IN PARTNERSHIP WITH

The Power of Breakthroughs in IT/OT Collaboration

JULY 2025

Introduction

Digitalization is advancing in manufacturing as companies press ahead with multiyear programs to future-proof their operations. The current climate of global uncertainty is a shot of adrenaline for those programs. It provides a sense of urgency for any activities that help organizations gain operational visibility and agility. According to our June 2025 research **Navigating Uncertainty**, manufacturers see digitalization as a way to mitigate near-term risks.

Progress in digitalization means continuing to narrow the chasm between IT (Information Technology) and OT (Operational Technology) by connecting networks, assets, and teams. By definition, security takes on new salience because having more connections correlates with more vulnerability. Hackers and cybercriminals have taken note. Manufacturing, once a backwater for cybercrime, has been the number one target for cyberattack for four years running, representing 26% of all attacks, according to the **IBM X-Force 2025 Threat Intelligence Index**. One executive captured the essence: “As places like hospitals and banks have become more secure, the bad guys are moving down the chain to try to pick on manufacturing because they know manufacturers are probably behind the times.”

Three in four companies with a high degree of IT/OT convergence prioritize shared goals and objectives that drive IT/OT collaboration versus only 44% of less converged companies.

To better understand how companies are managing the compound challenge of advancing digitalization programs, bridging the gap between IT/OT, and keeping their OT networks secure, Manufacturers Alliance Foundation partnered with **CDW** to study why some companies have made impressive progress while others are still struggling. We conducted focus interviews with IT and OT executives representing a variety of industries and surveyed 170 U.S.-based mid-cap to large-cap industrial companies. We also compared our findings with data from a 2023 Manufacturers Alliance Foundation **cybersecurity report** to provide insights into how priorities and capabilities have shifted over the last two years.

Key Findings

>> A commanding **majority of manufacturers (71%)** have started their IT/OT convergence journey, reflecting the extent to which this integration has become a digitalization imperative. (We identified these advanced companies by responses of exceptional or very good when rating their IT and OT integration and collaboration for OT security.)

>> **Network segmentation is a foundational step** for IT/OT convergence but remains an impediment. For many manufacturers, segmentation is an iterative process and therefore still a work in progress.

>> Companies that are more advanced in their IT/OT convergence journey demonstrate a clear set of behaviors and capabilities **setting them apart from less advanced peers**. Examples include dedicated reporting structures, clear definitions of roles, shared resources, effective communication, and the incorporation of IT and OT perspectives into decision-making.

>> As a result, **advanced companies are positioned to respond** and recover from cybersecurity threats across a range of data points, including disruption of critical operations, insider threats, and unauthorized remote access. They are also more confident in their ability to attract the cybersecurity talent they need to address increasingly sophisticated attacks.

>> **The impact of cybersecurity preparedness** on insurability is in flux, with some expecting to see a tightening of insurance requirements in the near future. Companies that can demonstrate a posture that is robust, resilient, validated by third parties, and in line with recognized standards will be better prepared if and when insurance requirements tighten.

>> **Benefits of IT/OT convergence** transcend security. Advanced companies already see the competitive advantage their journey has delivered. They are primed to seize the moment as breakthrough innovations occur and thereby solidify and expand their advantage over companies that lag behind.

Tracking Shifts in Attitudes

Views about the importance of IT/OT collaboration have remained fairly constant since our 2023 research with more than 80% citing the importance of this collaboration in both surveys. Manufacturers remain focused on cybersecurity as well, citing it as the number one challenge they face as they pursue IT/OT convergence.

Artificial intelligence (AI) is helping hackers and cybercriminals become more efficient and effective in building exploits and identifying victims. As in our 2023 research, three out of four manufacturers expect the sophistication of those threats to keep increasing. Most remain optimistic that manufacturing will be able to keep pace with these threats, although there has been a slight dip in the share that feels this confidence (89% in 2023, 82% in 2025). The skilled talent shortage may play a role in this decline. Companies are slightly less optimistic about talent, specifically, whether they will be able to acquire the talent needed to address these sophisticated attacks.

