THE STATE OF OT SECURITY:
A COMPREHENSIVE GUIDE TO TRENDS, RISKS, & CYBER RESILIENCE

Michael M. Amiri, *Senior Analyst*
Michela Menting, Senior *Research Director*

ABIresearch. THE TECH INTELLIGENCE EXPERTS℠ | paloalto® NETWORKS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Industrial operations are increasingly under threat. OT attacks are common, widespread, and extremely frequent. These attacks are primarily IT-borne, and ransomware, in particular, has had a devastating effect on industrial environments in the last few years. The business impacts have been immediate and major, forcing operational shut down, lost revenue, and significant remediation costs. This state of affairs has pushed cybersecurity to the top of the agenda for industrial operators.

Spending on OT cybersecurity is expected to grow over the next two years, but implementation of the right solutions is no easy feat. There are a number of obstacles that industrial operators need to overcome, not least being the siloed operations of OT and IT teams and their resulting misalignment on cybersecurity decision-making and cooperation. However, convergence of the two is progressing, albeit slowly, and most industrial operators expect decision-making on cybersecurity to be cohesively centralized for both IT and OT.

Beyond that, industrial operators will need to address increasing compliance requirements from upcoming regulations and standards in the field, as well as the risks posed by their adoption of new technologies and processes, including AI, remote access, cloud, 5G, and robotics. All of these pose their own unique set of challenges. Nonetheless, they also offer new ways to implement cybersecurity technologies for OT environments.

Ultimately, industrial operators are conscious of the need to adapt cybersecurity to the new demands of the day, and this is pushing them in the direction of Zero Trust implementation. The key to successful deployment will be to choose the right provider, and not least, one with expertise in both OT and IT environments, able to serve up the best security for both worlds.

A CHANGING ERA FOR INDUSTRIAL OPERATORS

3 out of 4 organizations have experienced a cyberattack on their OT environment.

Operational Technology (OT) teams once felt fortified against cyberattacks in industrial operations, given their air-gapped systems, legacy assets, proprietary technologies, fragmented end markets, etc. However, the narrative has greatly changed within the last several years; considering the many news headlines reporting on various OT attacks on industrial firms. Take the EKANS ransomware attack on Honda in 2020 as an example, forcing multiple factory shutdowns worldwide. Or look at the 2022 satellite-born attack disrupting the operations of 5,800 wind turbines in Germany. Other successful attacks include the Industroyer2 malware attack on electrical substations used by Ukrainian energy companies and the notorious Colonial Pipeline shutdown in 2021. What these recent attacks tell us is that the unabated expansion of cyberthreats has found ways to intrude into every corner of modern organizations, and industrial operations are no exception.

To illustrate, 3 out of 4 organizations state they have experienced a cyberattack on their OT environment, with most experiencing frequent attacks. This trend makes sense, given the acceleration of digital transformation happening in the industrial sector. While malicious actors have a wide range of motivations to target OT operations at industrial firms, a successful attack on these companies holds immense financial or political potential. Manufacturing plants cannot afford to be shut down for several days or even weeks; it would be a business disaster. Similarly, modern society cannot function if the railroads shut down or the electrical grid goes dark. The high-risk nature of industrial operations means that safeguarding an OT environment is essential not only for business continuity, but also for national security.

It is worth noting that 7 out of 10 industrial OT attacks originate in Informational Technology (IT) environments, signaling an urgent need for OT and IT departments and technologies to start working more closely together. OT-IT convergence will end existing silos and enable organizations to purchase cybersecurity tools that address both departments simultaneously. This tight cooperation between the two will be important as industrial firms adopt new technologies that pose new risks to the network environment. Artificial Intelligence (AI), robotics, 5G, the cloud, and remote access will accelerate the challenges that a holistic approach to cyber protection can mitigate.

Understanding the threat landscape is the first step. Is this driven by adversaries in political conflict, or is there a growing opportunity for organized crime where there was not one before? The answer is not so black and white. Threat actors engage for a variety of reasons, many of which can overlap: financial opportunities arise in targeting critical infrastructure because they are increasingly connected or because governments are turning a blind eye to targets that were once off limits. The reasons are endless and complex.

The second step is finding appropriate solutions to counter the threats and minimize the risks to OT. Industrial environments can differ significantly, presenting a highly fragmented ecosystem with different risk tolerance. Understanding the target, as well as the threat landscape, goes a long way to building an effective defense.

OT is a high-profile and lucrative target today for cyberthreat actors.

To obtain a better picture of the dangers and the risks to OT environments today, Palo Alto Networks commissioned a global survey of 1,979 respondents across 16 different end markets with the goal of investigating the state of OT security and taking the pulse of C-suite management and practitioners in large industrial organizations. The survey questions addressed major topics, including risks to industrial operations and organizational approaches to protection and incidence response, as well as trends, preferences, and demands in terms of applicable solutions.

The survey revealed some interesting findings across the board, but the biggest, loudest message was that OT is a high-profile and lucrative target today for cyberthreat actors, and that industrial operators still have a lot of obstacles to overcome in terms of securing their OT environments appropriately.

KEY FINDINGS

- **Cyberattacks can shut down OT operations.** Almost 70% of industrial organizations have experienced a cyberattack in the past year, and 1 out of 4 experienced a shutdown of operations as a result.
- **Cybercriminals are the most feared,** more so than state-sponsored groups or hacktivists. Malware, ransomware, and insider attacks are the top 3 threats according to industrial operators.
- **IT is the main vector,** with 72% of attacks targeting the OT originating there.
- **Regulatory pressure on OT is growing;** 74% of executives believe it will increase in the next 2 years.
- **5G security will become essential,** as 70% of respondents believe 5G devices to be an OT threat vector.
- **The move to the cloud will reinforce OT security,** according to 80% of respondents.
- **AI is a double-edged sword.** 74% say AI attacks against OT are a critical issue today, but 8 out of 10 also agree that AI will be key to stopping OT attacks.
- **Friction between OT & IT is a challenge.** 40% say that their OT and IT teams are frictional, and only 12% say they are aligned.
- **The importance of IT/OT platformization:** 7 out of 10 respondents are clear on their intention to consolidate IT & OT solutions from the same cybersecurity vendor.
- **Increasing remote access is a major concern:** 3 out 4 agree that remote access is on the rise for both employees and third parties.
- **Zero Trust is the North Star:** 87% of industrial respondents believe that Zero Trust is the right approach to securing OT environments.

OT ATTACKS COMMON, WIDESPREAD, AND EXTREMELY FREQUENT!

One of the most alarming findings revealed early on in the survey is that **more than 76% of respondents stated that their organizations had experienced a cyberattack in their OT environment.**

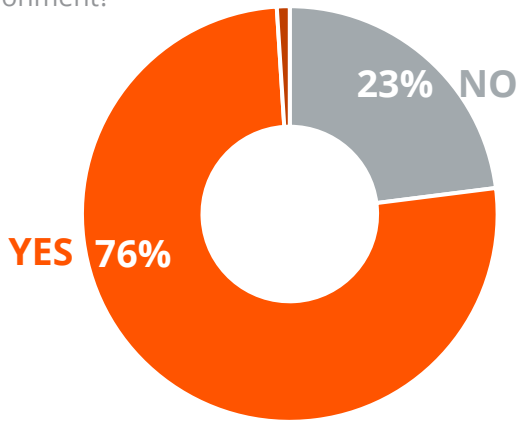
This completely dispels the illusion that industrial operations are immune to cyberthreats. Today, they are a real and common target, as evidenced by the high-profile attacks covered in the media in the last few years. These attacks are only the tip of the iceberg. Clearly, a vast majority of industrial operators are already feeling the heat of OT-targeted attacks.

The top 3 most feared attacks against OT were Malware, Ransomware, and Insider Attacks. From Stuxnet to Lockbit, the threat landscape has evolved from bespoke OT malware targeted against a specific adversary, to IT-borne, highly popular ransomware indiscriminately leveraged at industrial organizations. Extortion and organized crime have replaced state-sponsored war games as the biggest threat to industrial operators.

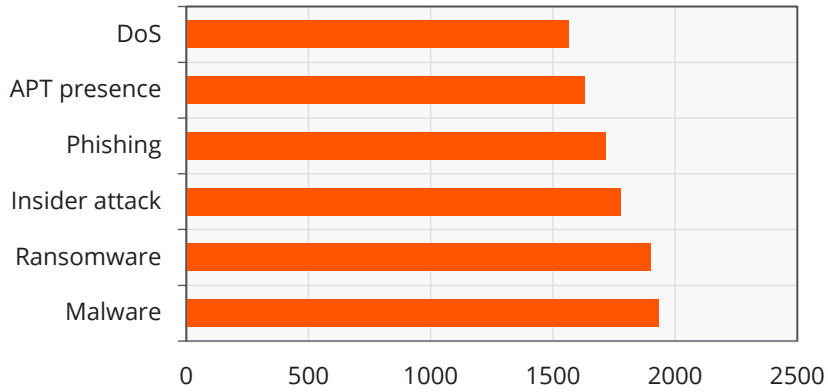
Ransomware is particularly prominent today, with syndicates such as DarkSide, BlackCat, and Ryuk having successfully breached the IT-OT gap to target OT environments, with a high success rate in utilities and the energy sector. With high payouts (US$4.4 million for Colonial Pipeline), ransomware attacks are a lucrative opportunity for cybercrime.

