OTORIO

The Growing Need for Exposure Management in OT Environments

June 2024

Table of Contents

Introduction and Key Findings

Introduction & Methodology

As IT and OT continue to converge, IT security controls and workflows must be extended into the operational environment so that companies can protect critical infrastructure, personnel, and business operations from the disruptive and financial consequences of cyber attacks. This is not just a matter of technology. Both physical and human factors are key differentiators between IT and OT security. OT security is a fast-evolving and nuanced industry with a significant knowledge gap and communication gap between departments and stakeholders.

As a market leader, OTORIO brings the worlds of IT and OT closer together through technology convergence and team collaboration, enabling more efficient and effective implementation of OT security strategies. OTORIO commissioned this survey to examine the challenges faced by CISOs in achieving this and in order to understand how well today's security leaders are bridging the many gaps.

This report examines the impact of cyber attacks on business operations, asks CISOs to share what is driving their operational security strategies – including budget, compliance, and communication – and delves into how OT and IT are increasingly converging on both the technical and human sides of the equation. It identifies a growing need for tailored solutions that understand the nuances of regional and industry-specific risks and compliance requirements, and shines a light on a market transitioning from IT-led reactive strategies to a proactive exposure-based approach to OT security.

Methodology

We commissioned a survey of 220 full-time employees from companies with more than 1,000 employees, evenly split across Manufacturing, Energy/Oil and Gas, Process industries, and Smart Infrastructure. Respondents are all CISOs, with a role in OT security, risk management, or compliance, and were split between the USA, Canada, and various regions across Europe.

This report was administered online by Global Surveyz Research, a global research firm. The respondents were recruited through a global B2B research panel, invited via email to complete the survey, with all responses collected during Q1 2024. The average amount of time spent on the survey was 6 minutes and 31 seconds. The answers to the majority of the non-numerical questions were randomized, in order to prevent order bias in the answers.

Key Findings

1

88% of security leaders cite significant disruption as a direct result of cyber attacks.

Operational environments are under attack, leading to a significant rise in concern among CISOs. 88% of security leaders cite moderate-severe disruption to their business over the past 12 months as a direct result of cyber attacks, and 75% of respondents are more concerned about the OT threat landscape than they were 12 months ago. These recent cyber attacks are now the top driver for making investments into security, with 99% of companies seeing an increase to their OT security budget, and the majority of companies being allocated a budget increase of 20-50% or more. There is no doubt that organizations see the value of adopting proactive cybersecurity measures, and draw a direct correlation between the growing risk landscape and a need for increased and targeted security investments.

2

40% of ransomware attacks lack an IT component, showing an increased direct risk to OT environments.

The OT cybersecurity threat landscape is evolving rapidly. In the past year, 95% of companies experienced a ransomware attack, with 40% of these attacks lacking an IT component, highlighting the growing direct risk to OT environments. A proactive approach and quick intervention are crucial for maintaining resilient operations. However, at least 25% of respondents prioritized every pain point, revealing a mixed state of the market and a gap in understanding how to navigate these challenges effectively.

3

45% have created joint IT OT security taskforces to bridge skill gaps and improve efficiency.

CISOs often inherit responsibility for defining, governing, and reporting on OT security strategies, and are liable for all related damage. However, they are not experts in operational technology and face fragmented cybersecurity ownership across regional and global teams, making efficiency and scalability hard to manage. Today, 95% of companies have a formal team structure in place for OT security, and 45% have created joint IT/OT task forces. Enhancing cross-functional cooperation between IT and OT teams is essential for effectively implementing OT security strategies, ensuring that the technical and operational perspectives are integrated to effectively bridge the gap between strategy and implementation.

4

40% use exposure management, indicating a notable shift towards a proactive OT security approach

Continuous Exposure Management is a powerful tool for managing OT vulnerabilities, uncovering risk in the OT environment, and prioritizing which issues to divert resources towards to avoid the risk of downtime or business disruption in the case of a cyber attack. In the 2023 OTORIO survey, just 18% of companies were found to be using Continuous Exposure Management. Today that number has increased to 40%, indicating a significantly heightened understanding of the unique requirements of managing cybersecurity for OT systems. This shift towards Continuous Exposure Management highlights the evolution towards proactive vulnerability management, stressing the importance of comprehensive and ongoing security practices above reactive measures.

5

71% say their cyber insurance policies don't fully cover OT, revealing significant gaps in coverage.

There is a critical need for enhanced and comprehensive cyber insurance policies to protect operational technology (OT). 71% of respondents report that their current policies do not fully cover OT environments, despite a significant percentage identifying insurance coverage as a top OT cybersecurity investment driver for 2024. Only 18% of respondents plan to address this coverage gap within the year, leaving many organizations vulnerable to severe risks. This underscores the urgent necessity for companies to reassess and upgrade their cyber insurance policies to ensure robust protection for their OT environments.

Survey Report Findings

The Impact of Cyber Attacks on OT Environments

Ransomware continues to be a significant and growing threat to Operational Technology (OT) environments, with 95% of companies experiencing a ransomware attack in the past year (Figure 1).

OT attacks used to be a byproduct of IT-related attacks, but due to growing digitization and the connected nature of OT/IT environments, today that is not the case. 40% of ransomware attacks impacted only OT or IoT devices, showing that attackers no longer need to leverage connected IT systems to launch attacks, and can target OT directly. When ransomware threat actors target OT, the risk to human life and the impact of operational downtime is so severe that many businesses will feel they have little choice but to pay the ransom, making OT a favorable target for attackers.

Figure two shows the significant impact of cyber incidents on OT/IoT environments over the past year, with 88% experiencing moderate-significant operational disruption. This highlights how important it is to implement a proactive strategy - rather than acting in reactive mode once a threat has been identified.