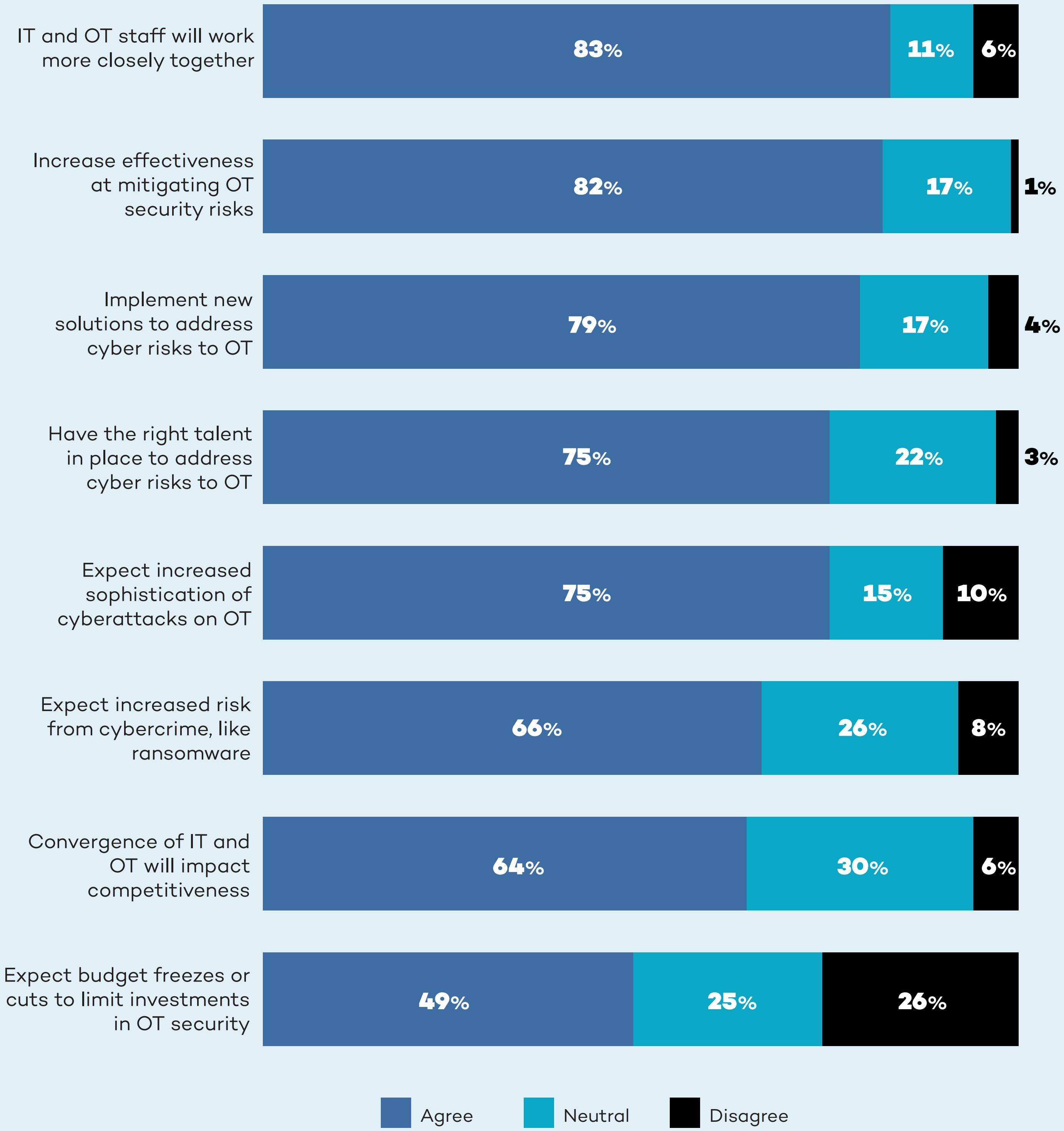
In both our 2023 and 2025 surveys, the majority agree that IT/OT convergence has a direct impact on overall competitiveness. Manufacturers understand that the benefits of digitalization start with securely connecting the networks, data, and teams of the IT and OT domains. While the journey can be long and take unexpected turns, companies that have made progress are already seeing an impact on their overall competitiveness.

82%

of respondents expect to increase effectiveness at mitigating OT security risks in the next 3 years

As will be discussed in more detail below, convergence leaders are much more likely to experience competitive gains than their less advanced peers.

How Manufacturers Think OT Security Will Change in the Next Three Years



Source: 2025 IT/OT Collaboration survey, Manufacturers Alliance Foundation and CDW

The Importance of Network Design

The first step in bringing IT and OT together involves the network. "Networking is the most important element, and it really starts with network security for us. That includes things like next-generation firewalls, segmentation, and micro segmentation within the OT network. It's all about limiting the devices that are allowed to talk to each other within the OT environment and then within the IT environment as well," according to Travis Ward, Director of IT Security and Compliance at **ConMe**t, a subsidiary of Amsted Industries.

The design of the network is critical. More than three in four (76%) manufacturers we surveyed understand the importance of a well-designed OT network in terms of the role it plays as an enabler of advanced manufacturing technologies.

The key characteristics of a well-designed OT network are a robust security posture as well as high reliability and availability. Segmentation of the network (to divide it up and prevent the lateral movement of threats) is typically part of the first phase of any OT network security program. Segmentation can be performed at the macro level (to cover multiple systems) or micro level (to isolate individual subsystems within the production process).

While the concept of segmentation is not new, it is a steep climb for most manufacturers because of the time and complexity associated with the process. For that reason, segmentation is ongoing and might start at the macro level but become more granular as time goes on. Travis Ward shared the overall vision: "Ultimately the goal is to connect everything, replace legacy systems, and then limit communication according to the principle of least privileged access."

For most, it's a matter of gradually increasing the share of connected assets. Jicky Kong, Vice President of Manufacturing at **Simpson Strong-Tie**, shared, "I wouldn't say that we have full digitalization across all plants in North America right now. About 80% of our assets are connected in one way or another to the network or to the internet. We are largely at the monitoring and data collection point of the journey."