As a result, cyberattacks in the OT environment have become a recurring problem. An overwhelming 75% of respondents reported frequent attacks, often monthly, but also weekly and daily. This reveals the existence of a dynamic cybercrime ecosystem, one that is clearly well engaged in targeting the OT environment.

Has your organization ever experienced a cyberattack (s) in your OT environment?

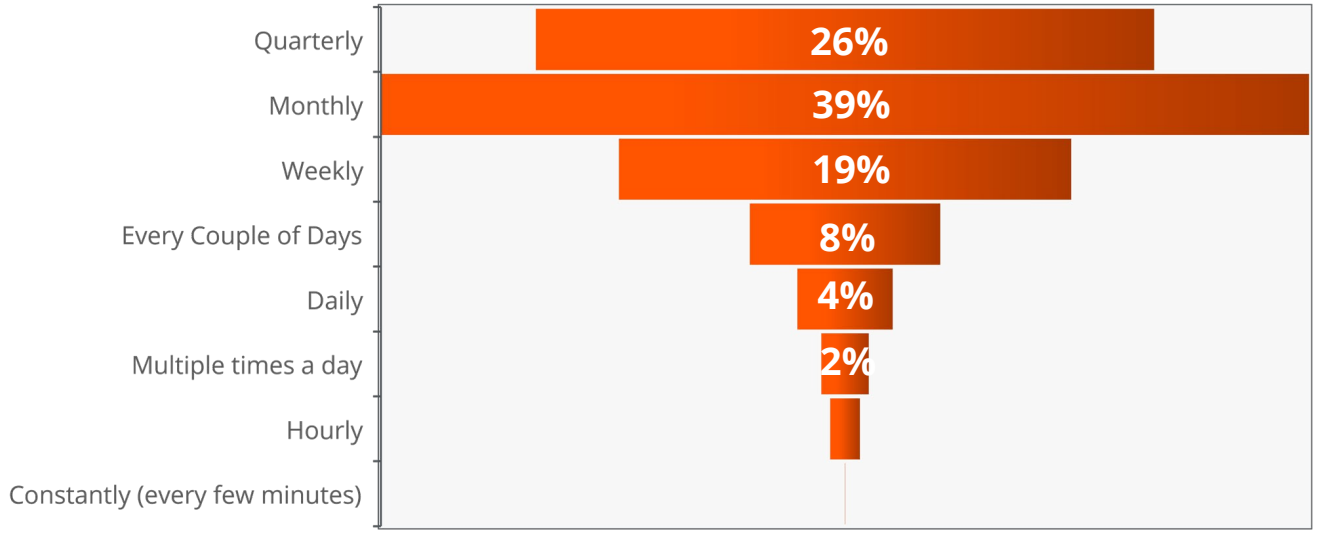


What types of OT cyberattacks do you fear the most?



Supply chain attacks are an increasingly problematic threat, used successfully to target a greater number of organizations. With industrial operators using more commercial off-the-shelf solutions in their OT, the blast radius can be significant and highly damaging.

How frequently do you typically experience attacks (or incidents) in your OT environment?



Insights from Industrial Operators

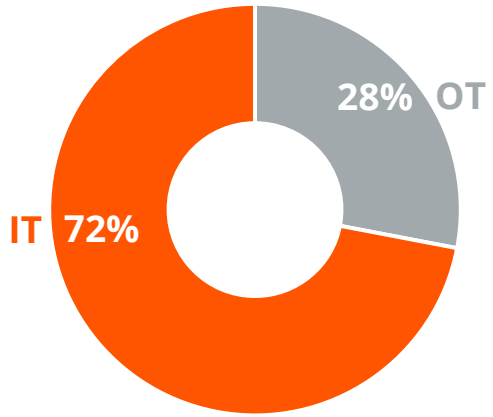
"Evaluate and validate supply chain vendors."

IT IS THE MOST POPULAR ATTACK ENTRY POINT

The success of ransomware is reflected in the survey responses, revealing that the primary point of origin for these attacks was in IT. This is confirmed by high-profile media coverage of ransomware, and the fact that it originated in the IT environment. Clearly, ransomware attacks have overcome obstacles related to the perceived isolation of OT environments.

Unfortunately, this success means that run-of-the-mill cyberthreat tools and attacks can realistically be leveraged to target OT and open the door to all kinds of malicious opportunists, keen to take advantage of an ostensibly vulnerable OT landscape.

Where did the attack originate?

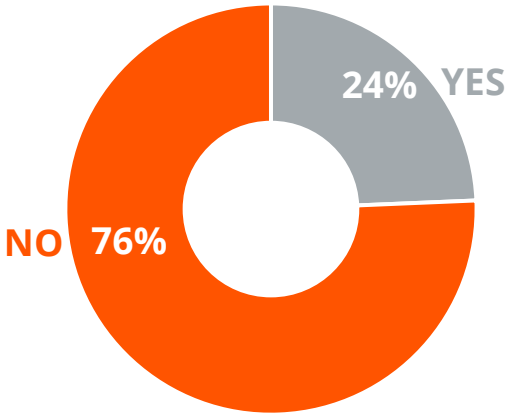


BUSINESS IMPACTS ARE CLEAR, IMMEDIATE, AND MAJOR

There is no doubt that a high success rate will translate into increased momentum and greater attractiveness of the OT environment for threat actors, particularly for organized crime.

Unfortunately, these attacks have had a significant and immediate business impact, with at least a quarter of respondents stating that they have had to shut down industrial operations in the last year due to a successful attack, whether as a preemptive measure or due to actual disruption. Shutdowns mean lost revenue opportunities, as well as damage control and event remediation costs, which can include additional security technologies and services, communications with customers and suppliers, law enforcement, and public relations. Longer-term costs can include reputational damage, regulatory penalties, higher insurance premiums, and supplier and customer costs due to late or non-deliveries, among others.

In the last year, have you had to shut down your OT operations due to a successful cyberattack?



Insights from Industrial Operators

"Improve incident response skills through periodic drills and simulations."
"Test and update incident response playbooks on a regular basis."

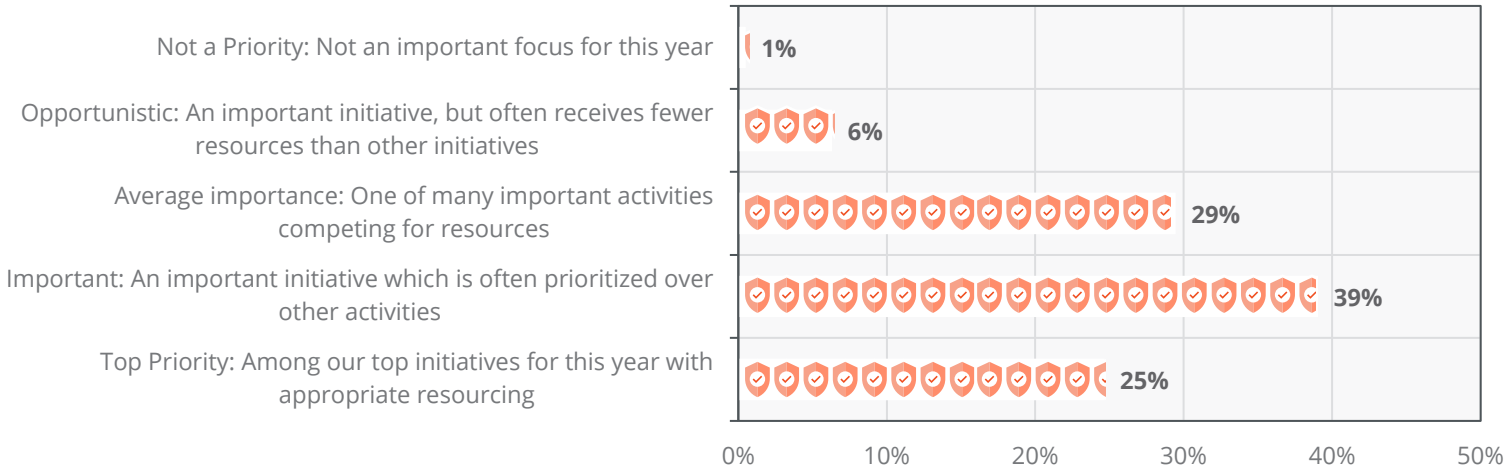
CYBERSECURITY INVESTMENT A BIG PRIORITY

This dangerous state of affairs is driving industrial operators to increasingly focus on security for their OT environments. Protecting their OT environments is a high priority for almost two-thirds of the respondents, and not likely to be overlooked. Investing in OT cybersecurity is financially feasible, as the estimated average cost of a single breach remediation for a connected asset (OT/Internet of Things (IoT)) is between US$10,000 and US$50,000.

