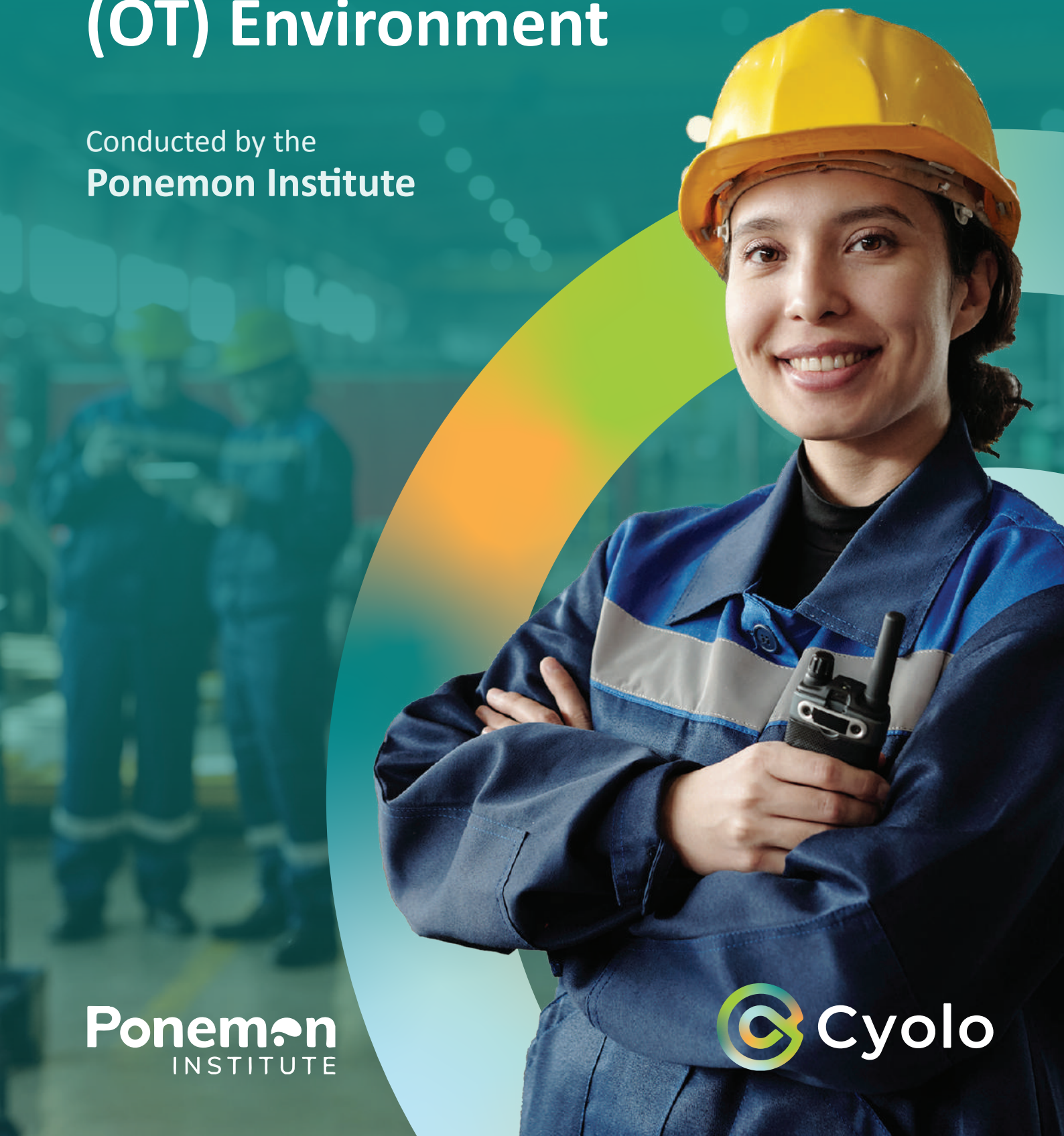
Managing Access & Risk in the Increasingly Connected Operational Technology (OT) Environment

Conducted by the
Ponemon Institute



Ponemon INSTITUTE

Cyolo

TABLE OF CONTENTS

INTRODUCTION

Ensuring secure access to operational technology (OT) environments is about more than just cybersecurity. These environments contain highly sensitive systems and critical infrastructure responsible for keeping the water running, the electricity flowing, and performing countless other tasks vital to the smooth functioning of our communities. An attacker who gains unauthorized access to a manufacturing production line or water treatment plant could cause far more damage than a data breach; the ability of the business to continue operating could be at risk, as could – in the worst case scenario – the physical safety of workers and the environment.

To help protect against such threats, OT environments were traditionally separated from other systems. This isolation, also known as air-gapping, kept OT largely shielded from the rising tide of cyberattacks targeting information technology (IT). But, **for better or worse, we no longer live in a world that supports isolation.** On the contrary, connectivity is now the expectation. To boost business agility, improve productivity, and support digital transformation, organizations are increasingly connecting their OT systems to IT networks and even to the internet.

At the same time, more users and devices than ever before are being granted access to OT environments and the critical infrastructure within them. Among those connecting to critical systems are third-party vendors and contractors, who carry out crucial work but can expose organizations to substantial risk if their access and connectivity privileges are not properly controlled.

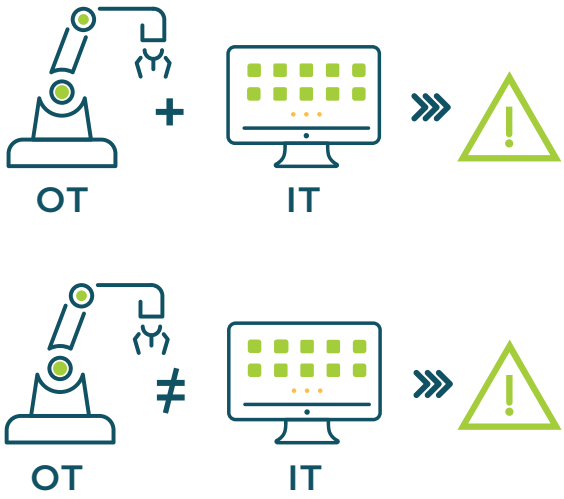
This research study, conducted by Ponemon Institute and sponsored by Cyolo, examines how organizations that operate critical infrastructure, industrial control systems (ICS), and other OT systems are managing access and risk in the face of unprecedented challenges. The data reveals that many organizations do not consider securing access to OT environments to be a top priority, while others lack the resources or collaborative processes to ensure secure access and effectively mitigate threats.

The report is based on a Ponemon Institute survey of 1,056 security professionals in the United States (607) and EMEA (449).[1] All respondents work in organizations that run an OT environment and are knowledgeable about their organization's approach to managing OT security and risk. More than one-third (37 percent) call themselves "significantly knowledgeable." Respondents come from a wide range of industries, including manufacturing, energy, oil and gas, transportation and logistics, life sciences, food and beverage, and others.

[1]Unless otherwise specified, all data refers to the consolidated results of the US and EMEA research.

Another phenomenon the research explores is the relationship between OT and IT, which is evolving in a way that presents both challenges and opportunities. Ideally, connections between IT and OT systems (also called IT/OT convergence or Industry 4.0) lead to improved business value and stronger security for organizations as a whole. For example, adding sensors and other data-collecting mechanisms to the previously isolated OT environment can provide the business side of the enterprise with highly valuable data it can then use to make more informed decisions that will impact productivity as well as revenue. In terms of security, data gathered by connecting real-time sensors to OT systems can help detect anomalies, make optimizations, reduce risk, and strengthen the security and safety of the OT environment.

Interestingly, however, **security is seen not only as a goal of IT/OT convergence but also as an obstacle.** Reducing security risk is the top objective of companies undergoing convergence (59 percent), and yet one-third (33 percent) of organizations *not* pursuing convergence cite security risk as a top factor for their decision.



While this may initially feel like a paradox, it actually demonstrates perfectly the need to prioritize OT security before and during any convergence initiative in order to achieve a successful, secure outcome.

Ultimately, just because organizations *can* connect their IT and OT systems does not mean they are ready to do so in a way that will not create additional security risk or other potential complications. **Before taking on an IT/OT convergence project, organizations should work to solve the many existing challenges around security tooling, access management for third-party vendors, and communications and alignment between IT and OT teams.** Tackling these issues first will help ensure that convergence leads to stronger security rather than the opposite.

Key Definitions

Operational technology (OT) is the hardware and software that monitors and controls devices, processes, and infrastructure within industrial settings. OT systems and devices control the physical world, while IT systems manage digital data and applications.

Industrial control system (ICS) is a collective term used to describe different types of control systems and associated instrumentation used to operate and/or automate industrial processes.

IT/OT convergence refers to the connectivity between IT systems to OT systems, allowing them to transmit data in one or both directions. The goal of IT/OT convergence is to use this connectivity to enhance the value these systems deliver.

Third-party users/vendors is a category that includes all types of external suppliers, partners, service providers, and contractors who perform important work for the organization but are not direct employees. Because it is difficult to monitor or control the access and activities of these users, they pose a higher-than-average risk to the organization's security. In this report, the terms third parties, third-party users, external users, and vendors are used interchangeably.

KEY FINDINGS

1

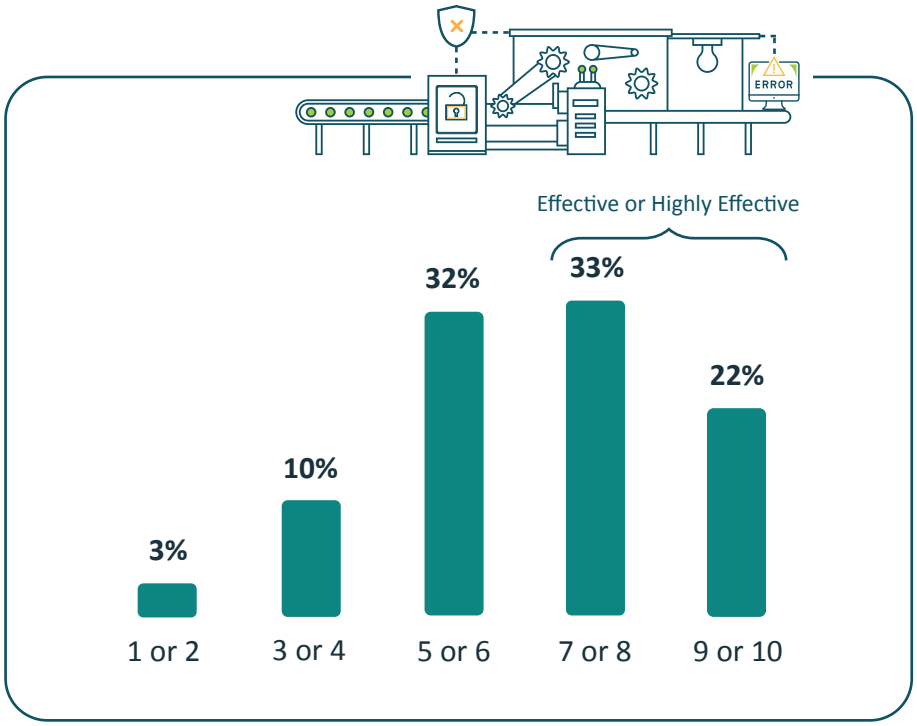
Only 55 percent believe their organization is effectively or very effectively mitigating risks and security threats to the OT environment.

