OTORIO

2022 OT Cybersecurity Survey Report

Jan 2022

Table of Contents

Introduction and Key Findings

Introduction & Methodology

Over the last two years, three different trends have converged to change the way people view industrial (OT) cybersecurity. The first; an acceleration towards a connected production floor, especially around remote operations and supply chain management. Driven by the pandemic, and in the hopes of becoming increasingly efficient and cost-effective, companies feel the continuing need to digitize their operations. As a result, formerly air-gapped industrial environments are today exposed to the web.

Secondly, the growth of cybercrime itself. Only a few years ago, the industry was mainly troubled by nation state attackers — the only ones that had the resources to target critical infrastructure, energy and industrial companies. Today, tools as sophisticated as those previously available only to nation states are leveraged by cybercriminal organizations and cause substantial damage. These criminals target industrial environments which they consider low hanging fruit due to accelerated digitization.

The final trend is the tightening of legislation and regulations, pushed forward by governments that are taking an increasingly active role in cyber defenses. The energy, utilities and transportation sectors are critical to both economy and national security – driving governments to implement new regulations, while updating and developing existing ones. This trend was accelerated in 2021 by the Biden Administration, and multiple US governmental agencies are now scrutinizing anything to do with operational technology.

To get greater insight into these OT cybersecurity drivers and to assess the impact of these trends, OTORIO conducted a survey of 200 senior cybersecurity leaders. We asked whether organizations have changed their processes or best practices? How are they impacted by the new regulations, and are they conducting new levels of analysis compared to the past? And most crucially, what are their plans moving forward, and will growing connectivity, OT-related cyber threats, and regulatory intervention impact how they protect their organizations?

Methodology

Survey respondents were selected and approached through a global B2B research panel, invited via email to complete the survey, and responses were collected during Q4 2021. Respondents were C-level managers, directors or heads of cybersecurity from companies that ranged from 250 employees to more than 10,000. The respondents were from North America, LATAM and Europe, and in industries ranging from energy and utilities to oil and gas, coal mining and alternative energy.

Key Findings

1

98% of respondents reported an increase in the level of digital and cyber risks to their operations over the past three years.

The concern over OT cybersecurity is well-founded. 67% of respondents reported that risks have increased significantly since 2019, and 31% noticed an increase that was slighter. Only 2% of respondents said they haven't noticed a difference in the level of cyber risks over the past three years.

2

Supply chain attacks are the top concern of OT cybersecurity experts

53% of respondents put supply chain attacks in their top three concerns when it comes to cybersecurity, with 99% reporting a supply chain attack in the last 12 months. Especially in OT, there is a very long supply chain, and strong dependence on suppliers. No matter how strong a company's security posture, it is only as strong as its weakest link.

3

Compliance is the number one driver for OT cybersecurity

Regulations and external threats are top of mind for decision-makers who are entrusted with keeping production environments secure. The three top drivers for cybersecurity are compliance (86%), growth (83%), and cyberattacks (82%). These are the real-world problems that are driving decision makers today.

4

Organizations can extract only minimal value from their existing OT cyber solutions

The main challenges with existing OT cybersecurity systems are a skills gap (57%), mitigation suggestions not being feasible (49%) alert fatigue (44%) and complexity (33%). The OT market was air gapped for so long that the right security measures are hard to gauge. A lot of solutions serving OT today are retrofitted IT solutions – with mitigation methods unsuitable for OT, in addition to patches or workarounds that add a layer of complexity.

5 The responsibility for OT security is shared between Engineering, IT and the C-Suite

According to the survey, the top three roles responsible for managing OT cybersecurity are VP/Head of Manufacturing/Engineering (31%), CISO (30%) and CEO (23%). The result is that in many cases, those responsible for OT security are not cybersecurity experts.

6 Less than 50% of companies manage their OT cybersecurity in-house

While 47% of respondents reported that they have an in-house team to manage OT cybersecurity, 53% rely heavily on managed services. 41% outsource OT cybersecurity completely, and 12% say they have a hybrid mix of outsourced and in-house teams.

7 Most companies are planning to increase their 2022 cybersecurity budgets by over 50%

With a clear rise in cybercrime, more regulations than ever before, digital transformation and the shift to a connected production floor, over half of respondents (54%) are planning to increase their 2022 cybersecurity budget by more than 50%. 92% will grow it by at least 10%.

