual components and systems across legacy and emerging technology domains.

I4.0 in manufacturing will continue to promote the integration of cloud, edge, device, and web server systems that connect at Level 4 to the underlying OT levels.

Increasing integration is a manufacturing priority

IT/OT systems are set to become even more connected

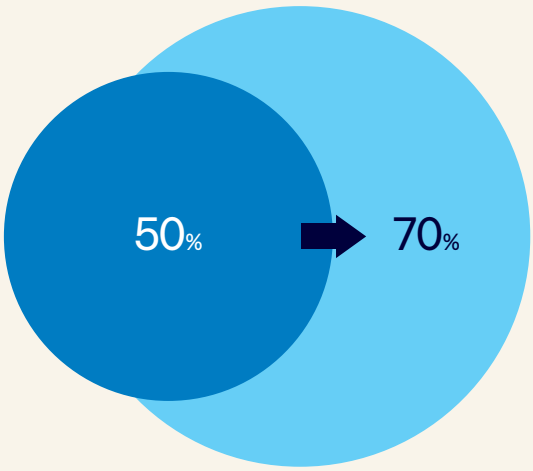
The percentage of OT systems connected to IT in most manufacturing firms globally will increase by 20% in the next two years (**Figure 6**).

However, there are variations in regional adoption rates and specific challenges related to cybersecurity as a result of this convergence, which is discussed in **Section 3** of this paper.

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

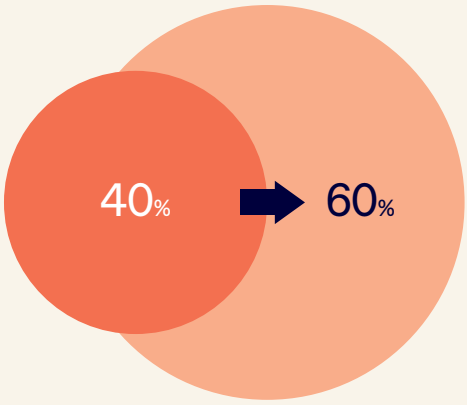
Manufacturing firms plan to increase OT/IT integration by 20%

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



The US, Latin America, and Europe

Approximately 70% of OT systems in manufacturing firms across the US, Latin America, and Europe will be connected to corporate (IT) within the next year, up from the current 50%.



Asia & Oceania

Approximately 60% of OT systems in manufacturing firms in Asia & Oceania will be connected to corporate (IT) networks within the next year, up from the current 40%.

Notes: n=513, global

Source: Omdia

Integration or simple connectivity encompasses various aspects, including devices (IoT and connected systems), networks (from IP to industrial), systems (shared floor space), enterprise applications (data extraction and analysis), remote monitoring (of operational technology from IT systems), personnel (IT cybersecurity teams responsible for OT security), as well as upgrades and repairs (new IoT-enabled devices).

Use cases for integration in manufacturing emerge

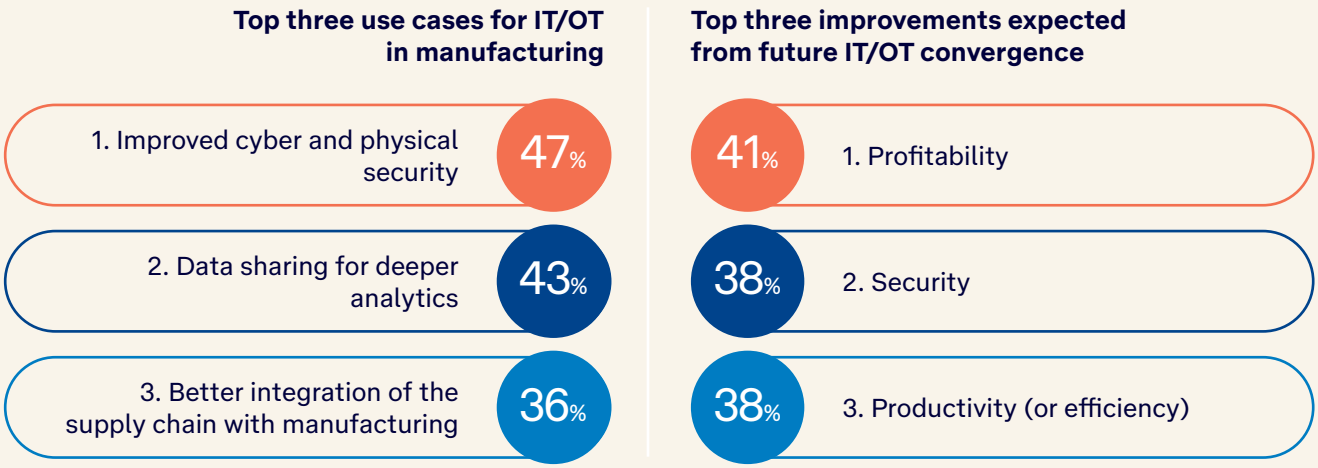
Real-life use cases of technology integrations include predictive maintenance and safety assessments, real-time monitoring and management, additive and smart manufacturing, advanced supply chain management (SCM), and modularized production, which offers greater resiliency at scale.

The flexibility of both cyber and physical technologies fosters greater convergence. This flexibility also amplifies the necessity for enhanced security measures across both new and legacy systems, integrating cyber and physical environments.

Our research indicated that security, data analytics, and supply chain management are the areas where IT/OT convergence will make the biggest improvements in manufacturing. In comparison, innovation, reliability, and security are the top three areas for improvement that manufacturing firms expect after IT/OT convergence (**Figure 7**).

Figure 7: Top use cases and improvements from IT/OT in manufacturing

Q. What are your top three use cases for IT/OT in manufacturing? Please rank the top three areas in which you expect the biggest improvements in future IT/OT convergence.



Notes: n=513, global

Source: Omdia

Security is a growing use case that represents both a constraint (for legacy OT) and a driver (for new deployments and hardware upgrades) of IT/OT convergence. This topic will be discussed in more detail later in this report.

While I4.0 is a crucial driver of IT/OT convergence, several other critical factors are also increasing the adoption of these technologies. These include:

- **Systems reaching their end-of-life:** Many systems, from Level 0 (production) to Level 4 (enterprise resource planning [ERP]/mainframes), are reaching the end of their operational life. Upgrading these systems can be expensive, risky, and complex.
- **Market forces:** New market entrants are utilizing innovative technologies to significantly reduce barriers to entry in established markets. In response, established firms must leverage similar technologies into their IT/OT infrastructure to drive efficiency, scalability, and the balance between cost and quality.

3.0 Manufacturing is significantly affected by IT/OT cybersecurity challenges

Manufacturing is facing increased cybersecurity risks

The scale, trajectory, and effects of cyber incidents are costly

Omdia's cybersecurity research confirmed that cybersecurity incidents are becoming increasingly sophisticated and impactful, often targeting critical infrastructure sectors for maximum effect and financial gains.

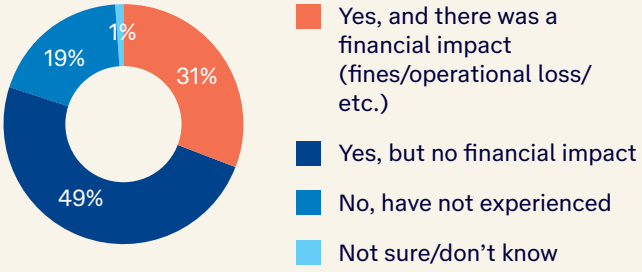
Unfortunately, the manufacturing sector is a prime target that has garnered attention from threat actors. Crime affiliates, nation-states, and cybercriminals are all seeking to exploit essential operations for lucrative gains through cyber extortion.

Figure 8 highlights the extent of the challenge.

Figure 8: Manufacturing firms are facing significant threats as attacks originate in IT and affect OT, with material consequences

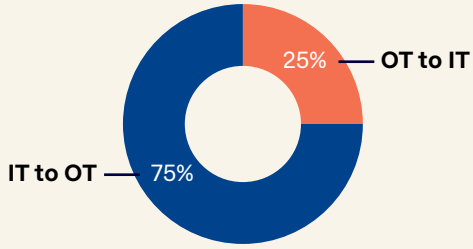
80% of organizations have seen a significant increase in security incidents across their IT/OT environments

Q. Has your organization experienced a significant increase in overall security incidents or breaches in the last 12 months?



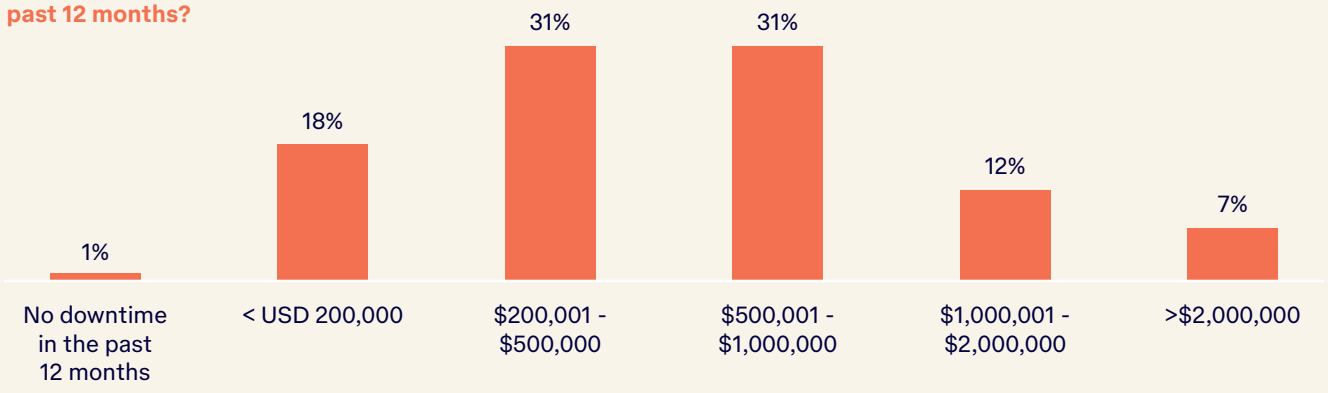
75% originated in the IT domains but affected OT

Q. What was the attack trajectory (direction) for the most significant security incident or breach that impacted operations?