When asked to rate their organization's effectiveness in reducing risks and security threats on a scale from 1 = not effective to 10 = highly effective, just 55 percent of respondents say their organization is effective or highly effective in achieving these objectives. **Thirteen percent admit to being ineffective when it comes to mitigating risks and threats**, and the remainder are what we might call "moderately effective."

Figure 1

How effective is your organization in mitigating risks and security threats to its OT environment?

Please use the scale from 1 = not effective to 10 = highly effective.



There are scenarios in which being "moderately effective" is sufficient, but OT cybersecurity is not one of them. **For the sake of both security and safety, organizations that lack confidence in their current threat mitigation strategies must adopt new approaches and possibly also new security and access management solutions.** This is the case whether or not organizations are working toward (or plan to work toward) any level of IT/OT convergence; however, improving OT security is even more urgent for those that are opening themselves to new potential risks through connections to IT networks and the internet.

First steps organizations can take to more successfully mitigate risks to OT environments include authorizing access according to identity-based parameters, requiring multi-factor authentication (MFA) for all connections, and granting access to the application-level only.

2

Visibility into industrial assets is dismal, putting organizations at significant risk.

Organizations cannot protect assets they do not know they have, and the research reveals a large majority of organizations in fact do not know exactly what can be found in their OT environment.

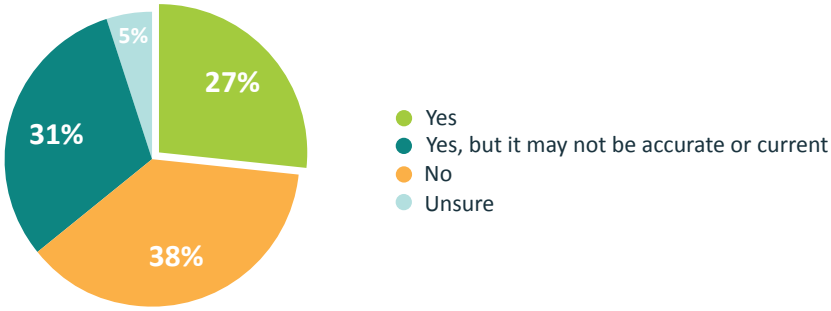
As shown in Figure 2, **only 27 percent of respondents say their organization maintains an accurate inventory of OT assets.** Sixty-nine percent have either no inventory or an inaccurate, outdated inventory, and the remaining 5 percent are unsure about the state of their asset inventory.

73%

of organizations lack an authoritative OT asset inventory.

Figure 2

Does your organization maintain an inventory of the industrial assets in its OT environment?



Without a clear picture of the number and types of industrial assets they hold, organizations will struggle to mount a comprehensive cyber defense. All who find themselves in this position should make the time to inventory their assets and then put processes in place to guarantee this inventory is maintained and regularly updated.

But **even in the absence of a complete inventory, organizations can and should begin enforcing policies to ensure secure access to the OT environment.** Creating an inventory will take time (especially because some asset owners will likely have left the organization), and during this time critical systems and resources will remain vulnerable. Implementing controls to manage OT environment access is therefore an even greater imperative than building an accurate inventory of assets.

3

Nearly half (49 percent) of organizations have not reassessed the security and effectiveness of remote access tools adopted during the COVID-19 pandemic.

In the early days of the COVID-19 pandemic in 2020, virtually every business on the planet was abruptly forced to find new ways of working. This change was particularly acute for organizations running OT/ICS. Until the pandemic, work on these systems typically took place exclusively in person, even when this meant that inspectors, technicians, and other operators needed to travel from factory to factory or from plant to plant. The thought of connecting remotely to critical infrastructure was, in many cases, simply unfathomable.

And then COVID-19 produced a new reality in which organizations that wanted to continue operating had to adapt by shifting to remote work. To make this possible, they needed new products and tools, and, because of the near chaos of the moment, these were often hastily selected and deployed.

As seen in Figure 3, **51 percent of respondents report that their organization invested in new tools to enable secure remote access during the pandemic.** This is not surprising, as organizations that did not previously allow remote work would have required new solutions to support it.

But what happened as the pandemic waned? Did organizations take the opportunity to reevaluate the tools they had adopted during the whirlwind of early 2020? According to the data, **49 percent have not reassessed the security and effectiveness of these solutions since their initial deployment.** In EMEA, this number crosses into a majority at 53 percent.

Figure 3

Even without a global health crisis that upends established work routines, security solutions need to be reevaluated frequently. Are they serving the designated purpose? Do they integrate easily with other security tools? How is the user experience? How much overhead is needed to support their use?

At the very least, an annual assessment should ask these questions of all solutions in the organization's security stack. Those that have not conducted an assessment since the pandemic should do so at the earliest opportunity, as **tools adopted hastily in 2020 may not adequately ensure secure remote access and, in some instances, could be actively hindering this goal.**

4

Organizations allow dozens of third-party users to access OT environments without fully understanding the risks.

Third-party vendors and contractors are crucial to the smooth operations of OT systems. Equipment manufacturers frequently require that their own technicians hold exclusive rights to perform maintenance on their products. In other cases, only external experts have the specialized technical skills to solve a specific challenge. And sometimes it is simply more cost-effective to hire a contractor rather than a full-time employee.

Whatever the reason for bringing them on board, the data shows that is becoming the norm for organizations to give more access, often including remote access, to more vendors. **Today, 73 percent allow vendors and other third parties to access the OT environment.** Thirty percent give third parties on-site access only, while 43 percent permit both on-site and remote access. As mentioned above, COVID-19 marked a sea change in organizations' willingness to enable remote connections to OT/ICS.

But just how many people are we talking about here? **Sixty percent of organizations have authorized OT systems access for more than 50 different vendors**, and 25 percent give such access to more than 100 vendors.

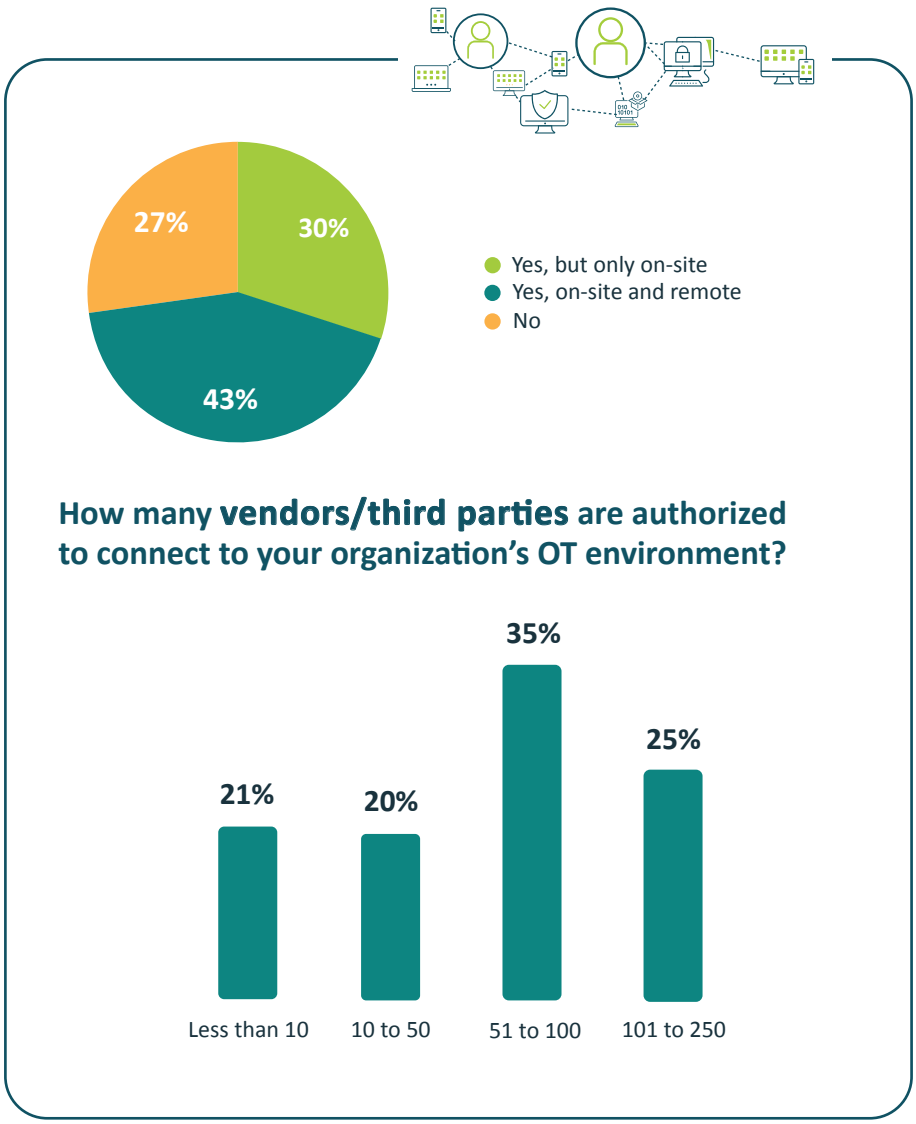
On average, organizations authorize

77

third parties to access the OT environment.

Figure 4

Does your organization permit **vendors/third parties** to access its OT environment?