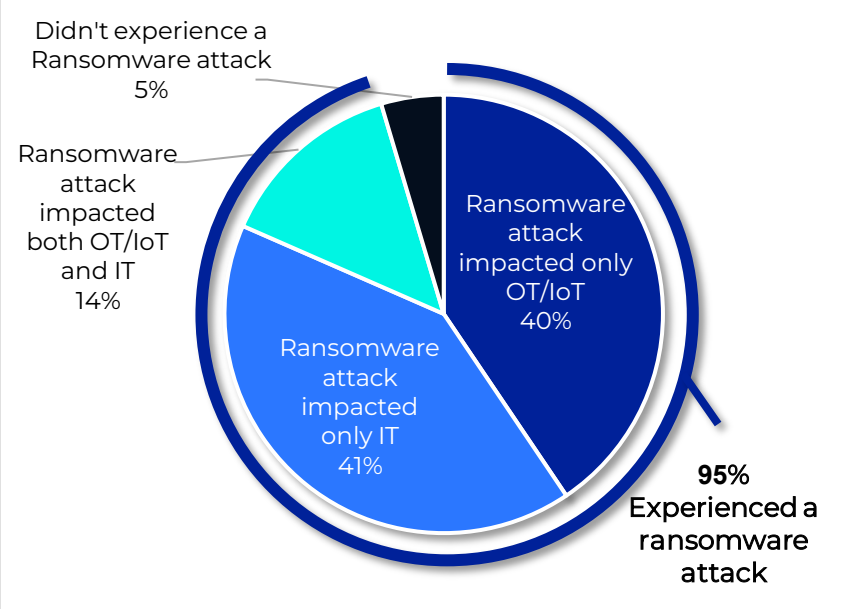

Figure 1: Experienced a Ransomware Attack in the Past Year that Impacted Companies' Environments

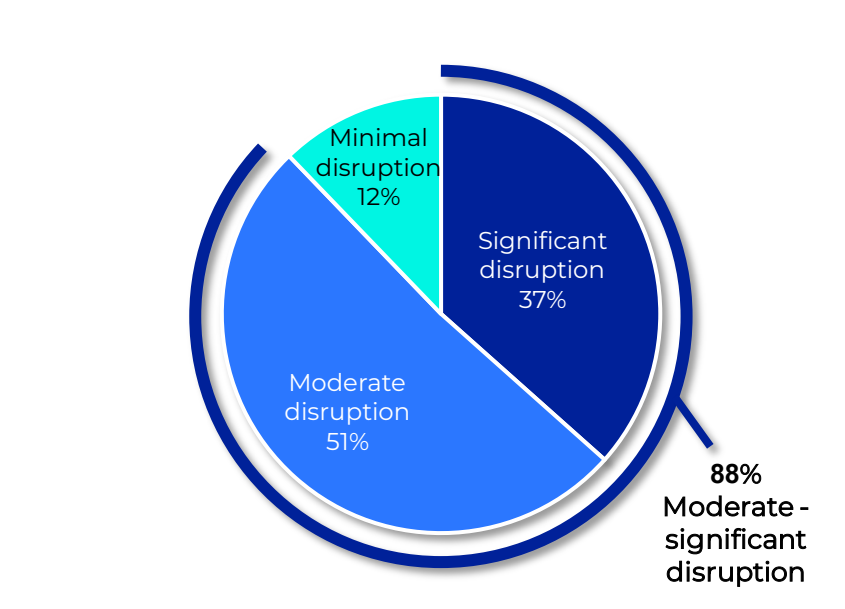

Figure 2: Operations Impacted Due to Cyber Incidents in OT/IoT Environments in the Past Year

Changes in Perception of The OT Cybersecurity Threat Landscape

The survey data indicates a growing recognition among respondents of the need for enhanced cybersecurity measures tailored specifically to protect operational technology (OT) environments.

Against the backdrop of significant disruption to operational environments, and new attacks that target OT directly, 75% of respondents are more concerned about OT cybersecurity threats than they were a year ago.

25% describe the OT threat landscape as significantly more concerning, and just 10% of companies are less concerned about the risk.

This overwhelming perception that the OT threat landscape is a cause for concern underscores how critical it is for businesses to implement OT-specific cybersecurity tools that meet the growing risk we saw in figure one.

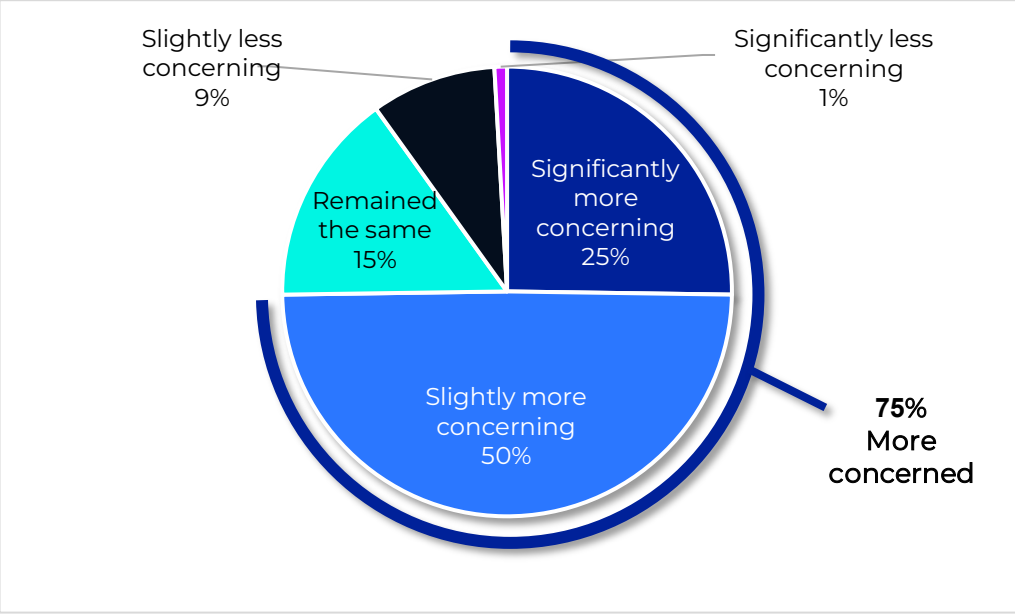

Figure 3: Changes in Perception of OT Cybersecurity Threat Landscape Over the Past Year