Demographics and Characteristics

Country of Residence

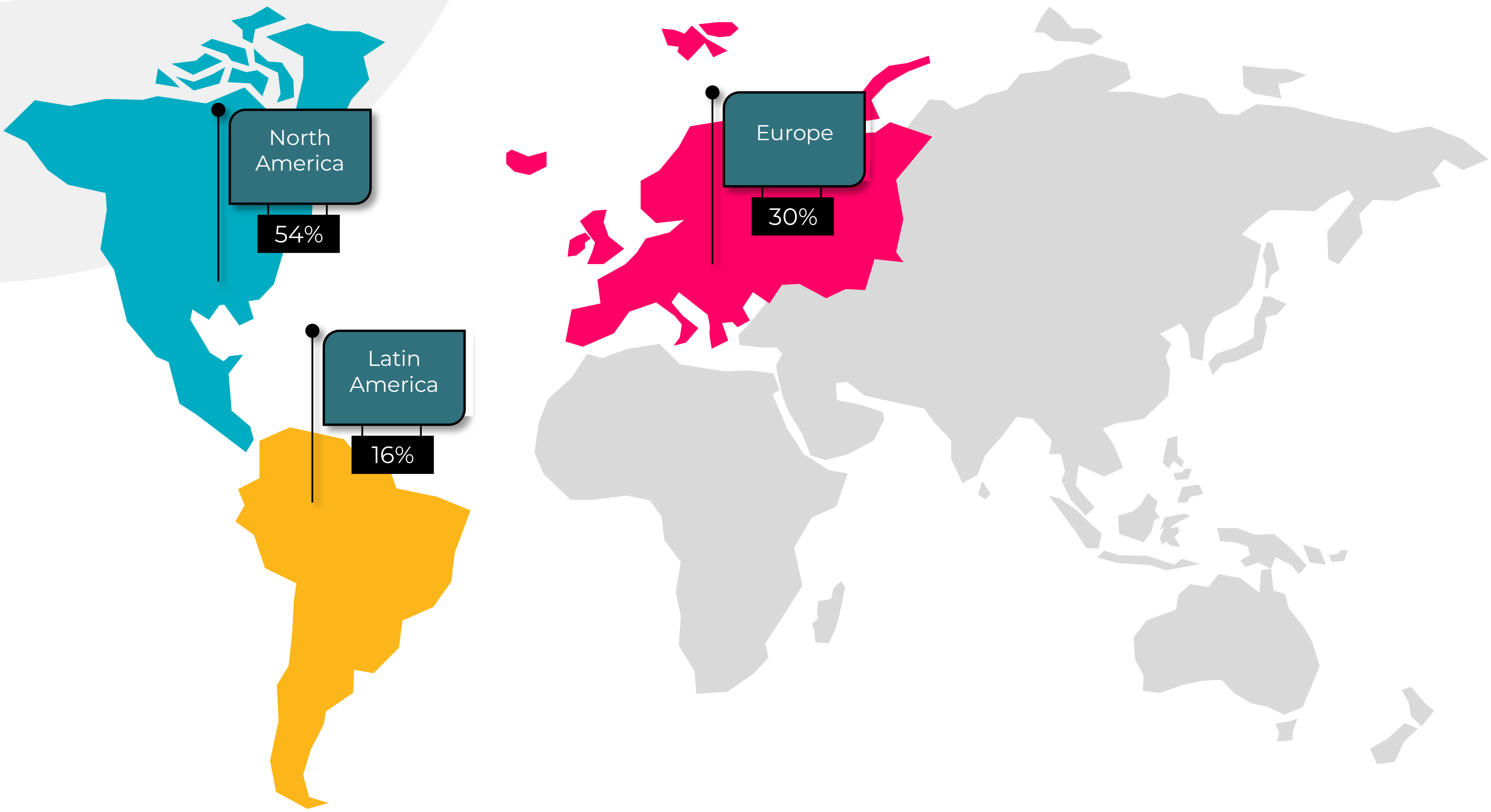

Figure 1 Country of Residence

Demographics: Industry, Size, Roles & Responsibilities

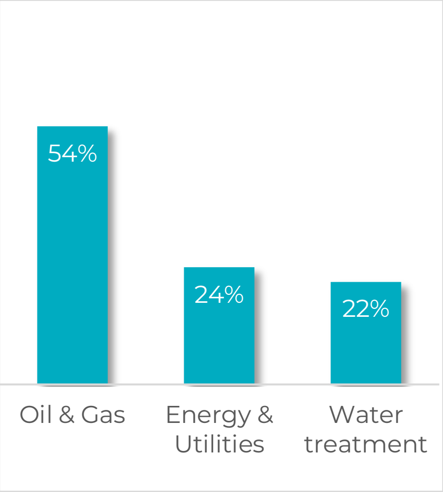

Figure 2 Industry

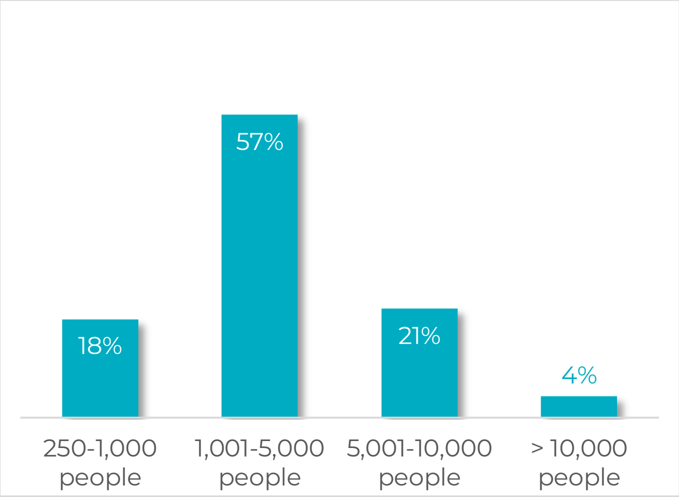

Figure 3 Company Size

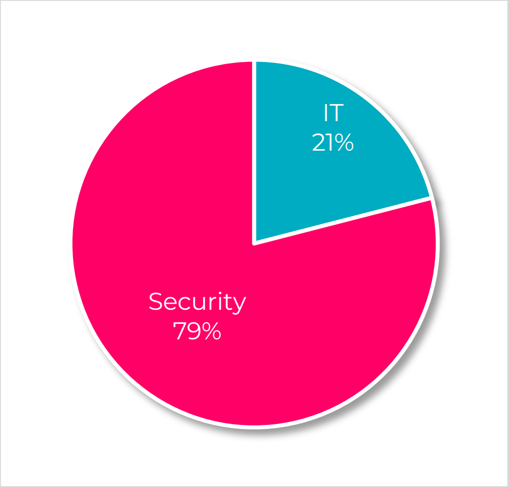

Figure 4 Department

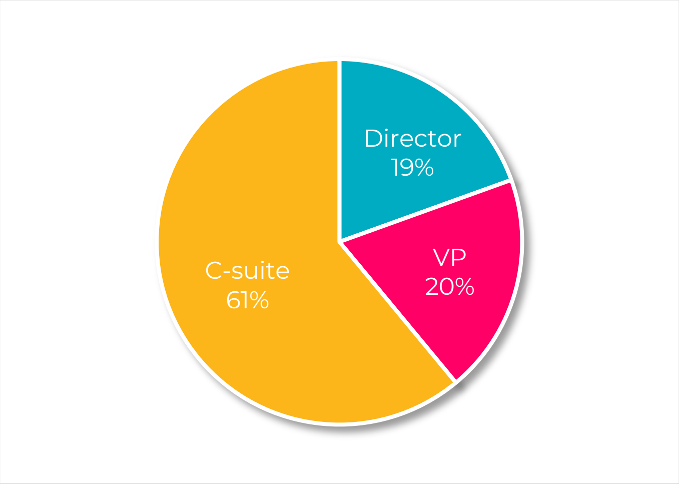

Figure 5 Seniority

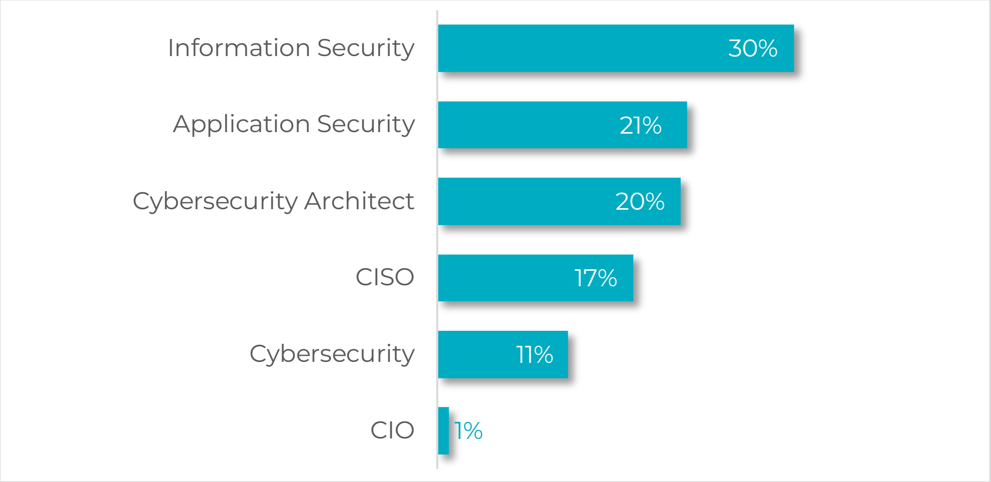

Figure 6 Job Title

Management and Responsibility of OT Cybersecurity

When asked how OT cybersecurity is managed, survey respondents were split into two primary groups. 47% have an in-house team, and 41% outsource it completely. 12% say they have a hybrid mix, relying on partial outsourcing alongside their own in-house team. (figure 7).

The top three roles responsible for managing OT cybersecurity (figure 8) are VP/Head of Manufacturing/Engineering (31%), CISO (30%) and CEO (23%).

It's interesting to note that the most likely person taking charge of cybersecurity is not a trained security expert, but rather the Head of Manufacturing.

