REPORT

2022 State of Operational Technology and Cybersecurity Report

TABLE OF CONTENTS

Infographic: Key Findings

People

33% of organizations entrust OT security to the VP/director of network engineering/ operations

67% of OT security leaders come from an OT engineering background

43% of respondents have security-incident response time as a top-three success measurement

Security Posture

56% of organizations report being at level 3 or level 4 of OT security maturity

50% say the OT security posture is a significant factor in the overall risk score

13% of organizations have centralized visibility of all OT activities

Security Practices

48% report security compromises to executive management

32% have deployed role-based network access control

52% say all OT activities are monitored and tracked by the SOC

Security Outcomes

93% of organizations had 1+ intrusions in the past year; **78%** had 3+

61% of intrusions impacted OT systems

90% of intrusions required hours or longer to restore service

Best Practices

Top-tier organizations are more likely to

- Have centralized visibility
- Be measured by vulnerability response time
- Deploy role-based NAC
- Report security compromises
- Use a single OT device vendor

Executive Summary

The 2022 State of Operational Technology and Cybersecurity Report, now in its fourth annual iteration, finds that organizations are still moving too slowly toward full protection of their operational technology (OT) assets. This comes at a time when OT systems are becoming more important to many organizations' well-being, geopolitical events are making attacks more likely, more OT systems are being connected to the internet, and IP-based threats are becoming more advanced and doing more damage. This combination of factors is moving OT security upward in many organizations' risk portfolio.

Based on a global survey of more than 500 OT security professionals, this year's report finds that while OT security has the attention of organizational leaders, it continues to be owned by relatively low-ranking professionals. Speculation that OT security will be rolled under the CISO has been active for years, but there is no sign that things are moving in that direction. And while security is a part of the performance measurements for most survey respondents, many are measured more on efficiency factors that might bring the temptation to cut corners on security.

Based on a global survey of more than 500 OT security professionals, this year's report finds that while OT security has the attention of organizational leaders, it continues to be owned by relatively low-ranking professionals.

Organizations repost modest moves forward in the overall maturity of their OT security posture, with slightly more of them having advanced to level 3. But looking at specific best practices brings nuance to the issue. Only 13% of respondents have achieved centralized visibility of all OT activities, and only 52% are able to track all OT activities from the security operations center (SOC). Only around half of respondents claim to track and report various basic security metrics, and fewer than half of respondents are using any of a dozen specific security technologies and practices. The latter indicates a diversity in how organizations address OT security and reflects a market that is still evolving.

One thing that has improved very little in the past year is organizations' security outcomes. A staggering 93% of organizations experienced an intrusion in the past 12 months, and 78% experienced more than three. Impacts included downtime, financial or data loss, brand degradation, and even reduced physical safety. Clearly, most organizations have work to do. Fortunately, a small percentage of respondents managed to avoid intrusions for the past year, and this report identifies several of the best practices they are more likely to employ.

Introduction

While OT is less visible than IT at most organizations—and certainly in the public consciousness—it is no less important to the economy and to people's everyday lives. After all, OT systems control the critical infrastructure that everyone depends on—the electrical grid, water and sewer systems, fuel pipelines, power plants, and transportation networks. And it is essential for the manufacture of all types of goods.

OT is an important component of digital transformation at industrial organizations. Rapidly evolving market conditions made the adoption of "Industry 4.0" methodologies and technologies virtually essential even before COVID-19. The pandemic only accelerated these trends, leaving technology "have-nots" scrambling to update and streamline their operations.[1]

Growing Security Threats

This trend has not escaped the notice of threat actors. Last year, the Global Threat Landscape Report from FortiGuard Labs noted a significant increase in intrusion prevention system (IPS) detections in OT systems.[2] This observation coincided with several high-profile security events affecting OT systems, including ransomware attacks on Colonial Pipeline and JBS that disrupted supplies of gasoline and meat in North America last May and June.[3]

One reason that cyberattacks have increased with OT systems over the past decade is that they have become more vulnerable to attacks from off site. While OT systems were traditionally air-gapped from IT systems, these two infrastructures are almost universally integrated today. This means that OT systems are now connected to the internet and theoretically accessible from anywhere. This in itself represents a significant increase in the attack surface for industrial organizations, and the increasing ubiquity of Industrial-Internet-of-Things (IIoT) devices extends that attack surface even further. At the same time, connected OT systems are vulnerable to an IT threat landscape that is getting ever more advanced.

The Russian invasion of Ukraine and related events have placed another spotlight on OT security. In April 2022, the U.S. Cybersecurity and Infrastructure Security Agency (CISA), along with its counterparts in Australia, Canada, New Zealand, and the United Kingdom, warned that Russian state-sponsored actors have stepped up their efforts in response to damaging sanctions imposed by the West. The agencies urge those responsible for critical infrastructure networks to "prepare for and mitigate potential cyber threats—including destructive malware, ransomware, DDoS attacks, and cyber espionage—by hardening their cyber defenses and performing due diligence in identifying indicators of malicious activity."[4]

Indeed, an increase in attacks attributed to Russia has materialized, and Ukrainian organizations have borne the brunt.[5] But organizations in the rest of the world are anything but immune, with seven in 10 critical national infrastructure (CNI) providers in the U.K. reporting an increase in cyberattacks since the beginning of the war.[6]

A Growing Spotlight on OT Security

The result is that companies in many industries are scrambling to provide security for increasingly vulnerable OT systems. Research for Fortinet by Westlands Advisory[7] finds that investment in IT/OT and OT-specific security technologies totaled $6.9 billion for all of 2022. And these investments are increasing more quickly than spending on IT-only cybersecurity, with a projected compound annual growth rate (CAGR) of 21% for OT security and 16% for OT/IT cybersecurity between now and 2027.