Top Drivers Influencing Security Investments in 2024

The real-world impact of cyber attacks remains a key driver for security investments, followed closely by the need to meet compliance, obtain insurance coverage, and provide detailed reports to stakeholders.

The main driver behind security investments this year has been the real-world impact of a cyber attack, with 37% citing this as the main reason for increasing investments.

This is closely followed by the need to meet compliance and obtain insurance coverage, and meeting reporting requirements for investors and shareholders, both cited by 31% of respondents.

In many ways, being able to communicate the value of risk-reducing initiatives and obtain detailed reports to be presented to different audiences is just as critical a motivator to security leaders as preventing the impact of an attack itself.

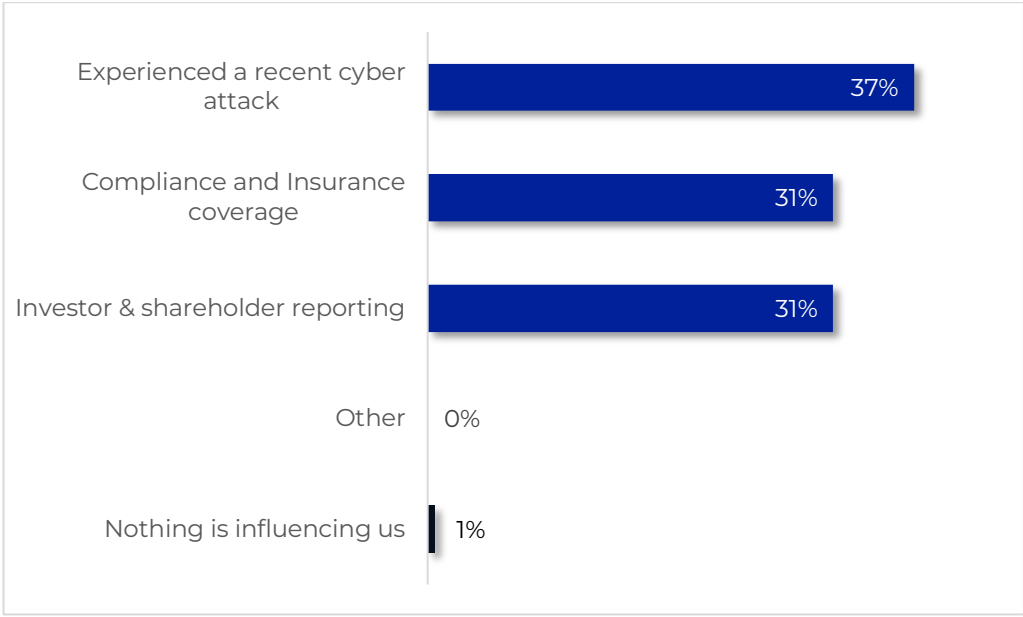

Figure 4: Top Drivers Influencing 2024 Security Investments

Budget Allocation for OT Cybersecurity in 2024

99% of security teams saw an increase in their OT cybersecurity budget this year.

While the average increase is 27%, it's clear that there is a strong trend towards significant increases in budget allocation for OT cybersecurity, with nearly all security teams seeing an increase. The range of increases, particularly the 20-50% range for 40% of companies, indicates a recognition of the escalating risk in the OT threat landscape.

This increase in budget suggests a proactive approach to investing in necessary improvements to enhance protection against these critical risks, despite challenges including geopolitical risk, economic conditions, and existing tech debt. The industry's commitment to justifying budget allocation for OT cybersecurity underscores its importance and the seriousness with which organizations are approaching this aspect of their security strategy.

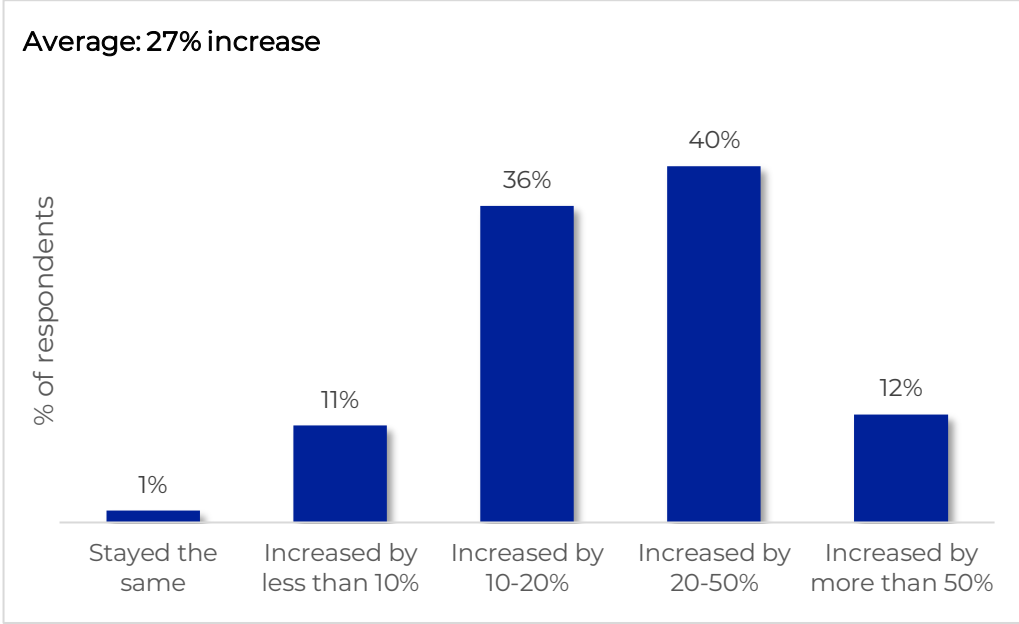

Figure 5: OT Cybersecurity Budget in 2024

OT Cybersecurity Pain Points in 2024: What's the Priority?