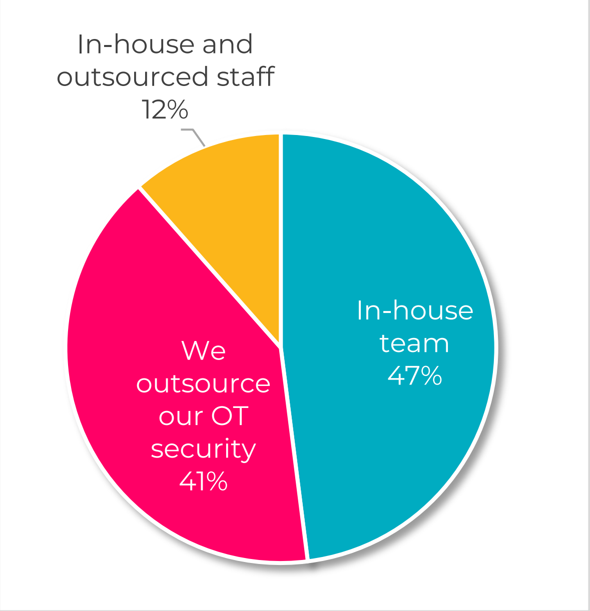

Figure 7 OT Cybersecurity Management

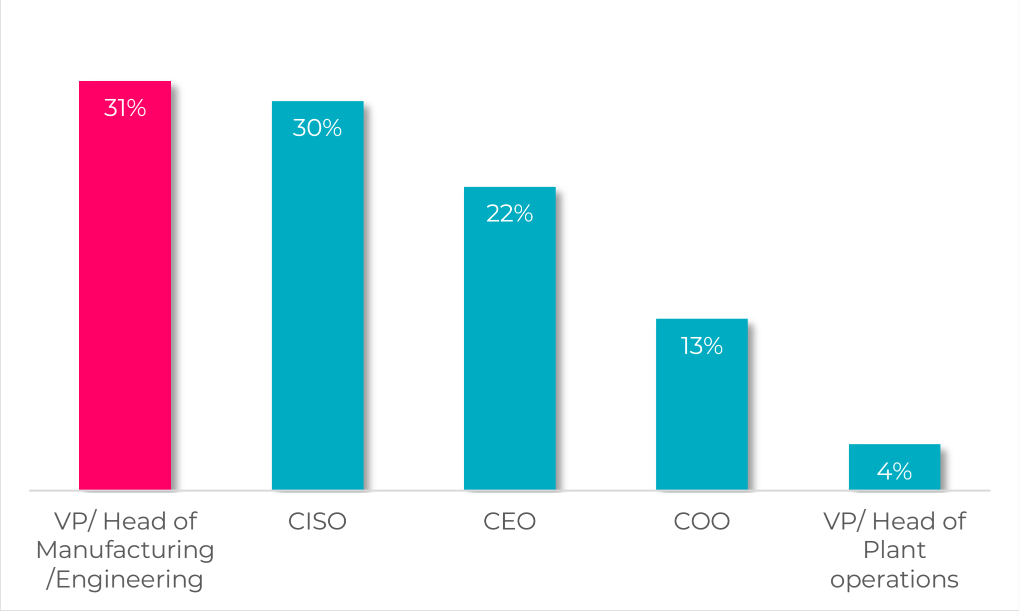

Figure 8 Direct Manager Responsible for OT Cybersecurity

**Percentages may not add up to 100% due to rounding*

OT Cybersecurity Importance to Organizations

100% of survey respondents said OT Cybersecurity is a priority for their companies.

The top three reasons for its growing importance are:

Compliance (86%)
OT cybersecurity is now mandatory for compliance with regulatory requirements and standards

Growth (83%)
Adding secure connectivity is a key enabler of digitization and growth, especially for areas like renewable energy that rely on a connected grid.

Cyberattacks (82%)

The recent spate of attacks on critical infrastructure has raised concerns about the consequences of a cyberattack.

It's interesting to note that failure to comply with regulations is even more of a concern for respondents than the consequences of a cyberattack.

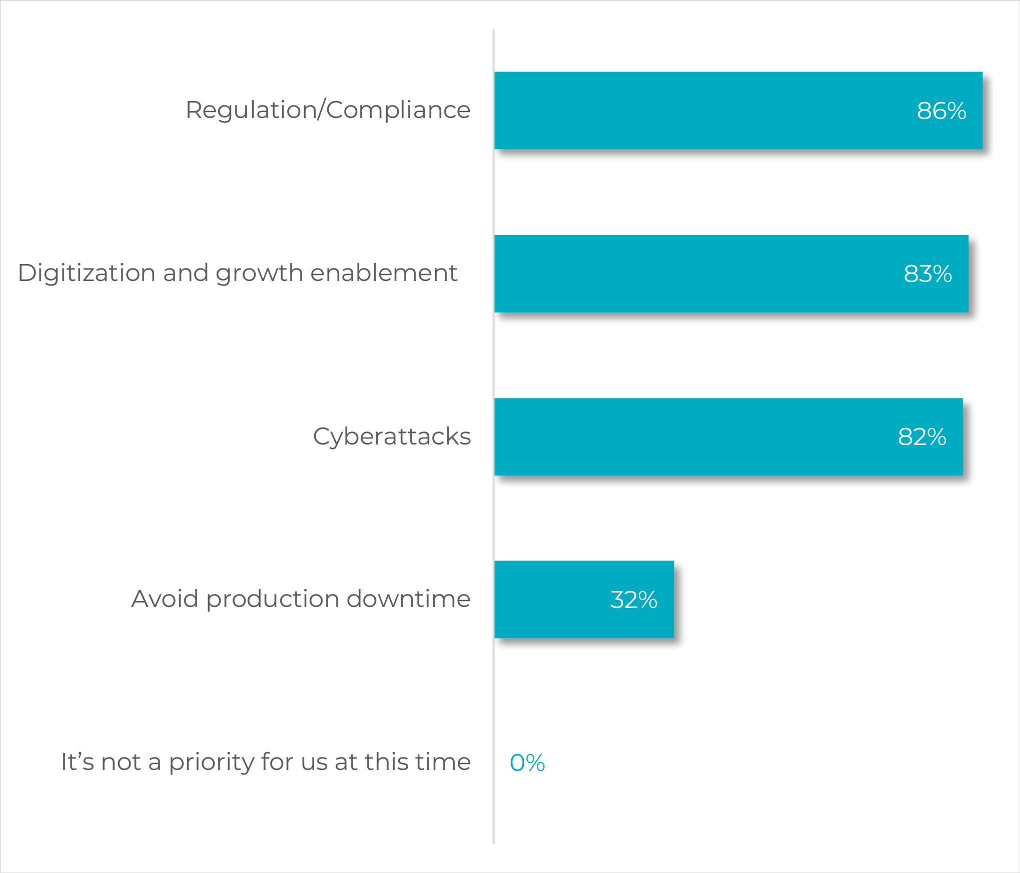

Figure 9 OT Cybersecurity Importance to Organizations

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

Level of Cybersecurity Risks

Increase in the Level of Digital and Cyber Risks (Past 3 Years)

98% of respondents reported an increase in the level of digital and cyber risks over the past three years.

67% of the respondents said that the risks have increased significantly, and 31% said there was a slight increase.

These findings are not surprising when considering headlines over the past year about OT cyberattacks like the Lockbit ransomware attack, the Colonial Pipeline attack, the Ultrapar interruption in the fuel industry, and the Wiregrass energy ransomware attack.

