CLAROTY

SURVEY REPORT

THE GLOBAL STATE OF INDUSTRIAL CYBERSECURITY 2023:

New Technologies, Persistent Threats, and Maturing Defenses

Executive Summary

This independent, global survey of 1,100 information technology (IT) and operational technology (OT) security professionals who work full time for enterprises that own, operate, or otherwise support components of critical infrastructure, explores industry challenges faced in 2023, their impact to OT security programs, and priorities moving forward. Key findings include:

1. Ransomware attacks impacting OT environments are on the rise and remain costly

- Compared to our 2021 survey results, the primary impact of ransomware attacks has shifted from only IT environments to both IT ***and*** OT environments.[1] In 2021, **32%** of ransomware attacks impacted IT only, while **27%** impacted both IT and OT. Today, **21%** impact IT only, while **37%** impact both IT and OT. The impact to both IT and OT increasing **10%** in just two years is particularly significant.
- On a global basis, **69%** of targeted organizations paid the ransom, with the majority (**54%**) of attacks impacting multiple sites or functions. Of these attacks, over half of the organizations that paid the ransom suffered financial ramifications of $100,000 USD or more.

37%

of ransomware attacks on industrial organizations impact both IT and OT environments, a 10% increase from 2021 and a significant lead over those impacting IT only (21%).

The primary impact of ransomware attacks has shifted from only IT environments in 2021 to both IT and OT environments in 2023.

[1] https://claroty.com/resources/reports/the-global-state-of-industrial-cybersecurity

2. Demand for cyber insurance spikes as heightened ransomware activity leads to significant financial losses

- With two-thirds (**67%**) of organizations experiencing ransom attacks incurring $100,000 USD or more due to an incident, it's no surprise that survey trends have shown a large majority (**80%**) of organizations opting for cyber insurance policies.
- In the event of an attack, about half (**49%**) have opted for policies with coverage of half a million dollars or more.

80%

of industrial organizations have cyber insurance policies, half of which are $500K or more.

3. Industry regulations and standards are driving OT security priorities and investments

- Significantly, **45%** of respondents stated that TSA Security Directives have had the most significant impact on their organization's security priorities and investments.
- Trailing closely behind TSA Security Directives are CDM DEFEND with a **39%** response rate and ISA/IEC-62443 with **37%**.

Top three government regulations driving OT security measures are:

TSA Security Directives, CDM DEFEND, and ISA/IEC-62443

RESPONDENTS' TOP THREE OT SECURITY CHALLENGES

Risk Assessment

Asset, Change, and/or Life Cycle Management

Vulnerability Management

4. Generative AI is on the rise, and is fueling significant security concerns

- **61%** of respondents are currently utilizing security tools that leverage generative artificial intelligence (genAI).
- However, **47%** of those respondents claim that the use of genAI capabilities within their tools have raised their security concerns.

5. Progress and advancements are being made to close gaps in processes and technology

- Respondents reported that the most significant challenges or gaps within their OT security today are risk assessment; asset, change, and/or life cycle management; and vulnerability management. Organizations are working to fill these gaps in the next year, reporting at **43%** that risk assessment is their number one security initiative for 2024.
- Over three-fourths (**77%**) describe their approach to network segmentation as "Moderate" or "Mature," which is essential for restricting the lateral movement of cyberattacks through the network, including from IT to OT.
- Vulnerability management efforts are maturing. Over three-fourths (**78%**) described their approach to identifying vulnerabilities as "moderately" or "highly" proactive, which is a notable increase from **66%** in our 2021 survey.

61%

of respondents are using security tools with genAI capabilities, yet nearly half say this raises their security concerns.

78%

of respondents' approach to identifying vulnerabilities is "moderately" or "highly" proactive, a 12% increase from 2021.

Introduction

In recent years, organizations have been plagued by cyber attacks that exploit weaknesses inherent to the increasing interconnectivity of the information technology (IT) and operational technology (OT) environments that underpin their operations. Although this level of IT and OT convergence has brought about tremendous business value — enabling improvements in operations, efficiencies, performance, and quality of service — it has also expanded the attack surface for cybercriminals looking to exploit weaknesses in these already-inherently insecure environments. Furthermore, the impact of these incidents are not just financial, and at times have caused extreme operational disruptions, as seen in recent cyberattacks on MGM Resorts International, Clorox, Dole, and many others in 2023.

Looking to resolve these issues, organizations are making great strides in areas such as network segmentation and vulnerability management, as well as understanding where the gaps are in their OT security frameworks and implementing new measures to close those gaps in the years ahead.

TO UNDERSTAND HOW INDUSTRIAL ORGANIZATIONS ARE NAVIGATING THESE UNCHARTED WATERS, CLAROTY'S 2023 SURVEY FOCUSED ON:

Existing security programs and concerns for the future	Key cybersecurity challenges and their impact to the cyber landscape	The impact of industry standards and regulations on security posture	Priorities moving forward

Methodology

Claroty contracted with Pollfish to conduct a survey of 1,100 IT and OT security professionals in North America (500), Latin America (100), EMEA (250), and Asia-Pacific (250). Only individuals who work full time in IT security, OT security, or as an OT engineer/operator completed the survey, for a total of 1,100 respondents. More than a dozen industries are represented including Automotive, Chemical, Electric Utilities, Food & Beverage, Oil & Gas, Pharmaceutical & Biotechnology, Transportation, Water & Waste, Consumer Products, Mining & Materials, IT Hardware, and Forestry, Pulp & Paper. The survey was completed in November 2023.