There is no one clear pain point across OT cybersecurity, and different organizations will prioritize varied issues depending on their specific business environment and their level of maturity.

As a result, we can see that all cybersecurity pain points are highlighted by at least a quarter of respondents, underscoring the complexity of the landscape and the market.

However, we can see that different regions certainly have different priorities and pain points. Employee training and awareness programs are much more of a priority in Europe than they are in North America, while in North America – there is a greater focus on vulnerability detection and mitigation than there is in Europe. These are cultural differences, perhaps showing that the EU market places more emphasis on human factors such as employee training while North America is more solutions focused.

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

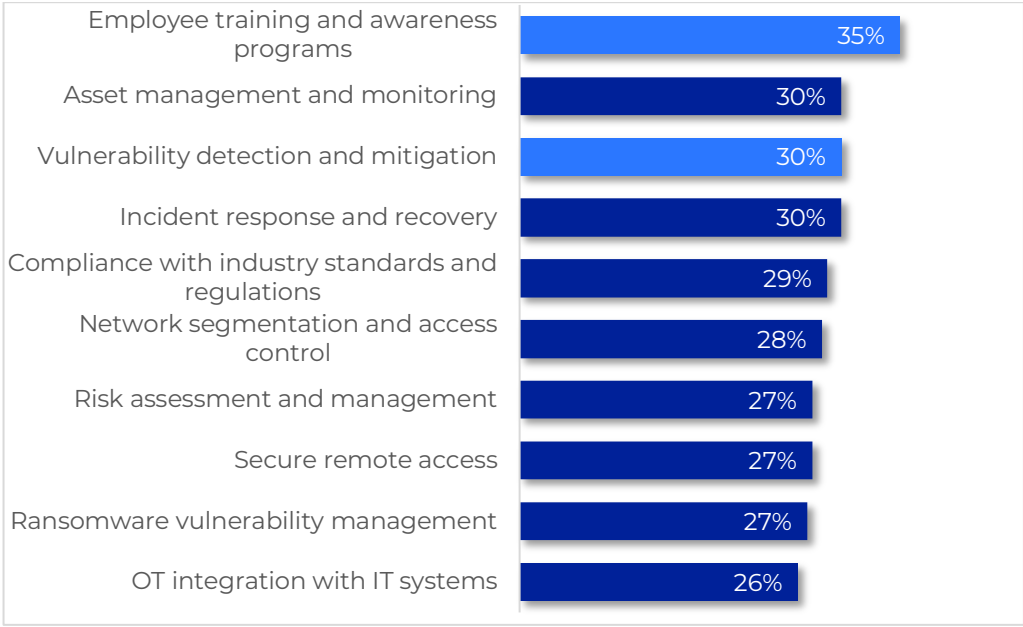

Figure 6: Top OT Cybersecurity Pain Points that Organizations are Prioritizing in 2024

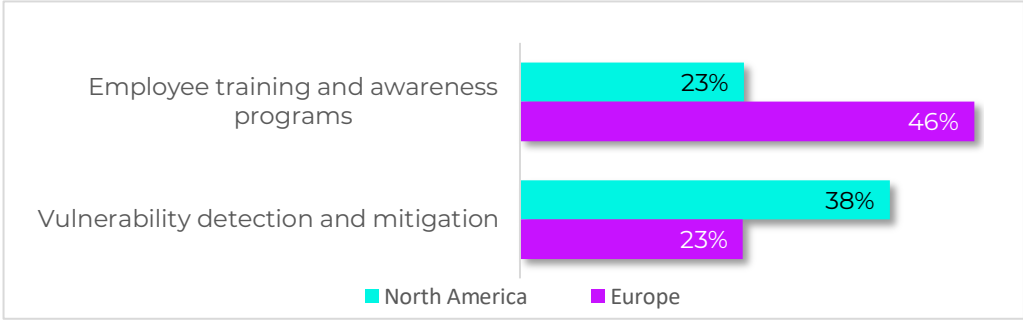

Figure 7: OT Cybersecurity Pain Points in 2024, by Region

How Do Companies Manage Responsibility for OT Security Risks?

Almost half of companies have built hybrid IT-OT teams to manage OT security, highlighting a growing emphasis on shared responsibility.

Taking responsibility for OT security is not just about onboarding technologies that take on both IT and OT risk but also about knowledge sharing and collaboration to manage the threat effectively.

95% of companies have a dedicated team in place to manage OT security, with a real mix between those who implement global and local teams. The remaining 5% who have no team for this purpose may be significantly vulnerable to cyber threats.

The differences in terminology, skill sets, and underlying knowledge and expertise can be extreme. Creating joint task forces helps to bridge those gaps, streamline workflows, and ensure optimized resources and more effective collaboration.