There is little doubt that cybersecurity initiatives are key to minimizing the cyber risks posed by threat actors, and achieving positive protection mechanisms requires making these initiatives a priority. This includes OT security evaluations; the better prepared an operator is, the faster they can remediate an event, and the lower the total cost of the fallout.

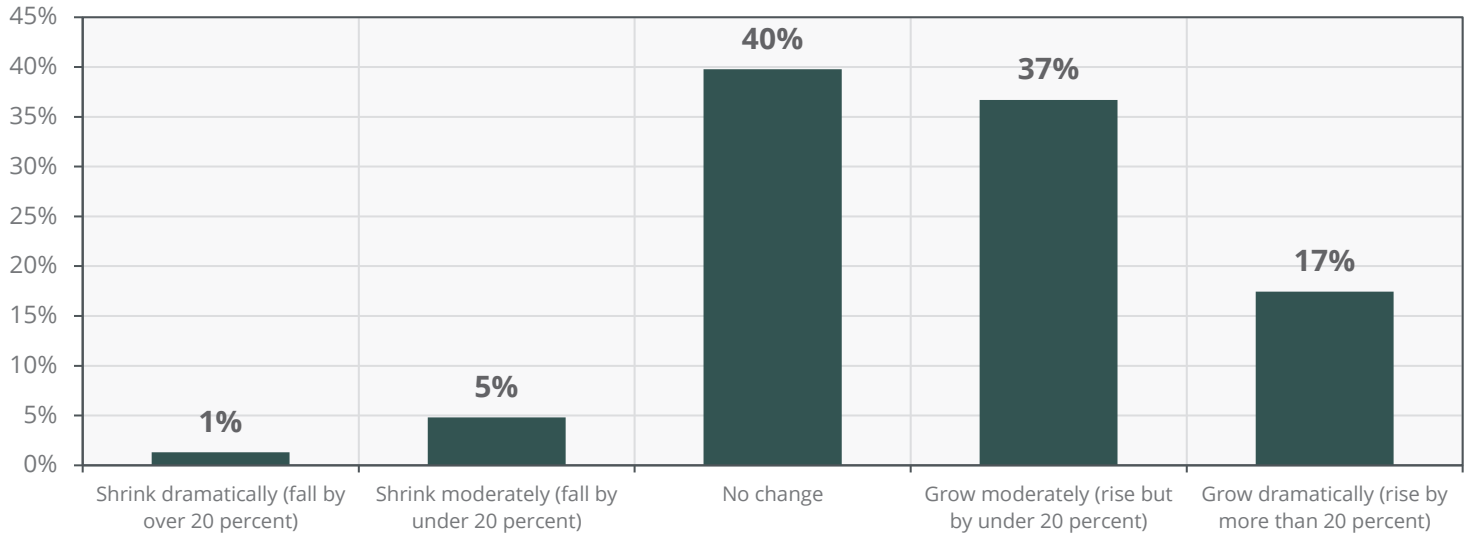
Spending on OT cybersecurity will continue to be a priority. It is expected to grow over the next two years, according to over half of all respondents. Very few—less than 5%, in fact—expect spending to shrink.

To what extent are cybersecurity initiatives to protect your OT environments a priority?



There is a clear correlation between the current threat landscape, which is focused and regularly engaged in attacks against OT assets, and the prioritization of cybersecurity strategies and investments by industrial operators to counter these. However, the success of these strategies is contingent on comprehensive and coordinated internal deployment, which is no easy feat.

How do you expect your company's spending on OT cybersecurity to change over the next 2 years?



OT AND IT: SILOED BUT MOVING TOWARD CONVERGENCE

Industrial operators have clearly understood that cybersecurity is a requirement for OT environments. Because a large majority of the attacks originate in IT, OT and IT teams must work together to address the threats. However, the survey reveals that there are obstacles to achieving a coordinated response between the two, especially concerning security investment.

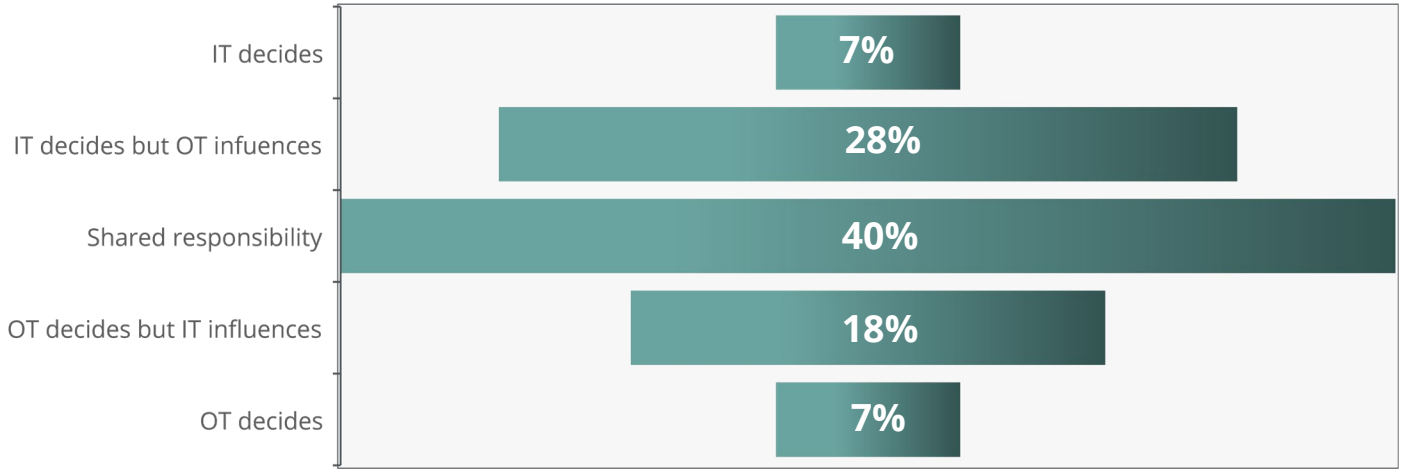
MISMATCHED DECISION-MAKING BETWEEN OT AND IT

When queried about the responsibility for OT cybersecurity purchase decisions, the respondents' answers were highly varied. **Only 40% of respondents stated that these decisions were shared between the two teams.**

In most cases, the decision was the prerogative of only one team, but while these were siloed, almost half stated that they had influence in the process.

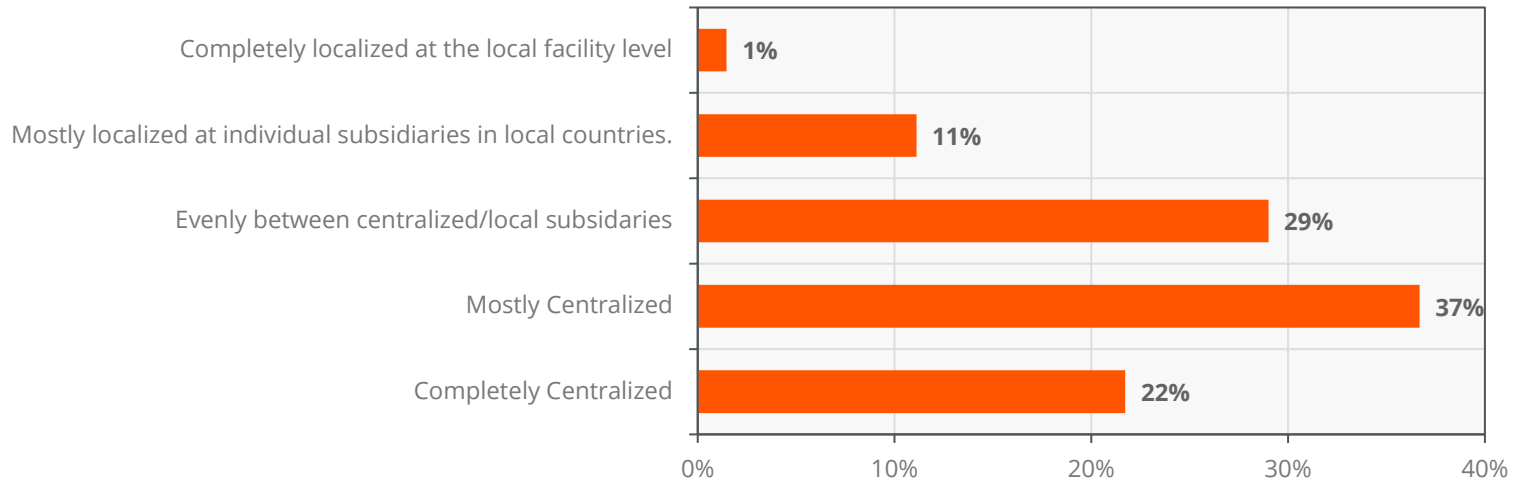
This discrepancy is due to the historical roles of both teams: IT has traditionally been in charge of security company-wide, while OT has not had much call to focus on that until recently, focusing instead on industrial operations.