Given the iterative nature of segmentation, most manufacturers are far from done because network optimization is a long journey and the rate of innovation can outpace the appetite for change. Less than half (46%) of the companies we surveyed use segmentation as part of their OT network security program today. Another 47% identify segmentation as an ongoing project or planned for the future.

Jill Klein of CDW explained, "Implementing network segmentation in a manufacturing environment is akin to performing spinal surgery on a conscious patient—each vertebra governs a distinct operational zone of the plant floor. Prior to any intervention, comprehensive asset discovery is essential to map system behaviors and interdependencies. The absence of full visibility, coupled with the risk of operational disruption, renders segmentation a complex and delicate undertaking. Each step in the process functions as a cog in the broader mechanism of organizational transformation—moved too hastily, it risks destabilizing the entire system."

The data on segmentation suggests that many companies still rely on a more extreme form of OT network protection – isolation – which cuts off all or part of the OT environment from the rest of the enterprise. While seemingly more secure, isolation is known to lull companies into a false sense of security unless there are strict controls on weak spots such as USB ports. Isolation also brings with it opportunity costs of not deploying more advanced technologies, such as edge networking or AI.

Legacy systems pose a tricky question for IT/OT convergence. They often represent the beating heart of the production environment and large investments that, while aging, still get the job done day in and day out. When asked what keeps him up at night, one IT director pointed to legacy systems: "We have equipment that has been running for 20 years, but it costs $3 million to upgrade. So it is a business decision not to replace that equipment and to accept the cybersecurity risk associated with it."

Oscar De Leon, Principal IoT Strategist at CDW explained why so many manufacturing companies are in this situation today: "Several decades ago, when those systems were built, manufacturers used to have automation engineers working directly for them. But over time, third-party automation integrators have taken on that role. What happens when the company that built that machine for you is no longer in existence? A lot of manufacturers are in this position today. They have lost that knowledge and they are doing whatever is necessary to keep those legacy machines running."

Manufacturers have a love-hate relationship with those systems and rank them as their third most difficult challenge, after cybersecurity and skilled talent. It is not surprising that interoperability between technologies came in fourth since legacy systems often have baggage, such as propriety protocols from multiple vendors, different generations of standards, and outdated operating systems.

Securing the OT network by preventing the spread of attacks is one side of the coin, but monitoring and recovery play a pivotal role as well, taking on increased prominence over the past two years. For example, Security Incident and Event Monitoring (SIEM), which leverages AI to aggregate and analyze data from multiple sources, has risen dramatically in popularity as a tool since 2023, reflecting the power of AI. In 2025, manufacturers are also gathering threat intelligence specific to the OT environment more frequently to improve their posture and proactively address specific vulnerabilities. For worst-case scenarios in which an attack is successful, more companies have deployed backup and recovery solutions for OT data to speed their ability to respond and recuperate from an attack.

Top 5 OT Network Challenges

1. Cybersecurity concerns
2. Lack of internal expertise in advanced OT networking
3. Legacy infrastructure limitations
4. Interoperability issues between technologies
5. Cost of upgrades and implementation

Source: 2025 IT/OT Collaboration survey, Manufacturers Alliance Foundation and CDW

Behaviors and Capabilities that Set Converged Companies Apart

Companies on both sides of the IT/OT convergence divide have deployed shared technology platforms, but this alone is not enough. Our survey reveals crucial differences between manufacturers with high versus low levels of IT/OT integration, and these differences go beyond the technology stack. The convergence mindset permeates how teams are deployed and the flavor of their interactions. Advanced companies are more than twice as likely (79% versus 31%) to have shared reporting structures ensuring the alignment of organizational expectations and the avoidance of silos.

The same is true of dedicated cross-functional roles, which are more than twice as prevalent among advanced companies (50% versus 24%). This underscores their commitment to cross-functional roles requiring accountability at the individual and organizational level. Similarly, advanced companies are six times more likely to offer job rotation programs that cover both IT and OT functions, giving participants broader institutional knowledge, expanding their cross-domain understanding, building empathy, and fostering personal connections among team members whose paths might never cross in siloed organizations. **Job rotation programs are popular** among job seekers and employees alike, helping employers offering them drive attraction, engagement, and retention at a time when skilled talent is in short supply. It is not surprising that leaders are more confident in their ability to attract the right talent needed to address cyber risks by a margin of 80% to 46%.

Jill Klein of CDW talked about the value of IT/OT convergence for the employer brand. “In the past, there was a single career path for IT and a single career path for OT. Now you see those paths intersecting. People who have both skills are considered top-tier talent. The next generation of industrial leaders aren’t choosing between IT or OT — they want both, and they’ll go where that’s possible.”