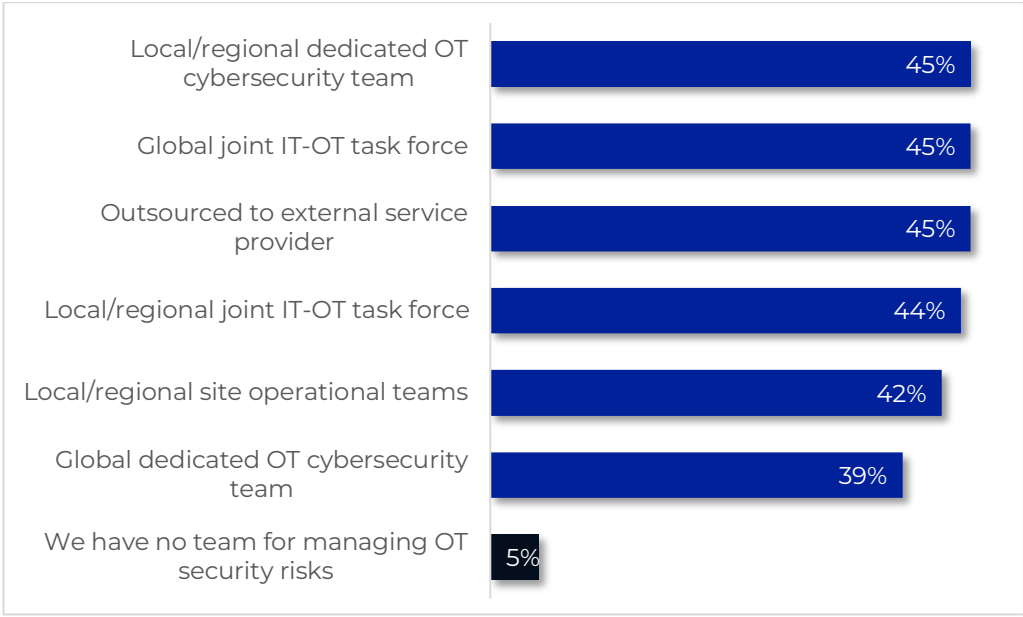

Figure 8: Teams Primarily Responsible for Managing OT Security Risks

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

The Importance of IT and OT Security Team Collaboration

Improved collaboration between IT and OT security teams is crucial for business resilience.

Just 32% of respondents say that their IT and OT security teams have a high level of collaboration, so there is a long way to go, but with almost half saying their collaboration levels are medium – teams are moving in the right direction.

While IT may have little experience with physically managing machines and, therefore, mitigating the challenges of an operational environment, on the other side, operational engineers don't have a background in cybersecurity and are mainly focused on safety and business continuity.

IT and OT teams are beginning to meet in the middle, with an understanding that despite differing priorities, the best results will come from working towards the common goals of business resilience and continuity. To do this, CISOs must invest in a comprehensive platform to accommodate the needs of different stakeholders simultaneously.

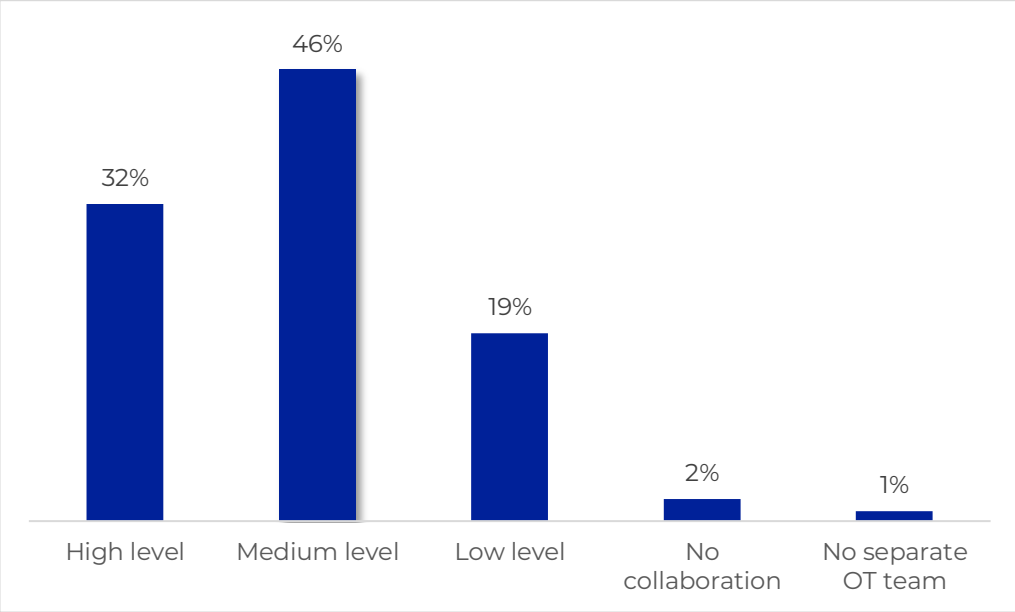

Figure 9: Level of Collaboration Between IT and OT Security Teams in the Organization

What is Your Current Approach to Managing OT Vulnerabilities?

There is a significant increase in companies using continuous exposure management for OT vulnerabilities, from 18% in 2023 to 40% today. This highlights a shift towards proactive approaches and a reduction in reactive and sporadic methods.

Just 4% of companies are working without a formal process in place for managing their OT vulnerabilities, and in 69% of cases, this approach is proactive.

In our 2023 survey, just 18% of respondents used continuous exposure management, which shows the growth in maturity levels in the market.

In contrast, reactive processes such as post-incident planning and response, or sporadic processes like periodic risk assessments have reduced in prevalence. In 2023, 41% of teams used post-incident planning as their approach to managing OT vulnerabilities, compared to 27% today, and 40% relied on periodic risk assessment.