While this increasing investment is a very good sign, this report finds that by and large, the organizations represented in this year's survey still have a considerable distance to go to adequately protect their OT systems. But a small subset of respondents got through the past 12 months without suffering an intrusion, and this report attempts to highlight some of what those organizations are doing right.

Methodology for This Study

This year's State of Operational Technology and Cybersecurity Report is based on a survey of more than 500 OT professionals conducted between March 14 and March 18, 2022. The survey questions largely mirrored those asked in similar surveys in 2019, 2020, and 2021, depicted in earlier versions of this report. Respondents fielded 40 questions about the state of their OT and OT security infrastructure, security best practices, and vendor selection process.

Diverse geographies, job titles, industries, and devices

One difference in the survey cohort this year compared with prior years is that the survey is global in nature rather than North America–focused (Figure 1). Overall, respondents come from a total of 28 countries, with 150 respondents based in North America (NA); 70 in Latin America (LATAM); 130 in Europe, the Middle East, and Africa (EMEA); and 170 in the Asia-Pacific (APAC).

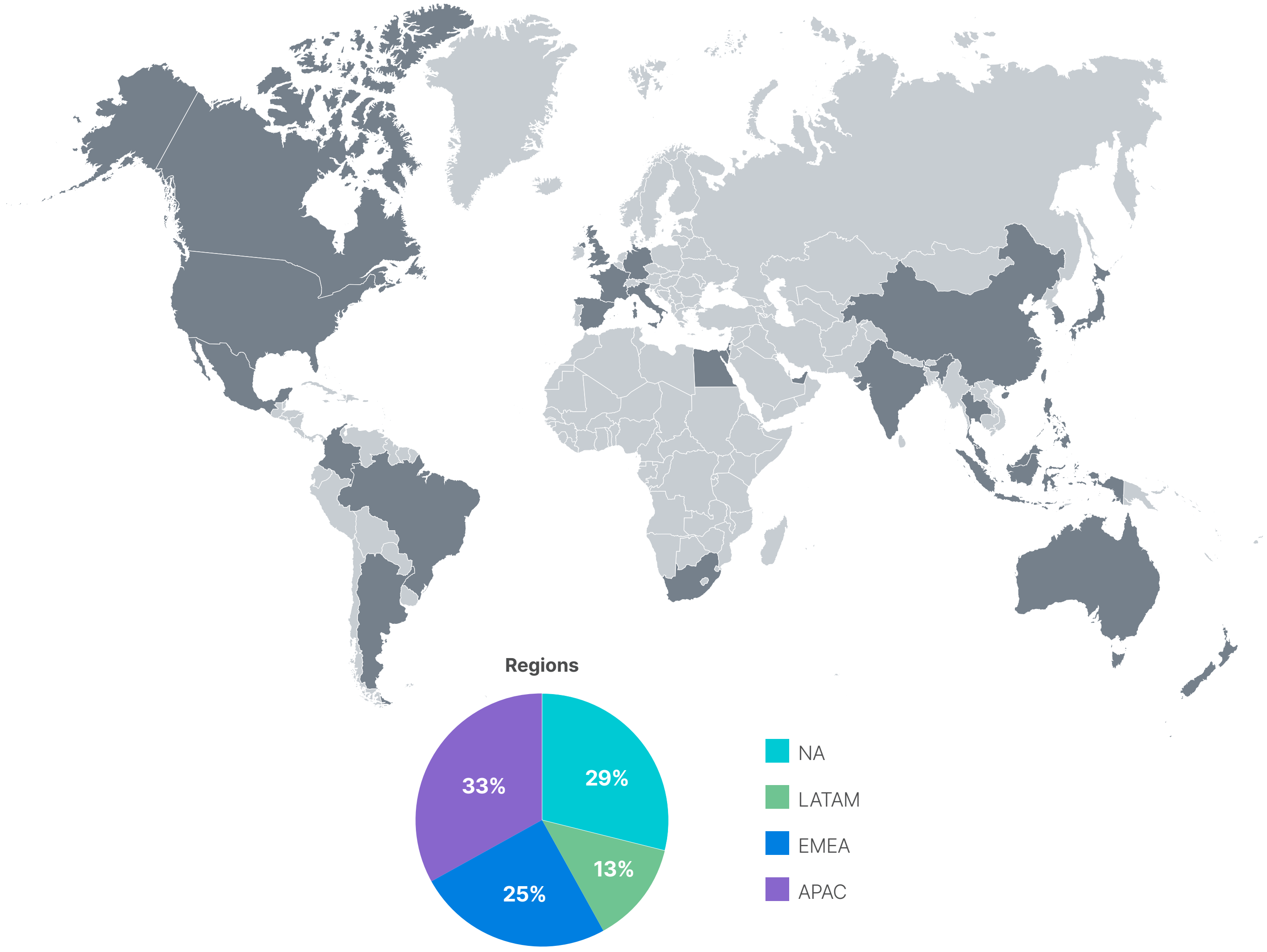


Figure 1: Countries and regions represented in the survey.