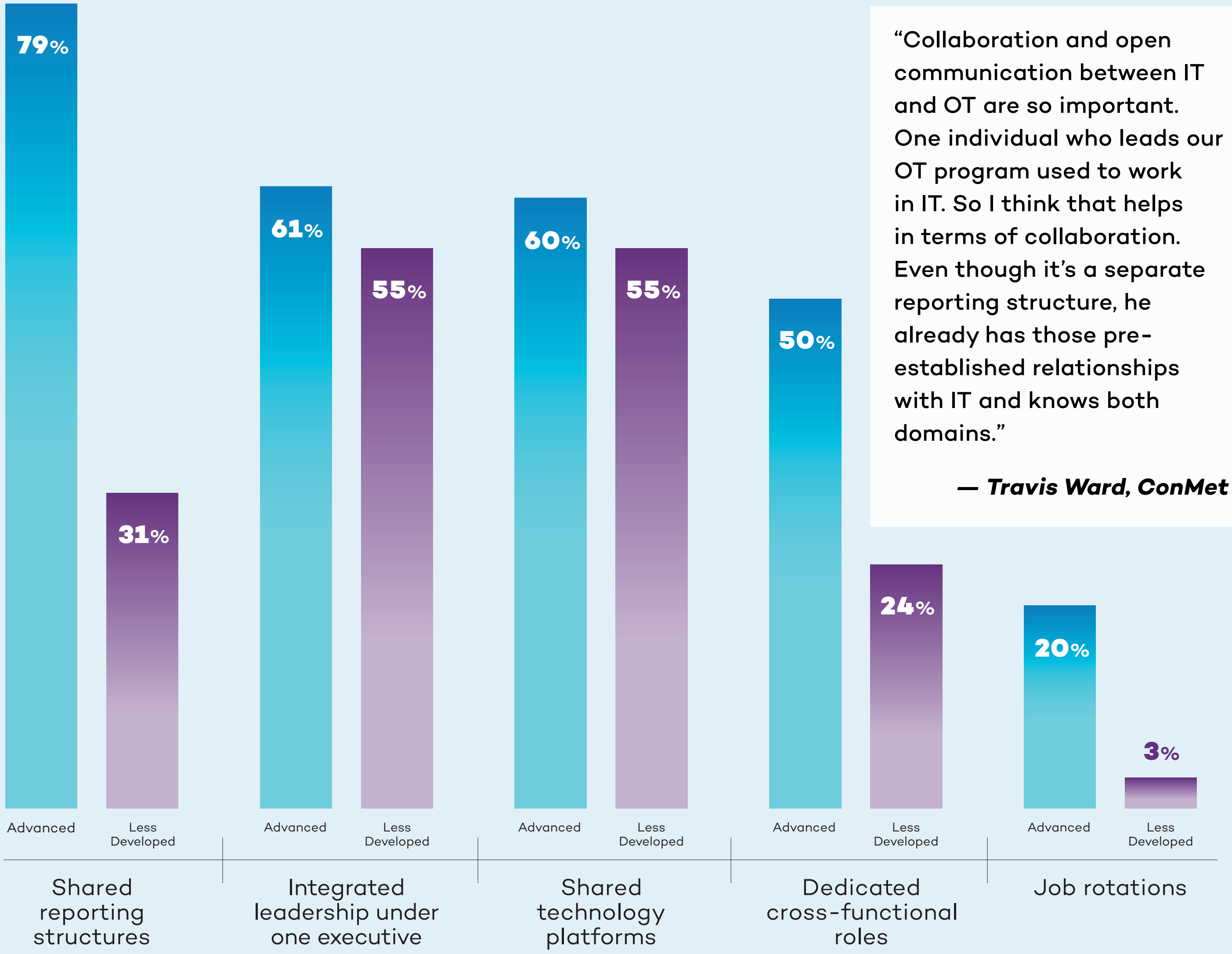
The blurring of the lines between IT and OT may start with resource sharing, another area where advanced companies stand out. When it comes to budget, personnel, and technology resources, IT and OT teams at advanced companies are nearly three times as likely (73% versus 26%) to share resources to achieve their

“Our IT team flagged some pieces of equipment in our manufacturing area that were running a potentially vulnerable operating system that required extra protections,” said one OT executive. “I didn’t like the machines either and already wanted to replace them, so this gave us the opportunity to collaborate and align with our corporate finance team from a couple of different directions. There was a substantial cost for replacing that equipment, so having IT on our side was helpful. We were able to remove a vulnerability, upgrade equipment, and gain more capacity, quality, and other features. This is one of those times when IT and OT can partner for a win-win, which is really helpful.”

objectives. Three in four companies (75%) with a high degree of IT/OT convergence prioritize shared goals and objectives that drive IT/OT collaboration versus only 44% of less converged companies.

