REPORT

2024 State of Operational Technology and Cybersecurity Report

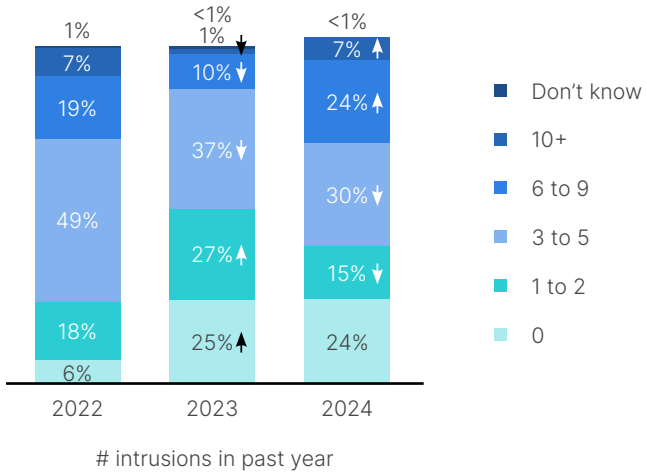
FORTINET

Table of Contents

Key Takeaways

Cybersecurity incidents

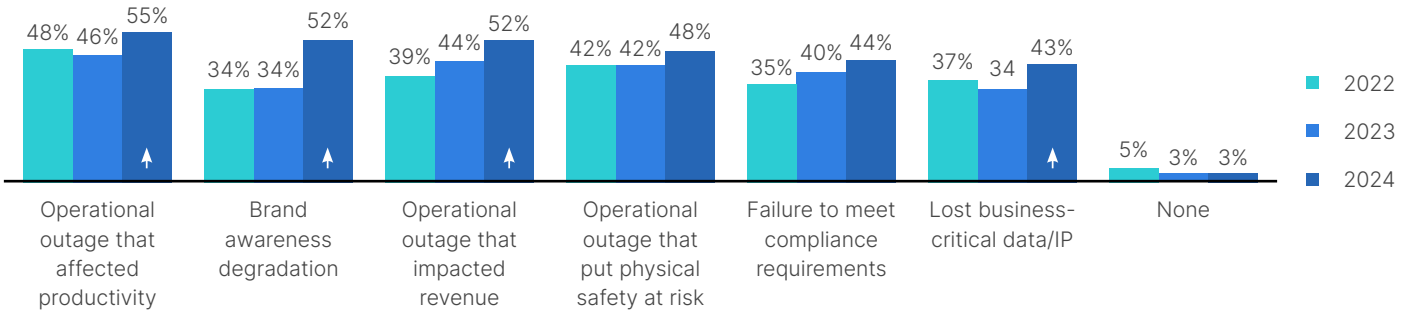
Nearly one-third (31%) of respondents reported 6+ intrusions, compared to only 11% last year. In particular, organizations with advanced maturity levels reported high intrusions for this cycle. **All intrusion types increased** compared to the previous year, except for a decline seen in malware. Phishing and compromised business email intrusions were the most common types, while the most common techniques used were mobile security breaches and web compromise.



intrusions in past year

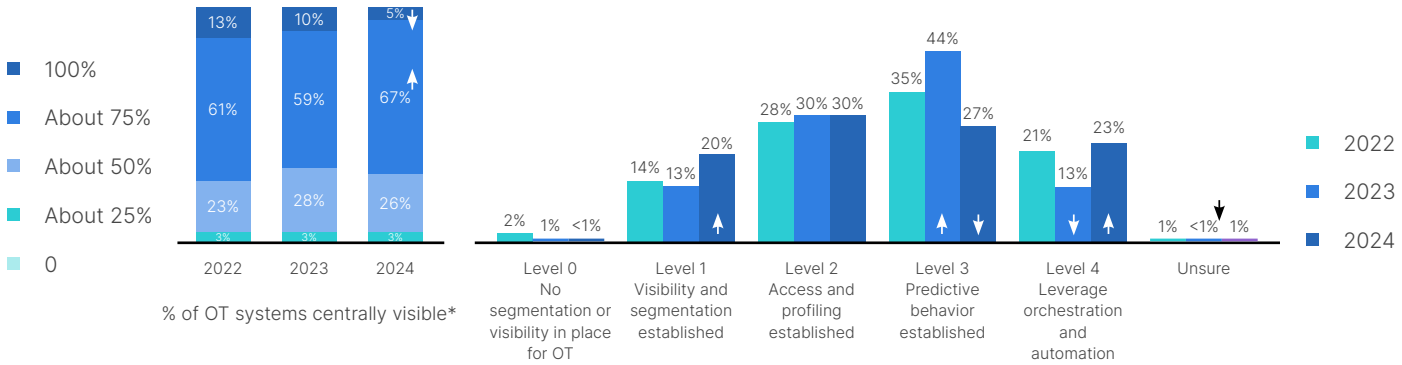
The impact of intrusions

The negative effects caused by an OT intrusion are also getting worse across the board in all impact categories. More than half of respondents (52%) saw a steep increase in **degradation of brand awareness,** up from only 34% in 2023. **Loss of business-critical data and productivity** was another notable trend (increasing from 34% to 43% year-over-year).



How OT factors into cybersecurity

There has been a significant **decrease in organizations reporting 100% visibility of OT activities** within central cybersecurity operations (from 13% in 2022 to 10% in 2023 to only 5% this year). This is perhaps because as an organization's OT security posture becomes more mature, it becomes more aware of blind spots in its visibility. This year's survey also shows that there have been **increases at both ends of the maturity spectrum**, at the basic level (establishing visibility and segmentation) and at the highest level (leveraging orchestration and automation capabilities).

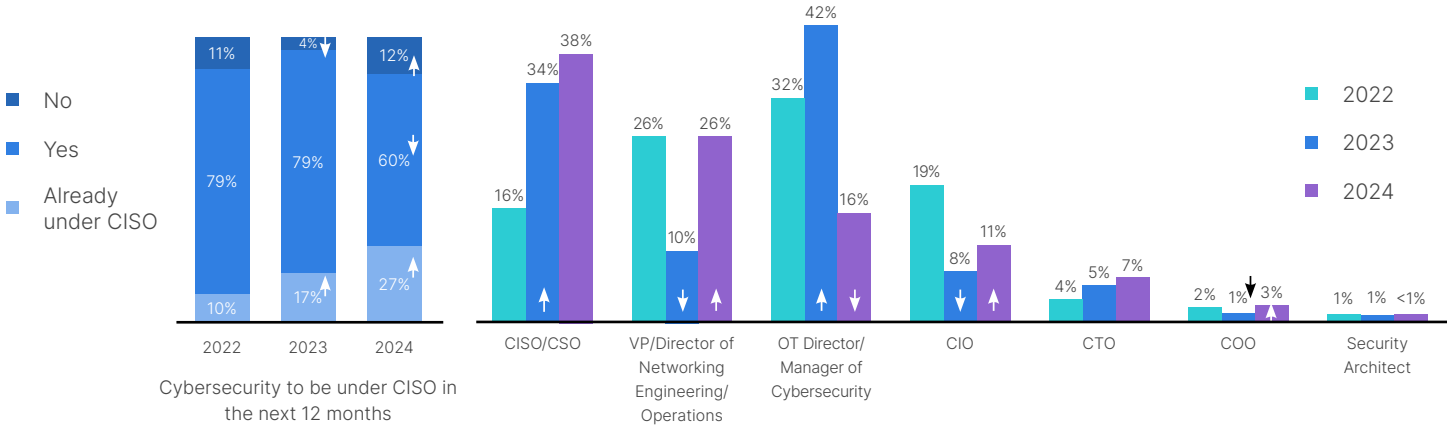


Maturity of OT security posture

People

Another clear sign of increasing maturity comes from steady growth in **organizations that have already rolled OT security under a CISO**, from only 10% in 2022 to 17% in 2023 to 27% this year. At the same time, we saw a reversal of last year's trend with organizations that were not planning to move OT security under the CISO in the next 12 months, which went from 11% in 2022 down to 4% last year, but back up to 12% in 2024.