62% of manufacturing firms faced issues related to resilience or availability, resulting in costs ranging from $200,000 to $2m

Q. Because you answered "Increasing resilience and availability" as one of your top 3 factors accelerating IT and OT convergence, was there a resilience and availability issue, and what was the total estimated cost of downtime in the past 12 months?



All respondents: n=176

Notes: n=513, global

Source: Omdia

- **Scale:** Globally, 80% of organizations have reported a significant increase in security incidents across their IT/OT environments, with 32% experiencing a substantial financial burden as a result.
- **Trajectory:** Notably, of these incidents, 75% originated in the IT domain, but they had a negative impact on OT through downtime, incident handling, or material breaches.
- **Impact:** Among the incidents that affected the resilience or availability of key manufacturing systems, 62% of manufacturing firms reported experiencing issues related to resilience or availability. The typical cost associated with these issues ranges from $200,000 to 2m.

The quandary of integration security

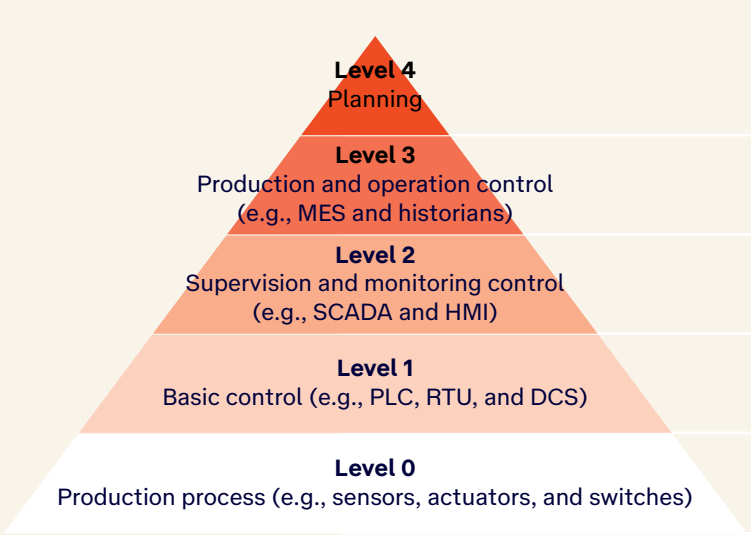
IT/OT convergence is essential for digital transformation; it can improve cybersecurity but also present risks

Manufacturing executives are increasingly turning to IT/OT integration to drive innovation, reliability, and security. However, the improved connectivity and data sharing, along with the use of multiple and interconnected (hybrid) clouds, has raised significant security concerns triggered by IT. These concerns must be addressed, and there are ways to mitigate them effectively.

Omdia's research revealed that those higher levels of the IT/OT stack, specifically Level 4 (planning), are more vulnerable owing to greater connectivity, which is essential for continued innovation (**Figure 9**). For instance, 93% of manufacturing firms globally have been affected by a cybersecurity incident at Level 4 (planning), of which 43% resulted in financial or severe impact.

Figure 9: All layers of IT/OT connectivity have been affected by cyber incidents

Percentage of manufacturing firms experiencing a cyber incident at each level



	Impacted/incident	Financial impact/ severe incident
Level 4 Planning	**93%**	**43%**
Level 3 Production and operation control (e.g., MES and historians)	**85%**	**41%**
Level 2 Supervision and monitoring control (e.g., SCADA and HMI)	79%	27%
Level 1 Basic control (e.g., PLC, RTU, and DCS)	73%	22%
Level 0 Production process (e.g., sensors, actuators, and switches)	65%	20%
Average across all levels	**79%**	**32%**

Notes: n=513, global

Source: ISA and Omdia

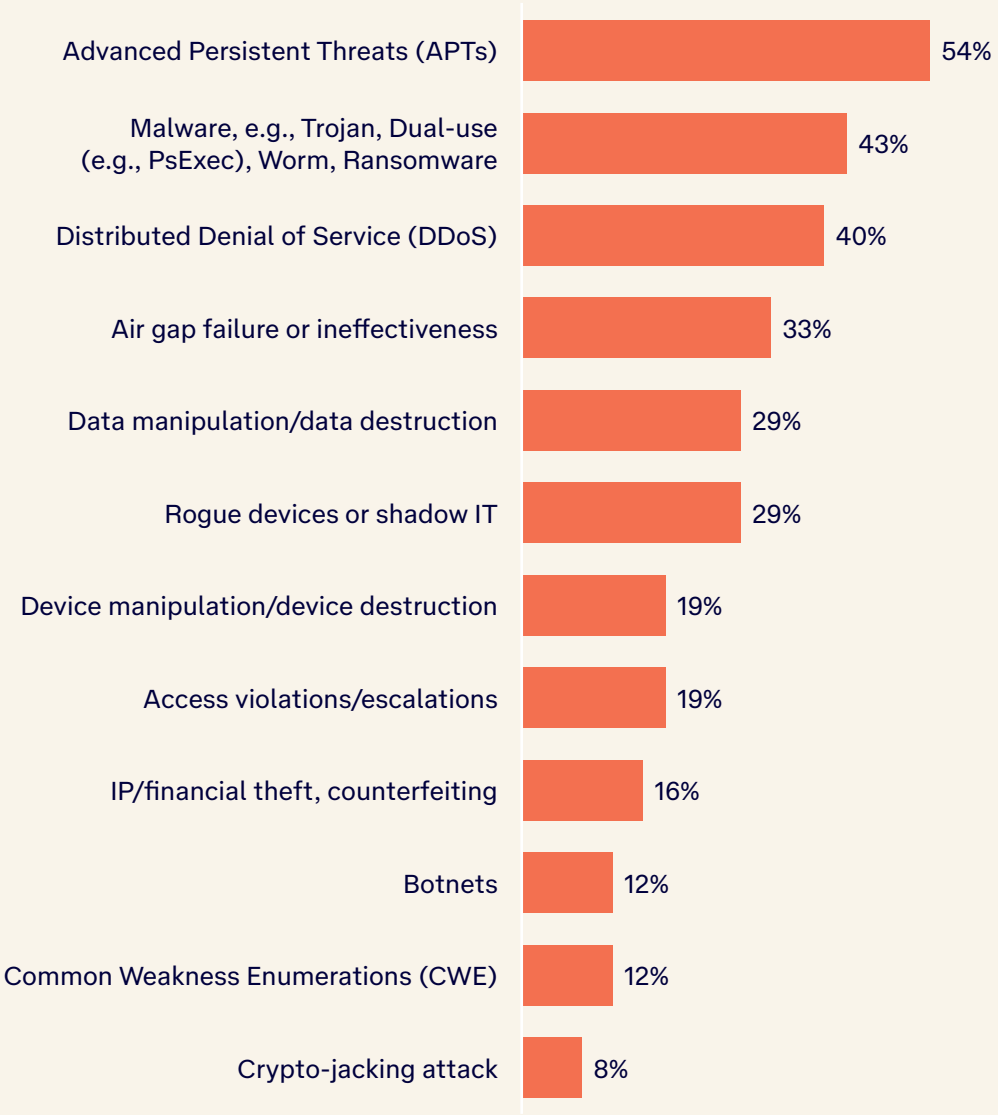
APT, malware, ransomware, and DDoS challenges from IT breaches to OT environments

Given the magnitude of downtime costs from any breach or network incident that affected operations, it is crucial to gain a better understanding of the causes to enable proactive remediation.

Figure 10 breaks down the most significant incidents experienced by firms globally in OT domains, excluding incidents related solely to IT.

Figure 10: APT, malware (especially ransomware), and DDoS attacks are the most common threats to OT systems

Q. Excluding IT-only incidents, what were the most significant IoT/OT-specific cybersecurity-triggered incidents, events, or threats you encountered in the past 12 months?



Notes: n=380, global

Source: Omdia

A deeper look at the top threats faced by the manufacturing industry

Figure 11: A deeper look at the top threats faced by the manufacturing industry

APTs

APTs are prolonged and sophisticated cyber attacks with malicious intent that seek to maximize undetected dwell time, cause significant impact, and facilitate data exfiltration across all levels (0 through 4) of the Purdue model. Common goals of APTs include disrupting operations for cyber extortion and stealing proprietary and confidential information.

Malware and ransomware

Cyber criminals are becoming more sophisticated in leveraging malware on unsecured endpoints to gain access and disrupt OT environments. Ransomware, in particular, is rife because manufacturers make lucrative targets for extortion. Historically, remote IoT, connected devices, and systems have been difficult to manage, leading to unmanaged blind spots in various product environments. Many also have not been sufficiently secured; for example, they often use default passwords, run outdated certificates, and lack necessary firmware updates.