The survey targeted people holding leadership positions responsible for OT and OT security, from managers to C-level executives (Figure 2). They represent a range of industries that are heavy users of OT, including manufacturing, transportation and logistics, and healthcare. Six in 10 respondents are the final decision-makers when it comes to OT purchase decisions, and 85% say they are regularly consulted on cybersecurity purchases (Figure 3).

Respondents are users of industrial control system (ICS) and supervisory control and data acquisition (SCADA) devices made by 15 different vendors (Figure 4). As in prior years, Honeywell and Siemens remain the most common brands in use by respondents, with more Honeywell and Schneider users than in prior years. Siemens and Yokogawa use has declined significantly over the same period. Some of these changes reflect the broader geographical representation in this year's survey.

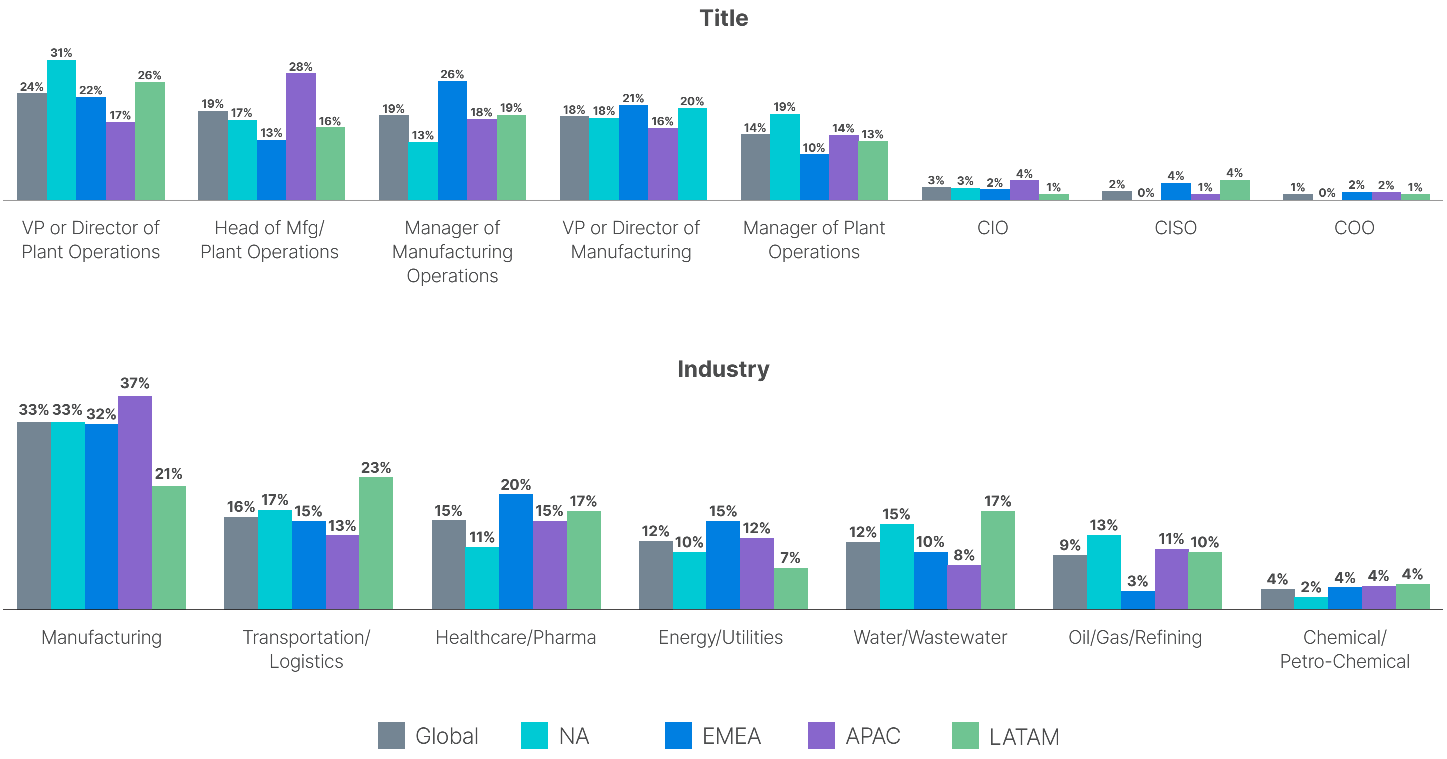


Figure 2: Job titles and industries by region.