This year's findings also show that the ultimate responsibility for OT cybersecurity is moving away from the OT director of cybersecurity in favor of a **VP/director of networking engineering/operations** role. This elevation into the executive ranks may suggest that OT security is becoming a higher-profile topic at the board level.



Executive Summary

This year marks our sixth edition of the *Fortinet State of Operational Technology and Cybersecurity Report*. The 2024 study is based on comprehensive data from a global survey of more than 550 OT professionals conducted by a respected third-party research company.

As OT organizations introduce new digital tools and technologies to their environments, their security challenges have grown more complex. As NIST notes, "While security solutions have been designed to deal with these issues in typical IT systems, special precautions must be taken when introducing these same solutions to OT environments. In some cases, new security solutions that are tailored to the OT environment are needed."[1]

This year's report shows that some progress has been made over the last 12 months in OT security posture and investment in essential tools and capabilities. But there's more work to be done to effectively manage an increasing number of attacks in a post-IT/OT convergence world. Three notable trends emerged from our 2024 survey responses:

- Intrusions and their impacts on organizations have worsened over the past year.
- Responsibility for OT cybersecurity is elevating within executive leadership ranks.
- OT security postures are maturing in key areas, but this remains a work in progress.

The critical insights and deeper analysis of these findings expose the dynamic and sometimes mercurial nature of managing OT risks. Considering these specific challenges, this year's report also offers some current best practices and tips for improving your organization's OT security posture.

Introduction

Threats to OT systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, malicious intruders, complexities, natural disasters, malicious actions by insiders, and unintentional actions such as human error or failure to follow established policies and procedures.[2]

Sensitive OT systems were not designed for today's digital world. They were built for a time and place where they could safely do their thing in relative isolation. As the world changed around them, adopting transformative digital tools brought new conveniences and capabilities, along with all the cybersecurity risks that come with increased network connectivity.

As the *2024 State of Operational Technology and Cybersecurity Report* shows, some of the positive gains highlighted in the previous year can slip away in just a few short months.

Endemic risks to OT

This year's survey respondents confirm media reports that OT attacks are on the rise.[3] According to the most recent *Global Threat Landscape Report* from Fortinet, attacks targeting industrial control systems (ICS) and OT were already trending up in the second half of last year, with half of organizations reporting exploits (energy and utilities were top targets).[4]

Organizations cannot afford to forget that OT systems present extremely attractive targets for attackers. Effective protection requires constant vigilance and resource allocation. A rise in intrusions and worsened impacts of attacks offer a clear sign to maturing organizations that their OT systems are not completely visible within the organization's central cybersecurity operations.

For certain industry sectors, such as manufacturing, organizations have been more willing to pay requested ransoms, and the amount requested has also been typically higher. In 25% of breaches among manufacturing companies, the demanded ransom was $1 million or higher.[5] Greater willingness to pay is understandable, given that the cost of downtime for manufacturers is typically very high.

Detection methods aren't measuring up

The *Global Threat Landscape Report* also showed that fewer organizations are successfully detecting ransomware than in the past (13% versus 22%), reaffirming that ransomware is becoming more sophisticated and targeted.[6] Our 2024 survey findings align with this research, as 56% of respondents experienced ransomware/wiper intrusions, which was a sharp increase from only 32% in 2023.

While respondents state that cybersecurity metrics are increasingly being monitored and reported, these measurements have not helped with intrusion detection and remediation. Organizations also seem to be performing fewer penetration and intrusion tests this year, perhaps as a cost-saving measure.

Protecting OT systems remains the goal

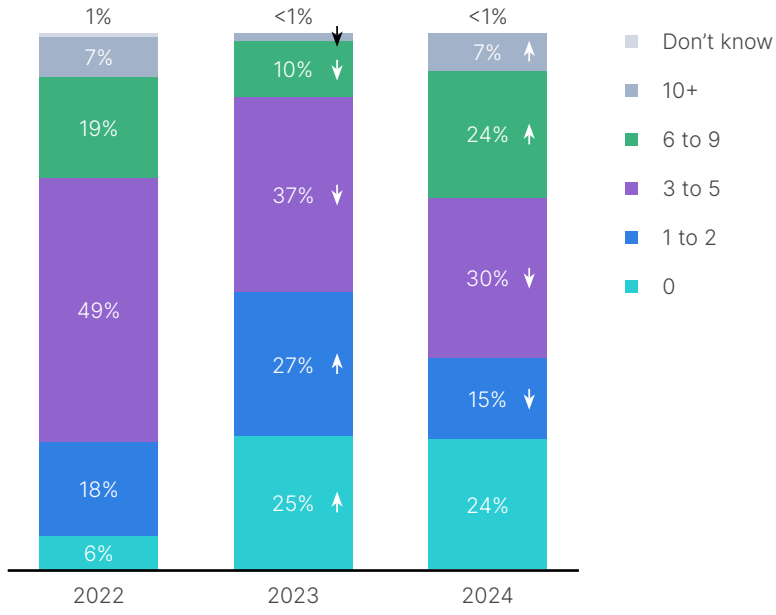
Last year's report expressed hope that one of the headlines in 2024 would be about the significant progress being made toward protecting OT systems. The sharp rise in reported intrusions means that we will have to put that hope aside for another year.

The following critical insights, deep dive trend analysis, and best practice recommendations can serve as a guide for making meaningful improvements to OT protections over the coming months.

Critical Insights for OT Security

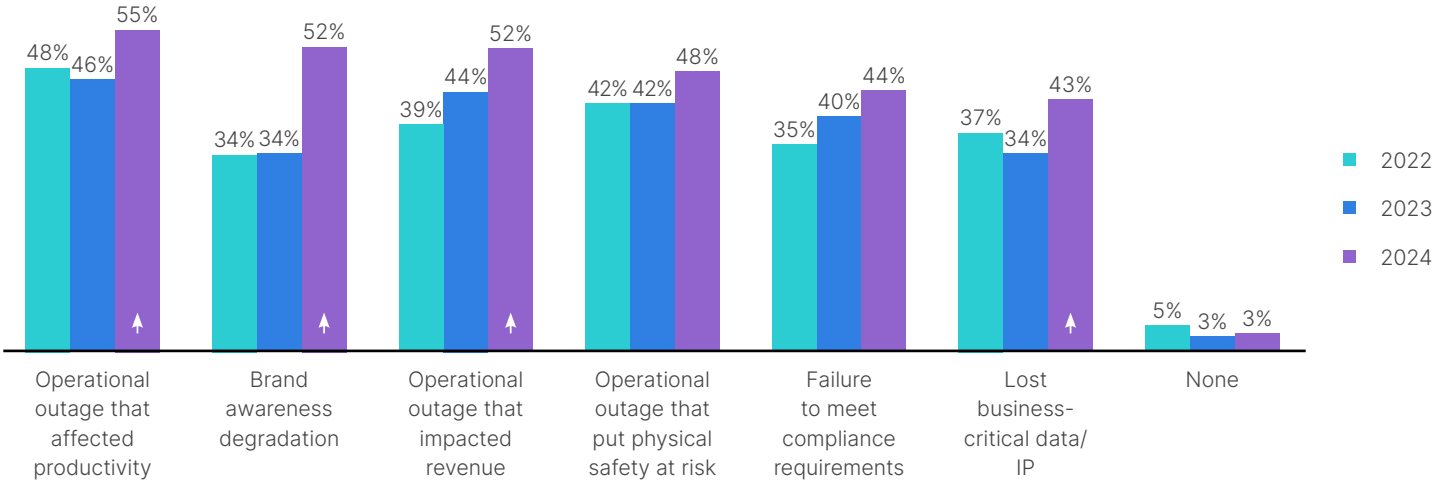
Critical insight #1: Organizations saw more intrusions and worsened impacts

The most significant insight from this year's findings is that more organizations are experiencing high numbers of intrusions. Nearly one-third of respondents had six or more intrusions, up from only 11% in 2023. It was also notable that all types of intrusions increased, except malware.