Today – who makes the purchase decisions for OT cybersecurity for your company and do you expect the decision making to evolve over the next 2 years?



And yet, it is clear that industrial operators understand the need to share some of that decision-making process for security investment.

In Two Years - How are decisions made today regarding OT security purchases and how do you expect this process change over the next 2 years?



When asked how they expected decisions to be made in two years, almost two-thirds said they would likely be centralized, while another third expected an even split between being localized and alternatively centralized. This shows that while convergence is clearly expected going forward, it will not be a fast process, and the process is still a fledgling one.

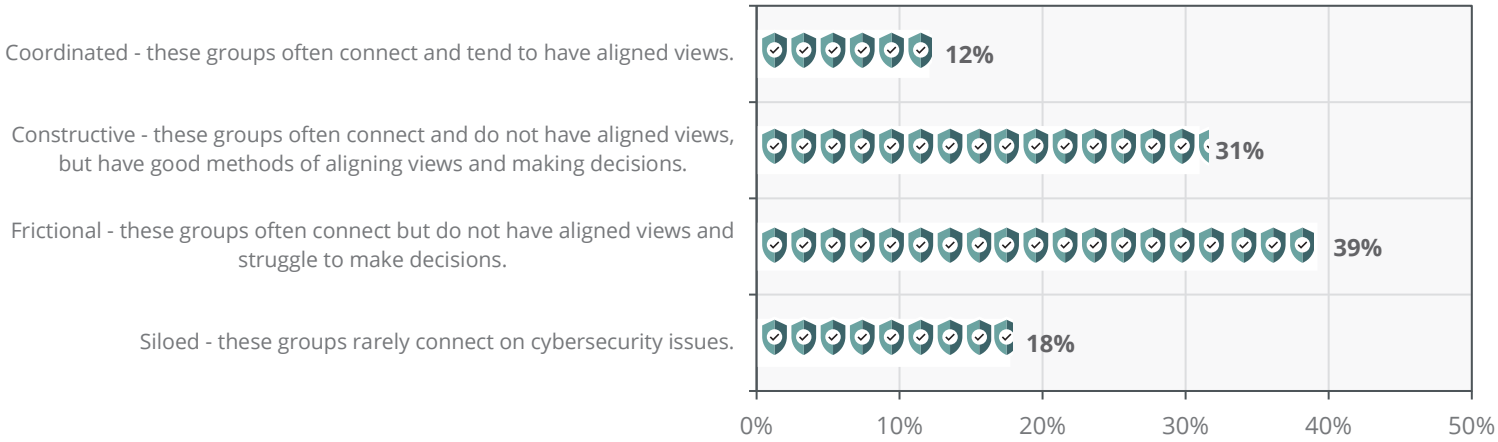
Coordinating that decision-making process in terms of security requires communication between the two teams: IT on the appropriate solutions to counter threats, and OT on the specific limitations and constraints of OT assets.

IT AND OT COLLABORATION NEEDS TO BE BETTER

In large part, this slow convergence is due to the difficulty that the two teams have in establishing an effective dialogue that can result in successful cooperation. When asked to describe the relationship between OT and IT in their cybersecurity efforts, 57% stated that it was either completely siloed or frictional. In other words, they indicated that the two groups rarely connected, and when they did, they were not aligned in their views and struggled to make decisions.

Ultimately, this difficulty in coordination is a significant obstacle that can impede the successful deployment and operation of OT cybersecurity. **A piecemeal approach to cybersecurity will help neither IT nor OT, regardless of the caliber of solutions invested in, resulting in the continued exposure of vulnerable OT assets.** While internal cooperation is key to creating a coordinated security response, there are external driving forces that will support this eventual convergence, both from a regulatory and an emerging technology perspective, driving internal dialogue.

Which of the following best describes the current relationship between OT and IT when it comes to cybersecurity?



Insights from Industrial Operators

"Boost cooperation between the OT and IT departments."

"Bridge the knowledge gap through joint training, incident response exercises and shared responsibility."

REGULATION AS A DRIVING SECURITY FORCE

Regulation can be a powerful catalyst for driving security investments. It forces organizations to conduct risk assessments, develop cybersecurity strategies, and raise awareness of the potential risks associated with disregard, or noncompliance, of these legislative mandates. The protection of critical infrastructure is a fundamental prerogative of any nation, and this extends to its OT environments. An increasing number of regulatory instruments are already in force to protect OT in critical infrastructure. But, the fairly new surge in attacks against OT is driving a renewed regulatory focus by governments, extending beyond critical infrastructure.

REGULATORY PRESSURE FOR OT SECURITY ON THE RISE

An important driver identified by 77% of respondents was the expected increase of regulatory pressure over the next two years to protect OT environments, especially within critical infrastructure, and this was consistent across all countries surveyed.

In Europe, the NIS2 Directive came into force in 2023, expanding the scope of the cybersecurity rules to new sectors and entities beyond critical infrastructure. In the United States, the Transportation Security Administration (TSA) updated its Security Directive Pipeline the same year (2021-02D), which was initially put together after the Colonial Pipeline attack in 2021 and focused on protecting critical pipelines and Liquefied Natural Gas (LNG) facilities.

As ransomware and other cyberthreats continue to target OT environments, and notably in critical infrastructure, governments will intensify regulatory requirements for operators, in a bid to minimize the risks of attacks.

This will undoubtedly impact industrial operations; **80% of respondents expected regulation to significantly affect the time spent on compliance processes.**

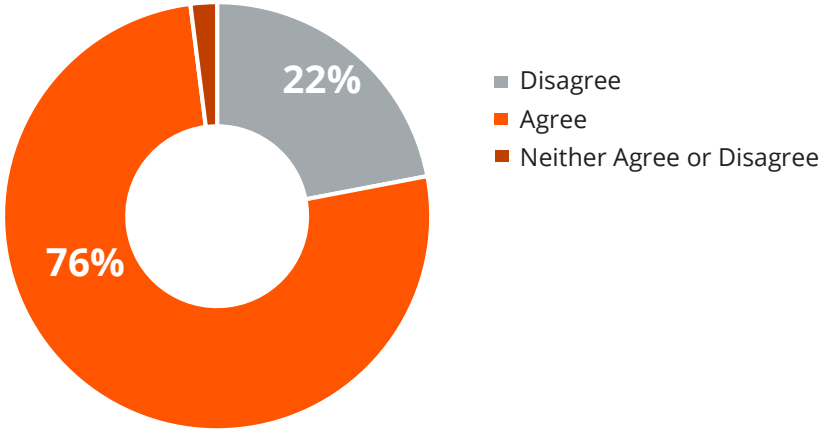
Regulatory compliance is a relatively rigid and formal process, with set requirements that need to be met, and then assessed and certified (often by a third party). These can be costly and time-consuming in their own right.

This increased pressure will inevitably result in demand for cybersecurity solutions that are pre-certified and compliance-ready, in a bid to simplify at least part of the security process.

Regulatory liability will keep industrial operators focused on meeting their obligations, and this is reflected in the survey.

Two-thirds of respondents stated that there would be pressure from the Board of Directors level to improve OT cybersecurity over the next two years.

Regulatory pressure to improve OT cybersecurity will increase in the next two years.



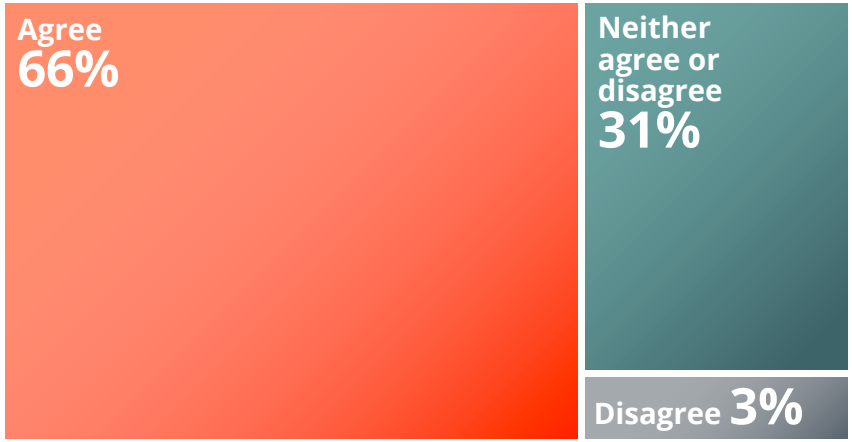
Over the next 2 years, I expect that my organization will spend too much time complying with OT cybersecurity-related regulatory requirements.

While increased attention to security is generally a good thing, poor implementation or too rigid a framework can mean less flexibility in terms of response from industrial operators. With pressure from upper management, external compliance requirements, an aggressive threat ecosystem, and the quest for better OT-IT coordination, operators have a lot on their plate. The onus is on industrial operators to look for effective technology solutions in the cybersecurity space that can help alleviate these concerns. Many are turning to emerging technologies to help them overcome these obstacles.