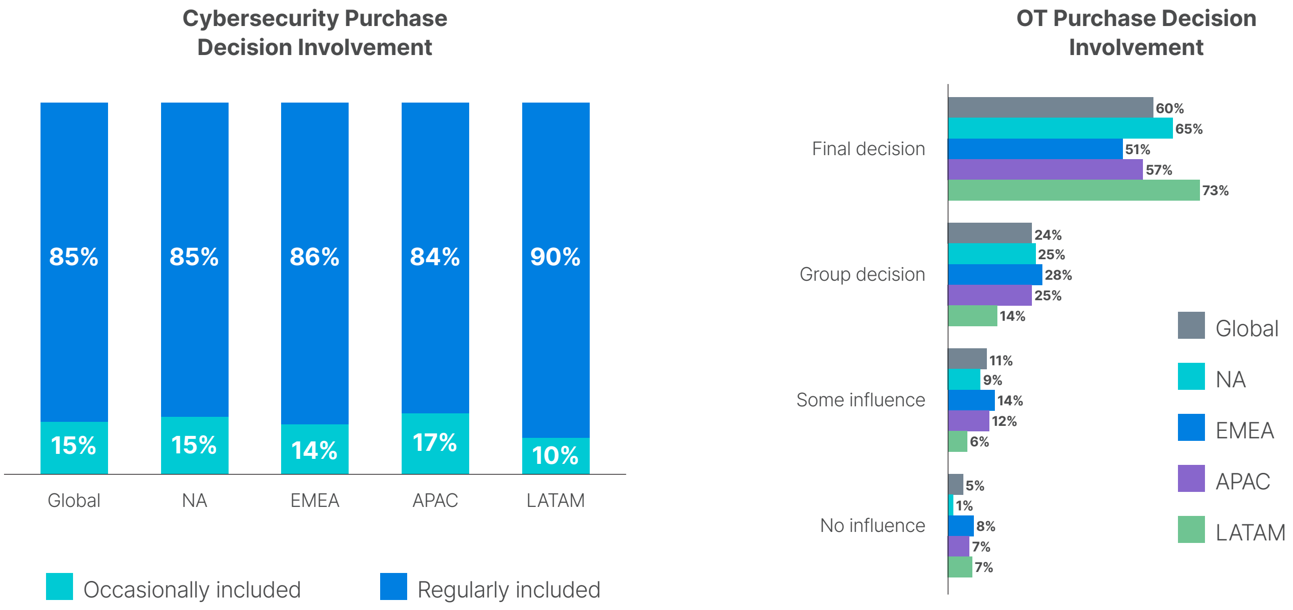


Figure 3: Respondents' role in cybersecurity and OT purchases.

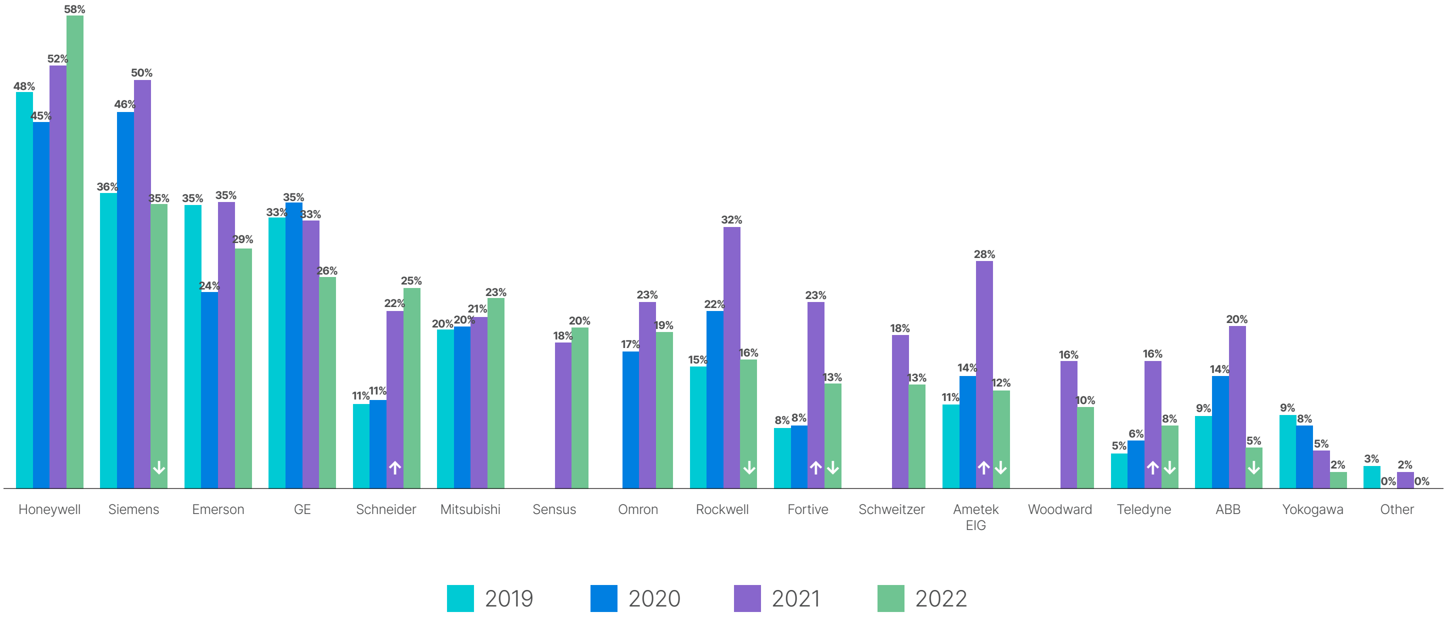


Figure 4: Vendors for OT devices in use.