DDoS

DDoS attacks are becoming increasingly prevalent as more IoT (including IIoT and Internet of Medical Things [IoMT]) devices connect to networks through fixed, virtual (SD-WAN), and mobile (5G) networks that interface with hybrid cloud and edge computing. Additionally, the tighter integration between enterprise resource planning (ERP), supply chain management (SCM), and other enterprise applications systems at levels 3.5 and 4 of industrial environments—both on-premises and in the cloud—creates new attack trajectories for adversaries.

Rogue devices

IoT, including IIoT and IoMT deployments, has been enabled by machine-to-machine (M2M) communication and advancements in 3G, 4G, and 5G technologies, as well as enterprise mobility. However, in some cases, these devices have not been secured or locked down correctly. Additionally, there also still many legacy OT devices at levels 0 through 2, for which visibility is difficult owing to unauthorized or untracked deployment in production environments without corporate or IT security involvement.

Air gap failure

This approach requires LAN segmentation, either physical or virtual, to segregate industrial networks from corporate systems with tight control over remote access. Traditionally, air gapping has been heavily relied on to insulate industrial control systems (ICS) from external threats. The challenge with this approach is the inevitability of IT/OT convergence across different OT levels over time and the ensuing risks where cybersecurity implications are not pinpointed or addressed. As the drive for business and operational benefits of IT/OT accelerate, physical air gaps remain important. However, it is essential to consider additional measures, such as micro-segmentation, next-generation firewalls (NGFW), zero trust architecture, and advanced IT/OT security operations (SecOps) tools.

Source: Omdia

4.0 IT/OT cybersecurity readiness in manufacturing

Firms are ill-prepared for OT security issues, even as cybersecurity leaders assume greater responsibility for OT environments

Only 19% of manufacturing companies are considered 'advanced' in securing their IT/OT systems, although this is essential to their core operations

Our research showed that most firms are yet to facilitate meaningful comparisons and benchmarking. Omdia has assessed the current maturity of organizations in securing IT/OT convergence across two different but relevant frameworks: the NIST CSF and ISA-95 (**Figure 12**).

Figure 12: Maturity assessments have been conducted against both NIST CSF and ISA-95

NIST CSF

The NIST CSF 2.0 guides industry, government agencies, and other organizations to manage cybersecurity risks.

It offers a taxonomy of high-level cybersecurity outcomes that can be used by any organization—regardless of its size, sector, or maturity—to better understand, assess, prioritize, and communicate its cybersecurity efforts.

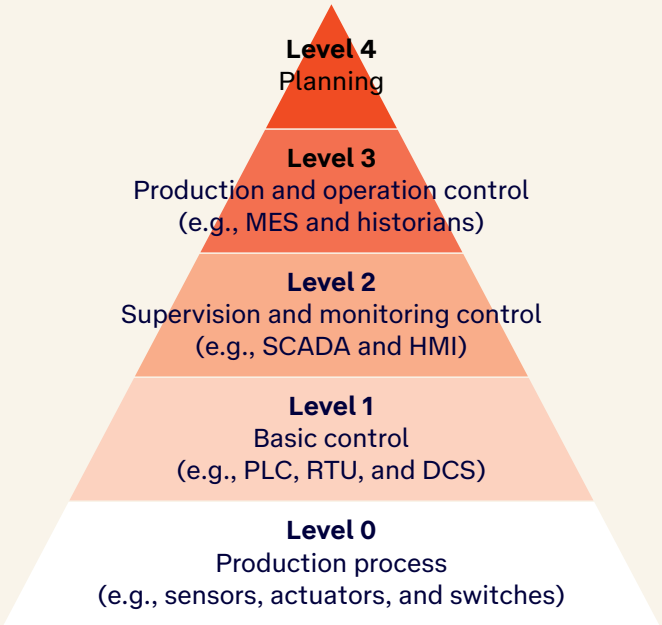
In this report, it offers a commonly used framework to assess the maturity of manufacturing firms across all IT and OT.

ISA-95

ANSI/ISA-95, or ISA-95, is an international standard from the International Society of Automation for developing an automated interface between enterprise and control systems.

ISA-95 is a reference model that categorizes an information hierarchy for computer-integrated manufacturing (CIM), which is still used for Industrial Control System design.

This report uses it as a framework to assess the maturity of manufacturing firms against the Purdue model.



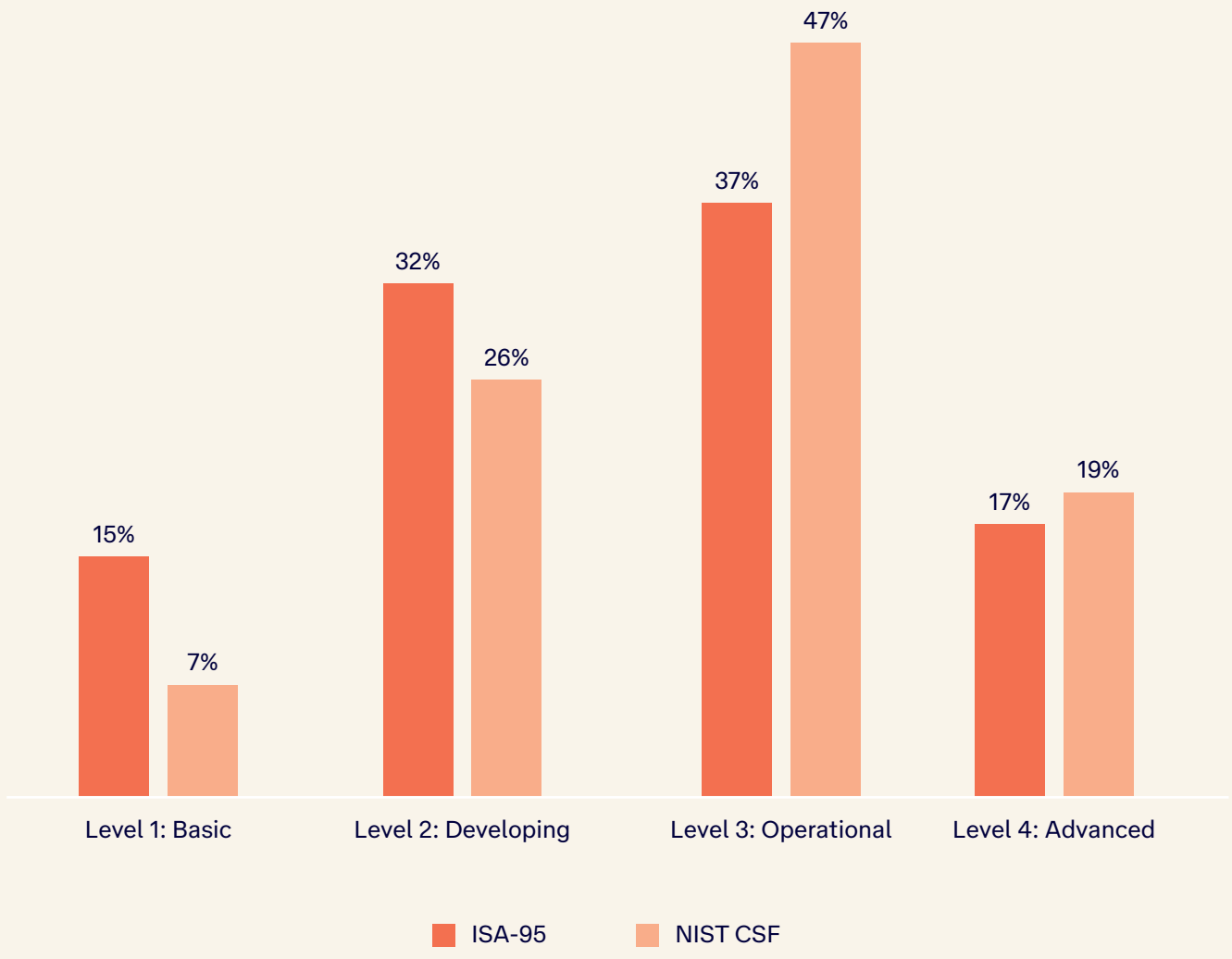
Source: NIST, ISA, and Omdia

OT security preparedness differs across frameworks, locations, and subsectors

The results are in: most firms are at an 'operational' or 'developing' maturity level, with few reaching 'advanced' status (**Figure 13**). Readiness levels are generally higher when evaluated through a threat lifecycle lens (NIST CSF) compared with the OT stack (ISA-95).

Figure 13: Most manufacturers are at operational levels of IT/OT cyber readiness, and few are advanced

Q. On a scale of 1 to 4, how mature is your organization in securing IT/OT convergence across the NIST cybersecurity attack framework? How mature is your organization in securing connected IT/OT each level of the Purdue model on scale of 1 to 4?