Communication plays a critical role as well. Will Spears, Associate Director of Business Systems, Products, and Planning at **Sonoco**, talked about the importance for both IT and OT professionals to "put on the glasses of the opposite group. Understand exactly what their viewpoint is. I always say let's have the two-way communication so that you understand my point of view, and I understand your point of view. Let's have a debate, let's deliberate, and then let's decide. At the end of the day, we all have one objective – to be profitable for our company and to make quality products in a safe manner. And to do that, we need the diversity of thought." Our survey bore

Behaviors that Set Advanced Companies Apart



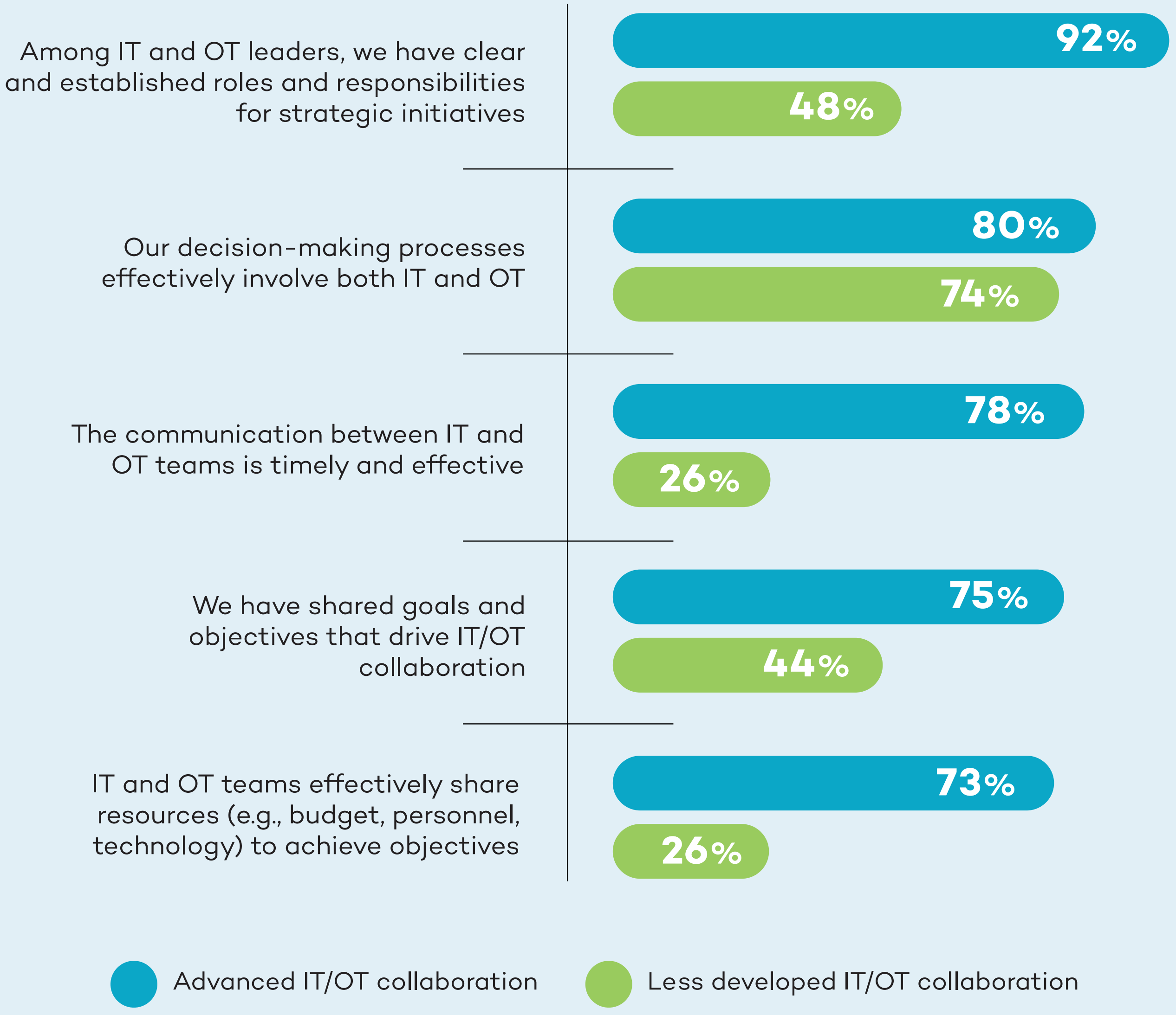
> "Collaboration and open communication between IT and OT are so important. One individual who leads our OT program used to work in IT. So I think that helps in terms of collaboration. Even though it's a separate reporting structure, he already has those pre-established relationships with IT and knows both domains."
>
> ***— Travis Ward, ConMet***

Source: 2025 IT/OT Collaboration survey, Manufacturers Alliance Foundation and CDW

out the importance of strong IT/OT communication as well, with advanced companies more than three times as likely (78% versus 26%) to report that communication between their IT and OT teams is timely and effective.

Taken as a whole, these practices highlight advanced companies' commitment to deeply embedded, accountable integration of resources, programs, and goals. It is clear that converged companies have mastered the fundamental elements of collaboration, creating a highly effective and aligned environment, whereas their less converged counterparts face an uphill climb for establishing basic clarity, communication, and resource synchronization.