Identifying insights and best practices

This report looks at the data for the entire cohort and according to region and industry. We also compare the North American results of this year's survey with similar surveys conducted within North America in 2019, 2020, and 2021. From this analysis, we identified five key insights about the state of OT cybersecurity today.

In the final section of the report, we analyze survey responses according to respondents' actual security outcomes, comparing organizations that had no intrusions over the past year with those that had more than 10 intrusions. This comparison results in several best practices to which "top-tier" organizations are more likely to adhere.

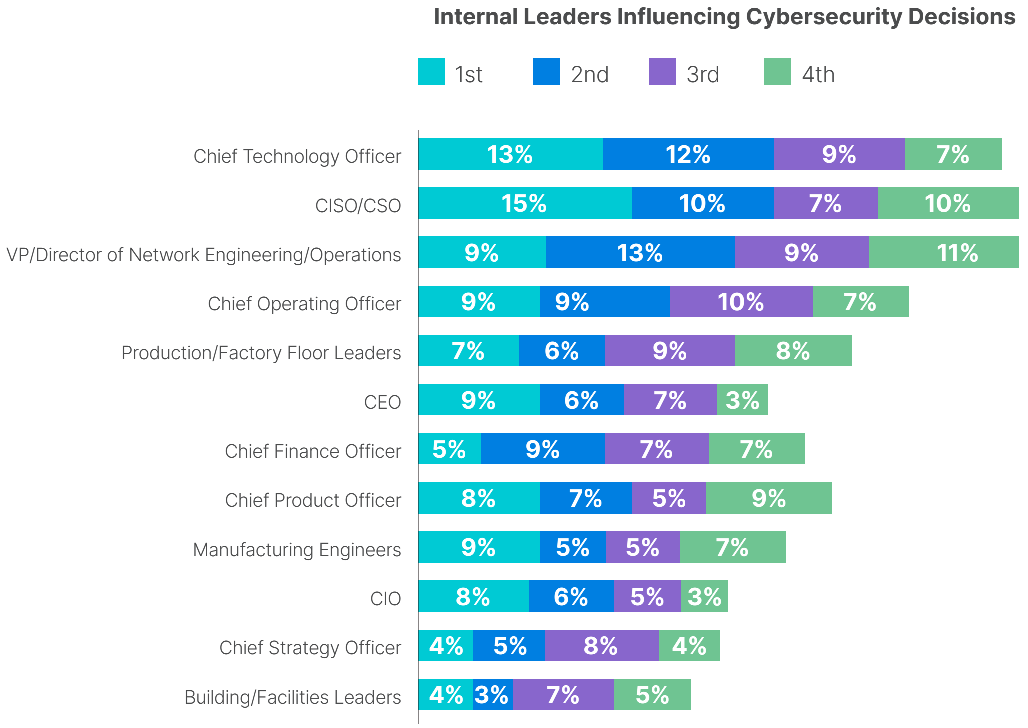
> "Recent Russian state-sponsored cyber operations have included distributed denial-of-service (DDoS) attacks, and older operations have included deployment of destructive malware against Ukrainian government and critical infrastructure organizations."[8]

Insights for OT Security

Survey results reveal that organizations have growing worries about the security of their OT infrastructure, but that their preparation for such threats is still piecemeal and incomplete. We identified five key insights from this year's research:

Insight 1: OT security is a concern at the corporate level, and different groups assume responsibility

Unsurprisingly, the security of OT systems has the attention of executives at many organizations, with the CTO and CISO/CSO most commonly cited among the top three leaders influencing cybersecurity decisions. However, survey responses indicate that these leaders have lost significant influence over the past year (Figure 5). Last year, 50% of organizations ranked the CTO among the top three security influencers, and 45% did so for the CISO/CSO. Those numbers declined to 35% and 33%, respectively, in 2022. The global nature of the survey was not a factor in the change, as the numbers were identical for North American respondents as for the overall cohort.



In Top 3

2022	2021	2020	2019
35%↓	50%	45%	32%
33%↓	45%	44%	55%
32%	24%	30%	35%
28%	22%	29%	30%
23%↑	7%	10%	12%
21%↓	44%	31%↓	52%
21%	14%	9%	8%
21%↑	10%	10%	12%
19%↑	3%	7%↓	21%
19%↓	44%↑	22%	18%
17%	15%	19%	14%
14%↑	0%	1%	6%

Figure 5: Internal leaders influencing security decisions.

Who leads—and will lead—OT security?

But when asked who bears final responsibility for OT security at their organizations, a plurality of one-third of respondents named the vice president or director of network engineering or operations (Figure 6). This is a big increase over last year's percentage and the highest in the four years the survey has been conducted. It reflects that OT security responsibility may have moved a bit upward in the org chart compared with past years, when a director- or manager-level person was responsible for OT security at a plurality of organizations.

There is speculation among respondents that this upward move in the org chart will continue. Only 15% of respondents say that the CISO holds responsibility for OT security today, but 79% say that they expect the function to roll under the CISO over the next 12 months (Figure 7). However, we are skeptical of that claim, as large majorities of respondents have made this prediction every year the survey has been conducted, and the percentage of organizations where the CISO is currently in charge of OT security actually declined slightly in 2022 compared with 2021. The CISO's declining influence on security decisions, referenced above, adds weight to this skepticism.