Q: How many intrusions has your organization experienced in the past year?

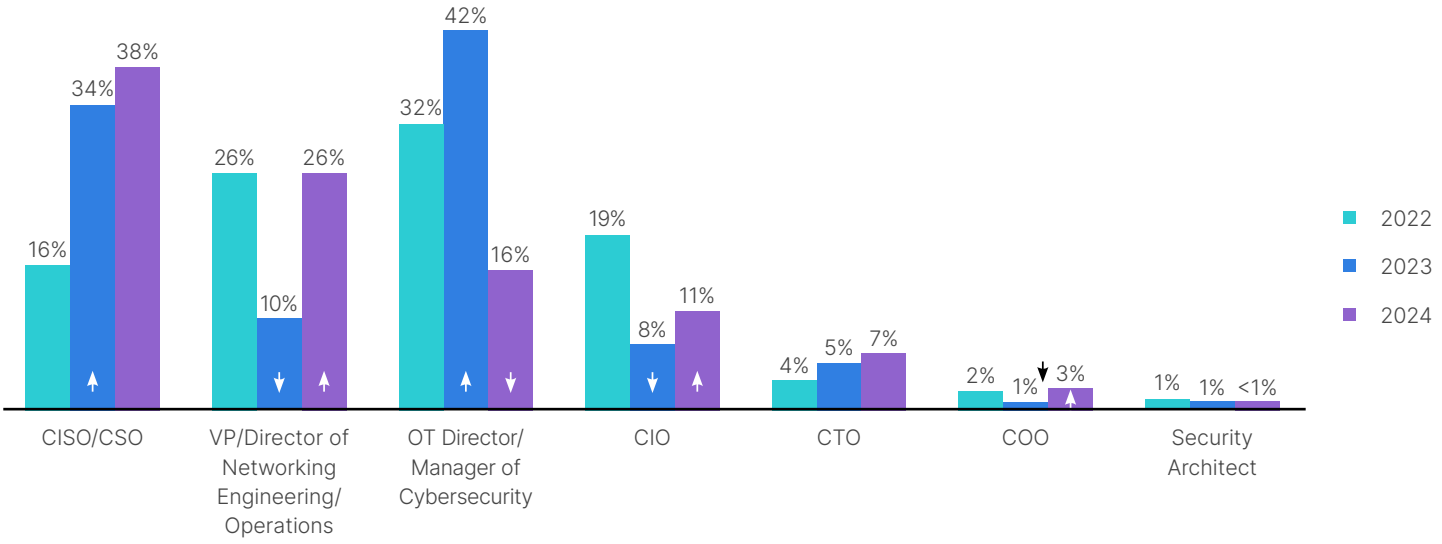
The subsequent impacts of intrusions have also gotten worse for organizations. More respondents reported degradation of brand awareness due to a successful attack. Many regulations, such as the Cybersecurity Incident Disclosure Provision by the U.S. Securities and Exchange Commission, now require timely public announcement of breaches.[7] Findings also showed that more organizations lost business-critical data and decreased productivity as a direct result of a breach incident.



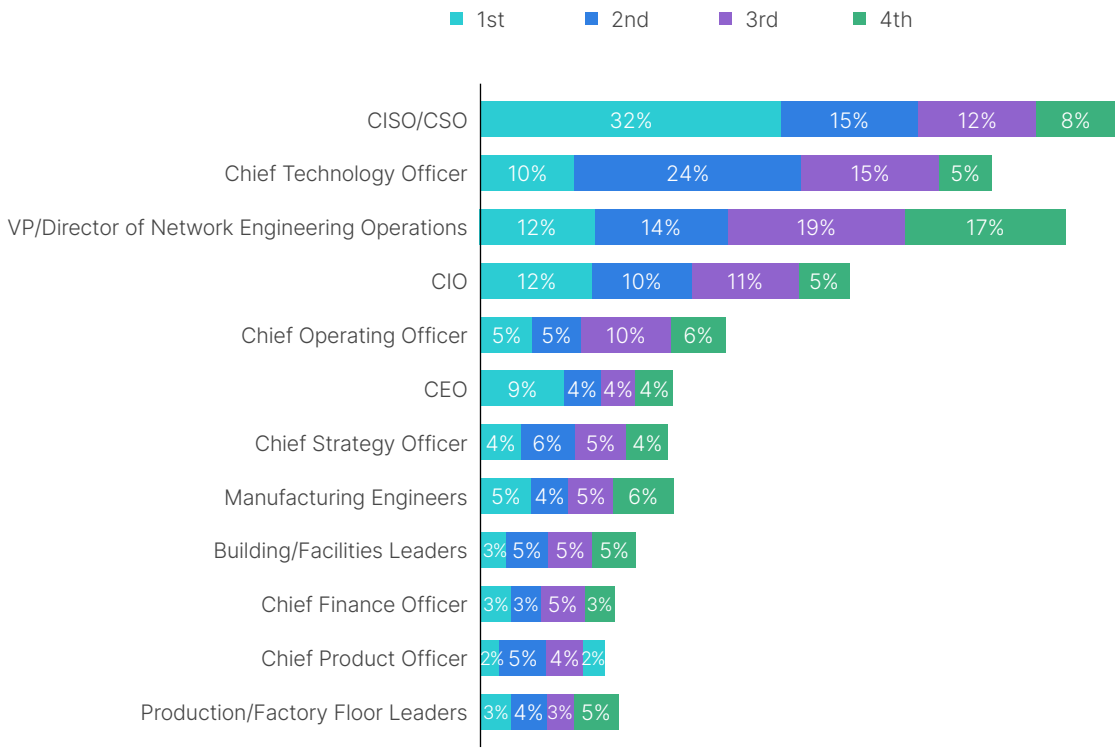
Q: What impact did the intrusion(s) have on your organization?

Critical insight #2: Responsibility for OT security is elevating

Management responsibilities for OT cybersecurity are shifting away from the OT director of cybersecurity toward the VP/director of networking engineering/operations and CISO. With accountability shifting up the food chain into executive leadership, OT security becomes a higher-profile issue at the board level. We're also seeing an interesting shift in the top internal leaders that influence cybersecurity decisions away from the CIO in favor of the CISO/CSO, CTO, and VP/director of network engineering operations.



Q: Who is ultimately responsible for OT cybersecurity?