Notes: n=513, global

Source: Omdia

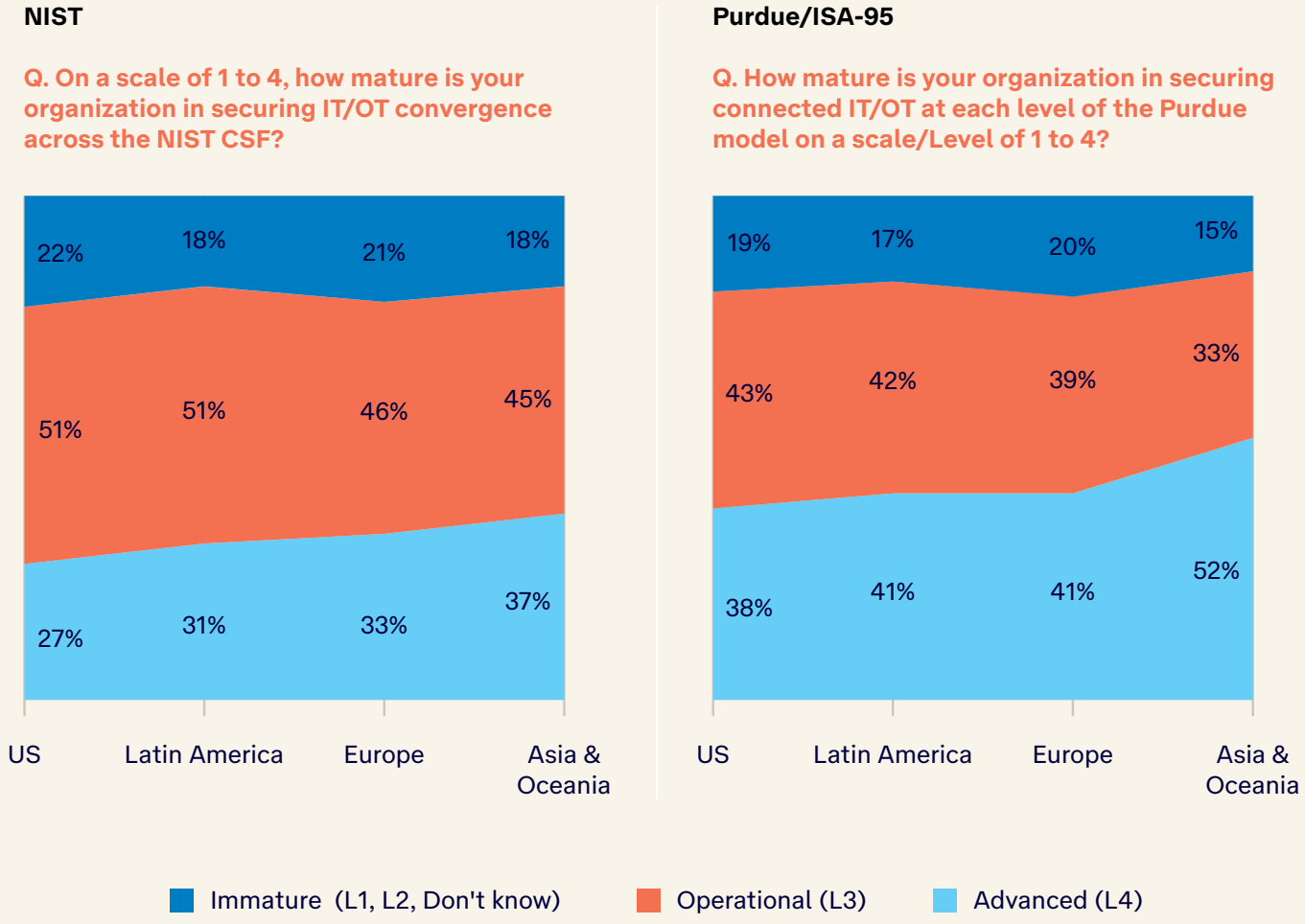
Confidence varies by security model

Security maturity tends to be higher when measured using an IT-centric framework that is familiar to those from traditional IT backgrounds. In contrast, this confidence is noticeably lower when assessed based on an OT-centric framework, such as the Purdue Model. This disparity in confidence is consistent across all regions, with the Purdue Model having higher percentages of respondents rating themselves as 'immature' regardless of geography. This aligns with the previous finding indicating that the primary decision-maker tends to be the CISO, followed by the CRO, and then the CTO.

Security maturity varies across regions

Figures 14 and **15** show regional comparisons for global and Asia & Oceania, respectively.

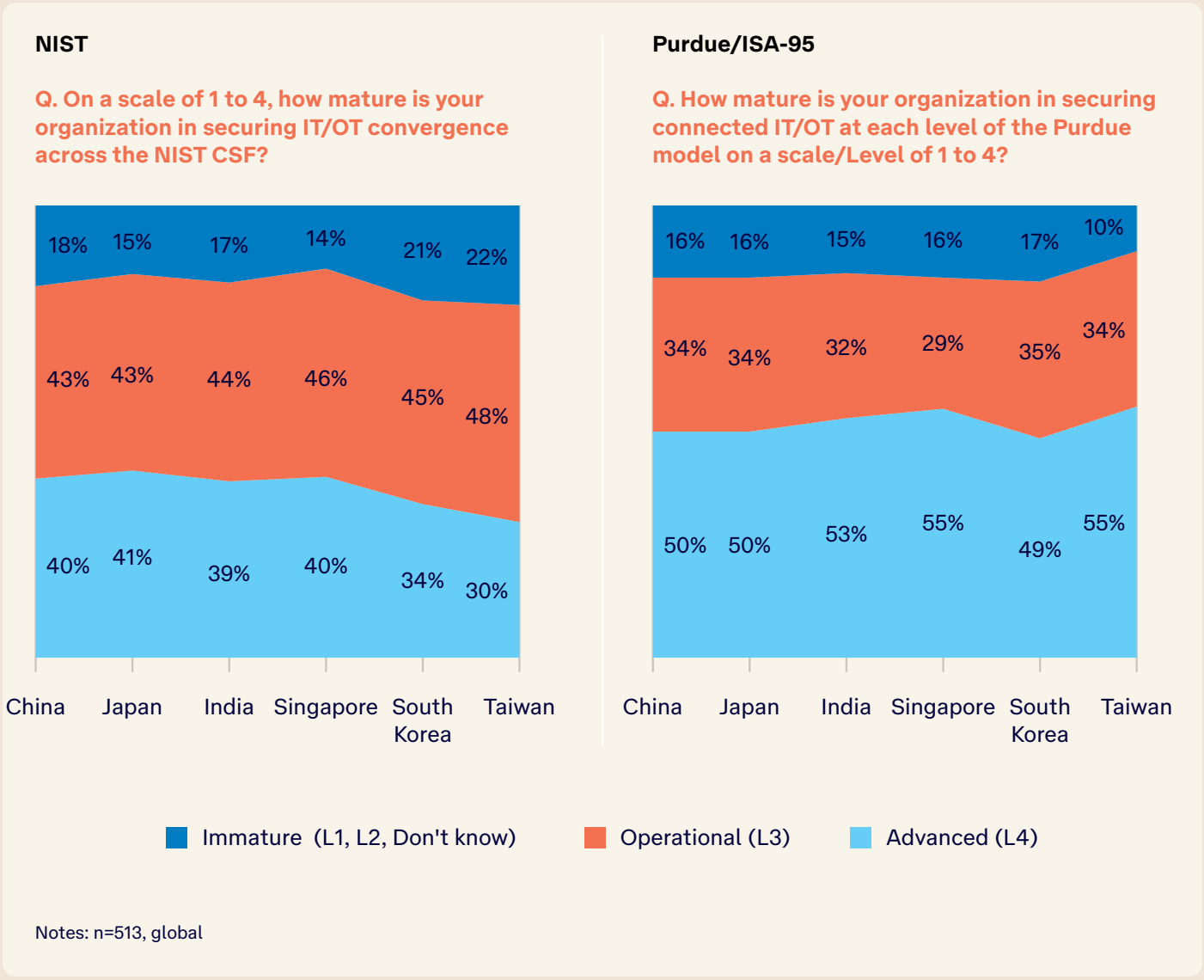
Figure 14: Global readiness for IT/OT cybersecurity in manufacturing