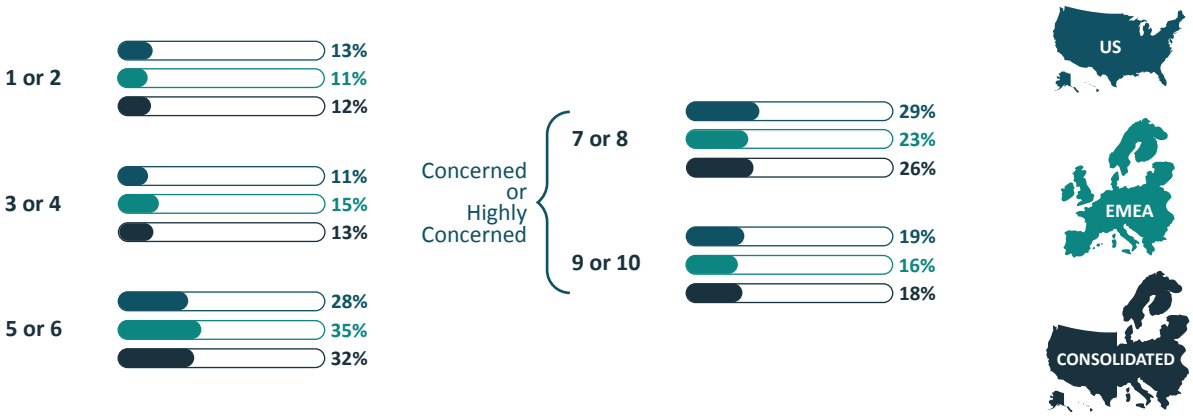
How many **vendors/third parties** are authorized to connect to your organization's OT environment?

Despite the large number of vendors accessing OT assets and environments, **only 44 percent of organizations are concerned or highly concerned about the risks of third-party access.** Respondents from EMEA are even less likely to be very concerned about third-party access risks (39 percent), although their organizations more commonly prevent third parties from accessing the OT environment at all (30 percent EMEA vs. 24 percent US).

Figure 5

How concerned is your organization about risks created by vendors/third parties accessing its OT environment?

Please use the scale from 1 = No concern to 10 = Highly concerned



Whether or not organizations recognize it, opening their OT environments to third-party vendors without implementing the proper access controls is inherently risky. There are a number of reasons for this, including third parties' lack of familiarity with internal security policies and best practices, the fact that they typically work on unmanaged devices, and the difficulty of monitoring or controlling their activity after access has been granted.

It should also be noted that many organizations use virtual private network (VPNs) to enable OT access for third-party users.[2] VPNs typically provide broad network access, meaning that connecting vendors via VPN is roughly equivalent to plugging vendor devices (or potentially even the entire vendor network) directly into the OT environment. This sort of full and unmonitored network access can not only leave organizations vulnerable to supply chain attacks but can also enable the rapid spread of malware or ransomware from a single compromised device.

To prevent unauthorized access, data exfiltration, and supply chain attacks, organizations must improve their awareness of third-party access risks and adopt strategies and solutions to mitigate these risks.

Recommended actions include augmenting or replacing VPNs with solutions that provide zero-trust access, enforcing MFA (including to the legacy systems typical to OT environments), setting access permissions for all third-party vendors according to the principle of least privilege, and adopting controls like session recording and supervised access to monitor what third-party users are doing while connected to critical systems.

[2] Forty-eight percent of survey respondents report using VPNs to provide access to OT environments, though the question did not specify whether this access is for employees, third-party vendors, or both.

5

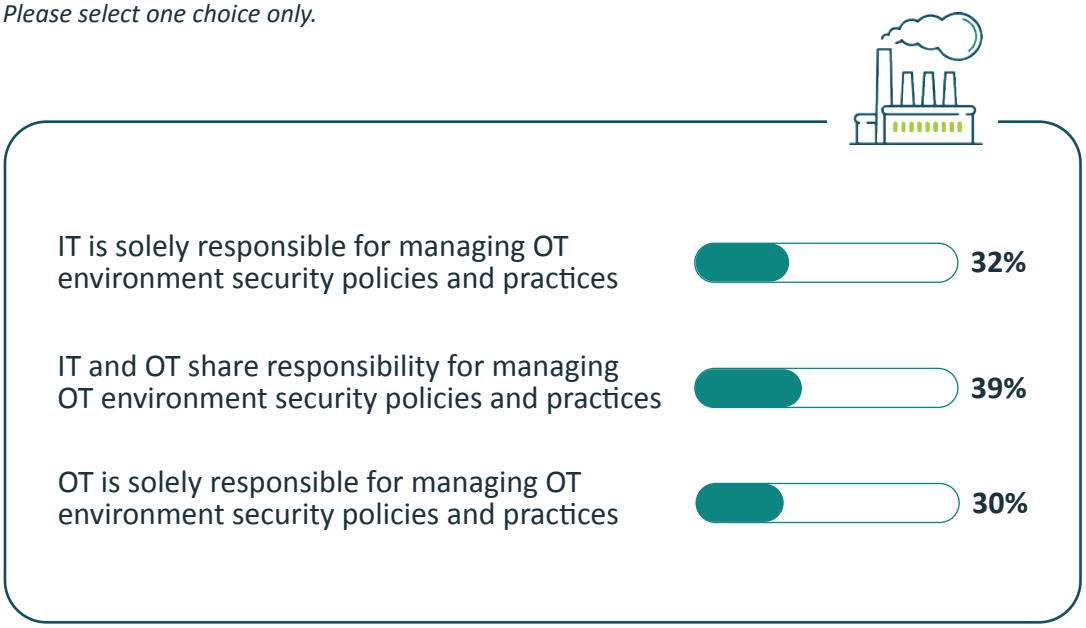
IT and OT teams share security responsibilities but do not communicate enough to achieve optimal outcomes.

More than two-thirds of respondents (71 percent) report that IT is either solely responsible for managing security policies and practices in the OT environment (32 percent) or that IT and OT teams share this responsibility (39 percent). In EMEA, it is more common for IT to have full responsibility (38 percent), while in the US the shared responsibility model is more prevalent (43 percent).

Figure 6

How does your organization allocate OT cybersecurity responsibilities?

Please select one choice only.



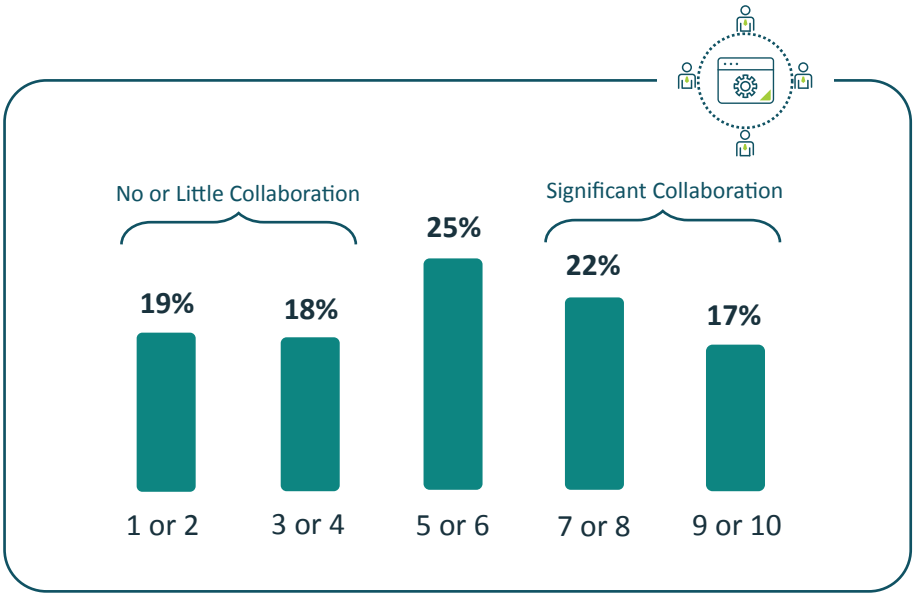
Even with these minor differences between regions, it is clear that collaboration between IT and OT teams is needed to achieve the best security outcomes. This is the case not just when IT and OT are jointly responsible for managing the security of OT environments but also when IT is managing OT security on its own. After all, OT team members have been working with the OT environment for years, whereas the IT team may be relatively new to understanding the distinct priorities and requirements of OT systems. This presents a perfect opportunity for OT to share valuable guidance and best practices with their IT counterparts, ultimately ensuring stronger security for the OT environment – a goal that is, of course, in everyone's interest.

And yet, when asked to rate the level of collaboration between IT and OT in their organizations on a scale from 1 = no collaboration to 10 = significant collaboration, **just 39 percent report strong or significant collaboration.** A similar number (37 percent) report precisely the opposite – little or no collaboration.

Figure 7

How would you rate the level of collaboration between the IT and OT teams in your organization?

Please use the scale from 1 = No collaboration to 10 = Significant collaboration.



We will explore the IT/OT relationship in more depth later in this report, but for now it suffices to say that the lack of collaboration is troubling. **When teams share a responsibility as important as OT systems access and security and yet do not act collaboratively, the outcomes could be disastrous.**

6

Seventy-two percent of organizations are pursuing IT/OT convergence, but most have limited tools in place to manage security or access between systems.

When asked about the level of connectivity between IT and OT systems in their organization, 28 percent stated there is no connectivity and no plan to enable connectivity in the future. However, the large majority (72 percent) are pursuing greater IT/OT convergence and find themselves at varying phases of progress.