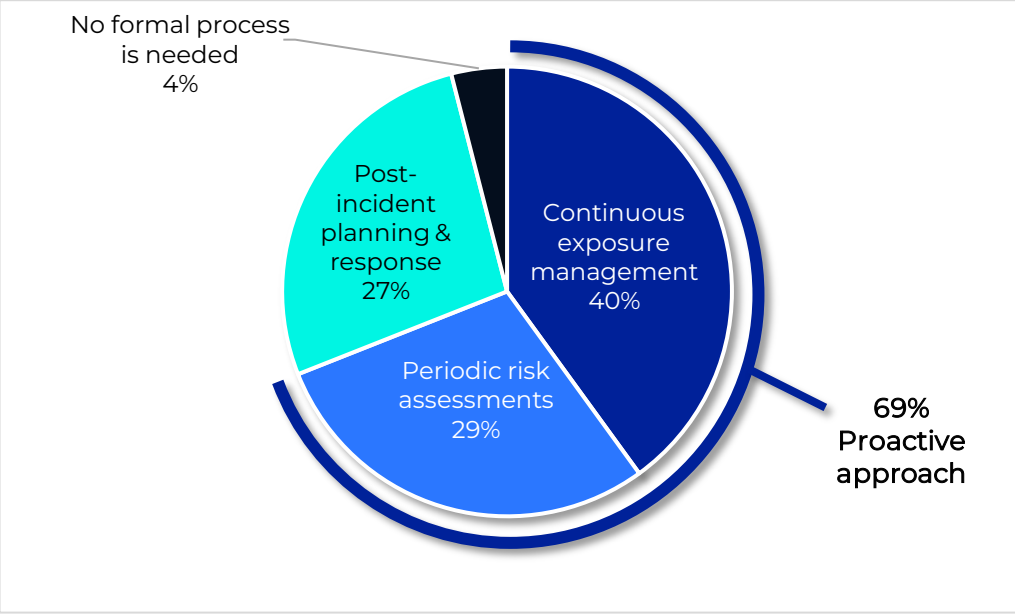

Figure 10: Current Approach to Identify and Respond to OT Vulnerabilities

Most Influential Regulations on OT Cybersecurity Strategy in 2024

With only 1% of respondents unaffected by regulations, it's clear that compliance is a universal concern for security leaders, though alone it is insufficient for ensuring business resilience in complex IT/OT environments.

There are a wide range of security and compliance regulations that today's security leaders are focused on meeting, and for which they are aware they may need to invest.

Some of these regulations are region-specific, or only apply to certain industries or environments, but just 1% of respondents say they are not influenced by regulations of any kind.

Whatever your business, and wherever you're based – you can't ignore compliance.

Of course, compliance doesn't guarantee security, and is insufficient alone to ensure business resilience in a complex and dynamic IT/OT environment.

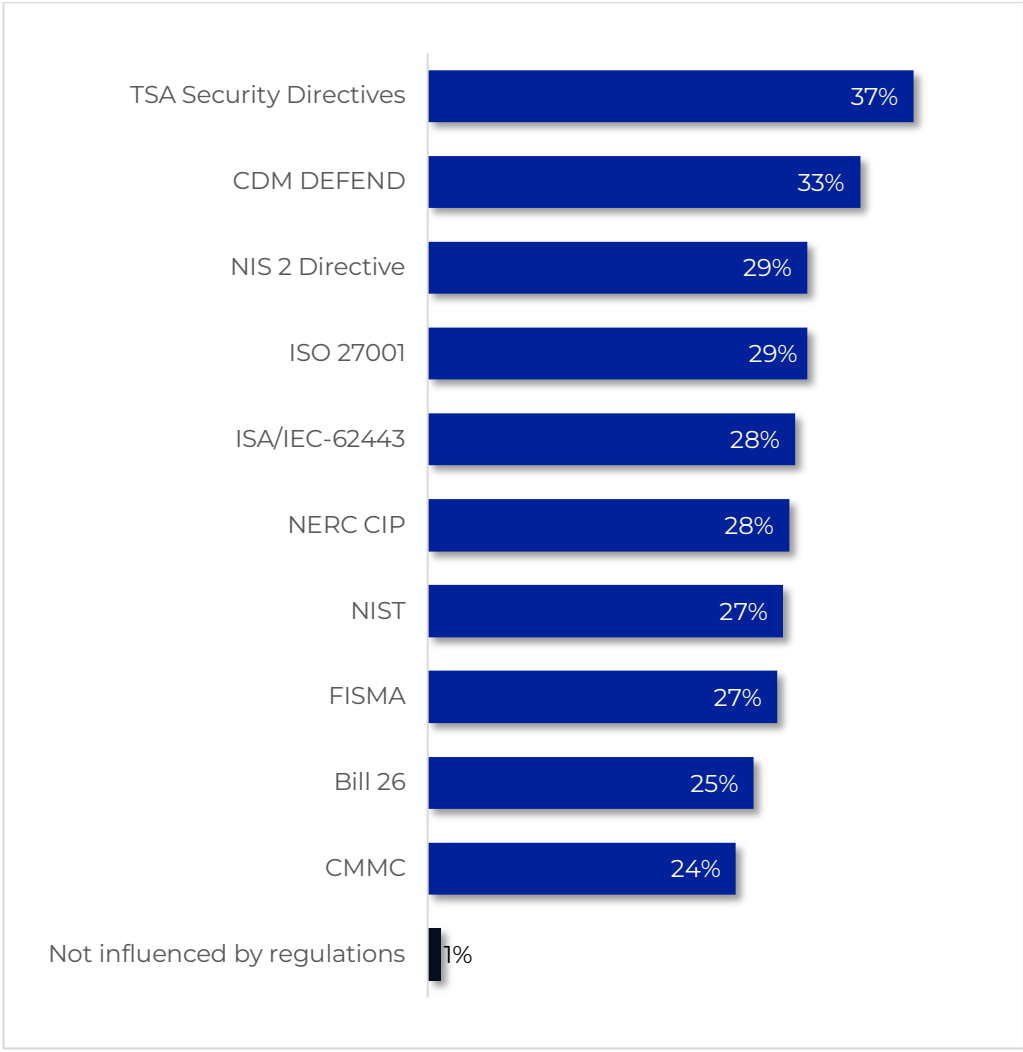

Figure 11: Most Influential Regulations on OT Cybersecurity Strategy in 2024

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

Insurance Coverage of Operational Technology in 2024

There is an urgent need for tailored coverage to mitigate financial risks and downtime from cyber attacks. While 81% say their cyber insurance covers OT, 52% say it is limited.