Notes: n=513, global

Source: Omdia

Figure 15: Asia & Oceania readiness for IT/OT cybersecurity in manufacturing



Notes: n=513, global

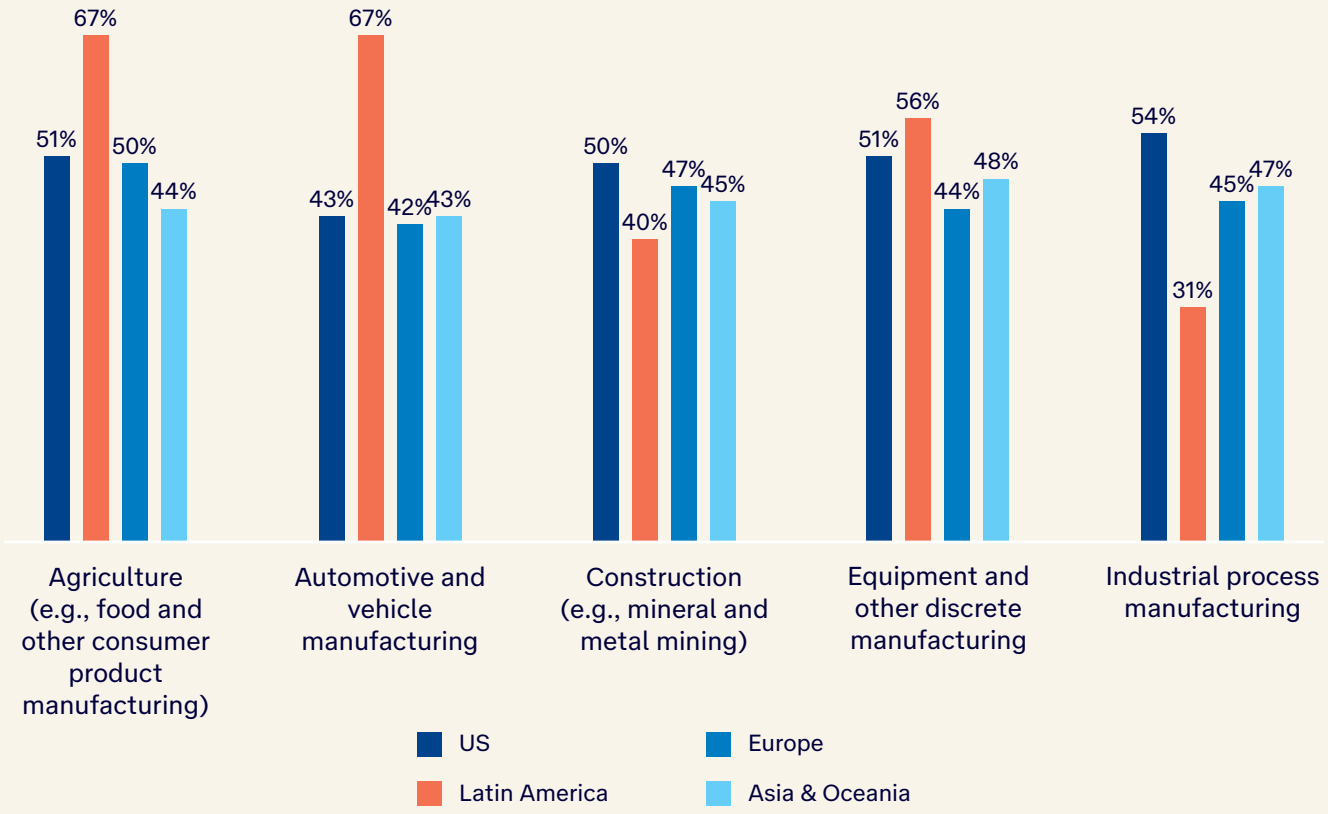
Source: Omdia

Confidence in security maturity varies by region, with organizations in the US demonstrating higher confidence compared with their global counterparts in both the NIST CSF framework and the Purdue Model. In Asia & Oceania, organizations are more likely to view themselves as 'immature' compared with their global counterparts. This variation extends to countries within a region as well. For example, there are significant differences among the countries in the Asia & Oceania region. While the NIST CSF generally instills greater security confidence at the country level, it is noteworthy that these differences are less consistent when examined at the individual country level.

Varying states of readiness across regions and subsectors of manufacturing

Figure 16 shows the percentage of respondents in each subsector and region with operational security maturity.

Figure 16: Subsectors in each region have varying maturity levels



Notes: n=513, global

Source: Omdia

As we have seen above, security maturity levels vary across different regions and countries. This variation is also evident within subsectors in each region, showcasing distinct differences in security maturity. Each subsector exhibits standout differences in security maturity across regions.

The US and Europe possess a similar level of security maturity across their subsectors. However, Europe's equipment and discrete manufacturing sectors are less advanced in terms of security maturity.

The Latin America region has two rather mature subsectors: agriculture and consumer products, as well as the automotive industry. In contrast, the construction and industrial process sectors in this region appear to have less mature security.

Asia & Oceania has a relatively uniform maturity across all sectors, with equipment and discrete manufacturing, as well as industrial process manufacturing, showing slightly higher levels of maturity.

This variation requires manufacturing firms with multiple sites and/or multiple OT environments to have individual OT cybersecurity programs for each site. This allows CISOs to address the specific needs of each site or environment. However, manufacturing firms should have an overarching OT security program that oversees and guides the individual OT cybersecurity programs at each site or environment.

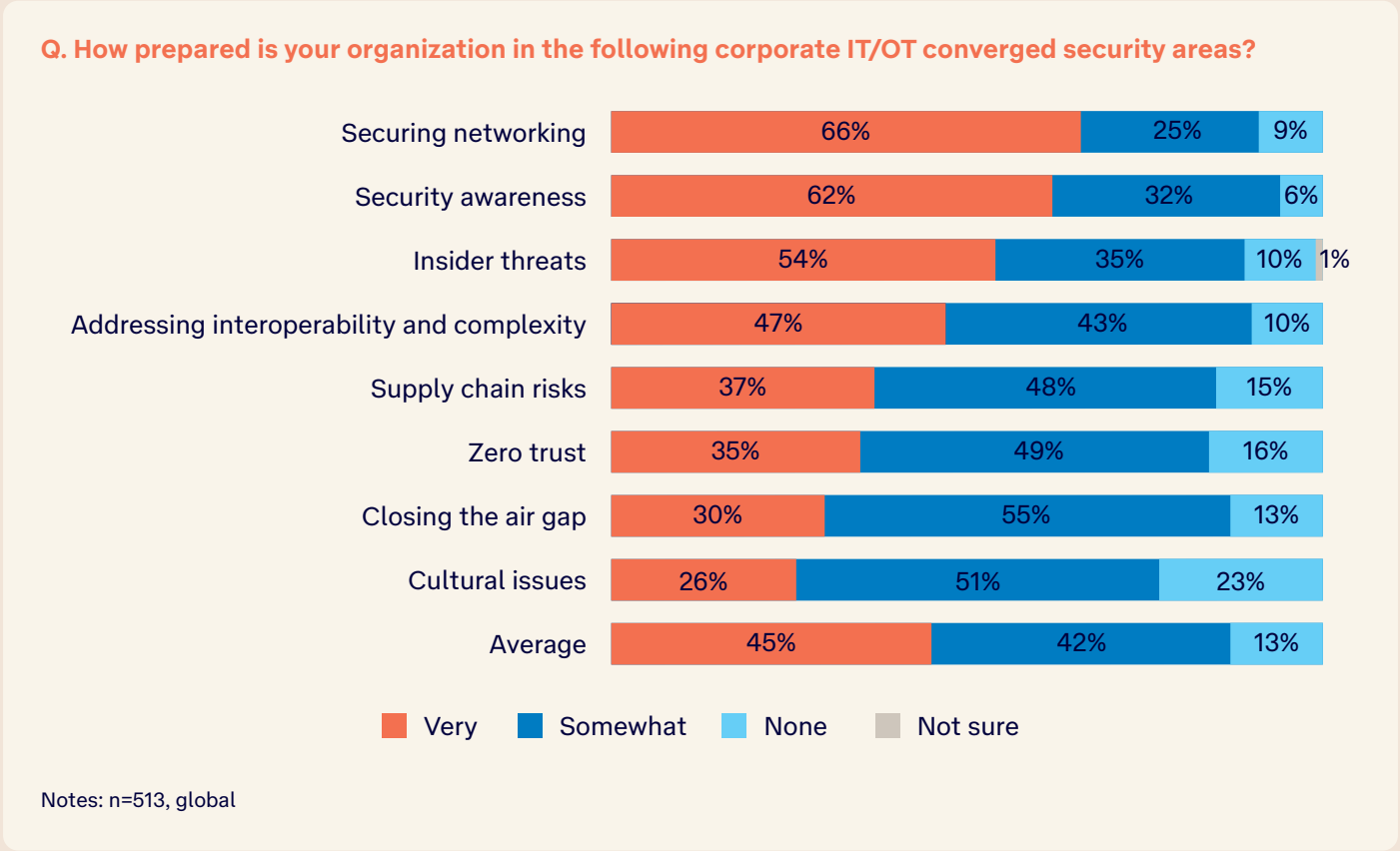
This aligns with the latest NIST guide on OT Security (Revision 3), which recommends the following:

An OT cybersecurity program is typically tailored to a specific OT environment. An organization may have multiple sites, each with multiple specific OT environments. In such situations, an organizational-level OT security program should be defined with recommendations that cascade down and adapt to the needs of individual sites and OT environments.

The importance of identifying challenges related to different types of threats in OT environments

Only 45% of manufacturers are well-prepared for converged IT/OT security across eight key areas (**Figure 17**).

Figure 17: OT cybersecurity leaders should prioritize addressing their weakest areas: culture, demilitarized zone (DMZ), and zero trust