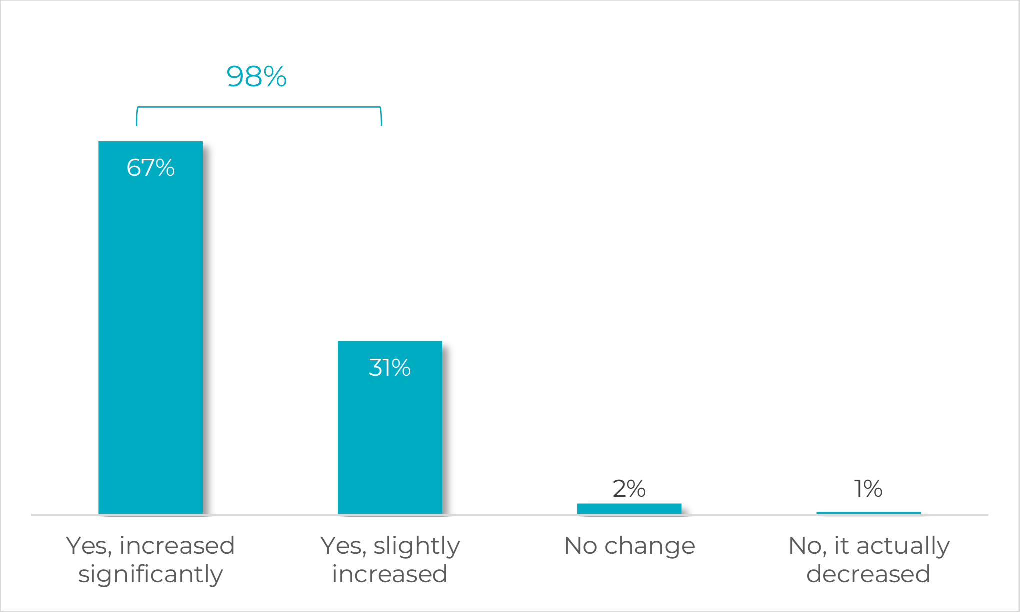

Figure 10 Level of Increase in Digital and Cyber Risks in the Past 3 Years

*Percentages do not add up to 100% due to rounding

Cybersecurity Incidents Reported to Government Agencies (Past 12 Months)

When asked what percentage of cybersecurity incidents respondents reported to government agencies during the past 12 months, all companies indicated they are reporting.

However, **58% are not reporting at least 20% of their incidents** and only 4% are reporting all of their incidents.

This means that the incidents that make it to the headlines are only a fraction of the true scale of OT cyberattacks affecting industry.

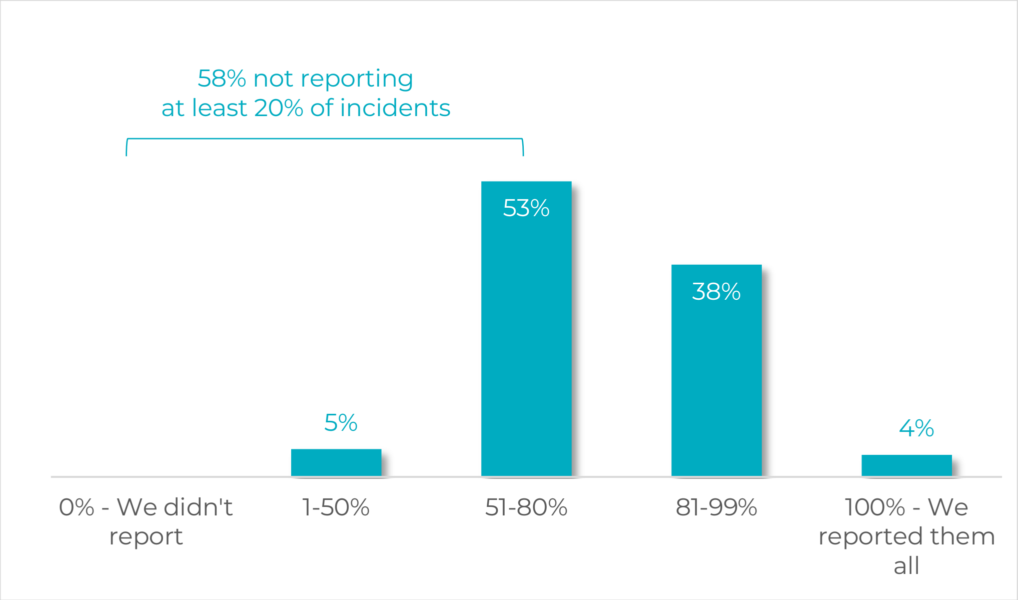

Figure 11 Cybersecurity Incidents Reported to Government Agencies

Supply Chain – A Top Concern

Supply Chain Tops the List of OT Cybersecurity Concerns

53% of survey respondents see supply chain attacks as one of their top 3 concerns.

The Kaseya and SolarWinds attacks, as well as the large-scale attack on the African port network are just a few examples of major supply chain attacks in 2021 - with hundreds of organizations impacted following exploitation of a vulnerability in one service provider.

Companies are only as strong as their weakest link. In an operational or industrial environment, this could be any vendor with remote access to the production environment, who may not even be visible to IT monitoring tools, since OT works differently.

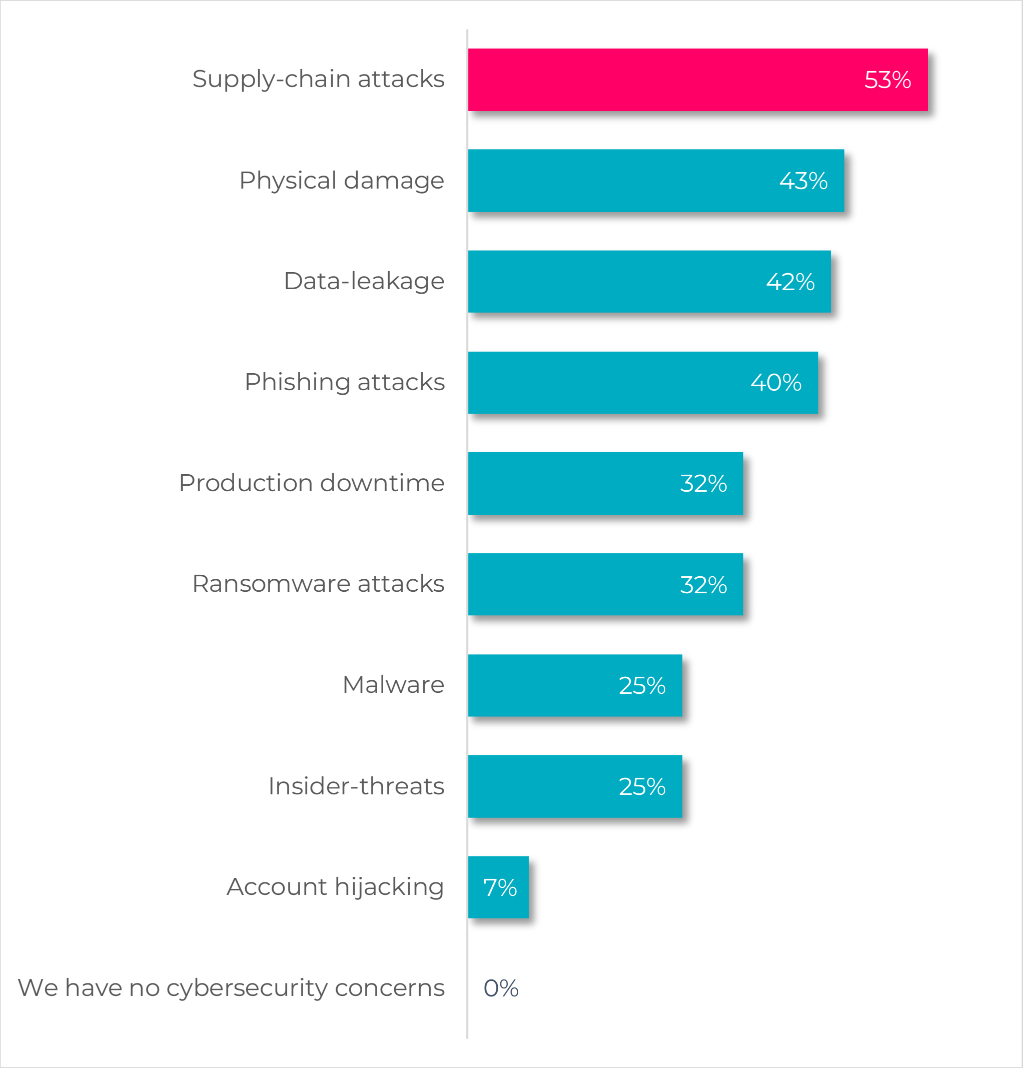

Figure 12 Top OT Cybersecurity Concerns

This question allowed more than one answer and as result, percentages will add up to more than 100%