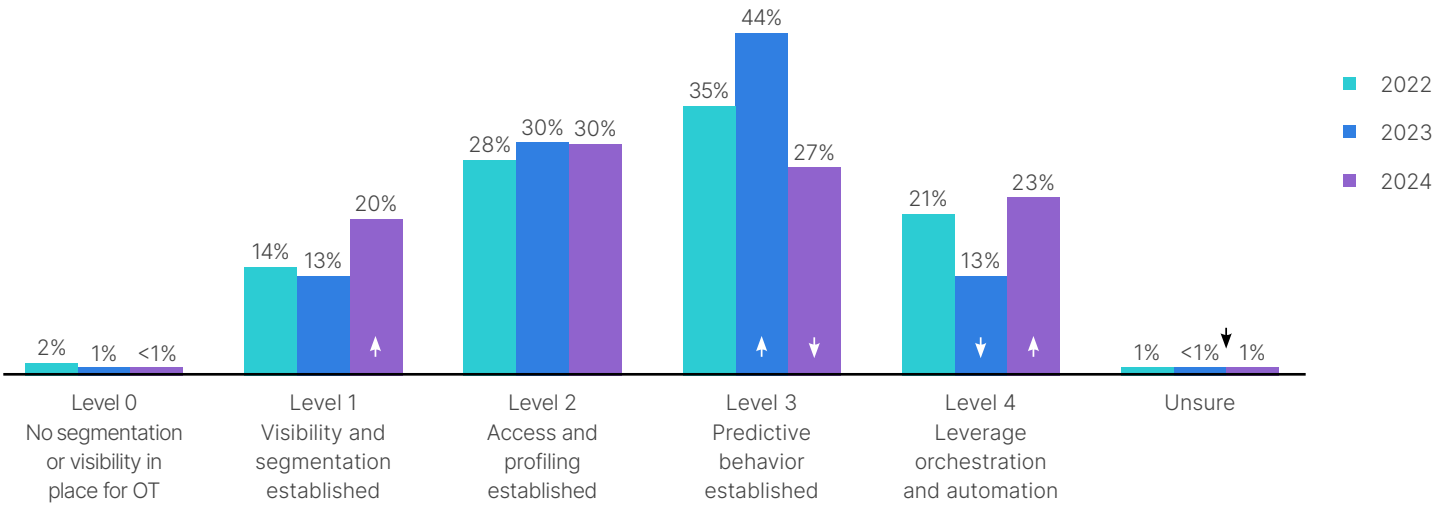
	2022	2023	2024
CISO/CSO	32%	59% ↑	**58%**
Chief Technology Officer	34%	45% ↑	**48%**
VP/Director of Network Engineering Operations	33%	40% ↑	**45%**
CIO	21%	41% ↑	**34%** ↓
Chief Operating Officer	24%	17% ↓	**20%**
CEO	22%	23%	**16%** ↓
Chief Strategy Officer	17%	14%	**15%**
Manufacturing Engineers	22%	10% ↓	**14%**
Building/Facilities Leaders	15%	10% ↓	**12%**
Chief Finance Officer	19%	8% ↓	**11%**
Chief Product Officer	15%	9% ↓	**11%**
Production/Factory Floor Leaders	21%	13% ↓	**10%**

% in top three

Q: Which internal leaders influence your cybersecurity decisions? (rank up to four)

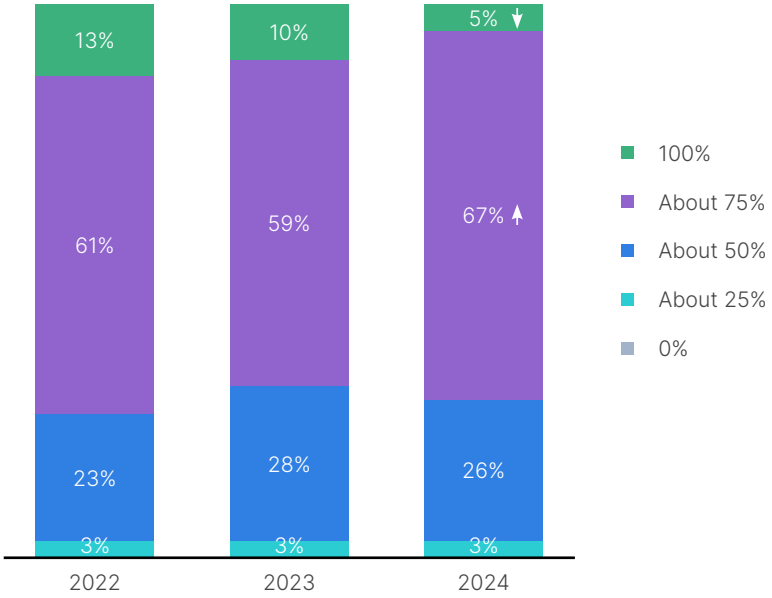
Critical insight #3: OT cybersecurity postures are maturing

IT infrastructure has had a massive head start on OT systems when implementing effective cybersecurity measures. But OT security posture shows notable progress on both ends of the mature technologies spectrum. At the most basic level, 20% of organizations report establishing visibility and implementing segmentation, up from only 13% in the previous year. The highest level of security posture maturity (leveraging orchestration and automation capabilities) also showed year-over-year growth, from 13% to 23%.



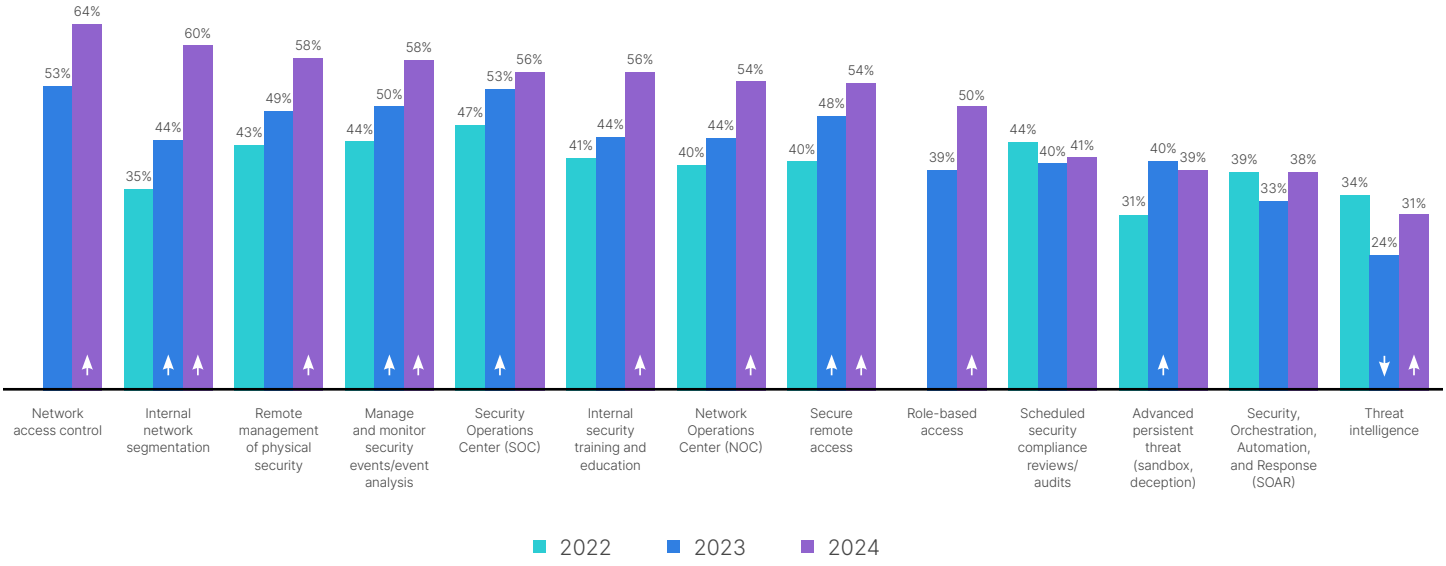
Q: How would you characterize the maturity of your OT security posture?

Fewer respondents claimed that their organization has 100% OT systems visibility within their central cybersecurity operations, which has decreased since last year (from 10% to 5%), while those reporting about 75% visibility increased. This adjusted confidence in visibility may also indicate advancing OT security maturity, in that organizations are gaining a more realistic understanding of their posture, even if it's that "they don't know what they don't know." As many organizations investigated the spike in security incidents over the last year, they likely discovered blind spots in their infrastructure.



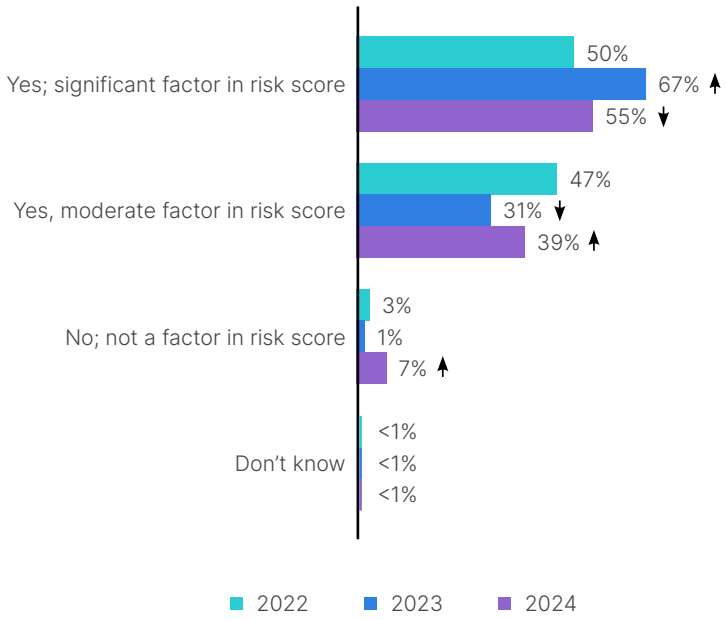
Q: What percentage of your OT systems are visible within your organization's central cybersecurity operations?