Key Findings

Rise in ransom attacks remain costly

As IT and OT converge, and the threat landscape continues to expand, ransomware has remained a growing concern for those tasked with defending cyber-physical systems (CPS). Over the past several years, these ransomware attacks have grown increasingly targeted and have proved to no longer be confined to an organization's IT environment. Attacks globally have served as a wake-up call for CISOs and other decision makers looking to protect their critical infrastructure environments.

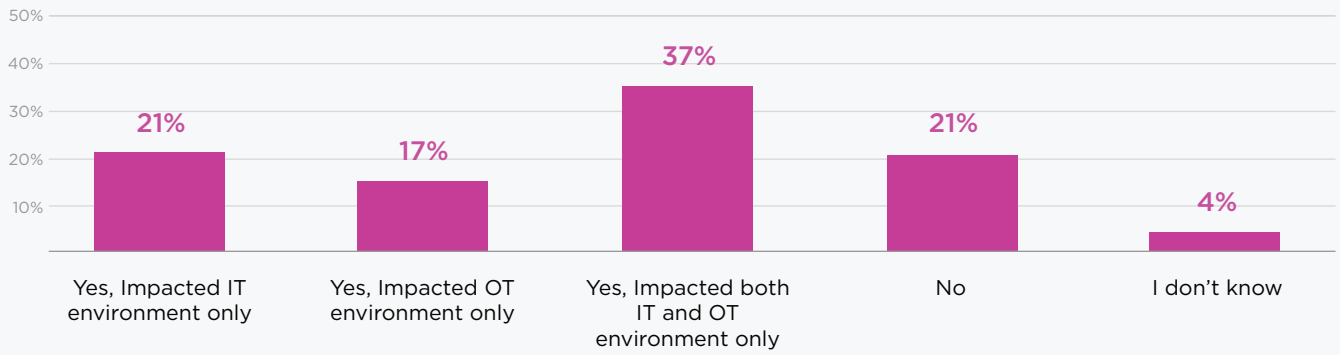
10%

increase in ransomware attacks from 2021 to 2023 that impacted both IT and OT environments.

On a global basis, **37%** of respondents reported that their organizations experienced a ransomware attack within the past year that impacted both IT and OT environments. This statistic is up **10%** in the last two years compared to findings from our 2021 Global State of Industrial Cybersecurity Report[2]. Of these incidents the majority of organizations suffered operational impact to their sites or functions. **32%** suffered moderate impact, while **12%** suffered extreme impact — causing operations to shut down for more than a week.

Q1. Has your organization experienced a ransomware attack within the past year?

GLOBAL

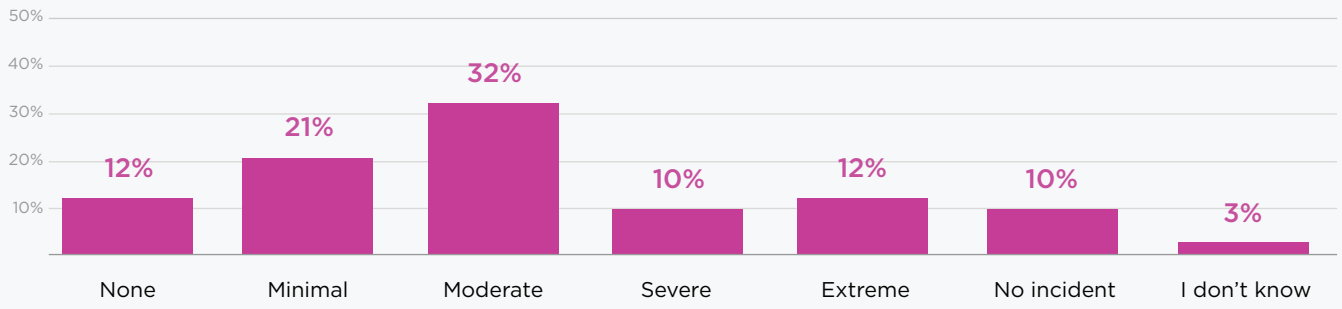


	NORTH AMERICA	SOUTH AMERICA	EUROPE	APAC
Yes – Impacted IT environment only	20%	30%	24%	18%
Yes – Impacted OT environment only	15%	24%	15%	20%
Yes – Impacted both IT and OT environments	48%	27%	29%	26%
No	16%	19%	26%	27%
I don't know	1%	0%	6%	10%

[2] https://claroty.com/resources/reports/the-global-state-of-industrial-cybersecurity

Q2. What was the scope of impact on operations?

GLOBAL



	NORTH AMERICA	SOUTH AMERICA	EUROPE	APAC
None - Operations were never shutdown	8%	12%	15%	15%
Minimal - Partially impacted a site or business/ government function	20%	27%	21%	21%
Moderate - Impacted more than one site or function for less than a week	36%	41%	31%	22%
Severe - Impacted more than one site or function for more than a week	10%	7%	10%	14%
Extreme - Significant or full operations shut down for more than a week	18%	5%	9%	8%
N/A - no incident	7%	8%	12%	14%
I don't know	1%	0%	2%	6%

Taking a deeper dive into the financial costs incurred, globally, the majority of organizations (**69% total**) made ransom payments following an incident. Of those paying ransom globally, the majority of the financial ramifications fell in the $100,000 - $499,000 USD range. Regionally, North America accounted for the highest respondents in this category at **23%**.

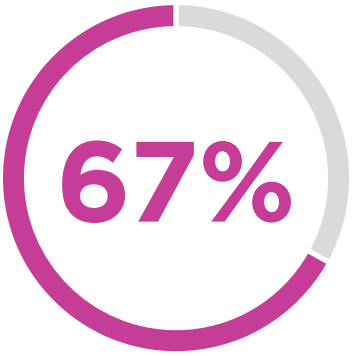
Over two-thirds of organizations made ransom payments following a ransomware attack in the past year.