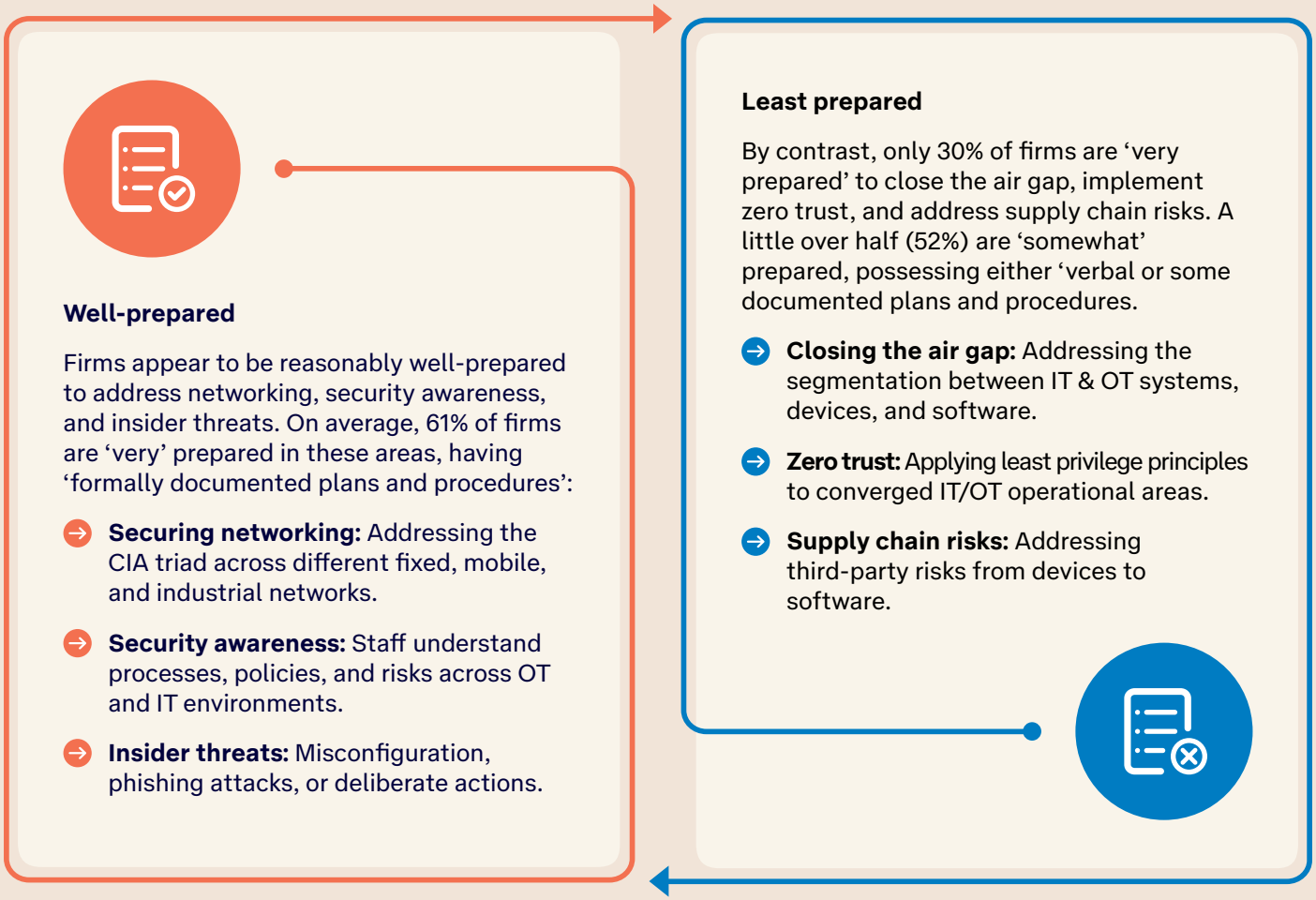


Notes: n=513, global

Source: Omdia

Companies that responded that they are 'not as prepared yet' are particularly vulnerable. Our analysis revealed that 42% of these companies are 'somewhat' prepared, while 13% are not prepared at all, with no formal process in place. A major incident or breach in any of these areas is sufficient to stall the primary goal of innovation and undermine the operational integrity of the manufacturing industrial control systems (ICS) environment.

Figure 18: Cybersecurity vulnerabilities (descending order)



Source: Omdia

Cybersecurity executives are increasingly responsible for managing OT security

OT security is shifting to IT, but is it fast enough?

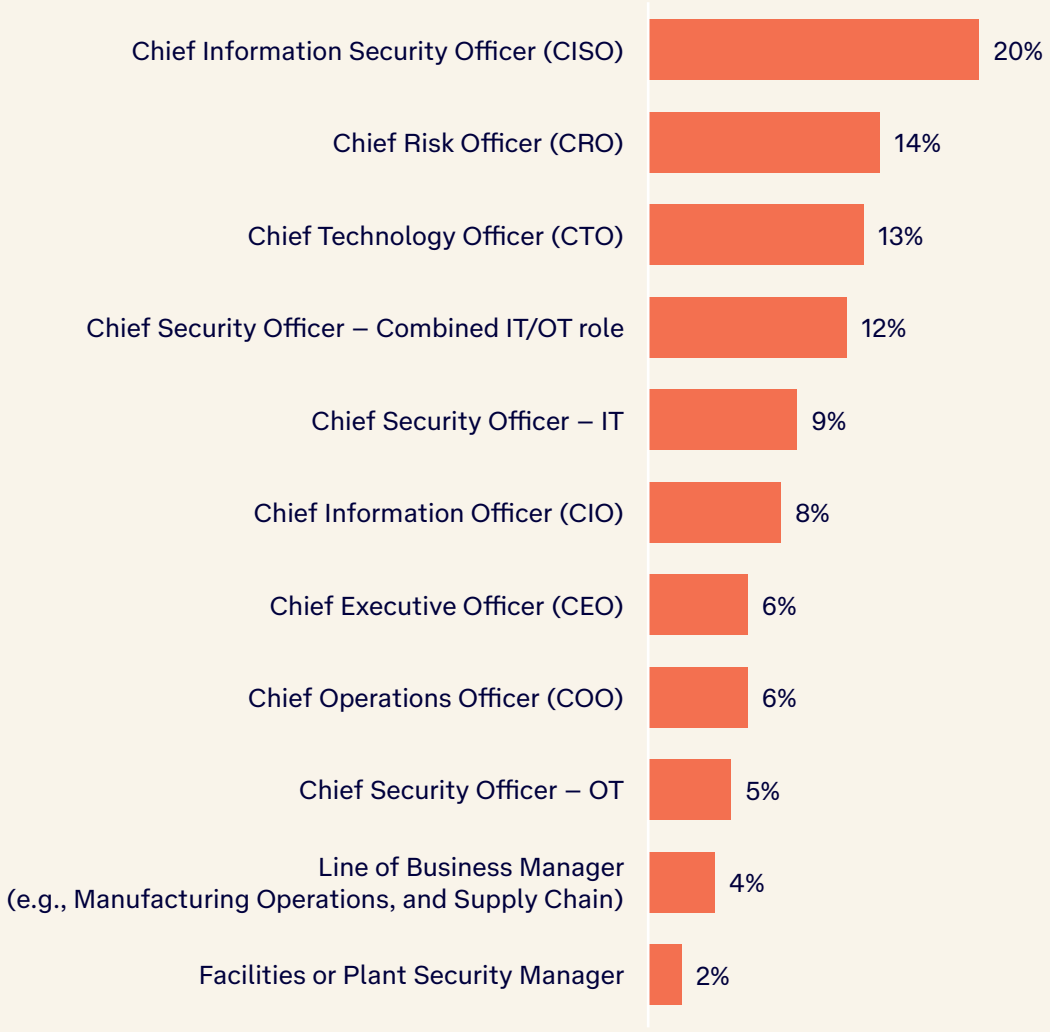
Historically, production managers with engineering backgrounds were responsible for manufacturing operations. This approach made sense owing to the physical nature of the tasks and the segregation of plants from corporate locations and systems.

However, things are changing. The fact that most cybersecurity incidents in manufacturing originated in IT but have affected OT and operations underscores and confirms the trend of making IT and cybersecurity directors responsible for OT in manufacturing, although traditionally, OT environments were solely managed by LOB and operational directors on-site.

Figure 19 shows that CISOs, who have typically specialized in cybersecurity, are now being tasked with the security of operational and production systems. Omdia predicts that this will extend beyond the cybersecurity for OT to include physical (premises) security over time as CROs and CTOs are assigned greater accountability for OT as well.

Figure 19: Cybersecurity executives are increasingly responsible for managing OT security, more so than COOs and LOB (production) managers

Q. Who has responsibility for understanding and implementing IT/OT converged security in your organisation?



Notes: n=513, global

Source: Omdia

As responsibility and accountability shift, Omdia has observed, through discussions with executives, that power is not moving at a commensurate rate: LOB managers in operations offices—such as those in production, logistics, hospitals, or management facilities—continue to be the gatekeepers and custodians of Level 0–3 systems owing to their close proximity to these operations.

Omdia believes that this shift lift is not happening fast enough. Given most manufacturers we surveyed have had an incident that originated in IT and caused significant OT downtime, firms need to appoint a clear and empowered executive with end-to-end responsibility across IT and OT across global and regional sites.

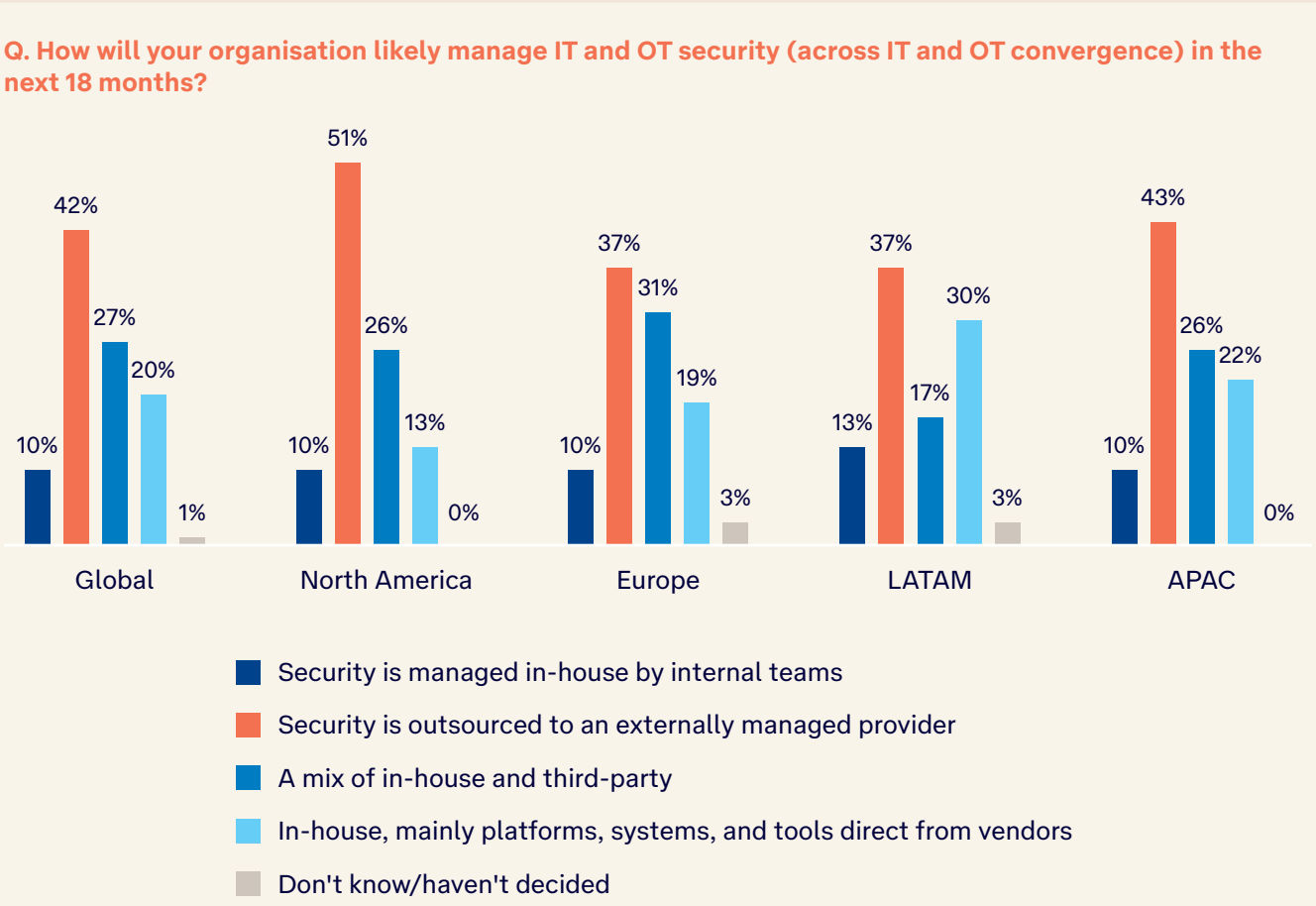
Firms will engage third-party providers to expedite their OT security readiness