Concerns and Experience with Supply Chain Attacks

99% of respondents have experienced the impact of a supply chain attack in the past 12 months (figure 17).

83% of respondents report that they are highly concerned about attacks that originated in their supply chain (figure 18). To reduce the risk, organizations should implement technology such as micro-segmentation and limit access to their environment for third-party suppliers according to the principles of least privilege and zero trust.

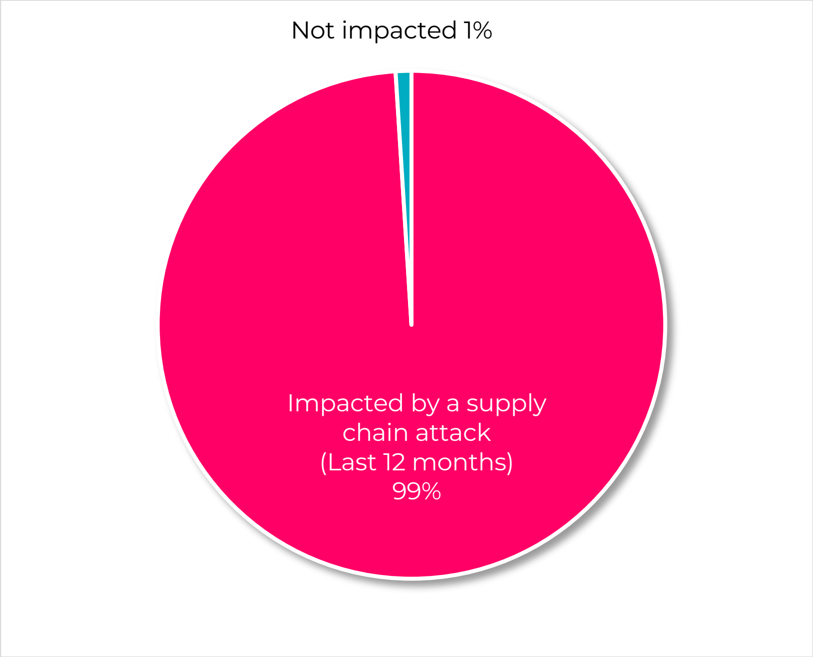

Figure 13 Supply Chain Attack in the Past 12 Months

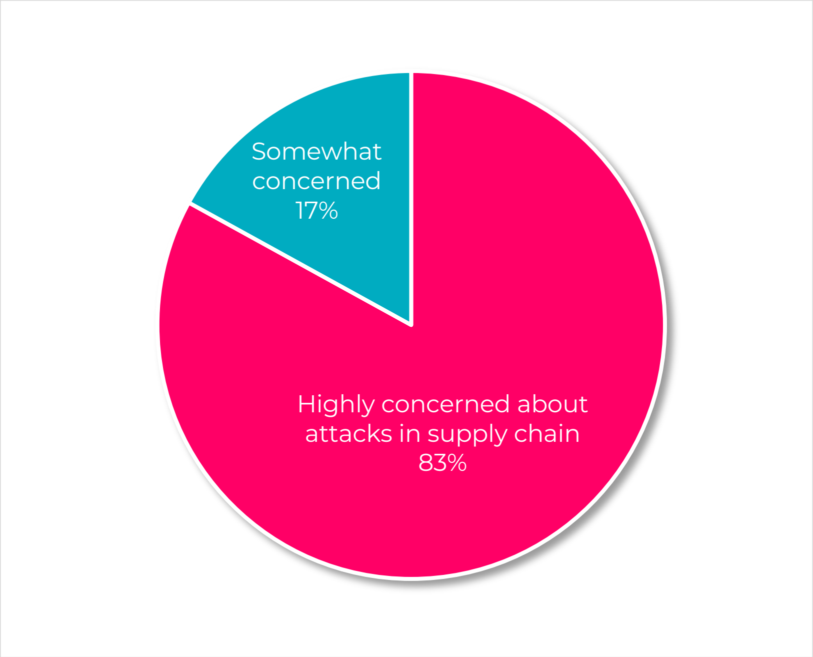

Figure 14 Concerned About Attacks in Supply Chain

Requirement of Cyber Certificate from Supply Chain Vendors

We asked survey respondents whether they require their supply chain vendors to provide a cyber certificate for their hardware and/or software.

64% indicated they have always required this, 32% started requiring it in 2021, and 5% plan to start requiring this in 2022.

This means that moving forward, every machine, system and device will need to be checked for cybersecurity, regulatory, and contractual requirements before delivery. In order to remain competitive, manufacturers will need to offer this cyber certificate - or risk losing business.

**Percentages will add up to more than 100% due to rounding*

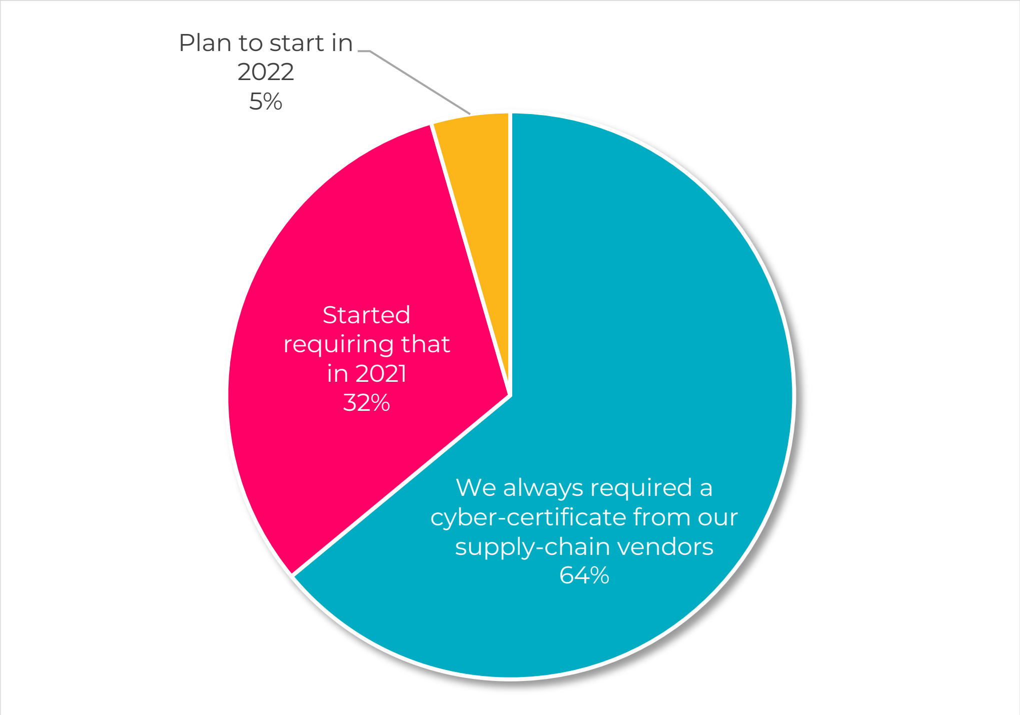

Figure 15 Requirement of Cyber Certificate

Broader Cybersecurity Challenges

Top OT Cybersecurity Concerns

100% of survey respondents are concerned about OT cybersecurity.