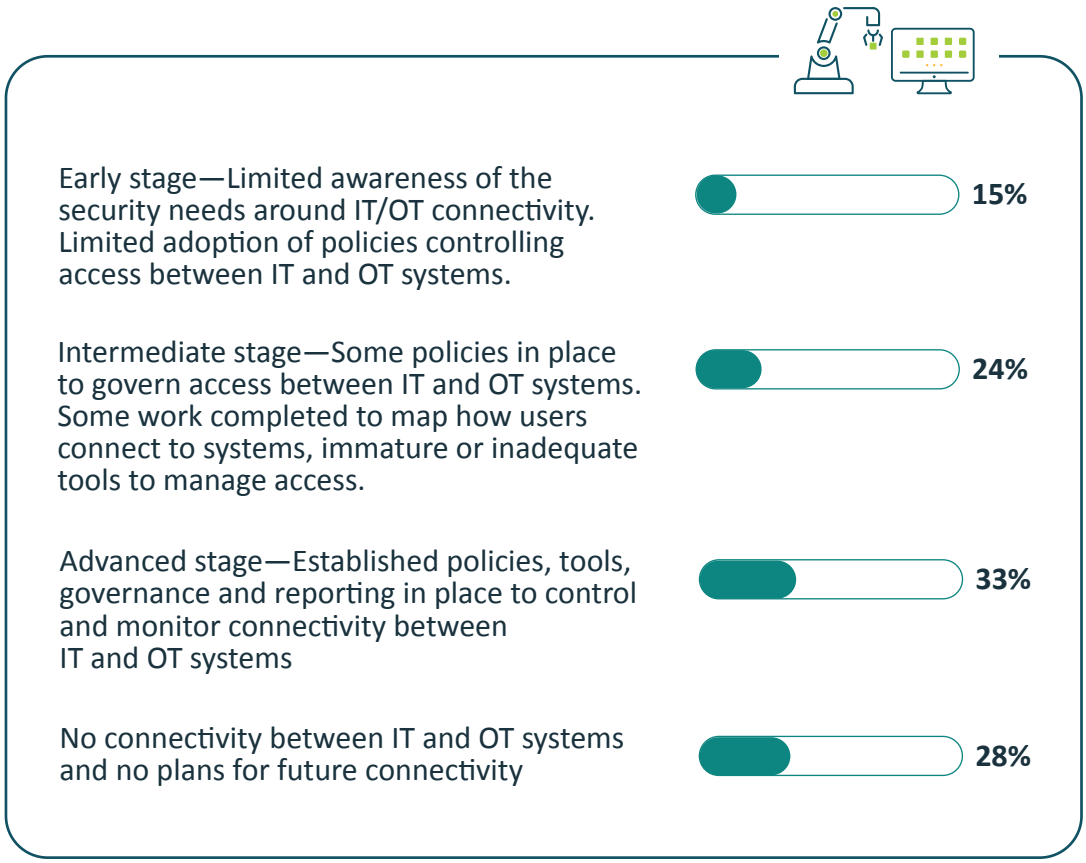
Fifteen percent are in the early stages of establishing IT/OT connectivity and have limited awareness of security needs as well as limited adoption of policies controlling access between IT and OT systems. Twenty-four percent report being at an intermediate stage, with some policies implemented to govern access between IT and OT systems, some mapping of how users connect to systems completed, and immature or insufficient tools to manage access. Combining these two groups, **thirty-nine percent of organizations are actively beginning to connect/converge their IT and OT infrastructure but have adopted few tools to manage access and security between the two sets of systems.**

The final third (33 percent) report that their organizations have reached an advanced stage of convergence and have established tools, policies, governance, and reporting processes in place to control and monitor connectivity between IT and OT systems.

Figure 8

What best describes your organization's level of secure connectivity between IT and OT systems in your organization?

Please select one choice only.



There is nothing wrong with being in the early or intermediate stage of an IT/OT convergence project; after all, there is no other way to progress to the advanced stage. The concern is that **organizations seem to be connecting their systems without first enacting the policies and access controls needed to enable safety and security.**

To help ensure that IT/OT convergence results in improved security, as a majority of respondents (59 percent) cite as a primary goal, organizations must establish a foundation of secure access before beginning to open their OT environments. This is true even if it means the convergence initiative will take a bit longer to complete. Then, organizations can start by connecting the systems that will deliver the biggest security benefit first.

Converging IT/OT infrastructure is not like flipping a light switch; it is a gradual process in which various systems are connected to one another, allowing data transmission in one or both directions. **By beginning with connections that will enhance security, meaningful results can be achieved relatively quickly, while security risk is minimized.**

Additional Insights and Recommendations

OT Security in the Age of Connectivity

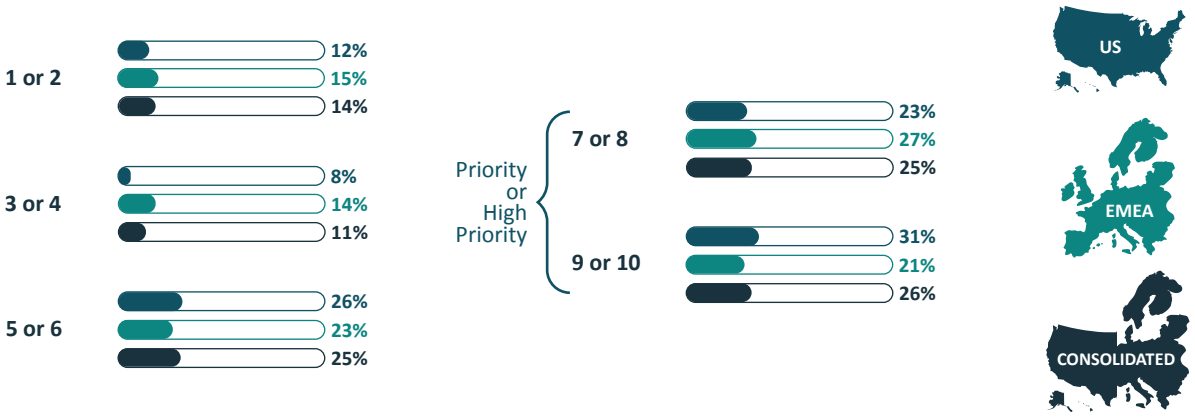
Perhaps due to the long history of isolating OT, many organizations today do not appear to recognize the crucial and urgent need to secure these systems against unauthorized access and its potentially disastrous consequences.

When asked to rate the priority of securing access to OT/ICS environments on a scale from 1 = not priority to 10 = high priority, **only slightly more than half (51 percent) report that ensuring secure access is a priority or high priority.** Twenty percent of US respondents and twenty-nine percent of EMEA respondents state that securing access to OT environments is a low priority at their organization.

Figure 8

How much of a priority is securing access to your organization's OT/ICS environments?

Please select one choice only.



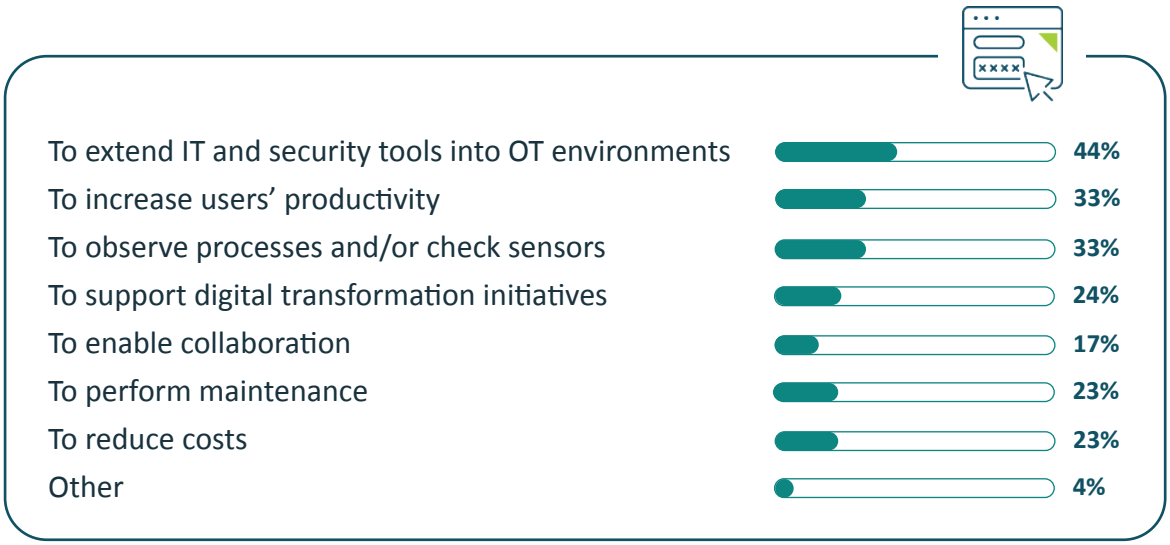
While security teams undoubtedly have many important tasks to fulfill (often with limited resources), it is nonetheless surprising that securing OT systems is not being treated as a top priority at more organizations — let alone that any organizations at all see it as a low priority. This is true not only because of the ramifications of failing to ensure secure access but also because a large and growing list of compliance regulations include specific provisions for securing OT environments. And respondents are aware of standards like NIST 800-82, NERC CIP, KRITIS, and others, with 59 percent reporting that their organization is currently required to comply with industry regulations. An additional 25 percent expects that future regulations will require compliance.

What is very clear is that neither compliance mandates nor concerns about data breaches and safety risks are keeping organizations from opening their OT environments to more users, tools, and connections than in the past. **Sixty percent allow OT team members as well as other employees to access the OT environment.** The reasons for enabling this access are multifold, with the most common being to extend IT and security tools into the OT environment (44 percent), to increase productivity (33 percent), and to observe processes and/or check sensors (33 percent).

Figure 10

Why does your organization enable access to its OT environment?

Please select all that apply.



In addition, **50 percent allow access to the OT environment in order to extract data and business intelligence,** including operator and maintenance data, environmental data, sensor data, run-time information, and more.

Also noteworthy is that while employees are being granted OT environment access for a variety of purposes, **fewer than half of respondents (49 percent) rate the user experience of their current access tools as very good or excellent.** User experience may not initially seem like a crucial component of a security product, but ease of use is in fact key to determining whether a product is actually utilized. If a tool creates friction or is overly complicated to work with, it will at best slow productivity and, at worst, users will find workarounds to avoid it, preventing the intended security benefits from being realized.

So, more people today are accessing the OT environment but few of them are fully satisfied with the experience of doing so. Meanwhile, as mentioned previously, just 55 percent believe their organization is effectively or very effectively mitigating OT security risks and threats. All of these data points reiterate that many organizations do not seem to have found the right strategies or solutions to ensure secure OT access. In light of this, how are they choosing what types of new security products to implement?

As shown in Figure 11, when asked how their organization plans to introduce new tools to better secure the OT environment, **63 percent plan to use either a blend of IT and OT security solutions (32 percent) or to use only OT-specific solutions (31 percent).** This is encouraging. However, 19 percent report they expect only to expand existing IT security solutions, and another 19 percent do not have any plans to introduce new security tools at all.

Figure 11

How does your organization plan to introduce new tools to better secure your OT infrastructure?