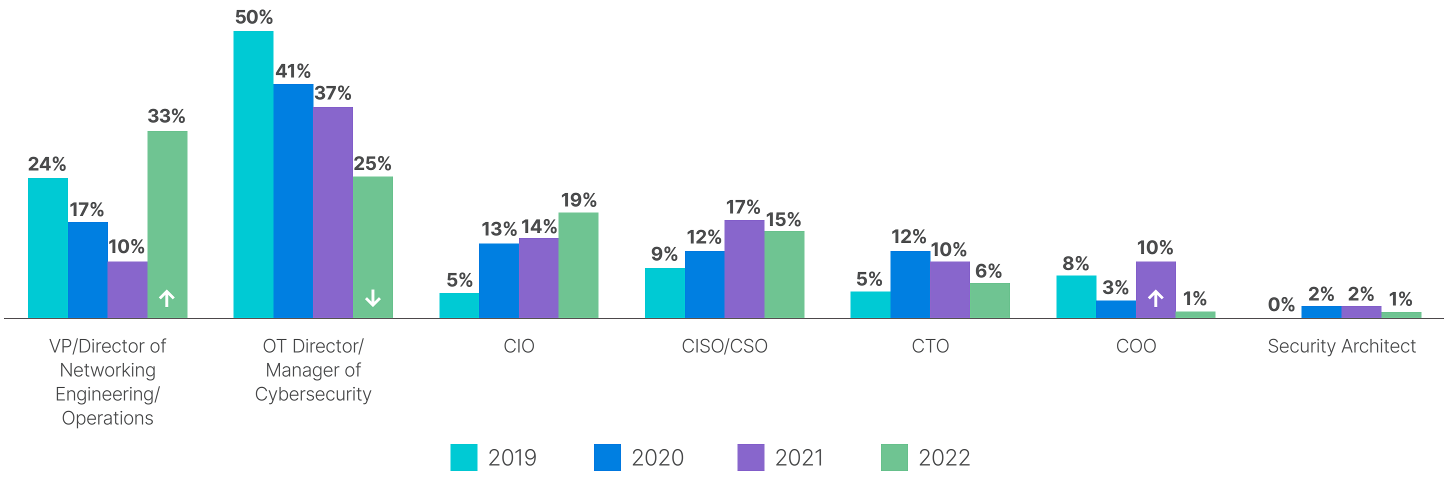


Figure 6: Leader currently responsible for OT cybersecurity.

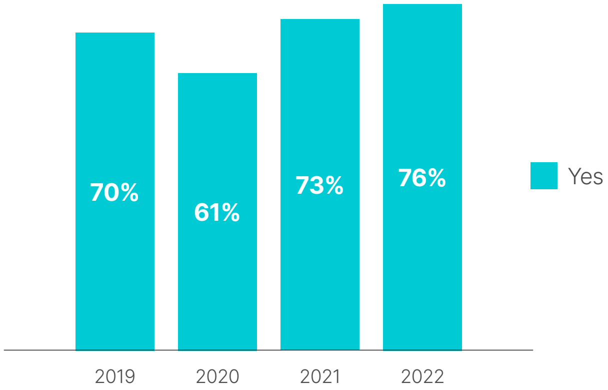


Figure 7: Respondents that expect that OT security will be rolled under the CISO in the next 12 months.

Career paths to OT security

To qualify for the survey, respondents were required to have significant responsibility for OT. Indeed, 85% of them spend more than half their time managing that function, and it consumes more than three-quarters of work hours for 28% (Figure 8). Two-thirds of respondents globally have a career background on the OT side—either at industrial organizations or OT solutions vendors (Figure 9). The remaining one-third come from an IT security background—including more than half of respondents from Latin America.

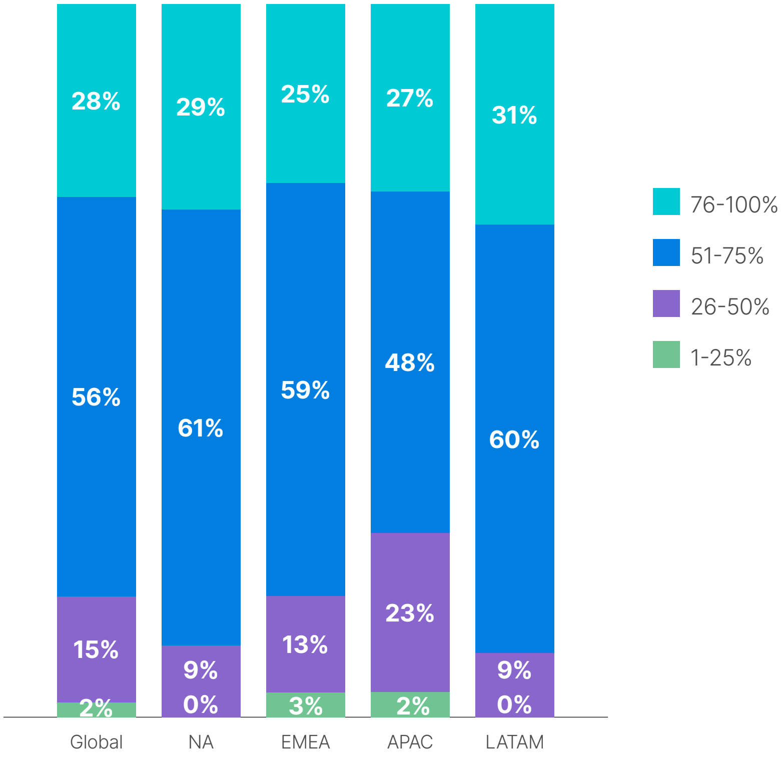


Figure 8: Percentage of time spent supporting/managing OT security.