Insights from Industrial Operators

"Examine current OT cybersecurity policy and ensure alignment with industry standards and regulations."

Pressure from the Board of Director level to improve OT cybersecurity will increase over the next 2 years.



AI: A DOUBLE-EDGED SWORD FOR OT

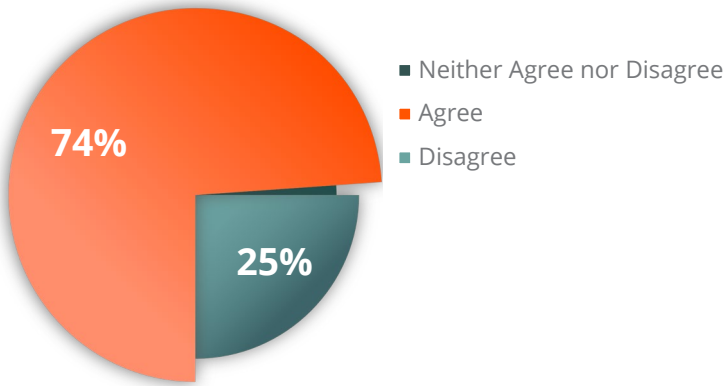
AI PART OF ATTACKS, BUT KEY TO PROTECTION

AI has already caught the attention of industrial operators, but the judgment on its value is split between fear of AI-enabled attacks and demand for AI-enabled protection.

74% of respondents identified AI-enabled attacks on OT infrastructure as a critical issue. There is little doubt that AI presents an opportunity for malicious actors. Threat actors are better at finding targets, accurately manipulating and taking advantage of users and systems, and automating complex and targeted attacks.

Machine translation, speech synthesis, and generative AI can all be used to minimize the amount of customization and manual supervision needed to carry out successful cyberattacks. There are already instances of ChatGPT being used to create malware.

AI-enabled attacks on our OT-infrastructure are a critical issue today.

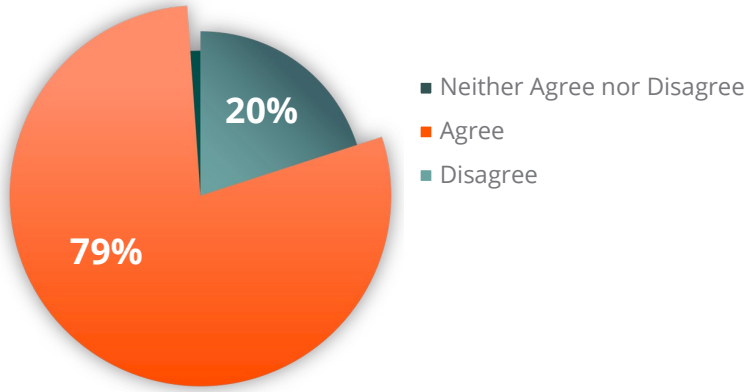


While AI can be used maliciously, it can also serve to enhance cybersecurity; **80% of respondents stated that AI-enabled security solutions would be critical for stopping attacks directed at their OT environments.**

Today, many cybersecurity solutions in IT already leverage Machine Learning (ML), heuristics, and AI in various forms, from automatic patching and malware classification to threat detection and incident response. This will (and must) expand to OT cybersecurity, especially because so many of the attacks originate from IT, as seen previously.

AI is clearly perceived as both a threat and a requirement for OT cybersecurity, which means that there are still a lot of discrepancies between the perceived and actual value of AI in industrial environments.

AI-enabled security solutions will be critical for detecting and stopping attacks on our OT-infrastructure.

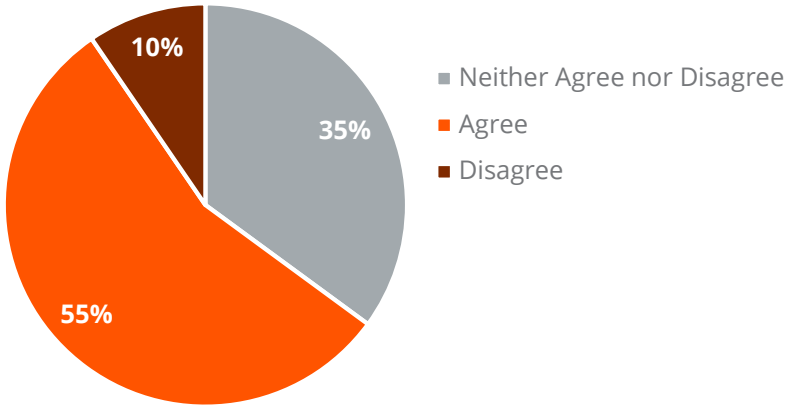


AI AS A FORCE MULTIPLIER FOR THREAT ACTORS

The dual role of AI tools is undoubtedly divisive in modern societies. The advances in generative AI in the last year have not only been lauded by pundits, but also denounced by doomsayers. This is reflected in the respondents' perceptions on whether AI is more beneficial to operators or to attackers. Just over half believe that AI will help hackers more than security teams in OT environments.

The role of AI as a digital tool for security is undisputed among respondents. However, opinions regarding whether AI serves an advantage or disadvantage seem evenly divided among survey respondents. Despite the ambiguity, the cybersecurity industry holds an advantage in combatting the malicious use of AI. Cybersecurity is a discipline that exists in an adversarial environment, and adversarial manipulation of AI and the use of malicious AI are expected responses (the fight against SPAM is probably one of the oldest examples of adversarial manipulation in ML).

AI will help hackers more than it will help security teams in OT environments.



The use of AI as a security tool is also viewed as a cost-saving measure, with **almost half of all respondents believing that it will reduce the number of security professionals hired.**

Rather than viewing it as complementary, AI is perceived as being a replacement for a security analyst. This belief may impede adoption of AI in OT security because OT environments require a specific skill set and knowledge that are not often informed by IT tools. OT engineers and analysts already have difficulties coordinating with IT; this may become marginally harder if they need to start negotiating with AI-based tools, especially in the fragmented industrial ecosystem. Despite this, the belief may be enough to impede AI investment in OT security.

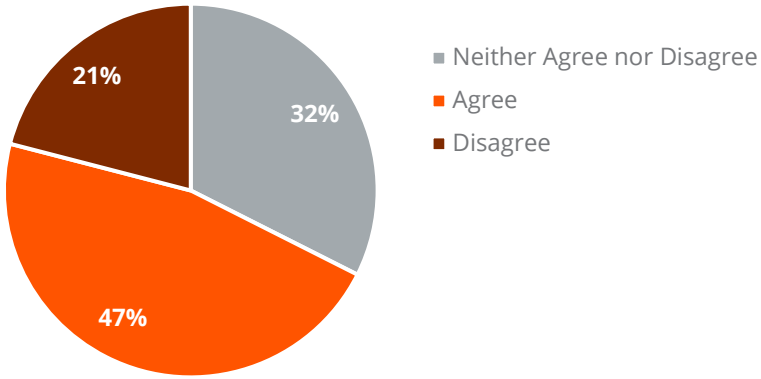
AI CAN ALSO BE A SECURITY TOOL FOR STRONGER AND BETTER PROTECTION

Regardless of its perceived role as an opportunistic tool for threat actors or a replacement for security professionals, AI is clearly considered an important technology, with half of the respondents stating that its use in OT cybersecurity will help solve the security skills gap problem.

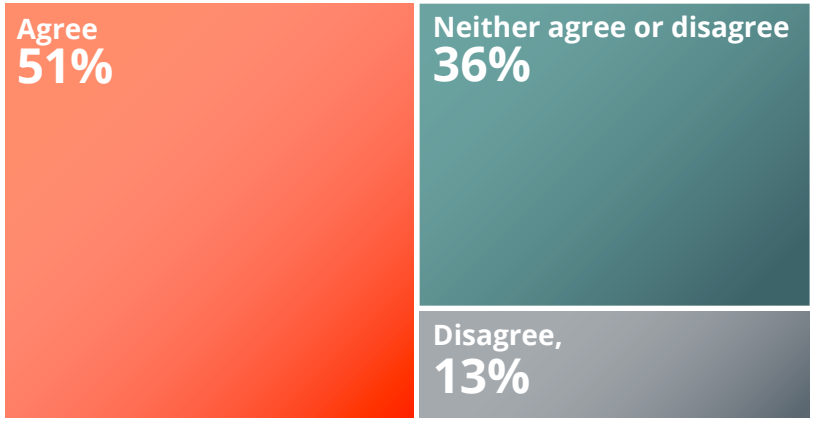
AI is successfully used in many cybersecurity solutions: from antivirus, intrusion detection and prevention, and user entity behavior analytics to authentication, data retrieval and analysis, threat hunting and threat intelligence, System-on-Chip (SoC) operational performance, etc.

While there is recognition that AI is being leveraged maliciously, there is also belief, and expectation, that it can enhance security in OT environments. The divergence of answers is almost evenly split in most cases, pointing to a lack of understanding around the perceived disadvantages and the potential benefits that AI can bring as value-added technology, including within OT.