Firms are driven by increasing risks, complexity, costly downtime, stricter government regulations, and a shortage of skilled staff

Executives surveyed highlighted the challenges in finding skilled and experienced staff who understand both IT and OT from a security perspective, especially in their industry context.

As a result, most firms will engage a third party through an outsourcing agreement or utilize in-house teams to bolster IT/OT-specific security services (**Figure 20**).

Figure 20: Over 79% of firms will engage a third-party service provider to address OT security challenges



Notes: n=513, global

Source: Omdia

Omdia recommends selecting third-party service providers that have expertise in core IT/OT integration technologies, such as networks, IoT, cloud computing, edge computing, and cybersecurity. With the expected increase in IT/OT integration by 20% in the near term, alongside rising cybersecurity risks, Omdia expects a growing demand for outsourcing, emergency incident response, and external advisory services.

5.0 A path forward

Recommendations

As digital capabilities take on a more strategic role in manufacturing, there will be a growing motivation to break those silos and converge IT/OT domains to improve innovation, resilience, and availability.

Importantly, managing cybersecurity risks across these converged systems, as well as among people and cultures, will be essential for ensuring operational resilience, improving customer experience, and maintaining competitive sustainability.

Based on the findings from this study and Omdia's research, we have identified six foundational recommendation areas that should be addressed.

Figure 21: Six foundational recommendation areas that should be addressed

Source: Omdia

Table 1:

Domain	Considerations	Recommendation
Plan for expanding integration Proactively harness IT/OT integration with robust cybersecurity to achieve business benefits.	• In most manufacturing firms globally, the percentage of OT systems connected to IT will increase by 20% over the next two years. • Leading firms are forging ahead with integration to achieve business, IT, and operational benefits. In fact, 86% of firms indicated that IT/OT integration is important for achieving positive business outcomes—not just technology goals—such as innovation, reliability, and security.	**Leverage IT/OT integration to achieve business benefits** • To remain innovative, manufacturing firms must consider where and how I4.0 technologies can materially affect their businesses. Those that fail to do so risk falling behind in terms of efficiency, innovation, safety, and security. • I4.0-led integration leverages emerging technology in tandem and unison with legacy technologies, systems, and devices. IT/OT (including IoT) integration improves information and data transparency, supporting better decision-making across manufacturing, finance, operations, and engineering. **Be aware of the resultant cybersecurity risks** • While greater connectivity provides operational and business benefits, firms must address the heightened risk of attacks and incidents as systems become less isolated and more interconnected. These challenges are manageable.
Proactively secure convergence Apply a converged security posture view across all layers of the manufacturing technology stack.	• 75% of attacks affecting critical infrastructure operations originated from IT cyber (corporate) systems. • Higher levels of the IT/OT stack are more vulnerable, with 43% of the most significant incidents in OT starting at Level 4 (e.g, ERP and SCM [planning]) or Level 3 (e.g., manufacturing execution systems [MES]). • For 70% of organizations, having good visibility of all IIoT and OT assets within the organization is essential.	**Maximize visibility to minimize blind spots** • To ensure security, visibility is essential. A proactive security posture requires network monitoring, security information and event management (SIEM), and behavioral anomaly detection, which are critical. Firms must assess and maintain accurate visibility across systems. This can be done by implementing configuration management across a wide range of increasingly integrated devices (Purdue layers) and throughout the enterprise architecture (IT and I4.0). This comprehensive visibility is crucial for effectively assessing and responding to potential threats. **Enhance visibility in supply chain and third-party risk management** • It is essential to extend visibility to all third parties (supply chain), including suppliers, vendors, partners, contractors, and other external entities. The critical technology domains that must be secured include cloud computing, IoT, edge computing, mobile devices, third-party OT, networks, AI, and data lakes.

Domain	Considerations	Recommendation
		Layered defense and defense in depth • Do not rely exclusively on an airgap—Ethernet, industrial networks, and device (wireless sensor) networks are vital in manufacturing. As convergence accelerates enhanced security across integrated (typically Levels 2–4) and isolated (Levels 0–2) networks, it requires careful segmentation in physical and virtual network architectures to balance connectivity with isolation and enforcement perimeters, including firewalls. Do not rely on an 'air gap' for assurance, as most attacks originate in IT, not from OT or devices.
Bolster people and technical expertise Uplift and invest in converged IT/OT cybersecurity to avoid costly downtime.	• Owing to emerging risks, 69% of firms either fully or partially outsource IT and OT security to a third-party managed services provider. • IT/OT integration experience is the most critical factor when choosing a provider for OT security.	**Partner for greater security** • Faced with rising risks and the potential impact of breaches in their IT or OT systems, many firms are planning to upskill their staff and hire IT/OT-specialized technology and security professionals who have expertise in both IT and OT. However, such professionals are in short supply, leading many firms to consider outsourcing providers for these services. **Re-evaluate the effectiveness of engaging third-party cyber experts** • IT/OT leaders must revisit the effectiveness of engaging third parties under outsourcing or professional services engagements for testing, training, upskilling, or security management with a managed services provider to achieve faster time to value and assurance.
Assign responsibility and accountability Ensure that IT and OT security responsibilities are clearly defined and empowered across both corporate and production environments.	• Only 26% of firms are 'very' prepared to address cultural issues owing to IT and OT misalignment regarding cyber risks. Most firms are not prepared. • Only 18% of firms have a CISO solely and directly responsible for understanding and implementing an IT/OT converged cybersecurity program; responsibilities are often shared. • Only 33% of firms have a centrally managed IT/OT cybersecurity approach.	**Responsibility must be clear and integrated** • The cybersecurity team and its leaders can be a conduit as market forces drive the need for internal innovation. They bring together engineering disciplines and practices in production that are complementary to IT and data-based fields when jointly working to maintain and improve OT systems. Demonstrable improvements in safety, integrity, and availability from IT improvements will address common goals across historically separated teams. • Executives must foster mutual efforts across teams to bridge the cultural divide between production (operations and engineering focus) and IT / Cybersecurity (data and corporate focussed). Further, one group or person must ultimately be responsible and have the authority to act on security challenges for mission-critical systems.

Domain	Considerations	Recommendation
Leverage the right tools Utilize standalone AI-powered tools and integrated platforms to enhance protection against a wide range of evolving attack vectors.	• The top three most significant IoT or OT-specific cybersecurity-triggered threats faced by firms in the region in the past 12 months were APTs (54% of respondents), Malware, including ransomware (43%), and DDoS (40%). • 62% of manufacturing firms faced issues with resilience or availability, typically costing between $200,000 and 2m. • 75% of attacks that affected critical infrastructure operations started in IT cyber (corporate) systems.	**Invest in OT-enabled cyber capabilities** • OT security is unique and distinct from IT security, but it must be addressed in an integrated manner. OT OEMs are embedding more cyber capabilities in their products. Leading cybersecurity vendors are also extending capabilities beyond IT and into OT, and Omdia is seeing massive growth in OT-specific security (i.e., Dragos, Claroty, Nozomi, and PAN among executives surveyed). However, most organizations struggle to effectively utilize automation and advanced features in these tools. Therefore, it is advisable to bring in platform and service expertise. **Balance point solutions with platforms** • Manufacturing budgets and margins are tight, making it essential to find the right mix of existing IT and OT security capabilities as integration accelerates. In the IT domain, many enterprises are shifting away from point solutions in favor of broader platform-based services for simplicity, value, and efficacy. Omdia expects a similar transition to occur in OT; however, the services component is vital, as these tools require specialized skills.
Expedite readiness with standards Improve governance, risk, and compliance readiness through industry tools and guidance.	• Only 17% of firms are advanced in securing IT/OT convergence, consistent with the NIST CSF assessment. • Firms demonstrated higher confidence (operational and advanced) in their security based on NIST CSF (69%) than the Purdue Model (60%). • Additionally, 46% of organizations are currently at either a basic or developing level of IT/OT security.	**Assess and understand application regulations, frameworks, and standards** • External standards offer repeatable, proven methods to expedite assessments and ensure compliance with regulations (e.g., NIST SP 800-82r3, ISA/IEC 62443 [series], ISO 27001 & 20772, MITRE ATT&CK for ICS and government agency support [CISA, ENISA]) **Seek guidance on addressing emerging regulations** • NIS2, announced in January 2023, affects a broader range of critical infrastructure firms(refer to Annex I and II). EU-based manufacturing firms are classified as 'important' with new requirements now in effect. The impact is changing and needs to be assessed against your particular sub-industry. Notable changes will affect ten key elements for compliance, including incident notification, cybersecurity risk management measures, supervisory responsibility, and enforcement/penalties. Regulations differ across Asia & Oceania, requiring regional-specific considerations.