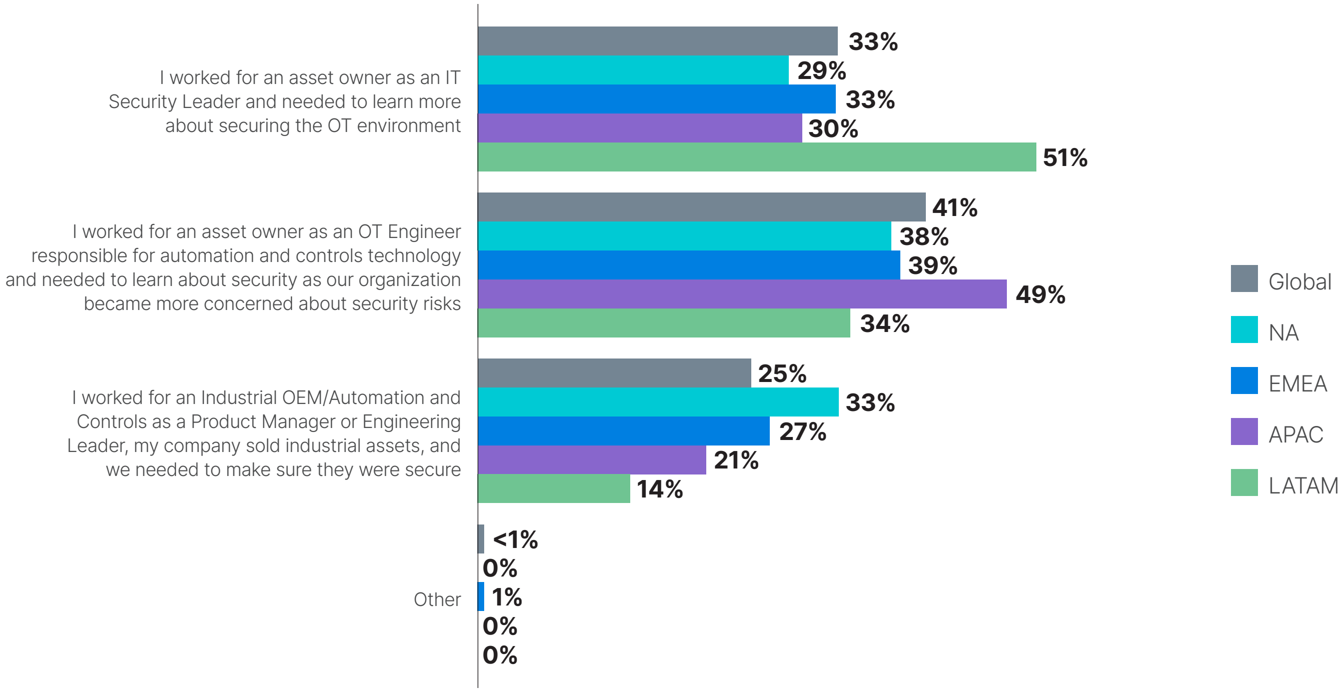
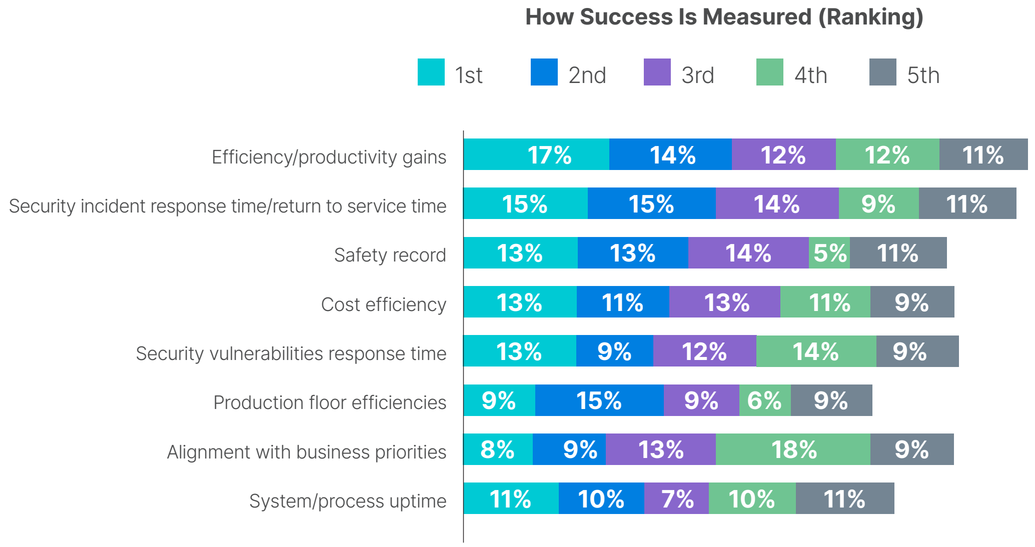


Figure 9: Career background that led to OT security.