OT professionals continue to expand the array of cybersecurity features and protocols they utilize. Internal network segmentation, internal security training and education, and role-based access are the areas that show the most significant growth this year. While these investments signify progress, the sharp rise in successful intrusions this year underscores that more needs to be done to keep pace with the escalating volume of targeted attacks against OT.



Q: What cybersecurity and security features do you have in place today?

One of the more troubling maturity trends shows a regression in how OT systems figure into broader risk calculations. Respondents say that their OT security posture is becoming less influential in determining their organization's overall risk score. Most notably, there was a significant year-over-year jump in respondents reporting that OT is "not a factor" in risk scoring, from only 1% in 2023 to 7% in 2024.



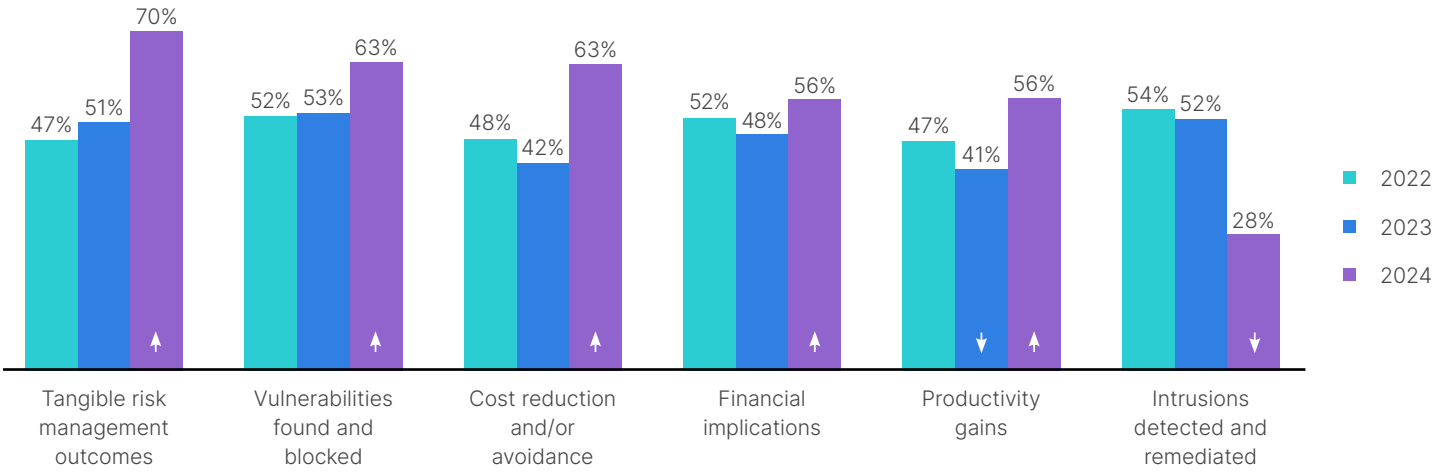
Q: Is the cybersecurity posture of OT included in the broader risk score that is shared with executive leadership and the board of directors?

Deep Dive into the 2024 Survey

Q: What cybersecurity measurements do you track and report?

Organizations are increasingly monitoring and reporting a diverse range of cybersecurity metrics. However, one notable exception was a steep decline in tracking intrusions detected and remediated, from 52% in 2023 to only 28% in 2024.

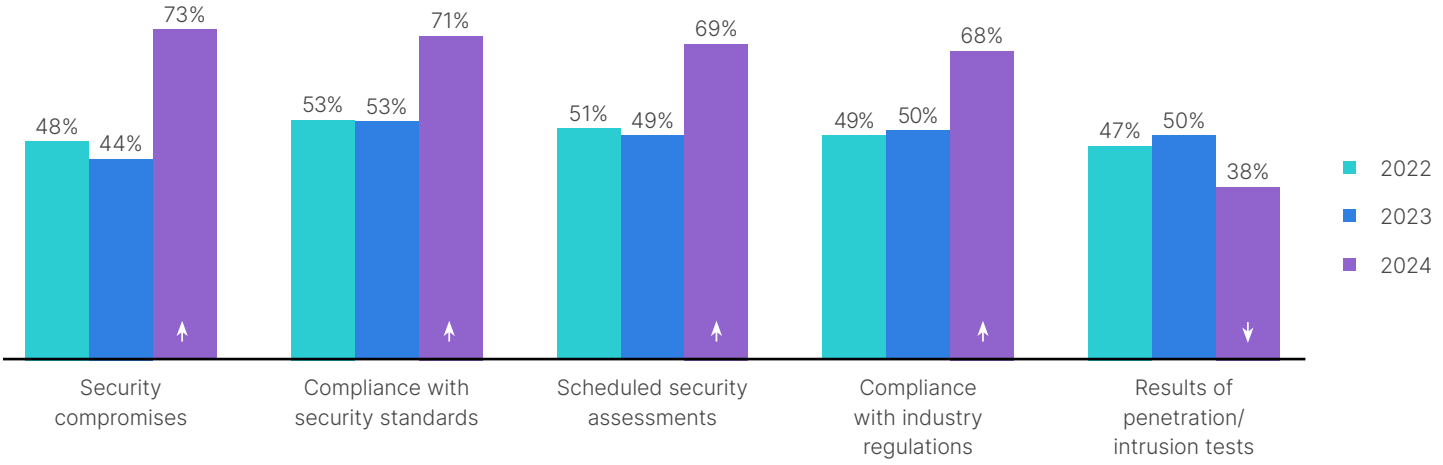
Combined with the reality that intrusions affecting OT increased this year, this disparity between increased tracking of cybersecurity measurements and worsened detection of actual intrusions may suggest that metrics may create a false sense of confidence.



Q: What OT cybersecurity issues are reported to senior/executive leadership?

The practice of keeping senior leadership informed has increased considerably for nearly all OT cybersecurity issues, including compromises, scheduled assessments, and compliance requirements.

One exception is that there has been a shift away from reporting the results of penetration and intrusion tests. These kinds of tests tend to be both expensive and involved; organizations may be investing less in this area in favor of increased cybersecurity metrics to determine their security posture.

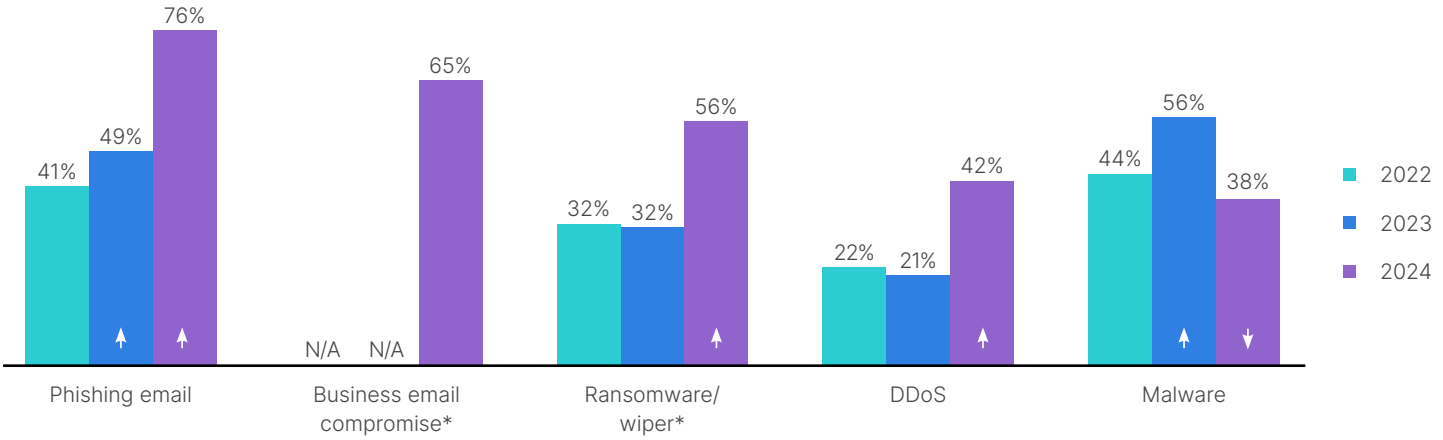


Q: What types of intrusions were experienced?