The use of AI in OT security solutions will reduce the number of security professionals my company needs to hire.



The use of AI in OT security solutions will help solve our security skills gap problem.



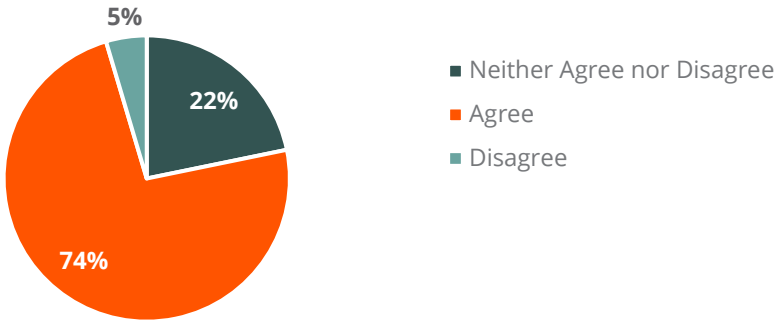
Insights from Industrial Operators

"Make security measures more effective by utilizing AI threat intelligence."
"Explore the use of AI driven security analytics."

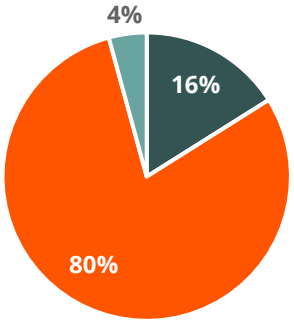
EMERGING TECHNOLOGIES CAN AMPLIFY OT SECURITY, BUT CHALLENGES PERSIST

AI is not the only new technology making way into OT environments. Operators are getting ready to implement 5G, robotics, cloud, and increased remote access, each presenting its own set of challenges.

Remote Access of internal employees and 3rd parties into OT will continue to increase.



Cloud-based architecture will be critical for OT in the next 3-5 years.



Respondents are in little doubt that remote access to OT, whether by internal employees or third-party contractors, is on the rise, with **74% in agreement that remote access will increase.** The increased adoption of remote access can offer many benefits, including improved monitoring capabilities, better response times in case of adverse events, and cost savings in terms of human resources and travel.

Lessons Learned: *Remote access management security controls on a regular basis are important. Evaluate and strengthen guidelines and tools for secure remote access.*

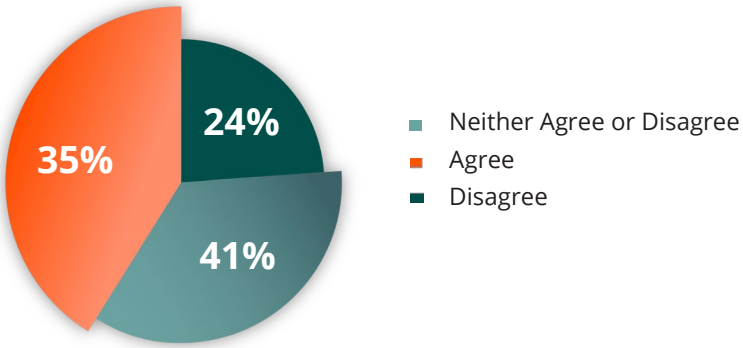
Remote access requires connectivity and access enablement platforms, many of which are offered as services tied to cloud-based architectures for better OT asset management. This aligns with the belief that the cloud will be a critical technology for OT in the next 3 to 5 years, according to 80% of the respondents. The concern here is to ensure the security of that access, regardless of origin, especially as the risk of man-in-the-middle attacks is high in such scenarios.

Lessons Learned: *Ensure the safe adoption of cloud services. Evaluate and improve cloud-based security solutions.*

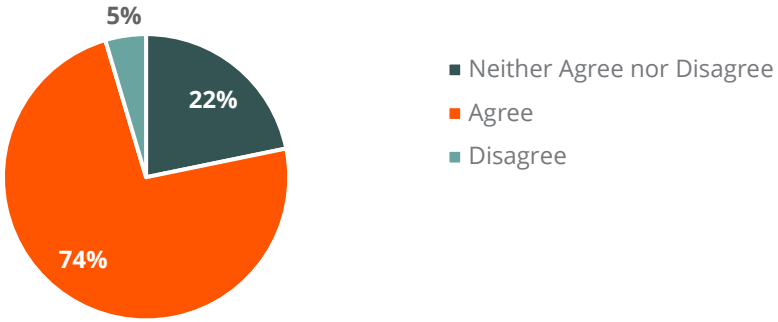
Respondents are also concerned with the potential dangers posed by using robotics in OT, with **a third stating that increased use will lead to cyberattacks that can cause physical harm or death.** This is not an insignificant data point, revealing the perceived physical threat that can be posed by the digital world, regardless of whether this could actualize.

Certainly, human error has accounted for physical incidents on countless occasions in industrial environments, and the fear that adding a digital element could lead to purposeful manipulation is not a far leap. The fear is rooted in the fact that cyber physical systems, industrial robotic platforms, and autonomous systems can be subject to tampering, jamming, Distributed Denial of Service (DDoS), ransomware, or any other number of cyberthreats that could dangerously impact their operation.

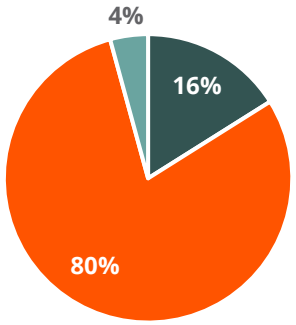
Increased use of robotics in OT environments will lead to cyberattacks that cause physical harm or death.



Remote Access of internal employees and 3rd parties into OT will continue to increase.



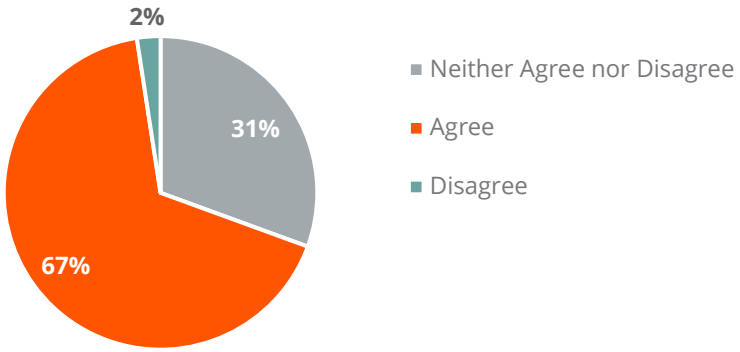
Cloud-based architecture will be critical for OT in the next 3-5 years.



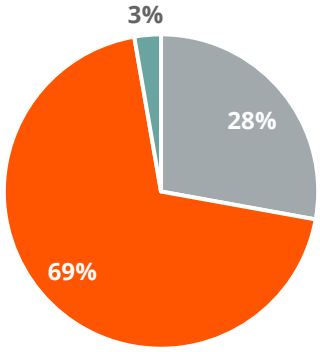
The use of robotics will require some form of connectivity for access. This will likely be served as much through Internet Protocol (IP) connectivity as through cellular, and notably 5G. **Among the respondents, 67% identified 5G technology investment happening for their OT environment. In parallel, 70% also recognized that 5G-connected devices are increasingly important OT threat vectors.**

It is important to highlight that **5G brings new dimensions to OT environments that did not exist before**. Firstly, 5G significantly expands the connectivity of OT assets (and notably the Industrial IoT (IIoT), but also offers dangerous potential for DDoS and other attacks. Numerous exploits against IIoT are published each year by security researchers at conferences such as Black Hat and DEFCON, but numerous malware variants are also out there in the wild. 5G connectivity is likely to accelerate targeted attacks, as Industrial Control System (ICS) assets become visible to the world. The second dimension is the software-defined focus of 5G, which will allow the migration of existing IT-based threats to the 5G core itself and the extended network.

My organization will be investing in 5G technology for my OT environment.



5G connected devices are an increasingly important OT threat vector.



Emerging and connected technologies are undoubtedly set to play an important role in OT environments, which is recognized by the large majority of respondents, irrespective of region and end market. Beyond that, there is clear apprehension as to the risks these will usher in, and a lack of deeper understanding is likely to preoccupy more than appease industrial operators.

Regardless, the advent of new technologies is set to permeate OT, and operators need to ready themselves for the inevitable change that these will bring. In many cases, they are already negotiating how such technologies will be rolled out and managed securely.

Insights from Industrial Operators

"Review and upgrade network design on a regular basis."
"Hold frequent meetings to evaluate security policies."

MOVING FORWARD WITH OT SECURITY

The role of cybersecurity within OT environments is visibly high on industrial operators' agendas. Moving forward, the exercise is for them to understand what types of security solutions will work best and how to implement them accordingly within OT.

While there are plenty of available cybersecurity technologies, part of the solution must focus on the need to eliminate inherent trust and preconceptions that threat actors cannot reach legacy or air-gapped systems. Another part is to address the coordination issue between IT and OT, ensuring that there is comprehensive integration and decision-making on security between the two groups.