Q3. Did your organization pay the ransom? If so, how much?

	GLOBAL	NORTH AMERICA	SOUTH AMERICA	EUROPE	APAC
No - we did not pay	26%	22%	31%	35%	25%
Yes - less than $100,000	15%	13%	22%	16%	16%
Yes - $100,000 - $499,000	19%	23%	19%	16%	16%
Yes - $500,000 - $999,000	16%	20%	11%	10%	14%
Yes - $1,000,000 - $5,000,000	12%	15%	11%	12%	8%
Yes - More than $5,000,000	6%	4%	6%	6%	12%
I don't know	5%	4%	0%	5%	8%

Demand for cyber insurance on the rise

As illustrated by our survey results, cybercrime is on the rise and the damage has continued to grow. According to Cybercrime Magazine, global cybercrime damage costs are expected to grow by **15%** per year over the next three years, reaching $10.5 trillion USA annually by 2025, up from $3 trillion USD in 2015[3]. This has contributed significantly to the global demand for cyber insurance.



Organizations who experienced a ransomware attack incurred **$100,000 USD or more** in financial costs.

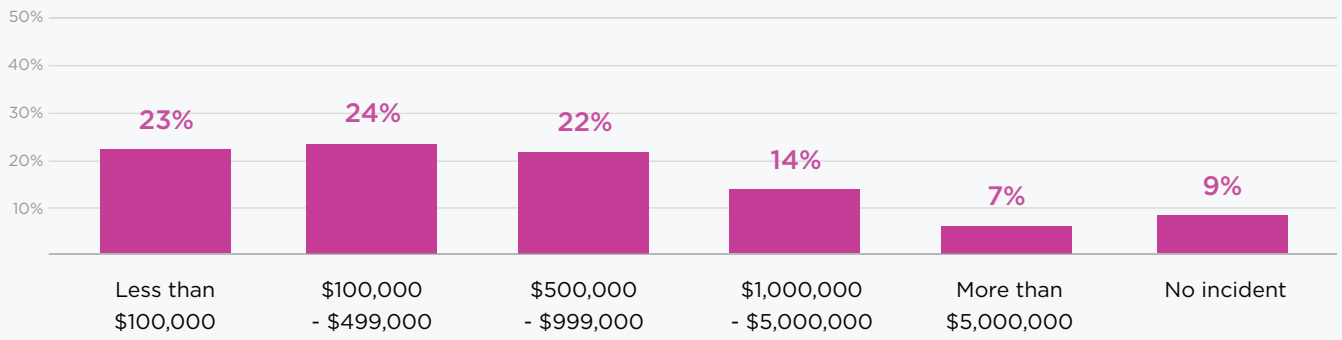
Organizations globally currently have a cyber insurance policy.

The escalating financial ramifications from incidents are displayed globally, with two-thirds (**67%**) of organizations who experienced a ransomware attack incurring $100,000 USD or more in financial costs. Regionally, the most significant impact financially was reported by the Asia-Pacific region (APAC) with **14%** of respondents stating that their estimated total financial cost incurred due to a ransomware attack was more than $5,000,00 USD. To address the growing threat of ransomware, we have seen that a large majority (**80%**) of organizations globally currently have a cyber insurance policy. In order to relieve the pain of significant financial ramifications, about half (**49%**) have opted for policies with coverage of half a million dollars or more.

[3] https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

Q4. What was the estimated total financial cost incurred by your organization due to the ransomware attack?

GLOBAL



	NORTH AMERICA	SOUTH AMERICA	EUROPE	APAC
Less than $100,000	18%	27%	31%	24%
$100,000 - $499,000	25%	25%	26%	20%
$500,000 - $999,000	28%	21%	14%	18%
$1,000,000 - $5,000,000	17%	13%	14%	11%
More than $5,000,000	6%	7%	3%	14%
I don't know	6%	7%	12%	14%

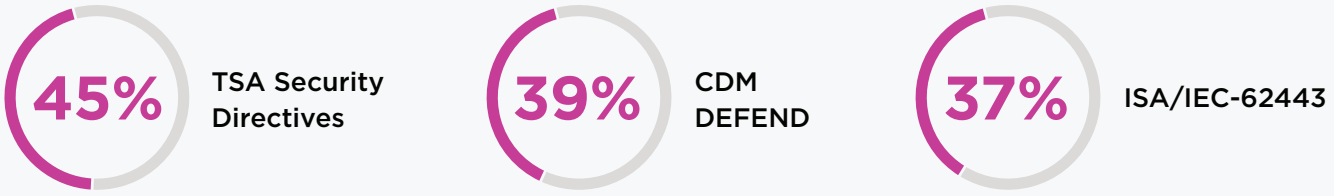
Q5. Does your organization currently have a cyber insurance policy? If yes, how much does the policy cover in the event of a cyber attack?

	GLOBAL	NORTH AMERICA	SOUTH AMERICA	EUROPE	APAC
No - we have not applied for a policy	10%	7%	12%	10%	17%
No - we applied for a policy, but were denied coverage	5%	2%	4%	9%	8%
Yes - less than $100,000	10%	9%	17%	11%	8%
Yes - $100,000 - $499,000	21%	23%	18%	22%	16%
Yes - $500,000 - $999,000	17%	23%	12%	14%	9%
Yes - $1,000,000 - $4,999,000	18%	18%	13%	19%	17%
Yes - $5,000,000 - $10,000,000	9%	12%	11%	5%	8%
Yes - more than $10,000,000	6%	4%	10%	6%	7%

Security priorities are guided by industry regulations and standards

Reiterated by our survey results, cybersecurity incidents are on the rise and show no signs of slowing down. These incidents, amongst many other high-profile attacks in recent years, have propelled the issue into the legislative and regulatory spotlight. As the threat landscape continues to expand, governments, regulatory agencies, and companies worldwide are taking action to increase oversight of cybersecurity incidents. Although this oversight has rapidly demanded organizations to strengthen their security measures, the primary challenge has become balancing the protection critical OT operations while adhering to strenuous rules and regulations.