As we discussed in figure 17, this data shows the top OT cybersecurity concern is supply chain attacks (53%). Other top concerns include physical damage (43%) and data leakage (42%).

Physical damage can cause revenue loss due to lost production time or the cost of repairing and replacing expensive equipment. It can also have a measurable impact on health and safety.

Data leakage is also a top concern, as seen in OTORIO's recent report on open industrial control systems, which highlighted the risk of stolen credentials. New regulations are also adding to the financial pressure on asset owners – requiring the adoption of processes that are both costly and time-consuming.

Other notable concerns are downtime and ransomware (32%) and insider threats (25%).

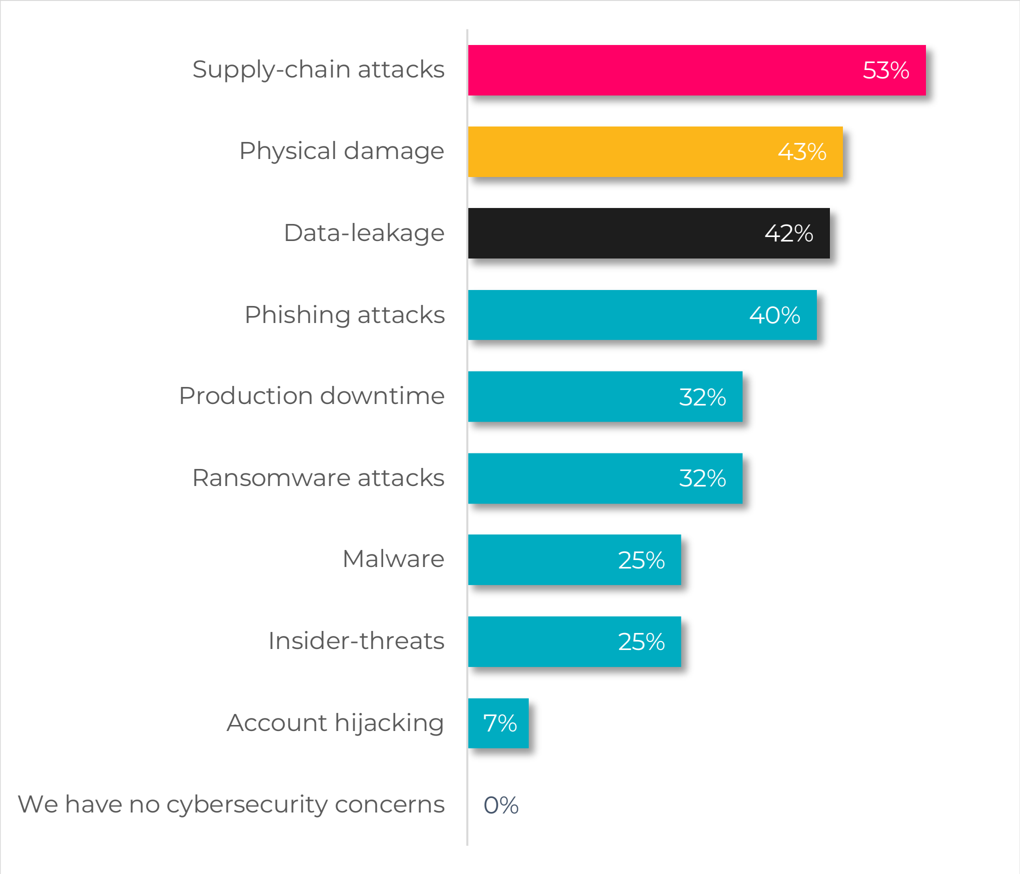

Figure 16 Top OT Cybersecurity Concerns

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

Visibility of OT Assets & Network Devices by Industry & Company Size

The adage "you can't protect what you can't see" holds true in OT cybersecurity. While organizations are aware of the need for visibility, not all attain it. Most companies (62%) report full, automated visibility. 36% report partial visibility and 3% report low visibility.

When comparing responses by company size, we see a trend similar to what we've seen before. The bigger the company is, the less full, automated visibility they have. Smaller companies lead with 81% indicating they have full, automated visibility, while only 49% of the large companies are reporting the same.

When comparing responses by industry, energy and utilities lead with 84% claiming full, automated visibility, followed by Oil & Gas (67%), while water treatment lags behind with only 26% indicating the same. It is notable that the water industry, which potentially has an immediate impact on health and wellbeing, has the lowest level of visibility of assets – and thus the highest level of cyber risk.

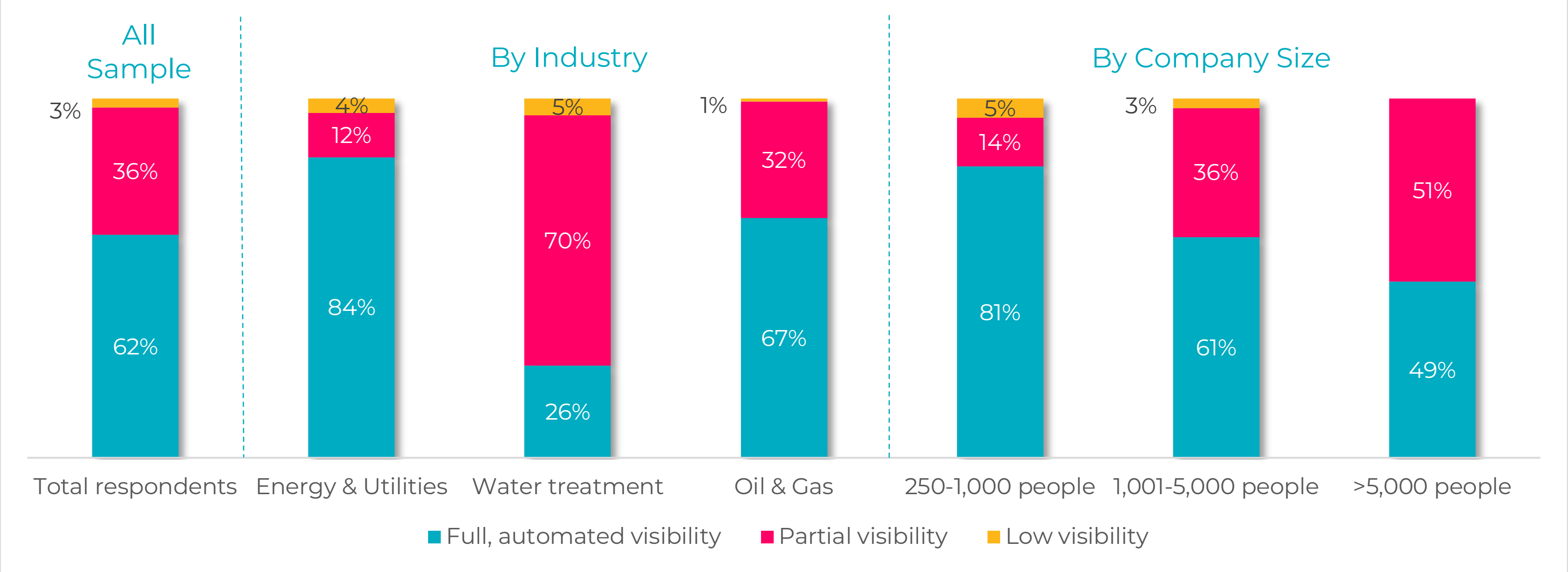

Figure 17 Level of Visibility of OT Assets & Network Devices by Industry & Company Size

Main Challenges with Existing OT Cybersecurity Solutions

Many organizations today are using a patchwork of cybersecurity systems - many of which are actually retrofitted IT solutions. These systems cannot provide either the contextual data or the relevant remediation steps for OT cybersecurity.