ZERO TRUST: AN ANSWER TO THE TRUST PROBLEM

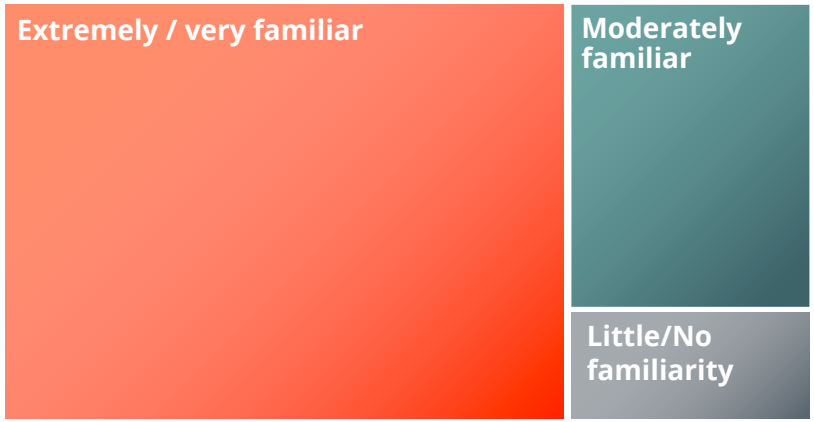
The issue of inherent trust in OT environments that are increasingly connected and open can be solved with the adoption of Zero Trust principles. No asset is trusted by default, requiring trust to be established each and every time using identity, access control, and authentication mechanisms on a continual basis.

Deploying Zero Trust is already top of respondents' minds, with 93% already familiar with the technology and 87% believing it to be the right fit for protecting OT environments.

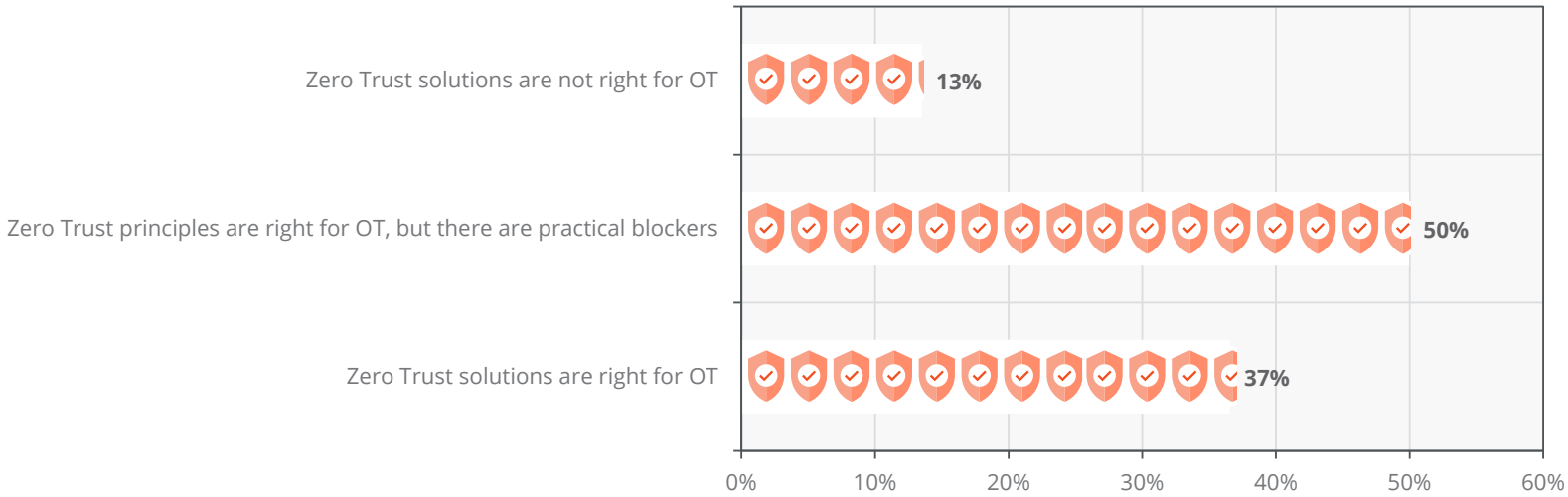
However, **50% state that there are practical blockers to implementation.** These can include policy control and configuration issues for legacy devices, or the default methods contractors and industrial Original Equipment Manufacturers (OEMs) access ICSs. Overcoming the practical blockers in the face of Zero Turst can be costly and time-consuming, utilizing resources that could potentially be used elsewhere. Nonetheless, the belief is evident among respondents that Zero Trust is the right answer to OT cybersecurity.

Consequently, industrial operators are likely to place a lot of emphasis on cybersecurity vendors offering a Zero Trust solution that can address these issues and provide high levels of customer support.

How familiar are you with Zero Trust?



Do you believe Zero Trust principles are the correct approach for protecting OT environments?



Insights from Industrial Operators

"Get a reliable mechanism for managing access and identification."
"Examine network segmentation for isolating OT cybersecurity devices."
"Integrate a Zero Trust network architecture into your operational technology systems."

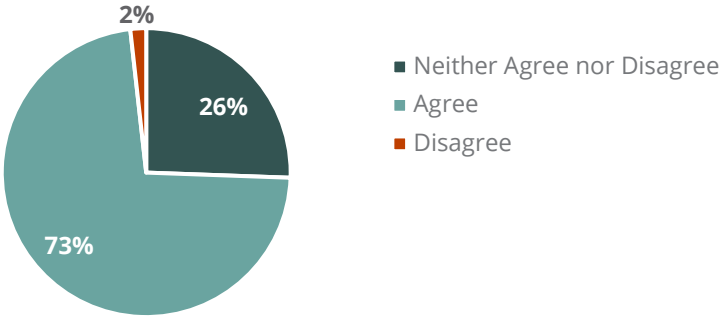
OT AND IT CONSOLIDATION ON THE HORIZON

In order to effectively implement Zero Trust and tackle challenges related to its implementation, there is a requirement to ensure an integrated response from the industrial operator, and this means better consolidation between IT and OT groups.

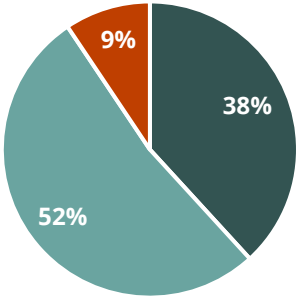
This understanding is reflected in the survey, with more than 70% of respondents clear on their intention to consolidate IT and OT solutions from the same cybersecurity vendor. In a similar vein, more than half of the respondents stated their intent to use the same Managed Security Service Provider (MSSP) for both OT and IT security.

For both questions, a third of respondents neither agreed nor disagreed with the statements, revealing that there was still an important segment of industrial operators that were undecided on how to proceed with IT and OT security integration. This shows that there are challenges in deploying OT security effectively as an integrated solution alongside IT security. This can not only be attributed to the difficulties in cooperation between IT and OT teams, but also to the complexity of available security solutions that may not easily cater to both IT and OT scenarios.

We intend to consolidate around solutions provided by cybersecurity technology vendors who also have OT security solutions.



We intend to use the same MSSP for OT and IT security.



Regardless, **79% of respondents agreed that, in the long term, OT and IT security would be seamlessly integrated and managed by the same solutions.**

This is a clear indication that OT security is as important to industrial operators as IT security, and that the two worlds are rapidly converging, both in terms of operation and in terms of protection.