TOP REGULATIONS DRIVING OT SECURITY MEASURES



According to our survey respondents globally, the top three government regulations and standards that significantly impact their organizations' OT security priorities and investments are the TSA Security Directives, selected by **45%** of global respondents, followed by CDM DEFEND at **39%**, and ISA/IEC-62443 at **37%**. Regionally, it appears that TSA Security Directives have had the highest influence in North America and Latin America (LATAM), selected by **49%** of respondents in both regions.

Q6. Which of the following government regulations and standards have a significant impact on your organization's OT security priorities and investments? Select all that apply:

	GLOBAL	NORTH AMERICA	SOUTH AMERICA	EUROPE	APAC
CDM DEFEND	39%	45%	38%	32%	35%
CMMC	33%	39%	20%	28%	34%
FISMA	35%	40%	28%	32%	32%
ISA/IEC-62443	37%	34%	38%	34%	44%
NERC CIP	29%	31%	16%	28%	31%
NIST-CSF	27%	28%	17%	22%	34%
NIS2	24%	24%	19%	22%	28%
FRCS and/or U.S. NDAA Section 1505	29%	36%	22%	20%	28%
TSA Security Directives	45%	49%	49%	41%	40%
I don't know	12%	5%	11%	16%	23%
Other	0%	1%	0%	0%	0%

Generative AI is on the rise and causing security concerns

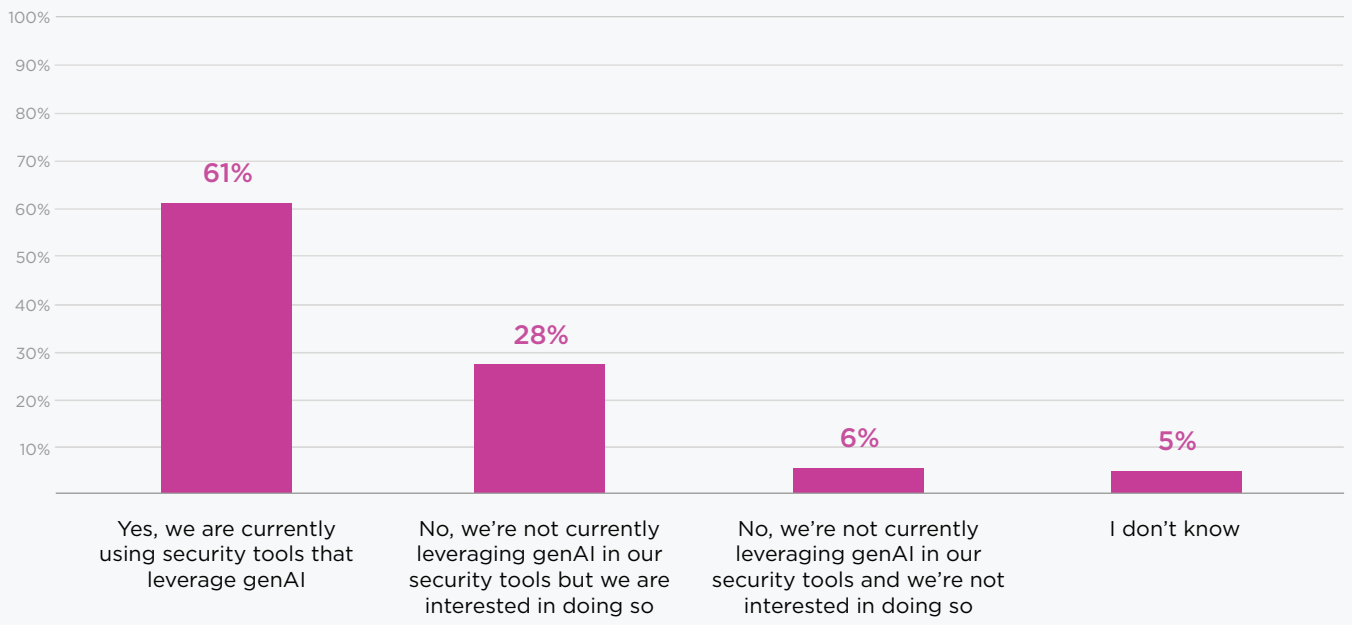
Recently, generative artificial intelligence (genAI) has become increasingly integrated into various aspects of our lives. It has the potential to revolutionize many industries and bring about significant advancements in technology; however, it has also brought about security concerns for many organizations. In cybersecurity, AI-powered solutions have the potential to enhance threat detection, incident response, authentication, and more. However, many fear that attackers will manipulate or deceive AI systems, the technology itself may be misused, or the large amounts of data that AI technology relies on will create privacy issues, among others.

> Most organizations are using security tools that leverage genAI, yet nearly half feel that this raises their security concerns.

Significantly, over **60%** of survey respondents reported that their organization is currently utilizing security tools that leverage genAI. There were some variations across regions, with LATAM reporting the highest use at **73%**, followed by North America at 69%, EMEA at **54%**, and APAC at **46%**. Although the majority of organizations have adopted genAI technology, of the **60%** average globally, **47%** of those respondents claimed that the use of genAI capabilities have raised their security concerns.