Manufacturers' Evaluation of IT/OT Collaboration



Source: 2025 IT/OT Collaboration survey, Manufacturers Alliance Foundation and CDW

Insurance Requirements in an Age of Heightened Cybersecurity Risk

The changing threat landscape raises questions about how cybersecurity hygiene will impact insurability in the future. As of now, manufacturers base their cybersecurity programs on a range of other factors – such as the heightened level of threat and regulatory requirements – rather than insurance. But some companies expect underwriters to take a stronger interest in their cybersecurity programs in the future. As Colby Hamilton, President of **McInnes Rolled Rings** told us, "You can kind of feel that this is going to be part of your insurance grade in the future. I would guess that might happen in the next three to five years."

More than half of manufacturers (60%) say insurance companies demand or strongly recommend that companies have clear visibility into cyberattacks through monitoring and anomaly detection. Insurers also require or strongly recommend IT/OT network segmentation, according to 56% of manufacturers. Nearly two-thirds (65%) of manufacturers report requests from insurers to provide third-party assessments or audits specifically focused on the OT environment as part of their documentation requirements. This explains the significant share (28%) of manufacturers undertaking vulnerability assessments in 2025, versus only 17% in 2023.

Insurers are seeking evidence that manufacturers take proactive approaches to OT cybersecurity. Companies that can demonstrate a posture that is robust, resilient, validated by third parties, and in line with recognized standards will be better prepared if and when insurance requirements tighten in the future.

OT Cybersecurity Requirements & Recommendations from Insurers

60%	Monitoring and anomaly detection tools
59%	Network segmentation between IT and OT
54%	Employee training and awareness for OT staff
47%	Asset inventory and vulnerability management for OT devices
44%	Regular risk assessments and security audits
42%	Incident response plans tailored to OT environments
36%	Access controls and MFA for any remote or local OT access
34%	Patch management strategies—even in sensitive uptime environments
28%	Backup and recovery procedures for both IT and OT systems

Source: 2025 IT/OT Collaboration survey, Manufacturers Alliance Foundation and CDW

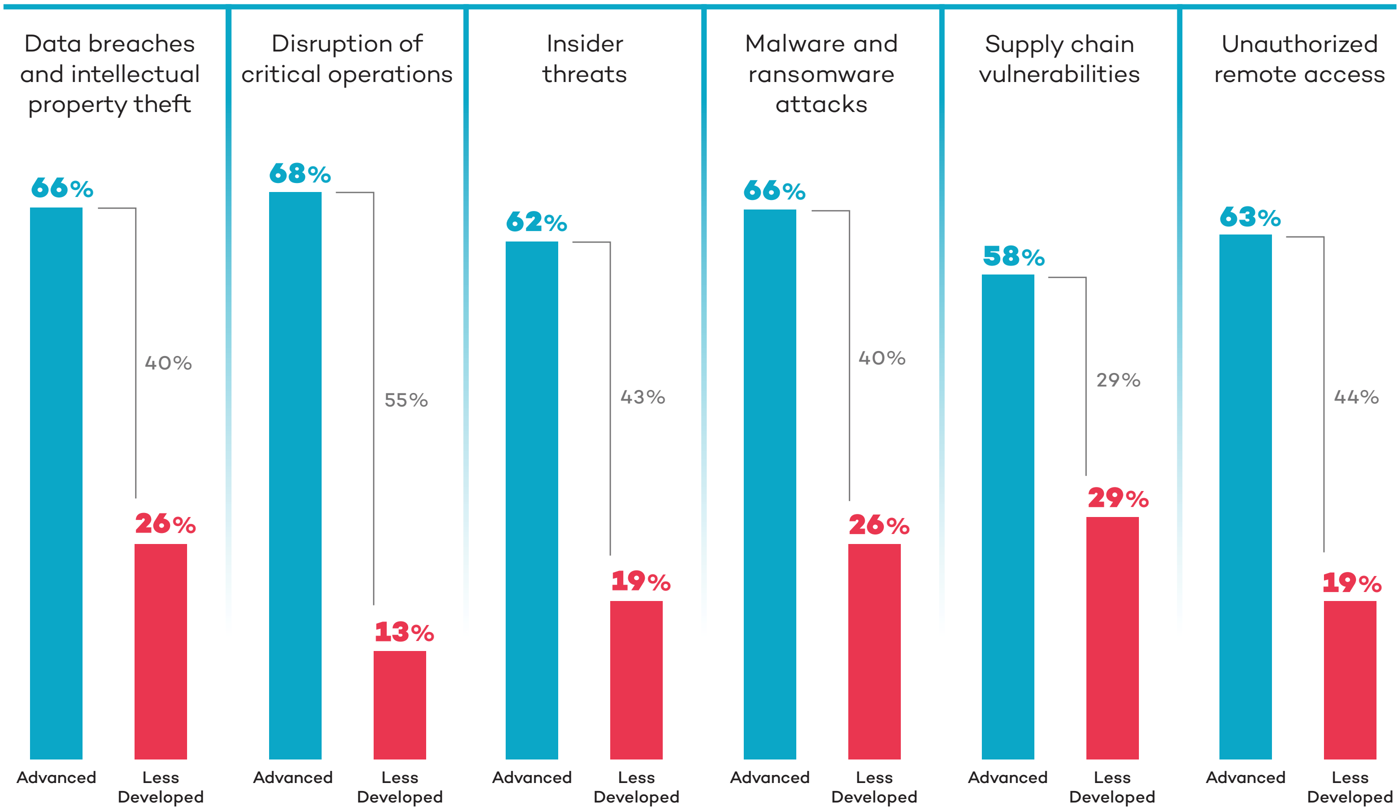
The Payoff of Being Ahead in IT/OT Convergence