Please select all that apply.

IT security solutions may do an excellent job of providing secure access to servers, data centers, and cloud-based applications, but this does not mean they can simply be deployed in the OT environment and expected to show the same results. OT and IT systems have fundamentally different architectures and are built to serve distinct functions and priorities. Because of this, many tools in the IT security toolkit do not work, or work significantly less well, in the OT context.

The nearly one-fifth (19 percent) of organizations planning to reduce OT security risk by implementing tools designed for IT would therefore be wise to reconsider their approach. **The best way to secure OT environment access is to use solutions that are purpose-built for OT or, at the very least, to adopt a blend of IT and OT security solutions.** In addition, in the 71 percent of organizations where IT plays a role in securing OT systems, all decisions regarding security tools should be made mutually to ensure that the needs of both teams – and the OT environment itself – are satisfied.

The Challenges of Securing Third-Party Access

The role that third-party vendors, service providers, and subject matter experts play in operating and maintaining OT systems cannot be overstated. Their expertise and distinctive skill sets augment in-house teams in vital ways, and their importance to the business will not be declining any time soon. Still, as noted above, external users create an inherent risk for organizations when they are given unfettered access to sensitive data and critical systems. Because functioning without their support is not an option, the only choice organizations have is to limit the risks posed by third-party access.

We have already seen that organizations allow an average of 77 third-party users to access their OT environment and that just 44 percent are very concerned about the risks of this access. The level of concern may not match the gravity of the potential risk, but organizations are clearly aware of the challenges to securing third-party access.

The research identifies top challenges as preventing unauthorized access (44 percent), aligning IT and OT security priorities (43 percent), keeping vendor/third-party access secure (40 percent), giving users too much privileged access (35 percent), and adding strong authentication to legacy systems (35 percent).

Figure 12

What are the top challenges to securing vendor/third party access to your organization's OT systems?

Please select the top three choices only.

The results vary somewhat between the US and EMEA, with US respondents most concerned about preventing unauthorized access (49 percent) and EMEA respondents more worried about keeping vendor/third-party access secure (45 percent). Controlling activity permissions (30 percent) is another common challenge across both regions.

These obstacles are significant, but none of them is insurmountable. What, then, are the barriers preventing organizations from securing third-party access to OT systems? As seen in figure 13, respondents cite budget-related issues (80 percent), lack of expertise (46 percent), lack of available solutions (38 percent), and several additional factors.

Figure 13

What are the biggest barriers to securing vendor/third party access to your organization's OT systems?

Please select the top two choices only.

The responses to this pair of questions once again make it plain that many organizations are not making sufficient use of advanced secure remote access solutions, leaving them with considerable gaps when it comes to verifying that third-party users 1) are who they claim to be, and 2) are doing (only) what they are meant to do. The more than one-third of respondents who cite a "lack of available solutions" as a barrier to securing third-party access may not even be aware of such tools.

The good news then is that currently available solutions do exist to help organizations overcome each of the secure access challenges identified in the research. Everything from preventing unauthorized access through the enforcement of least privilege access policies to retrofitting legacy systems with strong authentication capabilities can be accomplished today.

To protect the security, safety, and availability of the OT environment while also enabling the vital work of third-party vendors, organizations must invest in robust secure access solutions that will allow them to resolve their present third-party access challenges. Involving IT as well as OT teams in the decision-making process will help ensure that the concerns of both are addressed, preventing misalignment of security priorities (currently seen by 43 percent as a problem). Collaboration between IT and OT can also help solve the issue of lack of expertise, as combined teams will have a much wider range of knowledge and skills.

If budget is an obstacle, as the data suggests it is likely to be, organizations can seek out products that combine multiple security functions in a single tool. This type of consolidation can cut costs and also reduce overhead. But it may still be necessary to request additional budget from senior leadership. Such conversations should emphasize both the business necessity and the business risk that third-party vendors pose. Their work is crucial, but failing to secure their access could lead to catastrophic consequences. Given the high stakes of OT security, implementing solutions that limit third-party risk should be a top priority for all stakeholders in the organization.

Beware the Communications Gap

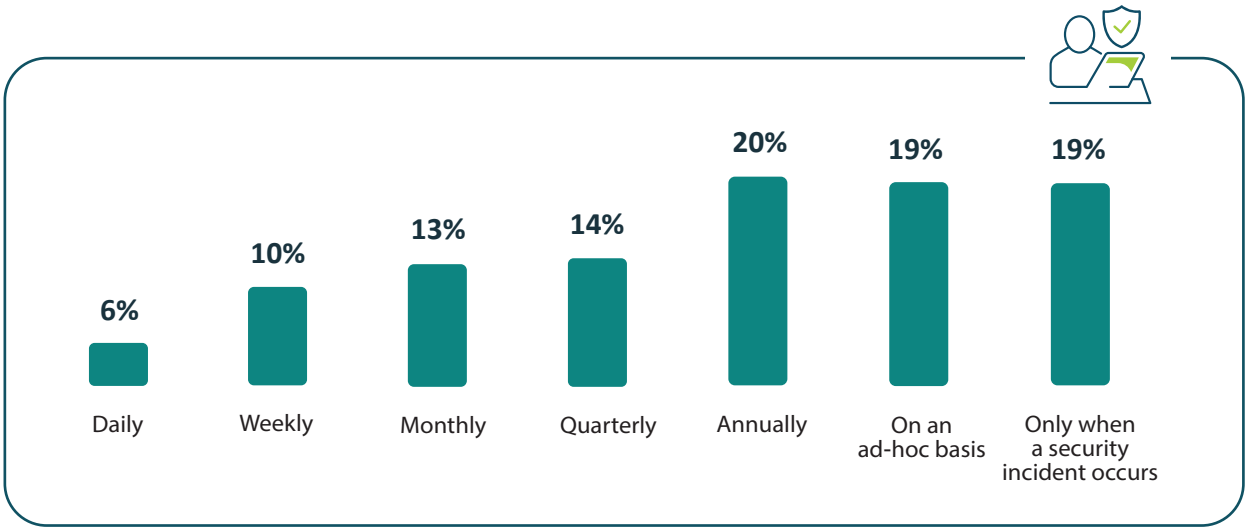
As has been mentioned several times, collaboration between IT and OT has numerous benefits. This is the case when teams share responsibility for OT security, when they are pursuing IT/OT convergence, and also when they are simply working alongside one another to help their organization realize its goals. **Even if IT and OT teams have different short-term priorities (security for IT versus availability and safety for OT), they ultimately have the same long-term priority of enabling the business to succeed.**

But without regular communication between IT and OT teams, any shared objectives will be difficult to achieve. We pointed out above that 37 percent of survey respondents report little or no collaboration between IT and OT. It is therefore not a huge surprise that **the data shows teams rarely communicate with one another about OT security issues.** As illustrated in Figure 14, 38 percent of respondents say IT and OT only communicate on an ad-hoc basis (19 percent) or when a security incident occurs (19 percent). Another 20 percent communicate once per year, and just 16 percent of respondents say that communication occurs daily (6 percent) or weekly (10 percent).

Figure 14

How often do your IT and OT teams communicate about OT security issues?

Please select one choice only.



Recalling that IT and OT teams share responsibility for OT environment security in more than a third of organizations (39 percent), the fact that they rarely speak about security issues is a substantial cause for concern. How many security incidents could be limited or prevented entirely through clear, open communication? This is of course not a question on which we can gather data, but the answer is presumably at least one and perhaps a far larger number.

To look at the situation from a slightly different lens, there is an enormous amount of experience and knowledge that is not being shared only because two siloed teams are not talking on a regular basis. **When IT and OT view each other as adversaries, or simply ignore one another, they are missing out on the chance to combine resources and tangibly improve security outcomes.** But by setting aside stereotypes and supposed cultural differences in favor of the shared goal of protecting the OT environment against potentially ruinous threats, they can together mount a significantly stronger defense.

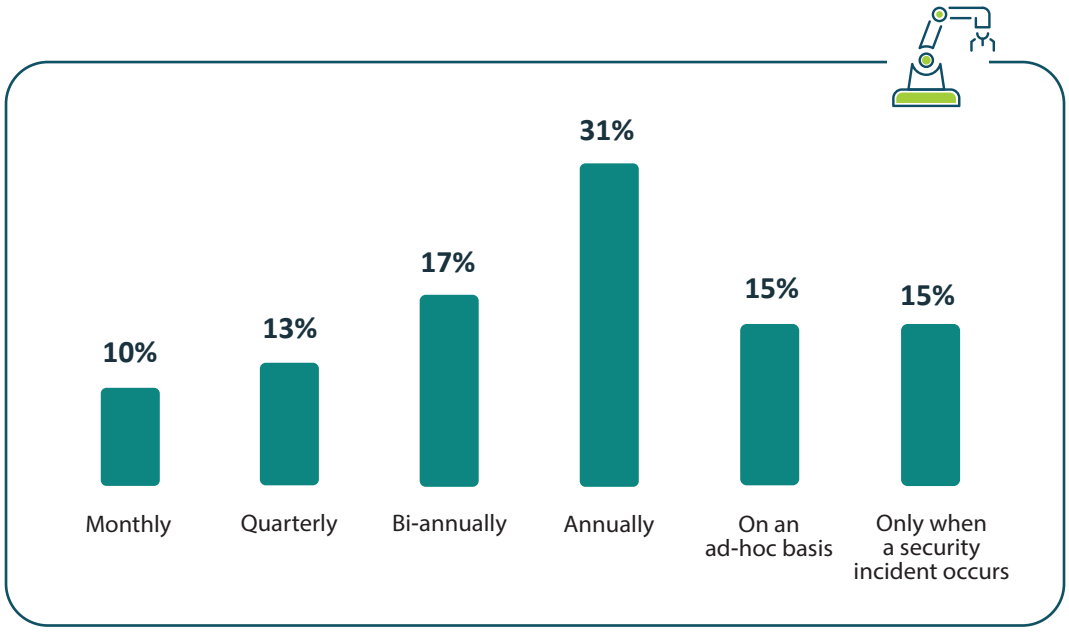
And while working collaboratively may be challenging at first, there is plenty of precedent for two disparate teams learning to cooperate. From the earliest days of network connectivity, IT and security have had little choice but to work together to implement policies and select tools that would satisfy the needs of both. IT and OT teams can make appreciable progress by following this example – and by remaining focused on their joint objective of enabling the business by ensuring the safety and security of the OT environment.