Q7. Do you ever receive inquiries from within your organization about whether you are using genAI or how you could be using genAI within your security tool set? Select the statement that best represents your response:

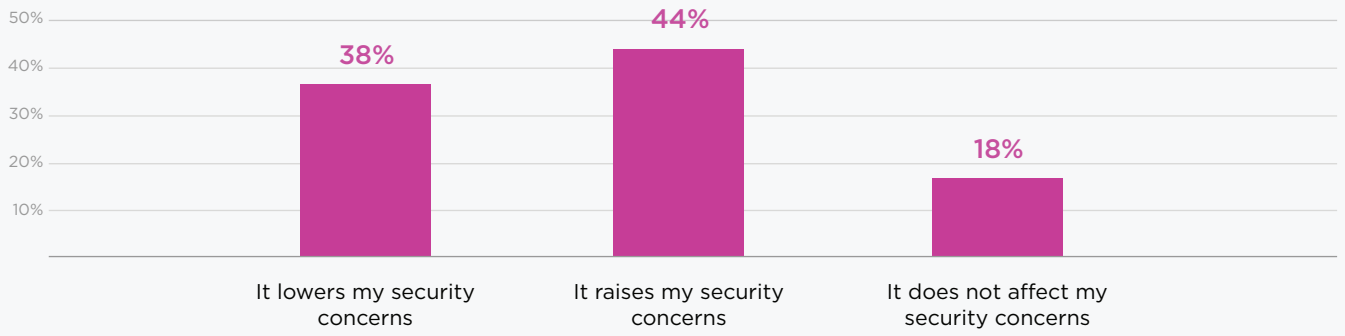
GLOBAL



	NORTH AMERICA	SOUTH AMERICA	EUROPE	APAC
Yes, we are currently using security tools that leverage genAI	69%	73%	54%	46%
No, we're not currently leveraging genAI in our security tools but we are interested in doing so	27%	26%	34%	26%
No, we're not currently leveraging genAI in our security tools and we're not interested in doing so	3%	1%	8%	14%
I don't know	1%	0%	5%	14%

Q8. Which of the following statements best represents your feelings towards the use of genAI capabilities within your security tools?

GLOBAL



	NORTH AMERICA	SOUTH AMERICA	EUROPE	APAC
It lowers my security concerns	35%	48%	36%	41%
It raises my security concerns	52%	36%	40%	38%
It does not affect my security concerns	14%	16%	23%	21%

> Many organizations have a difficult time prioritizing OT cyber risk to most effectively combat the most dangerous threats in their environment.

Organizations show continued progress and maturity, implementing new measures to close gaps in OT security posture

Many organizations understand how severe cyber attacks can be on their OT systems; however, they tend to have a difficult time prioritizing OT cyber risk to most effectively combat the most dangerous threats in their environment. Without OT risk management strategies and solutions to mitigate the potential risks and uncertainties in their critical infrastructure environment, organizations will continue to face challenges in managing their OT cyber risk. Our survey results show that industry professionals understand this need, as the top three OT security challenges are risk assessment (selected by **16%** of respondents globally), asset, change, and/or lifecycle management (**15%**), and vulnerability management (**14%**).

Q9. Which of the following would you consider to be the biggest challenge or most significant gap in your organization's OT security?

	GLOBAL	NORTH AMERICA	SOUTH AMERICA	EUROPE	APAC
Asset discovery	6%	5%	6%	5%	10%
Asset, change, and/or lifecycle management	15%	20%	12%	11%	12%
Risk assessment	16%	17%	18%	13%	15%
Vulnerability management	14%	13%	21%	14%	12%
Network segmentation	10%	8%	5%	10%	15%
Endpoint security	12%	12%	7%	16%	8%
Secure remote access	11%	11%	12%	10%	10%
Threat detection	12%	12%	19%	12%	12%
I don't know	4%	2%	0%	8%	5%
Other	0%	0%	0%	1%	0%

MOST COMMON INITIATIVES RESPONDENTS PLAN TO INSTITUTE NEXT YEAR

43%
Risk Assessment

40%
Asset, Change, and/or Life Cycle Management

39%
Vulnerability Management

Fortunately, the OT security initiatives that organizations have planned in the near future are consistent with the challenges cited above. According to survey respondents globally, the most common initiatives they plan to institute in the next year are risk assessment (selected by **43%** of respondents), followed closely by asset, change, and/or lifecycle management (**40%**) and vulnerability management (**39%**).

Q10. Which of the following OT-specific security initiatives do you plan to institute in the next year? Select all that apply:

	GLOBAL	NORTH AMERICA	SOUTH AMERICA	EUROPE	APAC
Asset discovery	35%	41%	33%	28%	31%
Asset, change, and/or lifecycle management	40%	48%	35%	30%	36%
Risk assessment	43%	46%	50%	38%	40%
Vulnerability management	39%	49%	46%	27%	29%
Network segmentation	35%	36%	33%	35%	34%
Endpoint security	37%	43%	36%	30%	33%
Secure remote access	36%	40%	39%	26%	35%
Threat detection and response via existing SOC	32%	41%	19%	24%	28%
Threat detection and response via new, OT-specific SOC	34%	42%	30%	27%	28%
I don't know	8%	2%	1%	11%	17%
None of the above	1%	1%	1%	2%	2%
Other	0%	0%	0%	0%	0%

Another positive is that organizations are demonstrating progress and maturity in other key areas. Over three-fourths (**77%**) of global respondents described their approach to network segmentation as "Moderate" or "Mature," meaning they have segmented enterprise IT, contractor, visitor, and other networks from industrial assets, as well as further segmented different types of industrial assets or functions to different zones. The **30%** who chose "Mature" have taken these measures even further by implementing granular microsegmentation between different asset types, functions, and/or production lines.