The complexity of IT/OT integration is considerable, but the benefits are real. IT/OT convergence brings with it the ability for teams in different domains to have a well-coordinated approach to addressing cyber threats. This is directly tied to better transparency and more collaborative decision-making. By a margin of nearly two to one (97% versus 53%), advanced companies say they have the necessary visibility and decision-making power to effectively detect and respond to threats. As Jill Klein of CDW put it, "It's not about adding a tool or a certain system. It's about giving the team a single pane of glass, so to speak, so that they have a shared view of what they're working with. This, in turn, acts as an accelerator for incident response, service management, change management, and a lot of other things."

When asked about specific types of threats, the advantage enjoyed by advanced companies widens. They are five times more likely (68% versus 13%) to express confidence in their

Confidence in Ability to Respond & Recover

Readiness of IT and OT teams ranked as well-prepared for these threats



Source: 2025 IT/OT Collaboration survey, Manufacturers Alliance Foundation and CDW

ability to withstand attacks aimed at disrupting critical operations. Advanced companies have prioritized the mission-critical parts of their operations as part of their OT network design.

It starts with an awareness about technology dependencies across the IT and OT domains. Colby Hamilton of McInnes Rolled Rings summarized it well: "Our business has become so dependent on technology. If those servers go down and don't come back up, we can't roll rings, we can't run our new saw, we can't do what is necessary to generate revenue which ultimately pays the bills, compensates our associates, and allows us to continually reinvest in the business. Most importantly, if we can't do those things, we would disappoint our customers, which is one of the worst things to happen in a tight economy."

Advanced companies are more confident in their defenses against attacks aimed at compromising their data or stealing their intellectual property, with leaders more than twice as likely to respond and recover from such an attack. Similar trends are evident with regard to insider threats, malware, ransomware attacks, unauthorized remote access, and supply chain vulnerabilities.

Advanced companies have clearly invested in and achieved a level of preparedness that helps them face a diverse range of cybersecurity threats in the OT environment. But the payoff transcends cybersecurity readiness. Nearly all leaders (94%) say their IT/OT collaboration journey enables them to support their organization's future ambitions in advanced manufacturing. They have laid a solid technological foundation, and this puts them in a much stronger position to seize the opportunity as soon as new technologies emerge on the horizon.

When it comes to turning IT/OT convergence into a competitive advantage, advanced companies are also well ahead. When asked about the impact of IT/OT convergence on competitiveness, 69% of advanced companies believe their progress in bringing the IT and OT domains together makes them more competitive, versus only 46% of lagging companies..

This is particularly striking during a time of geopolitical uncertainty, when companies prize their ability to change course quickly with smart, data-driven decisions. When IT and OT speak the same language, the business runs with speed, confidence, and resilience.

Lessons Learned: Building an OT Network

Belden Inc. recently put its own industrial networking products to the test by piloting a converged OT network solution with full-fledged OEE (Overall Equipment Effectiveness) data collection, dashboards, alerts, and action notifications. Logan Cooper, Senior Director of Digitalization at Belden, told us about the success of the program. “It was probably about 18 months from the initial kick-off of the concept to implementation with full data flowing.” When asked to identify the biggest challenge, Cooper mentioned silos. “Initially there was a lot of pushback about who would own the network, who would be responsible for changes, and which products should be utilized, even though they were our own products.” The solution currently in place involves central management from Belden’s IT department with site-specific responsibility for local tasks such as adding new devices to the network. The initial phase of the program covered about 25% of Belden’s manufacturing plants, and the rollout for its remaining plants is currently underway.

As a result of the program, Belden has seen measurable increases in productivity. “These OT networks are delivering a dramatic improvement in manufacturing efficiency,” Cooper said. “There is also a huge cost savings associated with these implementations. In the past, much of our productivity data was handwritten and manually collected. In the past year, as a result of the new OT networking as well as other actions we’ve taken alongside that program, we’ve seen a 10 percentage point improvement in OEE, about half of which can be linked specifically to the OT network. From a cost perspective, the pilot program paid for itself within about ten months.”

There is also upside for workforce development and recruitment, Cooper said. “The program has really attracted people who want a role that’s a little different than the traditional IT career path. People want to be involved in these projects, and the company values employees with knowledge of OT networks.” When asked about critical success factors, Cooper stressed the importance of leadership buy-in. “We learned early in the program that it is paramount to have engagement from the IT networking team and IT leadership up front when kicking off a project like this.”