As noted in the Critical Insights section, respondents reported a significant rise in intrusions this year. When asked about the specific causes behind these events, the biggest year-over-year increase was seen in phishing emails, a jump from 49% to 76%. The survey included a new category in 2024 for business email compromise, which also was a top intrusion type (seen at nearly two-thirds of all organizations).

In addition, ransomware and wiper intrusions saw a spike in activity, rising from about one-third of respondents in 2023 to over half in 2024. As FortiGuard Labs recently reported, ransomware volume isn't slowing down, with threat actors using more sophisticated and complex strains to infiltrate networks, largely thanks to the expansion of Ransomware-as-a-Service.[8]

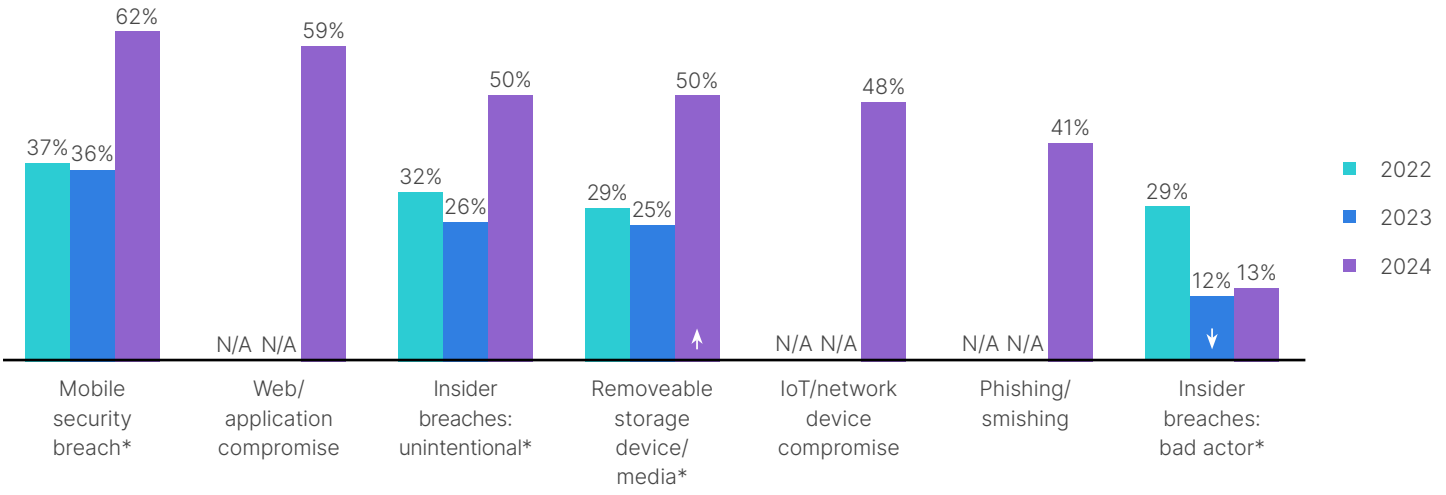
Findings also show that DDoS intrusions have doubled since last year. The only category that saw a decline was malware.



**Changes in the 2024 survey: "Ransomware" was updated to "Ransomware/wiper." A new category for "Business email compromise" was added. Categories for "Targeted Attack," Mobile Security breach," "Removable storage device/media," "Insider Breaches: Unintentional," and "Insider Breaches: Bad actor" were removed or moved to new questions.*

Q: What techniques were involved in the intrusion?

We made some adjustments to the survey questions this year to better separate techniques used by attackers from the type of intrusion. The findings show that multiple techniques were involved in the intrusions. Mobile security breaches and web compromises ranked highest, while insider breaches by bad actors were among the least common.

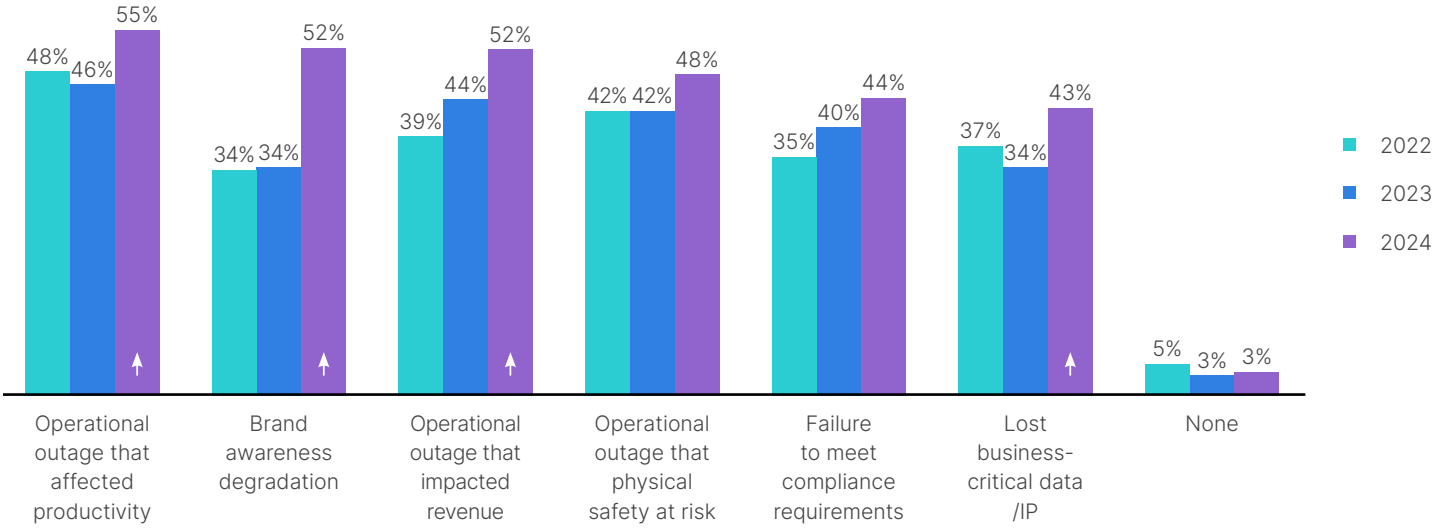


**Before 2024, these answers were part of "What types of intrusions were experienced?"*

Q: What impact did the intrusion(s) have on your organization?

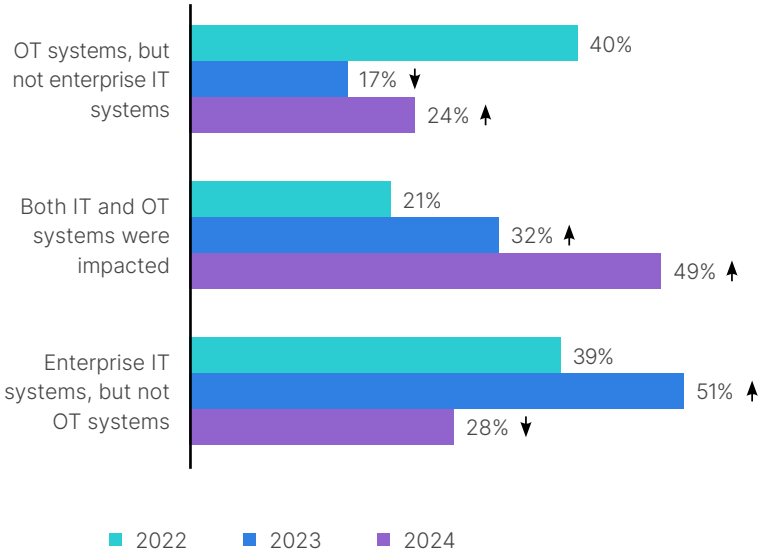
On top of higher numbers of reported intrusions this year, the negative impacts that organizations experience due to an intrusion have also risen across the board. Findings show that the largest increases were in the degradation of brand awareness, jumping from about one-third to over one-half of organizations year-over-year. As regulatory obligations generally require public disclosure of breaches, the reputational effects can be unavoidable. Negative publicity may eventually reduce customer retention and revenue growth.[9]

Operational outages that reduced productivity also affected more than half (55%) of organizations. Reported loss of business-critical data or intellectual property (IP) rose from 34% to 43% in 2024.