We asked survey respondents to rank their main challenges with existing OT cybersecurity solutions.

The top challenges were lack of skills to operate (57%), mitigation actions not being feasible (49%) and creating huge alert fatigue (44%).

It's clear that today, an OT-specific solution is needed that was built from the ground up to meet OT challenges.

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

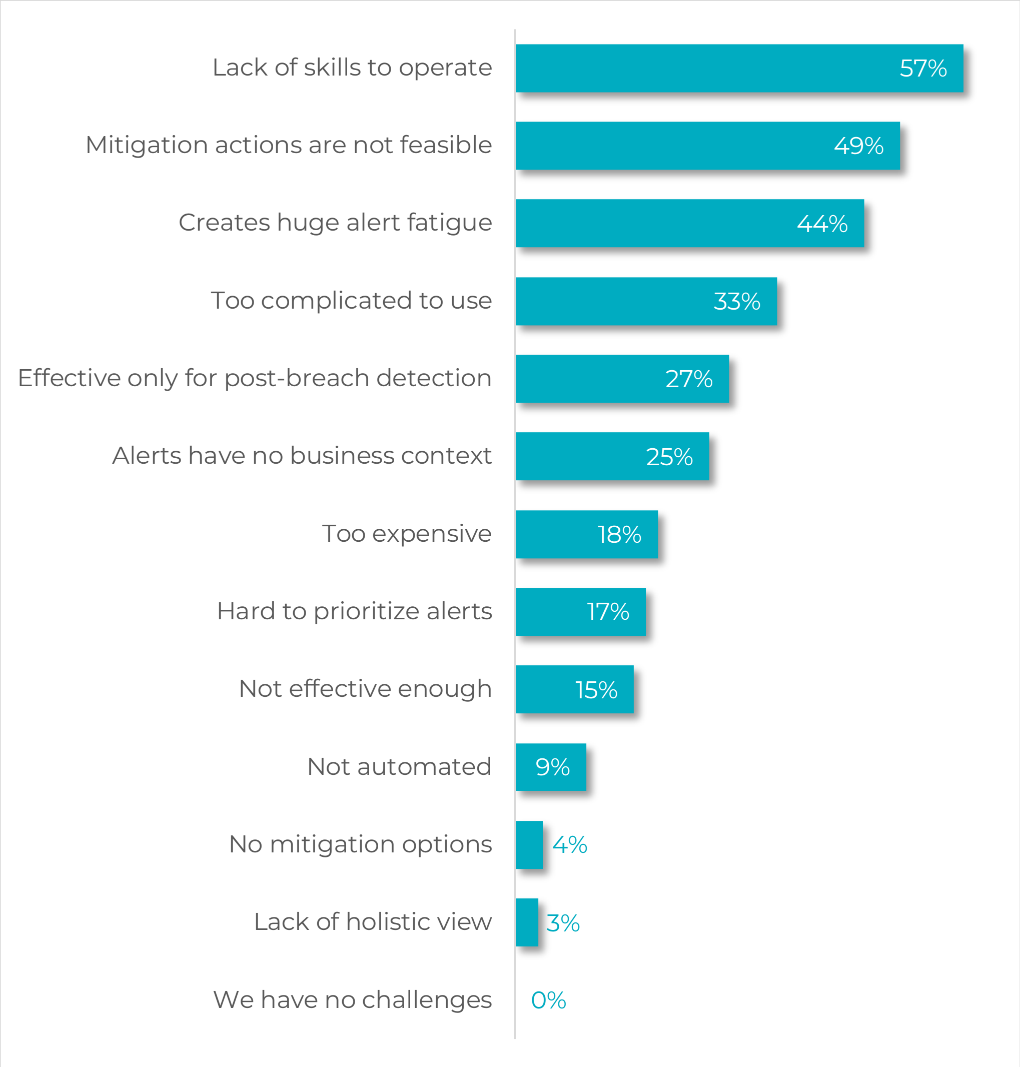

Figure 18 Challenges with Existing OT Cybersecurity Solutions

Changes in the Number of Regulations and Standards (Past 12 Months)

Most respondents (61%) indicated they are seeing a significant increase in the number of regulations and standards their organization needs to comply with. This aligns with the reasons respondents are making cybersecurity a priority.

When comparing responses by industry, energy and utilities reported the most significant increase in the number of regulations and standards (80%), compared to the Oil & Gas industry (61%) and the water treatment industry (37%).