Tone from the Top

Companies that make a C-suite commitment to prioritize IT/OT convergence and security are in a stronger position to accelerate their digitalization journey. By a wide margin (59% versus 39%), advanced companies cite executive leadership attention to cybersecurity as a driving factor. Colby Hamilton told us, “Our former CEO was also a board member in the banking sector, and he was hell bent on making sure that everything in our operations was segmented before he retired. So we had his full support and an open checkbook to make sure we did what we needed to do to protect the business.”

At another manufacturing company, the push came from the board and executive leadership team. One executive told us, “They had a desire to bring in someone to run cybersecurity who had experience in a large enterprise program.” He also mentioned the importance of putting talent in place with an outside-in perspective. “This gives them the ability to pull things together to get the right controls in place with the right outcomes.”

C-suite commitment must be evident from the C-suite and across the C-suite. IT and OT leaders must be on the same page. Advanced companies are nearly unanimous and almost twice as likely as less advanced companies (92% versus 48%) to highlight the importance of a clear understanding between the heads of IT and OT regarding roles and responsibilities.

The synergy between IT and OT at Teledyne is one example of how the tone from the top of IT and OT can make a difference. “IT acts very quickly on our OT requests because we are critical to manufacturing and customer support. We are prioritized for getting IT support. They are both a service to us and a protector in some capacity,” Maria Royston, MAST Engineering Manager at **Teledyne** explained.

Executive leadership often plays a leading role in making key investment decisions for strategic initiatives and digital transformation programs. This is significant because the digital transformation process can be a catalyst for addressing the problem of legacy systems as part of the overall goal of upgrading the company’s operating model and processes.

92%

of companies with advanced IT/OT collaboration have clear and established responsibities for IT and OT leaders versus 48% of those with less developed collaboration

The C-suite also has a unique role to play in providing the vision for a company’s digital transformation and holding teams accountable, which includes making progress on IT/OT convergence. Since digital transformation has an impact on every role and department, it is up to the leadership team to make expectations clear. Our survey bore this out as well. Strategic digital transformation initiatives are cited as a success factor for IT/OT convergence by advanced companies by a margin of more than two to one (55% versus 21%).

Conclusion – Continuing the IT/OT Convergence Journey

The progress of companies that have bridged the IT/OT divide is clear and compelling. Their cybersecurity posture is robust across multiple metrics. As a whole, they are in a better position to address the number one challenge facing OT environments today – a landscape of increasingly sophisticated threats.

The rewards of IT/OT convergence transcend security and go to the heart of business competitiveness. Leaders are expanding their advantage with regard to both talent and technology. They can attract the right skillsets and deploy the latest innovations because of the work they have done to bring IT and OT together. The synergy between talent-technology comes into play here, with leaders putting themselves in a stronger position to make tech moves that would otherwise be out of reach without the right talent in place.

Members of the C-suite have a unique role to play in continuing this momentum. Modelling IT/OT collaboration can start with the heads of those departments themselves when they demonstrate that digitalization is a team sport. The levers of investment, accountability, culture, and vision can play a crucial role in advancing companies on their digitalization and IT/OT convergence journey. The leading majority have delivered a clear proof of concept for what can be done, key behaviors and capabilities, and the impact on competitiveness and growth going forward.

About this Research

Manufacturers Alliance surveyed 170 leaders in manufacturing to better understand how companies are bridging the gap between IT/OT and keeping their OT networks secure. We identified advanced companies as those that rated their IT and OT integration and collaboration for OT security as exceptional or very good in our survey. This group of companies with advanced integration and collaboration represents 71% of respondents. Below, we have highlighted some statistics about the respondents and their companies.

Annual Company Revenue

$$$$$	1%	Less than $1B
$$$$$	30%	$1B to $3B
$$$$$	18%	$3.01B to $5B
$$$$$	17%	$5.01B to $10B
$$$$$	24%	$10.01B to $25B
$$$$$	10%	Greater than $25B

Top Subsectors Represented

15%	Machinery manufacturing
12%	Computer and electronic product manufacturing
9%	Fabricated metal product manufacturing
8%	Food manufacturing

Job Role

48%	Information technology and systems
32%	Cybersecurity
20%	Engineering, manufacturing ops/production, R&D

Number of Manufacturing Locations

Fewer than 10	18%
10 to 25	29%
26 to 50	29%
51 to 75	15%
76 to 100	2%
Greater than 100	6%

Manufacturers Alliance Foundation is the 501(c)(3) partner of Manufacturers Alliance®. The Alliance Foundation provides educational opportunities for the manufacturing community and its stakeholders through insights, events, and tools for today's most critical business decisions. The Alliance Foundation focuses on talent, technology, digital transformation, and competitiveness.

For more information, visit **ManufacturersAlliance.org/foundation**.

CDW Corporation is a leading multi-brand provider of information technology solutions to businesses, such as manufacturing, retail, energy, government and healthcare customers in the United States, the United Kingdom and Canada. A Fortune 500 company and member of the S&P 500 Index, CDW helps its customers to navigate an increasingly complex IT market and maximize return on their technology investments.

For additional information, please visit **www.CDW.com/manufacturing**.