Cybersecurity insurance coverage does not traditionally cover operational machinery, which often leaves businesses exposed to financial risk and downtime that is caused by a cyber attack against an OT environment.

Today, just 29% of respondents say that they have comprehensive coverage that includes operational technology and is tailored to OT security needs. This percentage increases to 35% when we drill down into respondents that work in Manufacturing – an industry that is heavily reliant on machinery. In contrast, the coverage gap is particularly pronounced in the Oil and Gas industry, which signals a concerning gap in risk mitigation strategies, leaving organizations open to financial risk.

Overall, the tide is turning, but slowly. 18% of companies are planning to increase their coverage in 2024 to address this coverage gap.

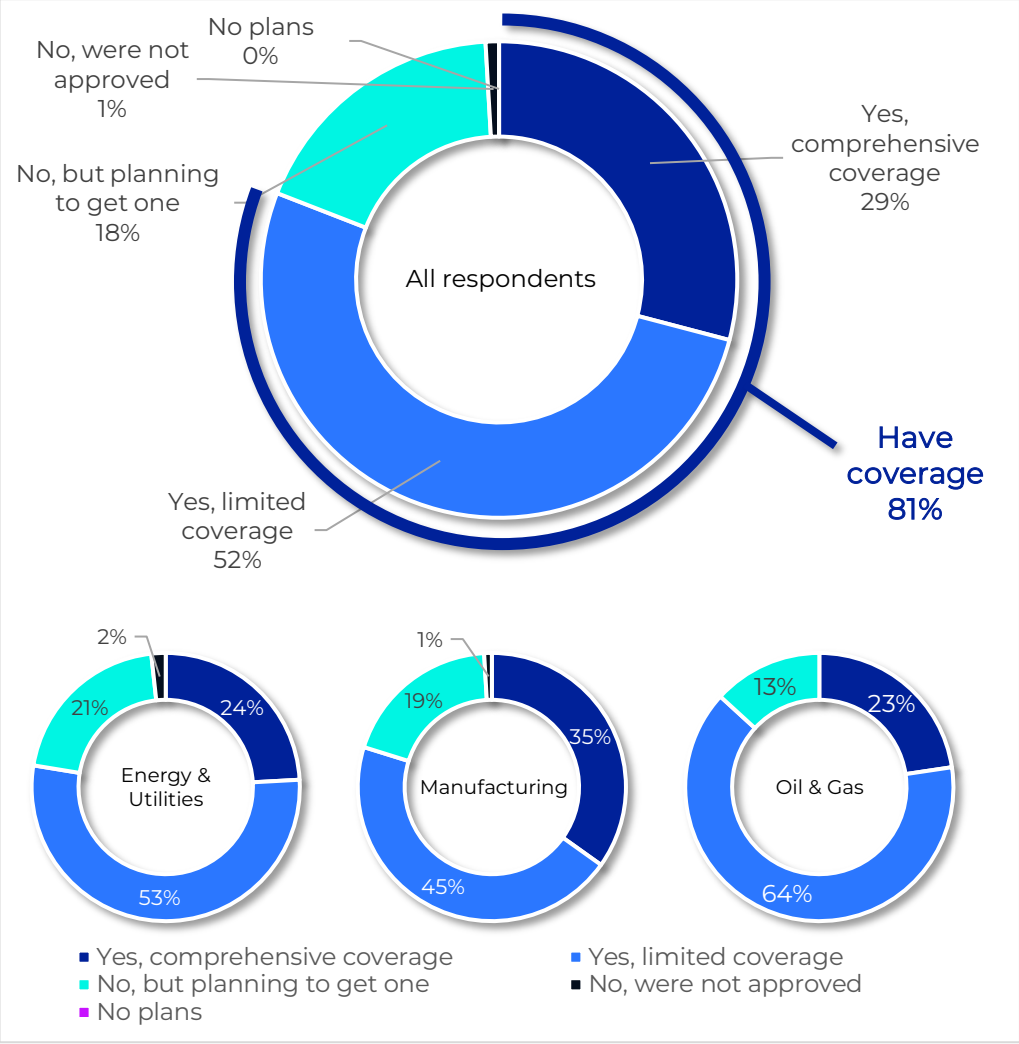

Figure 12: Insurance Coverage of Operational Technology in 2024

Demographics

Country, Industry, and Company Size

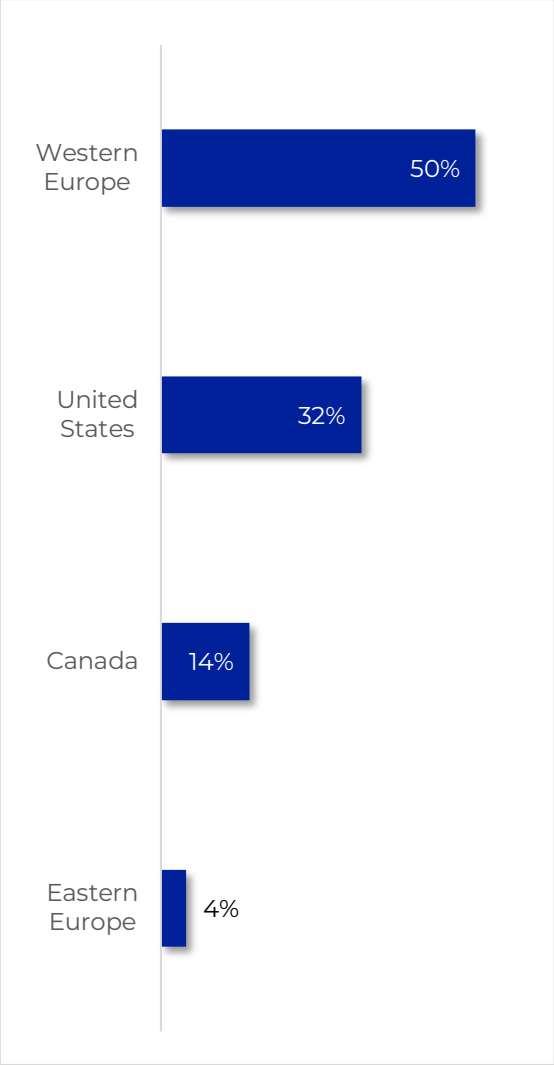