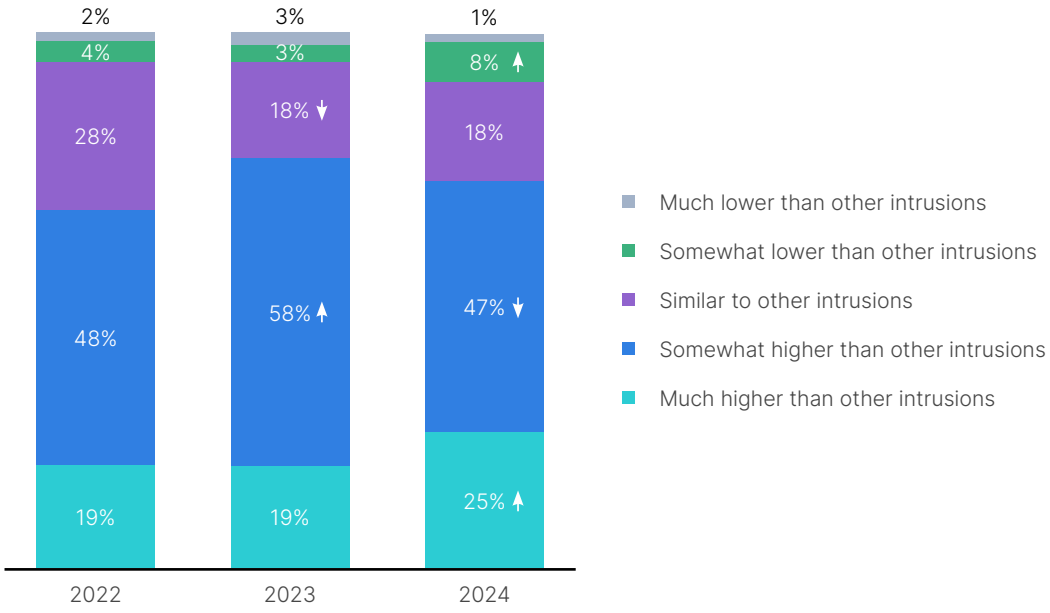
Q: Which of your environments have been impacted by cybersecurity intrusions in the past year?

The trend of intrusions increasingly impacting OT systems in some way continues to rise. In 2023, 49% of respondents experienced an intrusion that impacted either OT systems only or both IT and OT systems. But this year, nearly three-fourths (73%) of organizations are being impacted. We also saw a year-over-year increase in intrusions that only impacted OT systems (from 17% to 24%).



Q: Compared to other intrusions, how concerned are you about ransomware's impact to your OT environment?

Those who are "much more concerned" about ransomware's impact on their environment versus other types of intrusions rose from 19% in 2022 and 2023 to 25% in 2024. However, the total percentage of respondents with higher concern about ransomware (those with "much higher" plus those with "somewhat higher" levels of concern) decreased slightly from 77% to 72% year-over-year.

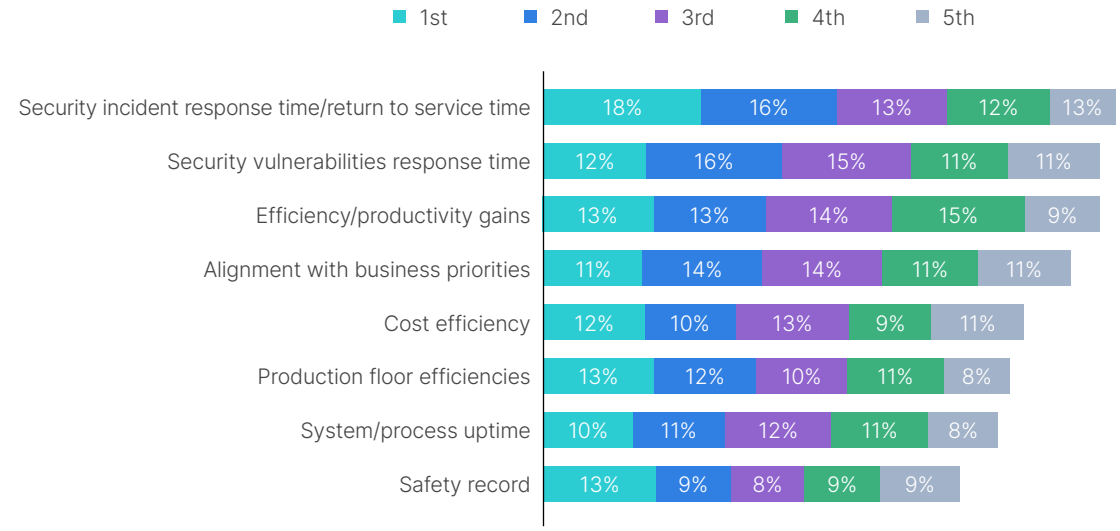


Global Impact

Q: How is your success measured? (rank up to five)

Organizations measure their success in several ways, but "response time to security incidents/return-to-service time" was the top answer overall, and nearly half (46%) of respondents ranked this as a top-three success factor. It's worth highlighting that companies are measuring success based on recovery.

Whether this speaks to their desire to not pay ransoms in favor of restoring systems as a path toward recovery or paying them quickly with the hope that attackers will actually allow them to resume operations, embracing readiness to recover from incidents is a notable insight. Many businesses find that cyber resilience, ensuring they can quickly respond to inevitable attacks by getting systems back up and running with minimal disruption, is a more realistic goal for their success.[10]



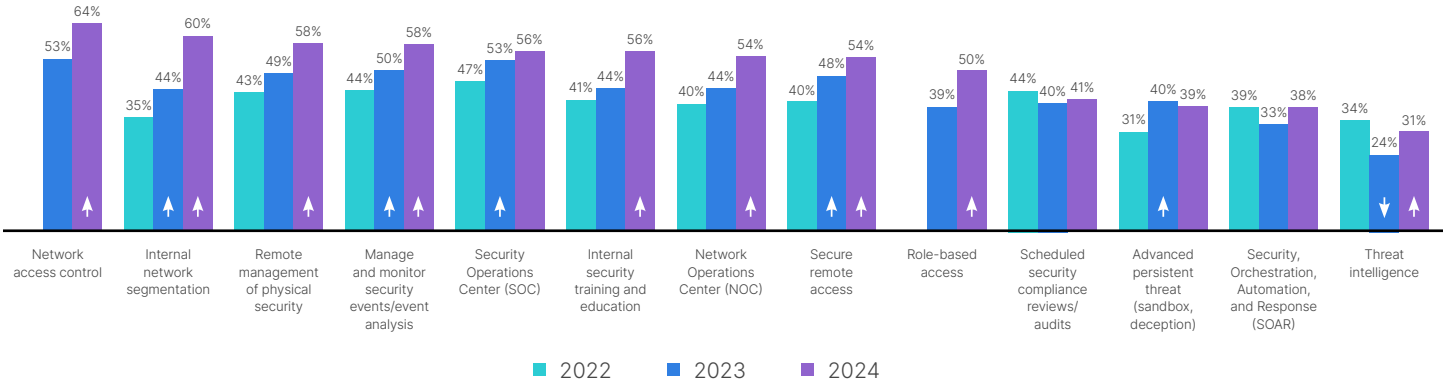
	2022	2023	**2024**
Security incident response time/return to service time	35%	41%	**46%**
Security vulnerabilities response time	33%	45% ↑	**42%**
Efficiency/productivity gains	43%	42%	**40%**
Alignment with business priorities	33%	36%	**39%**
Cost efficiency	39%	35%	**35%**
Production floor efficiencies	33%	31%	**35%**
System/process uptime	34%	36%	**33%**
Safety record	32%	27%	**30%**

Q: What cybersecurity and security features do you have in place today?