Appendix

Omdia is pleased to present this research in collaboration with Telstra International. The insights and trends outlined in this report are based on in-depth fieldwork conducted in mid-2024, capturing the latest experiences of organizations.

We trust this paper will guide security, technology, and business leaders in leveraging I4.0 technologies through mature OT cybersecurity for sustainable competitive advantage.

Methodology

This study reveals the convergence rate between IT and OT in manufacturing, highlighting cybersecurity challenges for executives responsible for ensuring the confidentiality, integrity, and availability (CIA) and availability, integrity, and confidentiality (AIC) triads at their firms.

The report focuses on the enterprise and industrialized use of IT/OT and IIoT (excluding consumer-specific technology).

IT/OT convergence refers to digital connectivity, digitalization, and digital transformation projects that link corporate and other IT networks to physical, operational components, including but not limited to ICS, SCADA systems, programmable logic controllers (PLC), and any other such systems controlling physical, operational components, such as robotic picking and automated production lines, 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.

From August through November 2024, Omdia conducted a direct primary research survey of 513 senior security decision-makers at mid- and large-sized firms across manufacturing in the US, Europe, Latin America, and Asia & Oceania.

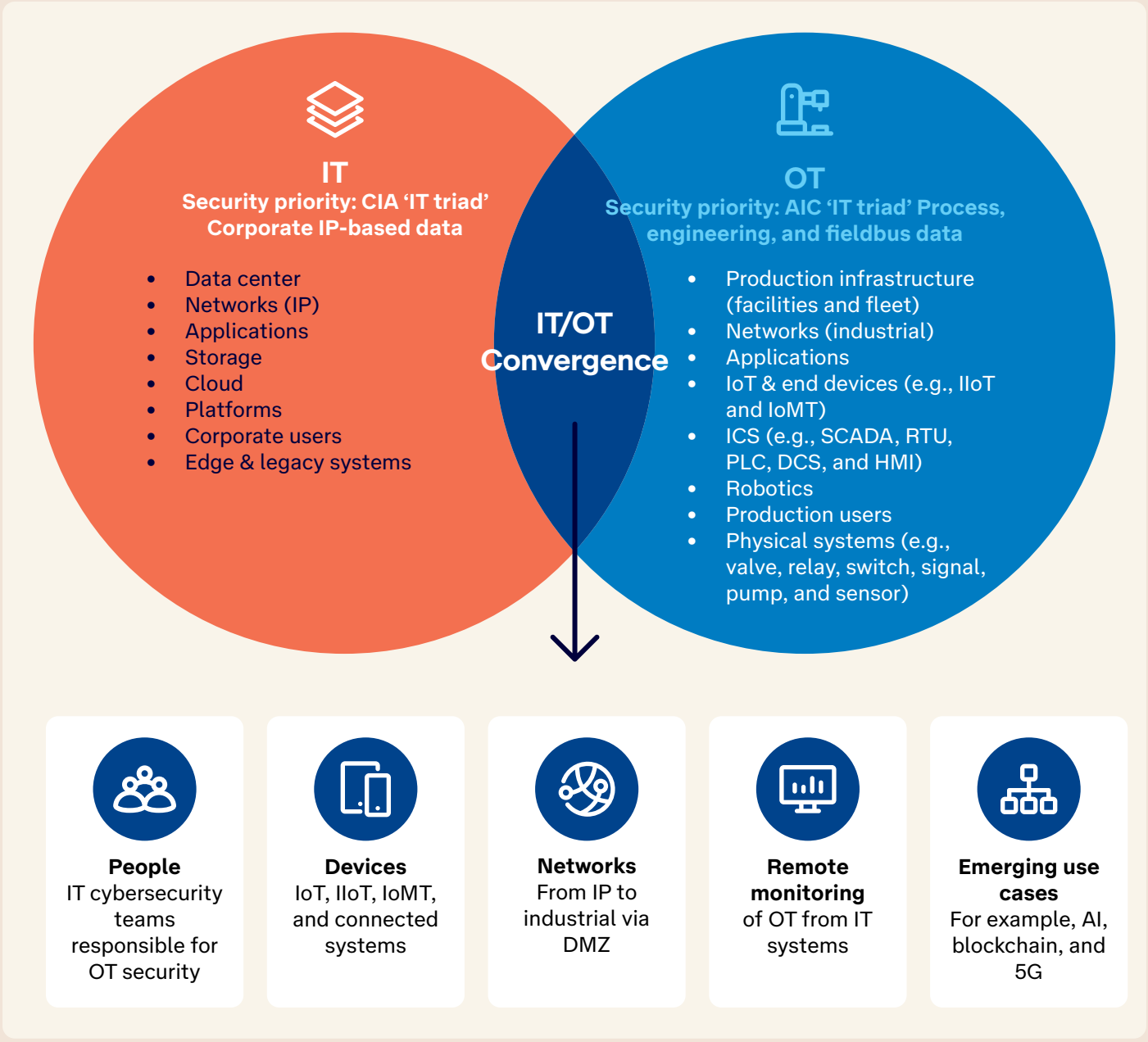
- 258 respondents were firms with headquarters (HQ) in the US, Mexico, UK, Germany, France, and Italy.
- 255 are firms with HQs in Asia & Oceania, including China, Japan, South Korea, India, Taiwan, Singapore, and Australia.
- Manufacturing firms in scope include equipment and other discrete manufacturing, automotive and vehicle manufacturing, industrial process manufacturing, construction (e.g., mineral and metal mining), and agriculture (e.g., food and other consumer product manufacturing).
- Firms in scope have over 500 employees.
- Survey respondents are either a technology or security executive or manager (e.g., CIO) or a LOB director or executive responsible for IT and/or OT security.

Global counterpoints in this research leverage Omdia's global expertise in digital enterprise and cybersecurity intelligence services, notably Omdia Digital Enterprise Services.

Appendix 1: Conceptualizing IT/OT convergence in manufacturing

Convergence is widespread across various areas, including devices (IoT and connected systems), networks (from IP to industrial), shared systems (utilizing common floor space), enterprise applications (for data extraction and analysis), remote monitoring (overseeing operational technology from information technology systems), people (IT cybersecurity teams responsible for OT security), and upgrades and repairs (involving new IoT-enabled product devices).

Figure 22: Conceptualizing IT/OT convergence in manufacturing



Source: Omdia

Appendix 2: IT/OT security is measured against four levels for each framework

The following table helps firms consider their relative maturity and common IT/OT integration challenge areas.

Table 2: Cybersecurity readiness table

Level #	Maturity	Status	Characteristics	Impacts
1	Immature	Nascent	IT and OT are managed in silos with little integration, automation, or shared experience.	High degree of operational risk from cyber and/or physical incidents. Inconsistent security posture and controls across IT and/or OT. Undetected exposures and highly reactive to threats and incidents.
2	Immature	Developing	Basic level of reporting, integration, and investigation capability across IT and OT.	Medium level of operational risk, automation, and detection. Pockets of improved, yet inconsistent cybersecurity posture and controls across OT. Ad hoc remediation and recovery.
3	Mature	Operational	Well-established IT/OT security that is integrated and well-automated across all critical cyber/physical production systems.	Medium to lower levels of operational risk from cyber. Defined and managed cybersecurity posture across IT and OT. Medium risk from poor remediation and recovery in APT and sophisticated attacks.
4	Mature	Advanced	Advanced and sophisticated use of IT/OT-specific automation tools, platforms, and processes across processes, people, and technology.	Lower levels of operational risk from cyber, but not eliminated. Proactive and well-defined cybersecurity posture across physical and virtual. Continuous, consistent and high-fidelity threat assessment, playbook response, remediation and recovery objectives, processes and procedures.

Source: Omdia

Author

Adam Etherington
Senior Principal Analyst, Digital Enterprise Services
adam.etherington@omdia.com

Jonathan Ong
Senior Analyst, Managed Security Services
jonathan.ong@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 capitalize 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 International

Telstra is a leading telecommunications and technology company with a proudly Australian heritage and a longstanding, growing international business. Today, Telstra International has over 3,000 employees based in more than 30 countries outside of Australia, providing 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, security, unified communications, cloud, industry solutions, integrated software applications and services. These services are underpinned by our subsea cable network, with licences in Asia, Europe and the Americas and access to more than 2,000 Points of Presences (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.

For more information, please visit telstraInternational.com.

Copyright notice and disclaimer

Contact your Telstra account representative for more details.

telstraenquiry@team.telstra.com telstrainternational.com

2025.02.18 1:30 PM