Figure 13: Country

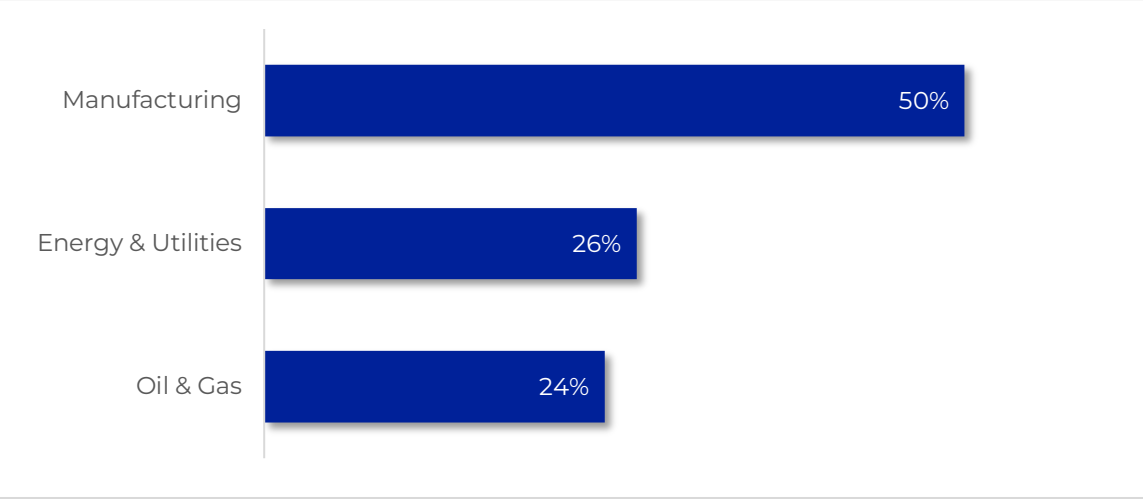

Figure 14: Industry

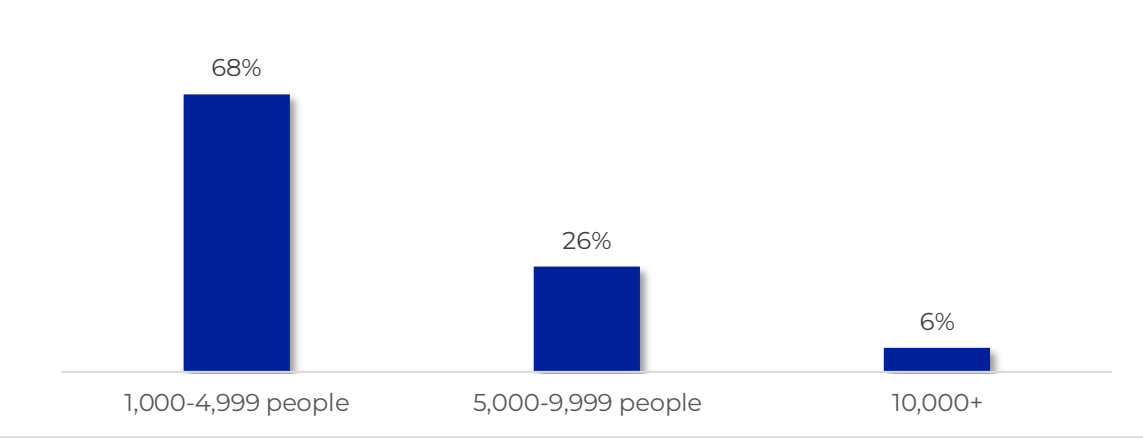

Figure 15: Company Size

About OTORIO

OTORIO is a provider of OT Security solutions delivering a Cyber Risk Management Platform designed to support every stage of the maturity journey, from unmatched visibility to tailored risk management. OTORIO's platform enables organizations to make informed decisions that boost security ROI and meet KPIs.

The platform leverages operational context for risk analysis, generating insights that empower stakeholder collaboration to prioritize risk reduction and optimize resource allocation.

With continuous monitoring and automated reporting, OTORIO's platform ensures resilient, compliant business operations and robust supply chain governance.

OTORIO, established in 2018 by experienced IDF cybersecurity experts and founding partner Andritz, is dedicated to seamlessly protecting ICS-CPS environments.

Book a Demo

For more information, please visit us:

Email: info@otorio.com