Communication between IT and OT is currently lacking, but is communication with senior leadership any more frequent or regular? As shown in Figure 15, 30 percent of respondents report that senior leadership and/or board members are updated on the organization's OT security posture, policies, and practices on an ad-hoc basis (15 percent) or when a security incident takes place (15 percent). Only 23 percent communicate at a relatively frequent, standard candence (10 percent say monthly and 13 percent say quarterly).

Figure 15

How often are senior leadership and/or board members updated on the organization's OT security posture and the policies and practices in place to maintain or improve it?

Please select one choice only.



When teams do not brief leadership on a regular basis about the status of security threats and the state of security across the organization, it will be much more difficult to get these stakeholders' support when the time comes to request budget increases, new tools, or more headcount. Regarding budget specifically, we saw previously that as many as 80 percent of survey respondents report lack of budget or other budget priorities as impediments to solving third-party access challenges. A good starting point for solving this issue would be to communicate more regularly with senior leadership and the board about the business risks posed by third-party access, helping them to understand why it is necessary to deploy or expand secure access solutions.

More broadly speaking, **by establishing a standard cadence to discuss OT security policies, problems, and priorities with top leadership, teams can build credibility and demonstrate how their efforts to keep OT systems operational are in fact a business-critical (and business-enabling) function**. By contrast, communicating solely when a security incident occurs or to ask for more resources may undermine efforts to showcase the team's valuable contributions to the organization and its wider goals.

The Trend Toward IT/OT Convergence is Real

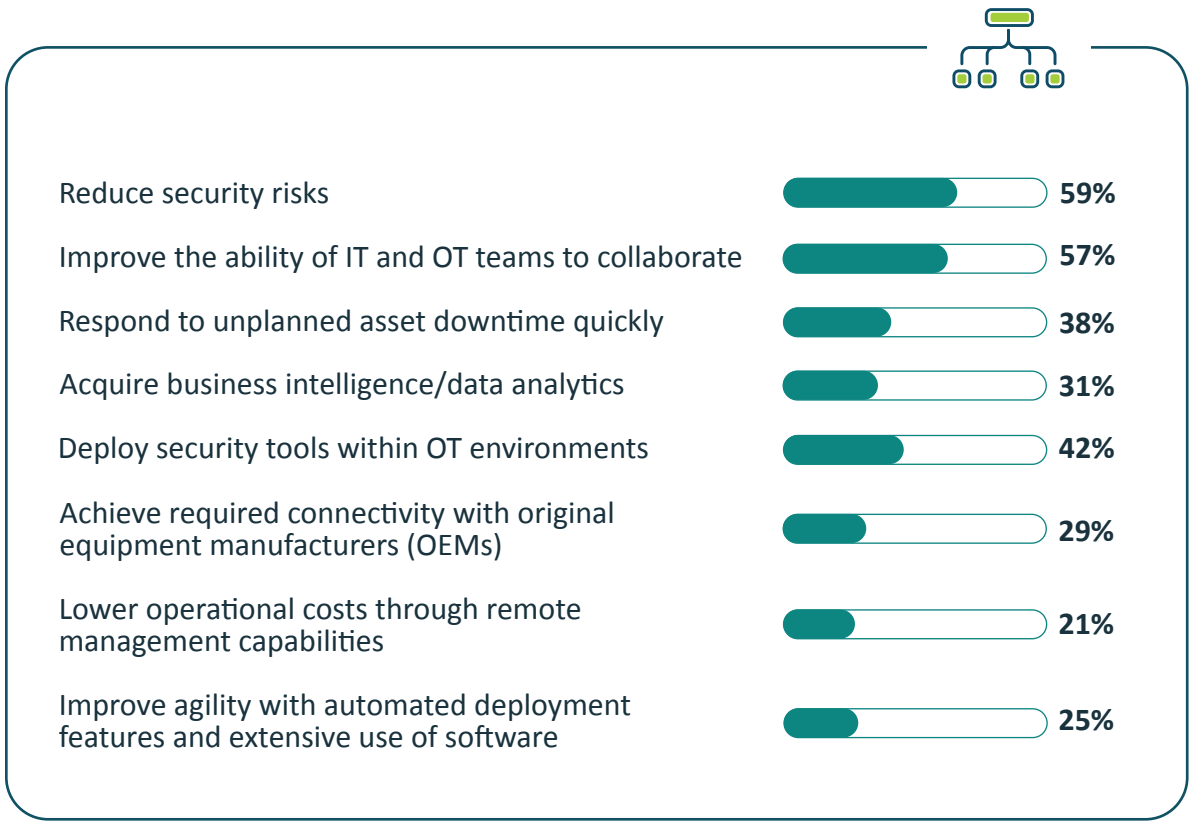
IT/OT convergence remains a controversial topic in at least some sections of the OT security community. As with any trend that comes along and contradicts what was previously considered a best practice (in this case, total or near total isolation of OT environments), there are those who remain hesitant to make a change. But even if some organizations are withstanding the pressure to open a connection between their IT and OT systems, the data shows that the pendulum is indeed swinging toward convergence.

Close to three-quarters of those surveyed (72 percent) state their organization is either pursuing or has reached a mature state of IT/OT convergence. When asked about the primary reasons for increasing IT/OT connectivity in their organization, the most common responses are to reduce security risks (59 percent), to improve collaboration between IT and OT teams (57 percent), to deploy security tools within the OT environment (42 percent), and to rapidly respond to unplanned downtime (38 percent).

Figure 16

What are the top three reasons for increased IT/OT connectivity?

Please select the top three reasons.

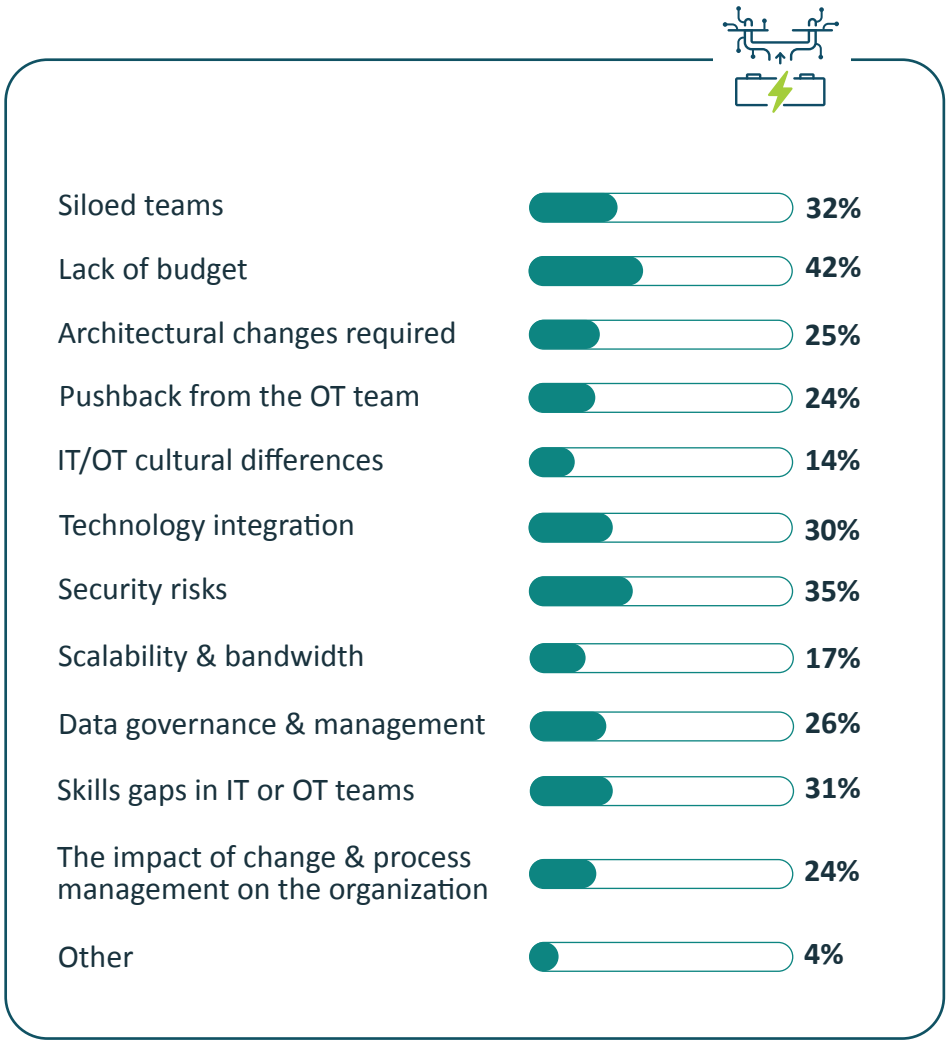


But despite the strong push toward convergence, substantial challenges remain when it comes to connecting IT and OT systems. Seven top challenges are faced by at least a quarter of organizations. These include lack of budget (42 percent), security risks (35 percent), siloed teams (32 percent), skills gap (31 percent), and technology integration (30 percent).

Figure 17

What are the most significant challenges to connecting IT/OT environments?

Please select the top three challenges.



Notably, security is seen as both a driver of IT/OT convergence and a challenge to convergence. Fifty-nine percent are pursuing convergence with the primary goal of reducing security risk, and yet 35 percent identify security risk as an obstacle to connecting IT and OT systems. In addition, 33 percent of organizations *not* planning to undergo convergence cite security risk as a major factor in their decision.

This somewhat contradictory data reveals the complex relationship between IT/OT convergence and security. The dangers of connecting systems without implementing sufficient security and access controls are real, as is exemplified by those who are avoiding convergence altogether due to the security risk. But **when the convergence process takes security into account from the start, with the proper mechanisms enabled to manage access and connectivity, the final result can be an improvement in organizational security.**

Also interesting is the fact that five of the top challenges to IT/OT convergence (architectural changes requested, IT/OT cultural differences, pushback from the OT team, siloed teams, and technology integration) indicate dissonance between IT and OT teams.

This is not a shock given other data points we have examined, but it does illustrate once again that IT and OT limit positive outcomes when they do not work together. **Especially when undertaking a large and complicated project such as IT/OT convergence, it is vital that teams overcome real or perceived cultural differences, longstanding siloes, and all other factors that prevent effective collaboration.** If initiatives of this scale are to succeed, they need not just the buy-in of both IT and OT but also a commitment from all parties to work as true partners.