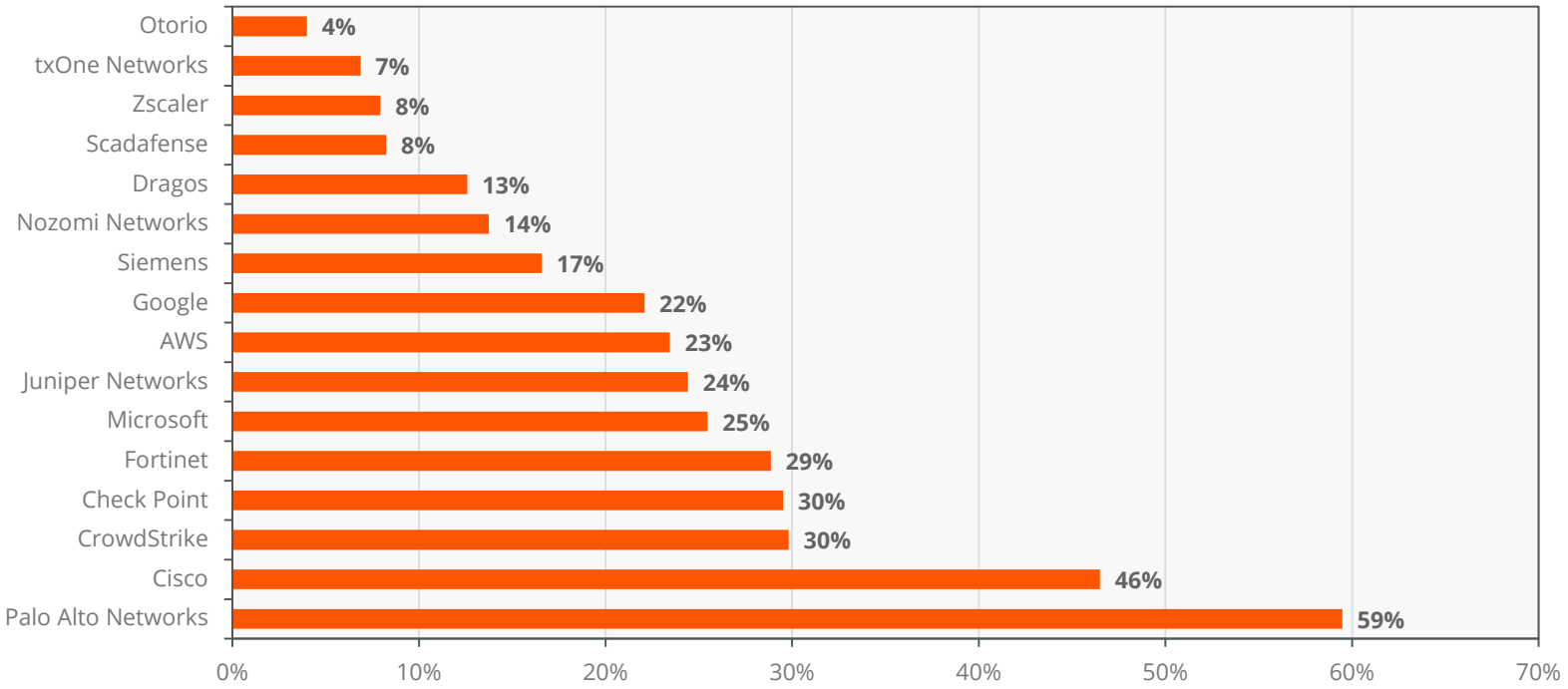
This is already happening outside of the security sphere, with digital transformation accelerating within industrial end markets. It goes without saying that security should, and will, follow closely.

In the long term, OT security and IT security will be seamlessly integrated and managed by the same solutions/applications.

CHOOSING THE RIGHT PROVIDER

The demand for cybersecurity vendors proficient in both IT and OT security is already a reality. The survey supports this, revealing that in the respondents' choice of cybersecurity solutions, there was a clear preference for vendors experienced in both areas. All of the top five vendors identified by the respondents offered both IT and OT security solutions, with Palo Alto Networks leading the pack by a fair margin.

Is a leading supplier - Which of the following vendors do you consider to be credible OT cybersecurity technology suppliers and/or leaders?



PALO ALTO NETWORKS PROMISE

Zero Trust OT Security by Palo Alto Networks is tailored for industrial asset owners and operators, offering comprehensive visibility and security for OT environments. Extending its protective capabilities from OT networks and assets, to encompass 5G-connected assets and remote operations, Palo Alto Networks addresses the evolving challenges inherent in modern industrial environments. By leveraging Zero Trust principles, organizations can strengthen their OT environments against potential threats while maintaining operational continuity and resilience.

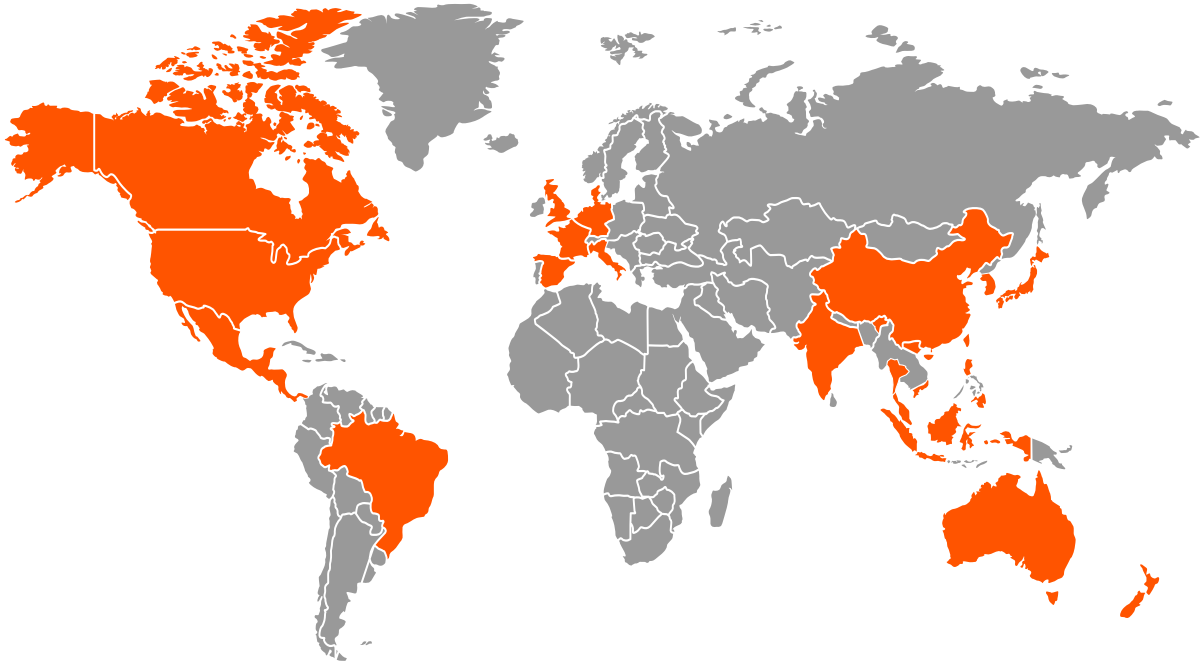
With Zero Trust OT Security, organizations gain accurate, context-rich visibility of all assets, applications, and users, enabling them to assess and prevent OT/ICS threats effectively, and helping simplify security and operations with a unified platform from a single vendor. It can be adapted to fit various architectures, from partially air-gapped to fully cloud-connected environments, providing a seamless security solution for industrial environments.

TOP FIVE LESSONS LEARNED BY INDUSTRIAL OPERATORS

1. Have a cybersecurity plan and supporting policies in place for all your operational aspects (people, processes, and technology) and revise these continuously, on a regular basis.
2. Communicate and collaborate on security best practices and around threat information, internally between your various teams, and externally with industry stakeholders.
3. Focus on identification, authentication, and access control mechanisms; this includes better OT asset and inventory management. Know what you have and do not implicitly trust anything. Aspire to Zero Trust, and look for security solutions that can address both IT and OT.
4. Plan for failure; ensure you have incident response plans, backup, and recovery procedures in place. Be ready to react quickly to any adverse event.
5. Enhance the security of the supply chain; perform better security assurance checks of your contractors and third parties and reevaluate them frequently.

METHODOLOGY

The survey was fielded in December 2023, representing 1,979 respondents from a sample base across the following countries:



The survey consisted of 37 objective questions, along with two open-ended qualitative questions for which respondents had the opportunity to write their answers. Those opting for non-English were translated. The questions addressed major topics in the OT space, spanning the main perceived threats by respondents, their investment objectives, and their OT cybersecurity provider preferences.

The survey questions were cross-tabulated accordingly to identify the main trends based on a variety of factors, including, but not limited to, company size, industry vertical, organizational role of respondents, and cybersecurity vendor deployment. Respondents primarily had roles in OT (37.5%), IT (41.5%), or both (21%). C-level executives, senior managers, and team leaders made up 78.6% of the respondents.

More than 54.3 % of respondents were from companies with 1,000 to 5,000 personnel and the rest were organizations with more than 5,000 personnel and individual practitioners of cybersecurity at industrial organizations.

UNITED STATES	**302**
CANADA	**102**
UNITED KINGDOM	**102**
FRANCE	**101**
GERMANY	**102**
ITALY	**100**
SPAIN	**100**
MEXICO	**50**
BRAZIL	**50**
JAPAN	**103**
SINGAPORE	**101**
INDIA	**103**
AUSTRALIA	**103**
NEW ZEALAND	**50**
THAILAND	**51**
PHILIPPINES	**51**
INDONESIA	**51**
MALAYSIA	**51**
VIETNAM	**51**
CHINA	**102**
HONG KONG	**51**
TAIWAN	**51**
SOUTH KOREA	**51**

ABOUT PALO ALTO NETWORKS

Palo Alto Networks, the global cybersecurity leader, is shaping the future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation to enable secure digital transformation. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across industries, clouds, networks, and devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

ABOUT ABI RESEARCH

ABI Research is a global technology intelligence firm uniquely positioned at the intersection of technology solution providers and end-market companies. We serve as the bridge that seamlessly connects these two segments by providing exclusive research and expert guidance to drive successful technology implementations and deliver strategies proven to attract and retain customers.

157 Columbus Avenue
New York, NY 10023 USA
Tel: +1 516-624-2500
www.abiresearch.com