To enhance security measures against intrusions, OT professionals continue to expand the array of cybersecurity measures and technologies they utilize to raise the levels of cybersecurity at their organizations. This year's responses show consistent growth in almost all categories, with significantly higher investment in solutions for internal network segmentation and role-based access controls and program features that support internal security training and education.

With IT-OT network convergence, organizations need to prevent common threats from accessing sensitive OT systems that were previously air-gapped. This requires comprehensive visibility, the ability to segment networks and protect network boundaries, and monitoring and controlling access to OT systems based on the user's defined role. In combination, these capabilities support a zero-trust approach to security.

As cybercriminal activity drives responsibility for OT security higher in leadership ranks, spend is also going up. While increased investments are certainly a positive trend, the expanding scale, sophistication, and subsequent impacts of OT intrusions demonstrate that even more resources are needed to keep pace with the attack volume and effectively protect OT systems.



Best Practices

Based on this year's survey results, we've assembled the following best practices:

1. Deploy segmentation

Reducing intrusions requires a hardened OT environment with strong network policy controls at all access points. This kind of defensible OT architecture starts with creating network zones or segments. Standards such as ISA/IEC 62443 specifically call for segmentation to enforce controls between OT and IT networks.[11]

Teams should also evaluate the overall complexity of managing a solution and consider the benefits of an integrated or platform-based approach with centralized management capabilities.

TIP: Implement a strategy for secure networking. Start with the basic steps of asset inventory and segmentation. Then consider more advanced controls such as OT threat protection and microsegmentation.

2. Establish visibility and compensating controls for OT assets

Organizations need the ability to see and understand everything that's on their OT networks. Once visibility is established, organizations then need to protect any devices that appear to be vulnerable. This requires protective compensating controls that are purpose-built for sensitive OT devices. Capabilities such as protocol-aware network policies, system-to-system interaction analysis, and endpoint monitoring can detect and prevent compromise of vulnerable assets.

TIP: A combination of application-layer policies, OT vulnerability protections, and virtual patching can greatly reduce the exposure of vulnerable legacy systems.

3. Integrate OT into security operations (SecOps) and incident response planning

Organizations should be maturing toward IT-OT SecOps. To get there, OT needs to be a specific consideration for SecOps and incident response plans, largely because of some of the distinctions between OT and IT environments, from unique device types to the broader consequences of an OT breach impacting critical operations.

One key step in this direction is to have playbooks that include your organization's OT environment. This kind of advanced preparation will foster better collaboration across IT, OT, and production teams to adequately assess cyber and production risks. It can also ensure that the CISO has proper awareness, prioritization, budget, and personnel allocations.

TIP: Security tools with effective machine learning capabilities can empower data aggregation and analysis to detect and respond more quickly to potential threats.

4. Consider a platform approach to your overall security architecture

To address rapidly evolving OT threats and an expanding attack surface, many organizations have assembled a broad array of security solutions from different vendors. This has yielded an overly complex security architecture that inhibits visibility while placing an increased burden on limited security team resources.

A platform-based approach to security can help organizations consolidate vendors and simplify their architecture. A robust security platform with specific capabilities for both IT networks and OT environments can provide solution integration for improved security efficacy while enabling centralized management for enhanced efficiency. Integration can also provide a foundation for automated responses to threats.

TIP: Security platforms featuring context-aware generative AI capabilities can help organizations further strengthen their security posture and increase operational efficiency with automated tools like troubleshooting device vulnerabilities and threat hunting analysis.

5. Embrace OT-specific threat intelligence and security services

OT security depends on timely awareness and precise analytical insights about imminent risks. A platform-based security architecture should also apply threat intelligence for near-real-time protection against the latest threats, attack variants, and exposures. Organizations should ensure their threat intelligence and content sources include robust, OT-specific information in their feeds and services.

TIP: Your threat intelligence and security services should include specialized intrusion prevention system signatures designed to detect and block malicious traffic targeting OT applications and devices.

Methodology

Most survey respondents have “plant operations” or “manufacturing operations” titles, with more than one-quarter (28%) being vice presidents or directors of plant operations. No matter their title, most of those surveyed are deeply involved in cybersecurity purchase decisions. While more than half (58%) of these individuals still have the final say in OT purchase decisions, this year’s survey found that a rising number of organizations (38%, up from 28% in 2023) now make these decisions as a group.

Study objectives

Fortinet retained InMoment, a third-party company with research expertise, to help us develop the persona of an OT professional.

The survey they helped us create is intended to understand the following better:

- How the persona fits in organizations
- How security features are utilized
- How information is tracked and reported
- Influences and success factors

Approach

A panel sample was used to obtain 558 completes with the following respondent type from a business of more than 1,000 employees (with select exceptions) in:

- Energy, utilities
- Healthcare/pharma
- Transportation, logistics
- Manufacturing
- Chemical, petrochemical
- Oil, gas, refining
- Water, wastewater

Other sample participation criteria included:

- Operations technology is within functional responsibility
- Has reporting responsibility for manufacturing or plant operations
- Involved in cybersecurity purchase decisions

Expanded to global reach since 2022:

- Survey respondents were from different locations around the world, including Australia, New Zealand, Argentina, Brazil, Canada, Mainland China, France, Germany, Hong Kong, India, Japan, Mexico, Norway, South Africa, South Korea, Spain, Taiwan, Thailand, United Kingdom, and the United States, among others.

Conclusion

OT is essential to businesses and governments around the world, including critical infrastructure, healthcare systems, and manufacturing operations. The indispensable nature of OT and ICS systems is precisely what puts them at elevated risk. According to NIST, OT security objectives typically prioritize integrity and availability, followed by confidentiality, but safety must also be considered as an overarching priority.[12]

As the *2024 State of Operational Technology and Cybersecurity Report* shows, there are positive signs that OT security is maturing in many organizations. However, at the same time, some of the gains seen in the previous year slipped in the current survey cycle, with organizations experiencing more intrusions and OT becoming less of a factor in determining risk score. To reverse these trends, there must be renewed evangelism for protecting sensitive OT systems and allocating resources for an effective, purpose-built security architecture.

[1] Keith Stouffer et al., Guide to Operational Technology (OT) Security, NIST, September 2023.

[2] Ibid.

[3] Ryan Daws, Global agencies warn of increased cyberattacks against OT devices, IoTnews, May 2, 2024.

[4] Global Threat Landscape Report, Fortinet, August 2023.

[5] Ibid.

[6] Ibid.

[7] Erik Gerding, Cybersecurity Disclosure, US Securities and Exchange Commission, December 14, 2023.

[8] Douglas Jose Pereira dos Santos, Key Findings from the 1H 2023 FortiGuard Labs Threat Report, Fortinet, August 07, 2023.

[9] Shashi Samar, The real impact of cybersecurity breaches on customer trust, CSO, July 3, 2023.

[10] Beth Stackpole, Cybersecurity plans should center on resilience, MIT Sloan, March 27, 2024.

[11] Maximillian Kon, How to Define Zones and Conduits, ISA, accessed May 7, 2024.

[12] Keith Stouffer et al., Guide to Operational Technology (OT) Security, NIST, September 2023.

FORTINET

www.fortinet.com

June 12, 2024 3:27 PM

2651469-0-0-EN