Conclusion

Organizations that operate OT environments face real and persistent obstacles when it comes to securing critical systems against unauthorized access and other cyberthreats. The isolation that once largely protected OT and ICS from such threats has given way to a new era of connectivity that promises greater productivity and security even while creating serious potential risks. At the same time, organizations depend on the specialized skills and subject matter expertise of third-party vendors to help keep operations running, but connecting these users and their devices to OT environments without implementing the proper access controls also increases risk.

The data collected in this study reveals major gaps in industrial organizations' current efforts to manage OT systems access and risk. Significant progress can and must be made in a variety of areas, including but not limited to risk mitigation, management and oversight of third-party access, and communications and collaboration between IT and OT teams.

What is promising, however, is that strategies and solutions already exist to address many of the challenges and gaps identified in the research. By following relevant security frameworks and implementing robust solutions for secure remote access and privileged access management, breaking down barriers between IT and OT teams, and prioritizing security in IT/OT convergence projects, organizations can achieve a tangible improvement in their ability to effectively manage access and risk in the increasingly connected OT environment.

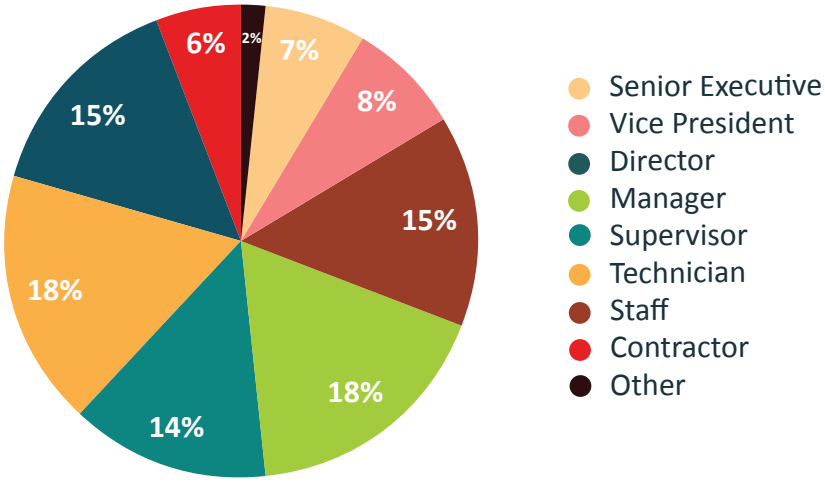
Methodology

A sampling frame of 30,116 IT and IT security practitioners in the United States and EMEA who are in organizations that operate an OT environment were selected as participants to this survey. Table 1 shows 1,174 total returns. Screening and reliability checks required the removal of 118 surveys. Our final sample consisted of **1,056** surveys or a 3.5 percent response.

Table 1. Sample response	Freq	Pct%
Sampling frame	30,116	100.0%
Total returns	1,174	3.9%
Rejected or screened surveys	118	0.4%
Final sample	**1,056**	3.5%

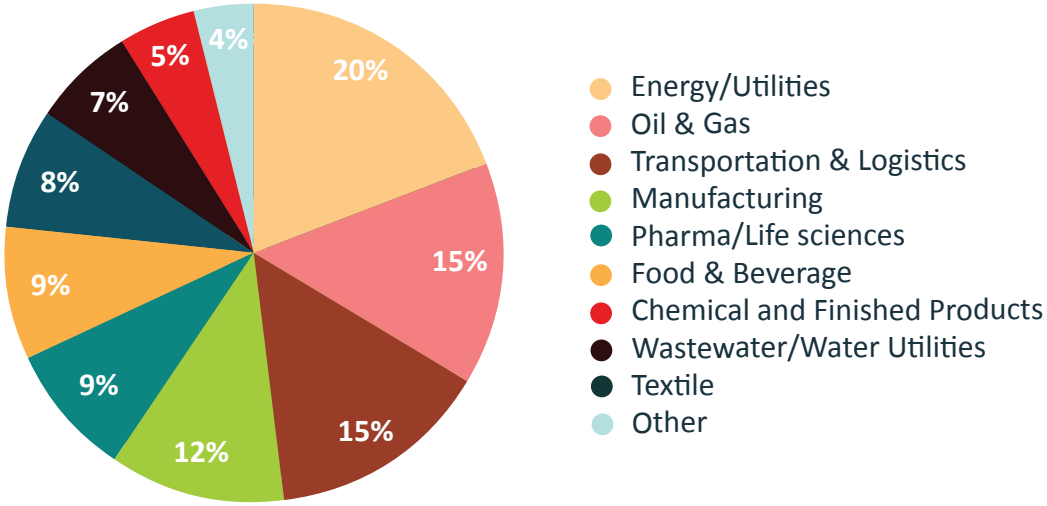
Pie chart 1 reports the respondent's organizational level within participating organizations. By design, more than half (61 percent) of respondents are at or above the supervisory levels. The largest categories at 17 percent of respondents are technician and manager.

Pie chart 1. Current position within the organization



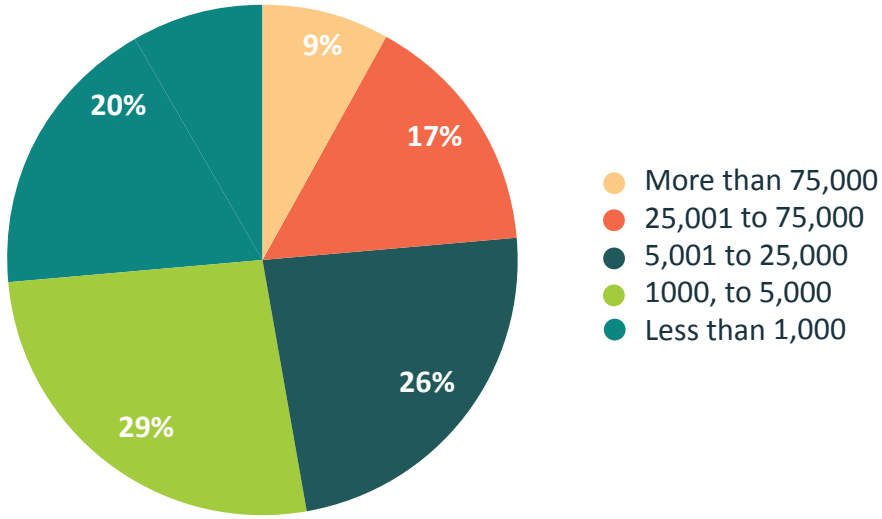
Pie chart 2 reports the industry classification of respondents' organizations. This chart identifies energy/utilities (20 percent) as the largest industry focus. This is followed by oil and gas (15 percent of respondents), transportation and logistics (15 percent of respondents), manufacturing (11 percent of respondents), pharma/life sciences, food and beverage, and chemical and finished products (each at 8 percent of respondents).

Pie chart 2. Primary industry classification



As shown in Pie chart 3, 52 percent of respondents are from organizations with a global headcount of more than 5,000 employees.

Pie chart 3. Primary industry classification



Caveats to this Study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are in organizations that operate an OT environment. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in September 2023.

Survey Response	Consolidated
Total sampling frame	30,116
Total returns	1,174
Rejected or screened surveys	118
Final sample	1,056
Response rate	3.5%

Part 1. Screening Questions

S1. Does your organization operate an OT environment, such as distributed control systems (DCS), Supervisory Control and Data Acquisition (SCADA) or other Industrial Control Systems (ICS)?	Consolidated
Yes	61%
No (Stop)	39%
Total	100%

S2. How knowledgeable are you about your organization's approach to managing OT system access and risk?	Consolidated
Significantly knowledgeable	37%
Knowledgeable	34%
Some knowledge	30%
No knowledge (Stop)	0%
Total	100%

Part 2. Business awareness of OT security needs, priorities and risks

Q1. Which role has the most responsibility for securing the OT infrastructure? Please select your top 2 choices.	Consolidated
CIO or CTO	21%
CISO or CSO	16%
Chief Risk Officer	32%
OT Vice president/Director	27%
Site/plant manager	26%
Control engineer	11%
Security architect	18%
Cybersecurity engineer/manager	30%
System administrator	16%
Other (please specify)	7%
Total	200%

Q2. What is your organization's total IT security budget in 2023?	Consolidated
Less than $100,000	3%
$100,000 to $500,000	4%
$500,001 to $1,000,000	8%
$1,000,001 to $5,000,000	19%
$5,000,001 to $10,000,000	19%
$10,000,001 to $50,000,000	17%
$50,000,001 to $100,000,000	15%
$100,000,001 to $250,000,000	11%
$250,000,001 to $500,000,000	6%
More than $500,000,000	0%
Total	100%
Extrapolated average	$ 55,154,500

Q3. Approximately, what percentage of the 2023 IT security budget is allocated to OT security activities?	Consolidated
0% to 5%	6%
6% to 10%	14%
11% to 15%	18%
16% to 20%	24%
21% to 30%	16%
31% to 40%	18%
41% to 50%	4%
More than 50%	3%
Total	100%
Extrapolated average	21%

Q4. Does your organization maintain an inventory of the industrial assets in its OT environment?	Consolidated
Yes	27%
Yes, but it may not be accurate or current	38%
No	31%
Unsure	5%
Total	100%

Q5. Is your organization required to comply with industry regulations forensuring secure access to OT environments such as NIST 800-82, NERC CIP, KRITIS etc.?	Consolidated
Yes	59%
No	17%
Not today, but we expect future regulations will require compliance	25%
Total	100%

Q6. How much of a priority is securing access to your organization's OT/ICS environments? Please use the scale from 1 = Low priority to 10 = High priority.	Consolidated
1 or 2	14%
3 or 4	11%
5 or 6	25%
7 or 8	25%
9 or 10	26%
Total	100%

Q7. How do users currently access your organization's OT systems? Please select all that apply.	Consolidated
Virtual Private Networks (VPN)	48%
Secure Remote Access (SRA)	49%
Zero Trust Network Access (ZTNA)	45%
Jump servers	35%
Equipment manufacturer supplied connection tools	39%
Direct connection to machine (no remote connection allowed)	30%
Other (please specify)	5%
Total	249%