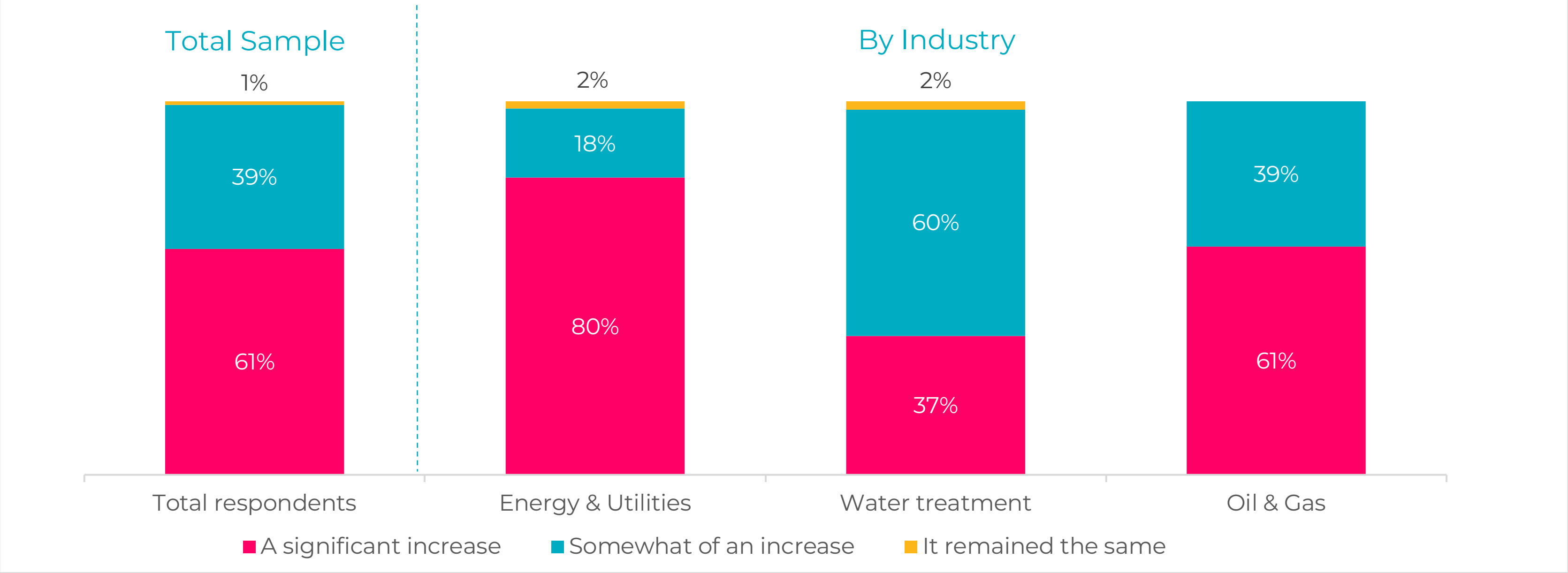

Figure 19 Changes in the Number of Regulations and Standards

Plans & Budgets

Top OT Cybersecurity Focus in the Coming Year

The top areas of focus in OT cybersecurity in the coming year will be to improve the organization's visibility and its asset inventory capabilities (39%), improve organization's detection capabilities (23%) and improve organization's response efficiency (20%).

To paraphrase Henry Ford – no one is thinking about the next innovation, everyone is looking for a faster horse! People are focused on improving what they have, but it's worth considering whether perhaps a new approach would solve more of their challenges.

One way to do so is to proactively identify risks and mitigate them before they become breaches. Moving from the Indication of Compromise (IOC) to an Indication of Exposure (IOE) approach makes OT cybersecurity simpler and far more efficient.

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

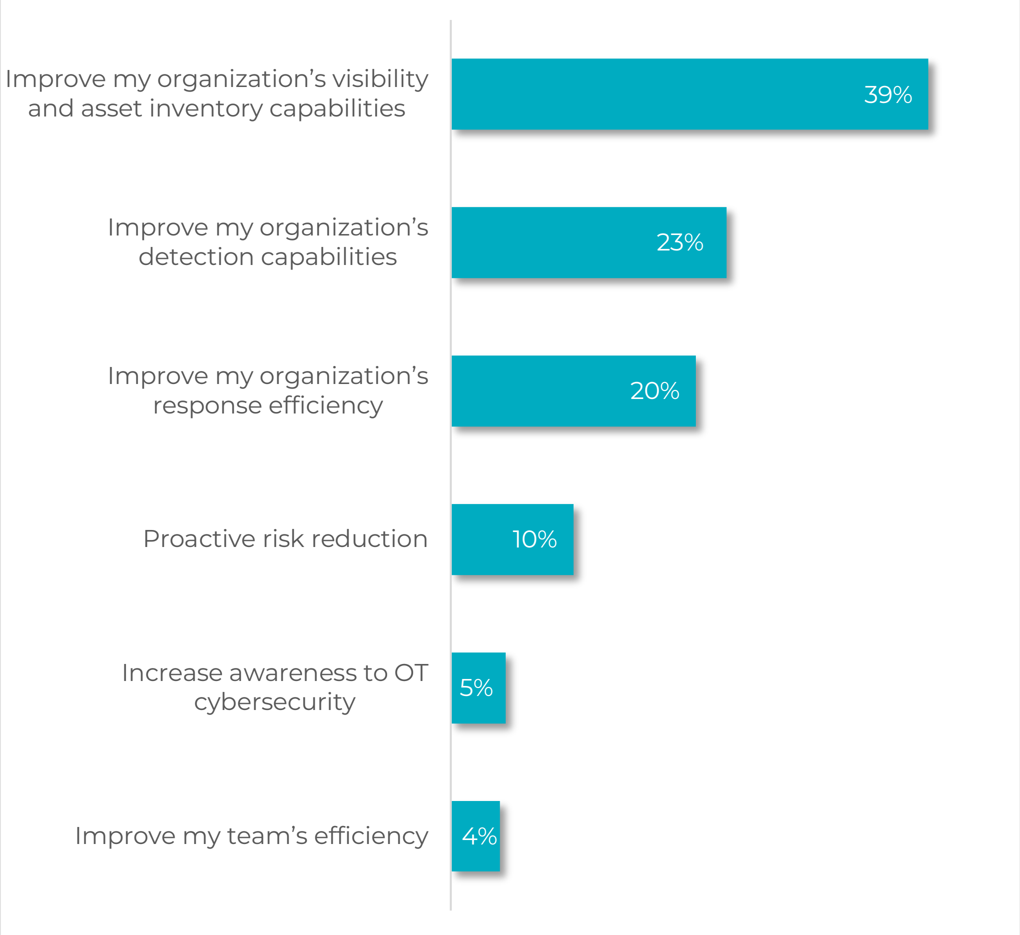

Figure 20 Top OT Cybersecurity Focus

OT Cybersecurity Budget Growth, 2022

99% of companies are planning to grow their OT cybersecurity budgets in 2022, with over half (54%) planning to grow it by more than 50%. OT cybersecurity is firmly on the organizational roadmap.

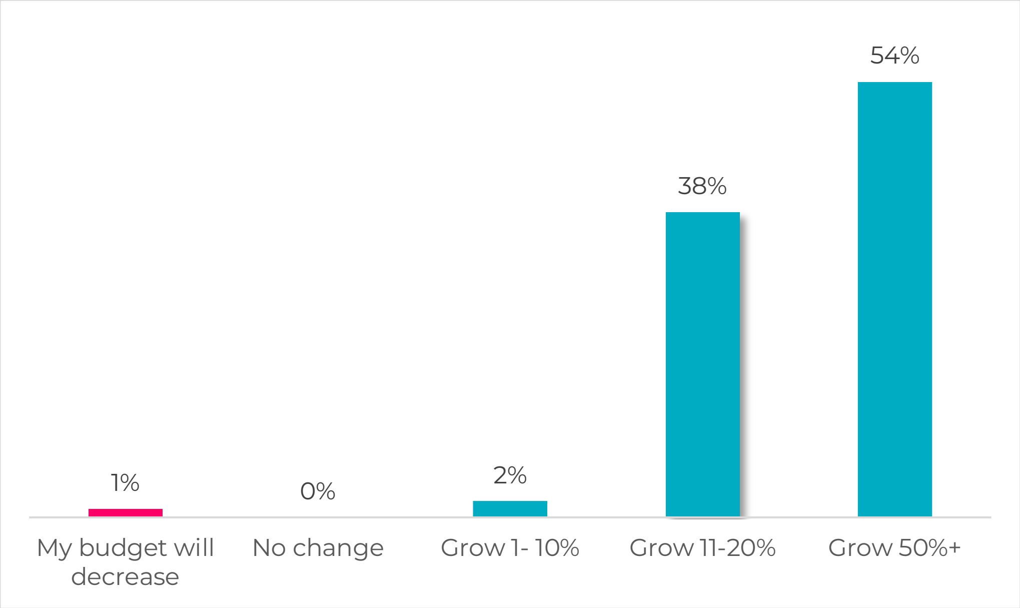

Figure 21 OT Cybersecurity Budget Growth, 2022

*Percentages do not add up to 100% due to rounding up of numbers

About OTORIO

OTORIO delivers the next generation of OT security and digital risk management solutions. The company combines the experience of top nation-state cybersecurity experts with cutting edge digital risk management technologies to provide the highest level of protection for critical infrastructure and the manufacturing industry. To learn more, visit our website at: www.otorio.com.

Request a Demo

For more information, please visit us:

Email: info@OTORIO.com