With proper OT network segmentation, organizations can prevent the spread of cyberattacks by restricting their lateral movement through the network. This security measure is particularly important in light of the earlier survey findings on the growing impact of ransomware attacks on both IT and OT environments (as shown in Q1).

77%

Over three-fourths (77%) of global respondents described their approach to network segmentation as "Moderate" or "Mature."

Q11. Which of the following best describes your approach to network segmentation for industrial cyber-physical systems (OT/ICS/IIoT)?

	GLOBAL	NORTH AMERICA	SOUTH AMERICA	EUROPE	APAC
Mature: We have fully segmented our enterprise IT, contractor, visitor, and other networks from our industrial assets, as well as implemented granular microsegmentation between different asset types, functions, and/or production lines	30%	36%	32%	27%	21%
Moderate: We have segmented our enterprise IT, contractor, visitor, and other networks from our industrial assets, as well as further segmented different types of industrial assets or functions to different zones	47%	51%	57%	47%	34%
Basic: We have segmented our enterprise IT systems, contractor, visitor, and other networks from our industrial assets	12%	10%	9%	12%	16%
Entry: We are in the process of implementing network segmentation between our industrial assets and enterprise IT systems	5%	2%	1%	6%	11%
None: We have not implemented network segmentation	3%	0%	1%	4%	10%
I don't know	3%	1%	0%	4%	9%

RESPONDENTS WITH MODERATELY TO HIGHLY PROACTIVE VULNERABILITY MANAGEMENT

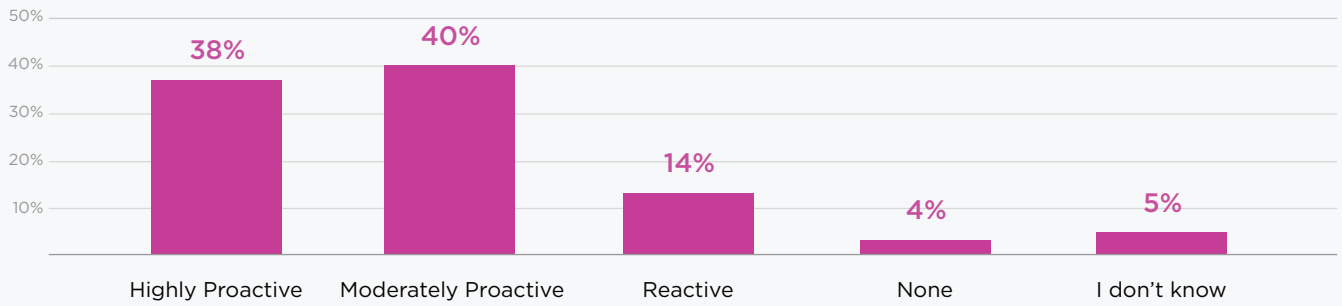
12%

Increase from 2021 when respondents described their approach to identifying vulnerabilities as "moderately" or "highly" proactive.

Additionally, organizations' approach to identifying vulnerabilities has improved over the last two years. As industrial environments often contain legacy systems riddled with unpatched vulnerabilities, reducing risk requires the ability to identify, prioritize, and remediate common vulnerabilities and exposures (CVEs) effectively and efficiently. Over three-fourths (**78%**) of respondents described their approach to identifying vulnerabilities as "moderately" or "highly" proactive, meaning they frequently or continuously assess industrial assets for vulnerabilities – a notable increase from **66%** in the 2021 survey results.

Q12. Which of the following best describes your current approach to identifying vulnerabilities in industrial cyber-physical systems (OT/ICS/IIoT)?

GLOBAL

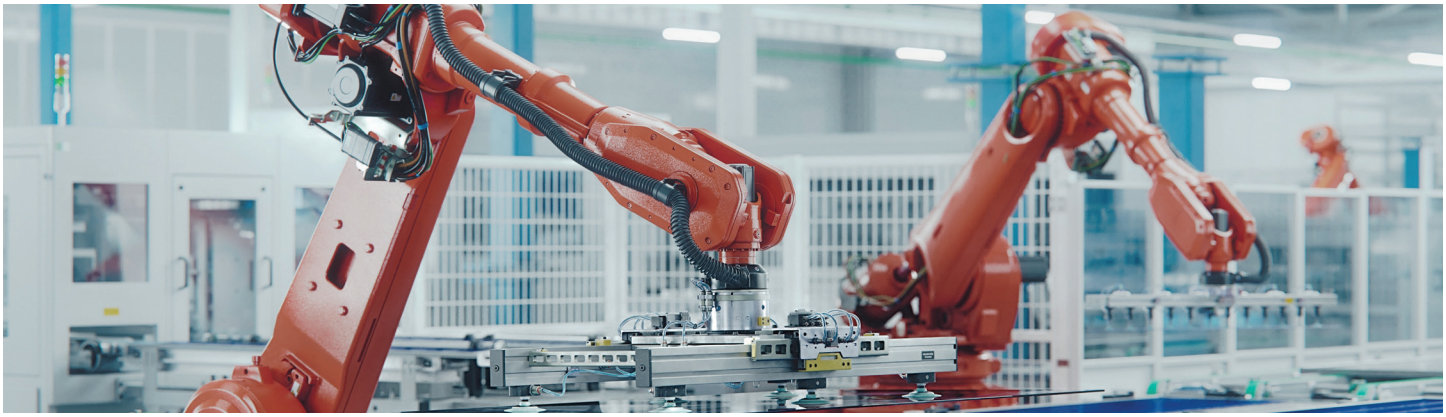


	NORTH AMERICA	SOUTH AMERICA	EUROPE	APAC
Highly Proactive: We continuously assess our industrial assets for vulnerabilities	42%	45%	32%	33%
Moderately Proactive: We frequently assess our industrial assets for vulnerabilities	42%	45%	44%	30%
Reactive: We have a dedicated team/process for assessing vulnerabilities affecting our industrial assets when brought to our attention by a third party	13%	7%	14%	16%
None: We do not have an established process for assessing our industrial assets for vulnerabilities	1%	2%	4%	10%
I don't know	1%	1%	6%	11%