Q8. How effective is your organization in mitigating risks and security threats to its OT environment? Please use the scale from 1 = not effective to 10 = highly effective	Consolidated
1 or 2	3%
3 or 4	10%
5 or 6	32%
7 or 8	33%
9 or 10	22%
Total	100%

Q9. How does your organization plan to introduce new tools to better secure your OT infrastructure? Please select one choice only.	Consolidated
Expand existing IT security solutions	19%
Use only OT-specific security solutions	31%
Use a blend of IT and OT security solutions	32%
We have no plans to introduce new security tools to our OT environment	19%
Total	100%

Part 3. OT connections and risk

Q10. Does your organization permit access to its OT environment? Please select one choice only.	Consolidated
Yes, for the OT team only	24%
Yes, for the OT team and other internal employees	36%
No (please skip to Q23)	41%
Total	100%

Q11. Why does your organization enable access to its OT environment? Please select all that apply.	Consolidated
To extend IT and security tools into OT environments	44%
To increase users' productivity	33%
To observe processes and/or check sensors	33%
To support digital transformation initiatives	24%
To enable collaboration	17%
To perform maintenance	23%
To reduce costs	23%
Other (please specify)	4%
Total	198%

Q12. How would you rate the OT team and other internal employees' experience of accessing OT systems with your current tools? Please use the scale from 1 = Poor to 10 = Excellent.	Consolidated
1 or 2	8%
3 or 4	16%
5 or 6	29%
7 or 8	26%
9 or 10	23%
Total	100%

Q13. Does your organization enable access to the OT environment to extract data and business intelligence?	Consolidated
Yes	50%
No (please skip to Q15)	50%
Total	100%

Q14. If yes, what types of data does your organization extract? Please select all that apply.	Consolidated
Statistics	30%
Telemetry	25%
Sensor data	34%
Machine health data	18%
Process data	26%
Environmental data	43%
Operator and maintenance data	45%
Run-time information	30%
Other (please specify)	2%
Total	251%

Q15. How does your organization plan to introduce new tools to better secure your OT infrastructure? Please select one choice only.	Consolidated
Expand existing IT security solutions	19%
Use only OT-specific security solutions	31%
Use a blend of IT and OT security solutions	32%
We have no plans to introduce new security tools to our OT environment	19%
Total	100%

Q16. How many vendors/third parties are authorized to connect to your organization's OT environment?	Consolidated
Less than 10	21%
10 to 50	20%
51 to 100	35%
101 to 250	25%
Total	100%

Q17. How concerned is your organization about risks created by vendors/third parties accessing its OT environment? Please use the scale from 1 = No concern to 10 = Highly concerned	Consolidated
1 or 2	12%
3 or 4	13%
5 or 6	32%
7 or 8	26%
9 or 10	18%
Total	100%

Q18. How would you rate vendors/third parties' experience accessing OT systems with your current tools? Please use the scale from 1 = poor to 10 = excellent.	Consolidated
1 or 2	12%
3 or 4	15%
5 or 6	31%
7 or 8	29%
9 or 10	14%
Total	100%

Q19. What are the top challenges to securing vendor/third party access to your organization's OT systems. Please select the top three choices only.	Consolidated
Keeping vendor/third party access secure	21%
Giving users too much privileged access	16%
Preventing unauthorized access	32%
Controlling activity permissions	27%
Monitoring user activity in real time	26%
Recording sessions for forensics and auditing purposes	11%
Terminating connections once work is completed	18%
Adding strong authentication to legacy systems	30%
Identifying specific users from the vendor/third party who us generic logins	16%
Aligning IT and OT security priorities	7%
Other (please specify)	200%
Total	

Q20. What are the biggest barriers to securing vendor/third party access to your organization's OT systems? Please select the top two choices only.	Consolidated
Lack of budget	42%
Budget is committed to existing projects	38%
Lack of expertise	46%
Lack of available solutions	38%
Potential impact to operational uptime	15%
Recording sessions for forensics and auditing purposes	19%
Not a priority	4%
Other (please specify)	4%
Total	200%

Q21. During the Covid-19 pandemic, did your organization invest in new tools to allow secure remote access to OT environments?	Consolidated
Yes	51%
No (please skip to Q23)	49%
Total	100%

Q22. If yes, have you reassessed the security and effectiveness of these solutions since their initial deployment?	Consolidated
Yes	51%
No	49%
Total	100%

Part 4. IT/OT communications and collaboration

Q23. How would you rate the level of collaboration between the IT and OT teams in your organization? Please use the scale from 1 = No collaboration to 10 = Significant collaboration.	Consolidated
1 or 2	19%
3 or 4	18%
5 or 6	25%
7 or 8	22%
9 or 10	17%
Total	100%

Q24. How does your organization allocate OT cybersecurity responsibilities? Please select one choice only.	Consolidated
IT is solely responsible for managing OT environment security policies and practices	32%
OT is solely responsible for managing OT environment security policies and practices	30%
IT and OT share responsibility for managing OT environment security policies and practices	39%
Total	100%

Q25. How often do your IT and OT teams communicate about OT security issues? Please select one choice only.	Consolidated
Daily	6%
Weekly	10%
Monthly	13%
Quarterly	14%
Annually	20%
On an ad-hoc basis	19%
Only when a security incident occurs	19%
Total	100%

Q26. How often are senior leadership and/or board members updated on the organization's OT security posture and the policies and practices in place to maintain or improve it? Please select one choice only.	Consolidated
Monthly	10%
Quarterly	13%
Bi-annually	17%
Annually	31%
On an ad-hoc basis	15%
Only when a security incident occurs	15%
Total	100%

Q27. How do you learn and stay up to date on the latest trends and best practices in OT security? Please select your top two choices.	Consolidated
Blogs	26%
Industry press	31%
Conferences/trade shows	15%
Associations	13%
OT co-workers	41%
Webinars	13%
Continuing education	9%
Social media	18%
Other (please specify)	6%
I am not actively keeping up to date on OT security practices	31%
Total	200%

Part 5. IT/OT convergence

Q28. What best describes your organization's level of secure connectivity between IT and OT systems in your organization? Please select one choice only.	Consolidated
Early stage—Limited awareness of the security needs around IT/OT connectivity. Limited adoption of policies controlling access between IT and OT systems (please skip to Q30)	15%
Intermediate stage—Some policies in place to govern access between IT and OT systems. Some work completed to map how users connect to systems, immature or inadequate tools to manage access (please skip to Q30)	24%
Advanced stage—Established policies, tools, governance and reporting in place to control and monitor connectivity between IT and OT systems (please skip to Q30)	33%
No connectivity between IT and OT systems and no plans for future connectivity	28%
I am not actively keeping up to date on OT security practices	100%

Q29. If your organization has no plans for connectivity between IT and OT systems, what are the reasons? Please select the top three reasons.	Consolidated
Not a priority	22%
Too costly	24%
Siloed teams	35%
Lack of budget	43%
Architectural changes required	12%
Pushback from the OT team	33%
IT/OT cultural differences	17%
Technology integration difficulties	27%
Security risks	33%
Skills gaps in IT or OT teams	30%
Lack of C-level support	23%
Other (please specify)	3%
Total	300%

Q30. What are the top two reasons for increased IT/OT connectivity? Please select the top three reasons only.	Consolidated
Improve the ability of IT and OT teams to collaborate	57%
Reduce security risks	59%
Respond to unplanned asset downtime quickly	38%
Acquire business intelligence/data analytics	31%
Deploy security tools within OT environments	42%
Achieve required connectivity with original equipment manufacturers (OEMs)	29%
Lower operational costs through remote management capabilities	21%
Improve agility with automated deployment features and extensive use of software	25%
Total	300%

Q31. What are the most significant challenges to connecting IT/OT environments? Please select the top three challenges.	Consolidated
Siloed teams	32%
Lack of budget	42%
Architectural changes required	25%
Pushback from the OT team	24%
IT/OT cultural differences	14%
Technology integration	30%
Security risks	35%
Scalability & bandwidth	17%
Data governance & management	26%
Skills gaps in IT or OT teams	31%
The impact of change & process management on the organization	24%
Other (please specify)	4%
Total	300%

Q32. How concerned is your organization about IT/OT convergence impacting the availability of IT systems/services? Please use the scale from 1 = Not concerned to 10 = Highly concerned.	Consolidated
1 or 2	12%
3 or 4	15%
5 or 6	22%
7 or 8	28%
9 or 10	24%
Total	100%

Q33. How concerned is your organization about IT/OT convergence impacting the safety and uptime of the OT environment? Please use the scale from 1 = Not concerned to 10 = Highly concerned.	Consolidated
1 or 2	7%
3 or 4	12%
5 or 6	26%
7 or 8	32%
9 or 10	24%
Total	100%

Part 6. Demographics and roles

D1. What organizational level best describes your current position?	Consolidated
Senior Executive	7%
Vice President	8%
Director	15%
Manager	18%
Supervisor	14%
Technician	18%
Staff	15%
Contractor	6%
Other (please specify)	2%
Total	100%

D2. What industry are you employed in?	Consolidated
Energy/Utilities	20%
Chemical and Finished Products	8%
Pharma/Life sciences	9%
Manufacturing	12%
Oil & Gas	15%
Wastewater/Water Utilities	7%
Food & Beverage	9%
Textile	5%
Transportation & Logistics	15%
Other (please specify)	4%
Total	100%

D3. What is the worldwide headcount of your organization?	Consolidated
Less than 1,000	20%
1,000 to 5,000	29%
5,001 to 25,000	26%
25,001 to 75,000	17%
More than 75,000	9%
Total	100%

About Ponemon Institute

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

For more information about this study, please contact Ponemon Institute by sending an email to **research@ponemon.org** or call at 1.800.887.3118.

About Cyolo

Cyolo enables privileged remote operations by connecting verified identities directly to applications with continuous authorization throughout the connection. Purpose-built for deployment in every type of environment, Cyolo's Remote Privileged Access Management (RPAM) solution combines multiple security functions required to mitigate high risk access, including zero-trust access for users and devices, MFA for the last mile, local IdP capabilities, credentials vaulting, secure file transfer, supervised access, session recording, and much more into a single, cost-effective, easy to deploy, and user-friendly platform.

Consolidate your security stack and experience the power of seamless and secure operations across any application in any environment, from critical infrastructure to cloud. Visit **https://cyolo.io** to learn more.