TOP VULNERABILITY RISK SCORING METHODS

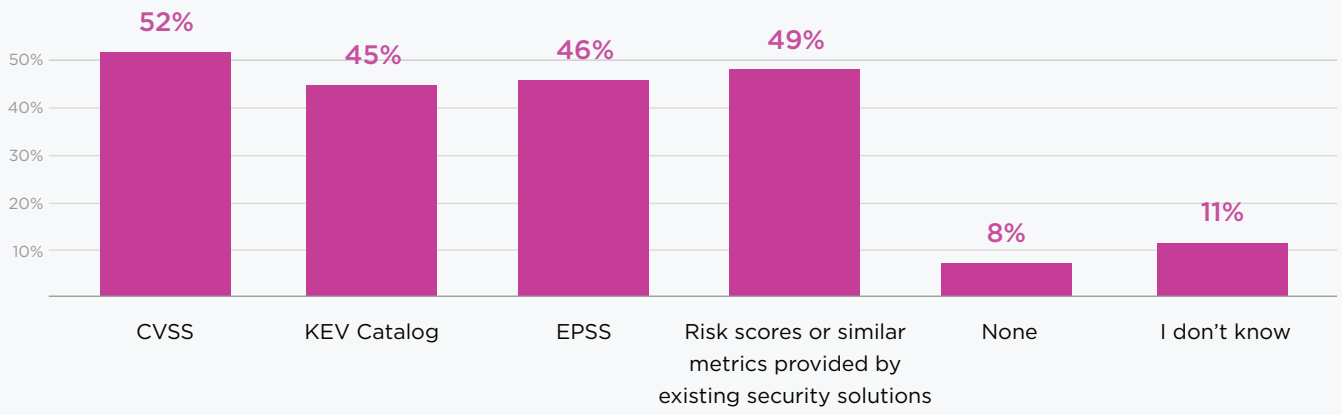
Common Vulnerability Scoring System (CVSS)	Existing Security Solutions' Risk Scores	Exploit Prediction Scoring System (EPSS)	Known Exploited Vulnerabilities (KEV) Catalog

Looking further into vulnerability and risk management strategies, respondents indicated that they use multiple risk scoring methods to prioritize vulnerabilities impacting their industrial CPS assets. The most popular is the Common Vulnerability Scoring System (CVSS), used by **52%** of global respondents, followed by existing security solutions' risk scores (**49%**), the Exploit Prediction Scoring System (EPSS) (**46%**), and the Known Exploited Vulnerabilities (KEV) Catalog (**45%**). These results highlight just how difficult vulnerability management can be, especially in CPS environments, where patching everything is often impossible or too complex to execute.



Q13. Which of the following are used to inform your current approach to prioritizing vulnerabilities in industrial cyber-physical systems (OT/ICS/IIoT)? Select all that apply:

GLOBAL



	NORTH AMERICA	SOUTH AMERICA	EUROPE	APAC
Common Vulnerability Scoring System (CVSS)	62%	54%	42%	43%
Known Exploited Vulnerabilities (KEV) Catalog	54%	42%	40%	36%
Exploit Prediction Scoring System (EPSS)	54%	49%	36%	38%
Risk scores or similar metrics provided by existing security solutions	59%	49%	40%	38%
None - We do not have an established process for prioritizing vulnerabilities in our industrial assets	5%	5%	8%	16%
I don't know	2%	2%	17%	25%

Recommendations

This survey shows that industrial organizations are increasingly prioritizing cybersecurity and compliance. However, given the prevalence, variety, and impact of cyber attacks, there are opportunities to further strengthen their security programs in order to ensure cyber and operational resilience. The following three recommended practices can help security leaders and their teams address their top pain points and priorities head-on as they navigate today's hyper-connected world:

Identify

Integrate

Extend

1. Gain visibility into all CPS in your OT environment

A comprehensive inventory of all CPS assets – OT, IoT, IIoT, and BMS — within the environment is the foundation of effective industrial cybersecurity. However, gaining this visibility is one of the most challenging tasks facing security and risk leaders today. This is largely because CPS assets typically use proprietary protocols that are incompatible with, and therefore invisible to, generalized security tools. Critical infrastructure environments may also encompass a diverse mix of new and legacy devices that communicate and operate in different ways, making it even more difficult to answer the question of what devices are in the environment. Further complicating matters is the fact that there is no one-size-fits-all path to asset discovery. Every CPS environment is unique, and most contain complexities that render certain asset discovery methods ineffective. That's why it is key to ensure your CPS security solutions offer multiple, highly flexible discovery methods that can be mixed and matched to deliver full visibility in the manner best suited to your distinct needs.

2. Integrate your existing IT tech stack and workflow

Chances are, once you have an understanding of all connected devices, you may notice gaps in governance across traditional IT workflows. Responses to Q7 indicate that respondents already utilize some IT-oriented solutions and tools in their cybersecurity program, including genAI. Rather than expanding your already-extensive tech stack, it is important to find CPS security solutions that integrate with these solutions. By extending your existing tools and workflows from IT to CPS, you can safely uncover risk blindspots without endangering operational outcomes. This strategy will help industrial organizations to take control of their environment and create further visibility across traditionally siloed teams by simply extending existing tools and workflows from IT to CPS.

3. Extend IT security controls & governance to the CPS environment

Unlike their IT counterparts, most CPS environments lack essential cybersecurity controls and consistent governance. That's because legacy systems in many CPS environments were built with a focus on functionality and operational reliability, rather than security, as these systems were not initially intended to be connected to the internet. The rise of internet connectivity has caused these previously "air-gapped" systems to converge with IT networks, which were not designed to be connected and managed in the same way. The rapid advancement of digital transformation, as well as remote and hybrid working environments, have left security teams with a lack of awareness and understanding about the unique challenges of these newly interconnected CPS environments. Without CPS-specific security teams or solutions in place, organizations will suffer from a lack of consistent governance and controls. To resolve this, organizations should evaluate CPS security vendors that can help to extend your IT controls to CPS by unifying your security governance and driving all use cases on your journey to cyber and operational resilience.

Once these three key principles are established, they can be utilized to achieve any, or all, of the following goals on your organization's journey to cyber and operational resilience:

Asset Management

Network Protection

Vulnerability & Risk Management

Threat Detection

1. **Asset Management.** Effective, efficient asset management is integral to operational resilience. However, because industrial assets use proprietary protocols that are incompatible with standard inventory tools, require manual maintenance, and error-prone inventories remain common, achieving asset management can prove difficult. Operational risks are also prominent as manual asset management processes are no match for the pace at which vulnerabilities, end-of-life indicators, outdated firmware, and other risks are emerging. Industrial organizations require a solution that supports proprietary industrial protocols through multiple collection methods, continuously monitors and analyzes asset activity with alerts to any changes, and optimizes workflows via reporting and integrations. These functionalities help streamline SLA tracking and create alignment across enterprise IT and industrial CPS environments.

2. **Network Protection.** Network segmentation and secure remote access are Zero Trust controls that help protect industrial environments. However, effectively segmenting industrial networks can be a tedious, error-prone process that entails defining and constantly tuning policies to your unique environment. Monitoring and ensuring compliance with regulatory and organization measures is also a challenging task — requiring granular, properly tuned policies that many organizations lack. Unsecured remote access is also a widespread challenge, as common practices are risky and inefficient in industrial environments. To combat these challenges, industrial organizations require a solution that provides recommended segmentation policies that can be easily and automatically enforced via your existing infrastructure, enables continuous monitoring to understand how assets communicate under normal circumstances (allowing for automatic alerts to any policy violations), and ensures support for all industrial use cases by tightly controlling, monitoring, and securing remote sessions.

3. **Vulnerability & Risk Management.** Finding a vulnerability is only the first step. You then need to assess the affected asset's context and potential impact on your operations to prioritize and remediate the risk, as the sheer volume of vulnerabilities is often too overwhelming to address all at once. However, industrial assets and environments have a low tolerance for downtime and the traffic generated by standard vulnerability scanners, so patching occurs rarely, no matter the vulnerability or risk. That's why industrial organizations need a CPS security solution that accurately matches exact assets with known CVEs based on vendor, model, and firmware version, identifies and analyzes known risks to calculate the most likely scenario in which an attacker could compromise the network, and evaluates and scores vulnerabilities based on not just severity (CVSS scores) but also exploitation likelihood (KEV catalog and EPSS scores) — enabling more efficient and effective prioritization and remediation.

4. **Threat Detection.** Although discovering, assessing, and protecting CPS environments are essential to preventing cyberattacks, sometimes a breach is inevitable no matter what measures you have in place. This is because the complexity of industrial environments makes it extremely difficult to identify potentially malicious deviations from accepted baselines. Additionally, the proprietary protocols in industrial environments are incompatible with traditional threat detection tools, rendering them ineffective and potentially disruptive. Due to the complexity, inherent insecurity, and a growing CPS attack surface, industrial environments are increasingly targeted by malicious actors. Therefore, industrial organizations require a security solution that offers multiple detection engines to automatically profile all assets, communications, and processes in industrial networks, and has a deep understanding of proprietary protocols and asset behaviors to ensure each asset receives the security policy appropriate for it. The solution should also provide a portfolio of threat capabilities that seamlessly integrate with your existing tech stack to bridge the IT-OT expertise gap.

Conclusion

Cybersecurity challenges in the industrial sector continue to grow, as IT and OT networks converge and the attack surface for cyber criminals expands. This was clearly revealed in the responses to our survey questions on ransomware attacks and the financial and operational damage they cause. Unsurprisingly, due to the rise in ransomware attacks and resulting payments, the majority of respondents indicated that their organizations have opted to elect for cyber insurance policies. As another subsequent result of increased cyber attacks, we have seen a rise in industry regulations and standards, which have driven security priorities and investments. As generative AI solutions continue to advance, and new and more advanced threats emerge, organizations must adhere to cybersecurity best practices and partner with the right CPS security vendor to ensure that their unique environment is protected. With strong security leadership in place, well-rounded security programs implemented, and adherence to guidelines and frameworks from regulatory bodies, industrial organizations are on the right track to ensuring cyber and operational resilience.

About Claroty

Claroty empowers organizations to secure cyber-physical systems across industrial, healthcare, commercial, and public sector environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide comprehensive controls for visibility, risk and vulnerability management, threat detection, and secure remote access. Backed by the leading investment firms and industrial automation vendors, Claroty is deployed at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America.

For more information, visit claroty.com or email contact@claroty.com.