Insight 2: Some organizations still tend to prioritize efficiency over OT security

While every organization likely claims to be concerned about OT security, one way to discern the importance of security is by looking at how OT leaders are measured. In this year's survey, efficiency and productivity gains are still most commonly cited as the number one success measurement, and it is among the top three metrics at 43% of organizations (Figure 10). This measurement has been most cited as a top-three success measurement every year the survey has been conducted, but its prevalence declined by 14% from 2021 to 2022.

The CISO is a top influencer of OT security decisions at only 33% of organizations, down from 45% in 2021.



	In Top 3			
	2022	2021	2020	2019
Efficiency/productivity gains	43↓	57%	46%	55%
Security incident response time/return to service time	43%	N/A	N/A	N/A
Safety record	40%	34%	44%	41%
Cost efficiency	37%	41%	40%	53%
Security vulnerabilities response time	34%↓	47%↑	32%	44%
Production floor efficiencies	32%	42%	41%↓	42%
Alignment with business priorities	29%	33%	24%	29%
System/process uptime	29%↓	41%	40%	35%

Figure 10: Ranking of success metrics.

At the same time, a security metric—incident response or return to service time—was also cited by 43% of respondents as a top-three measurement, certainly a good sign. There were also significant declines in the prominence of security vulnerability response time and system/process uptime, but the fact that the incident response metric was new for the 2022 survey may be one reason that the other security-related choices are down.

Specific concern about ransomware

Ransomware has dominated media headlines in the cybersecurity space for several years, and organizations report significant concern about the tactic—despite the fact that it is less common than some other attack types. More than two-thirds of respondents globally—and three-quarters in North America—say that they are more concerned about ransomware than other intrusions (Figure 11). Ransomware has caused significant damage and economic cost over the years, and one good result of its high visibility is that organizations are duly concerned. However, other damaging attack types may not get the attention they deserve due to their lower visibility.

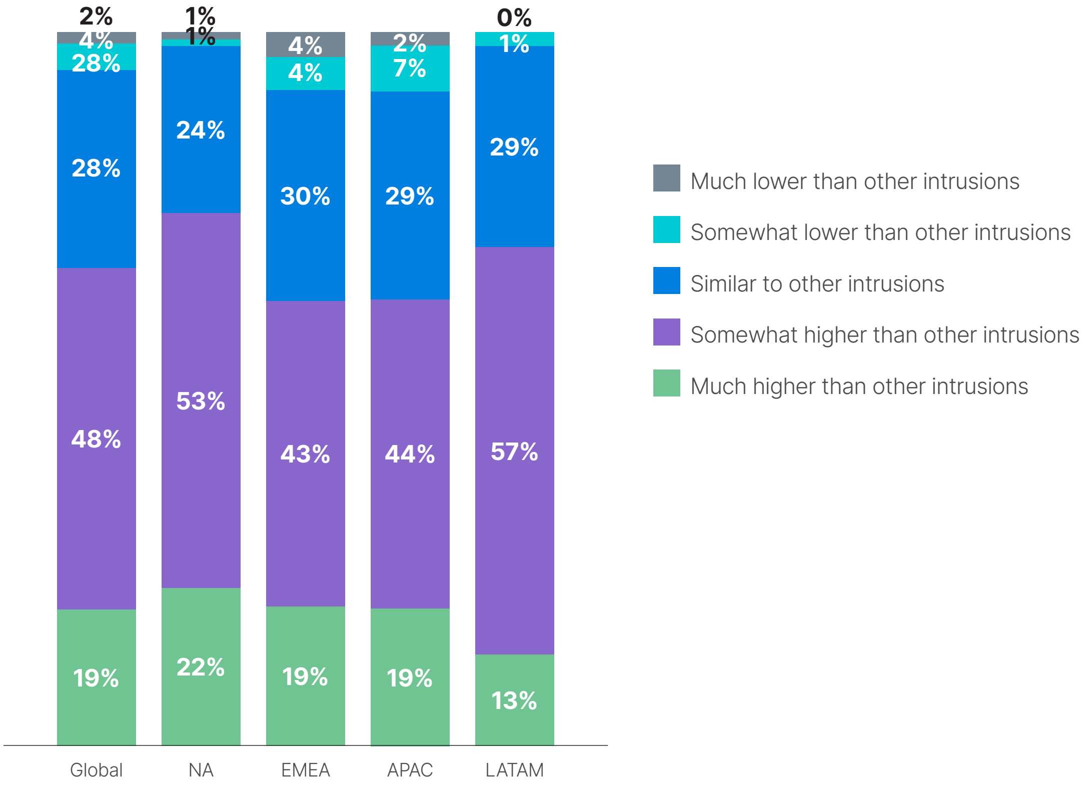
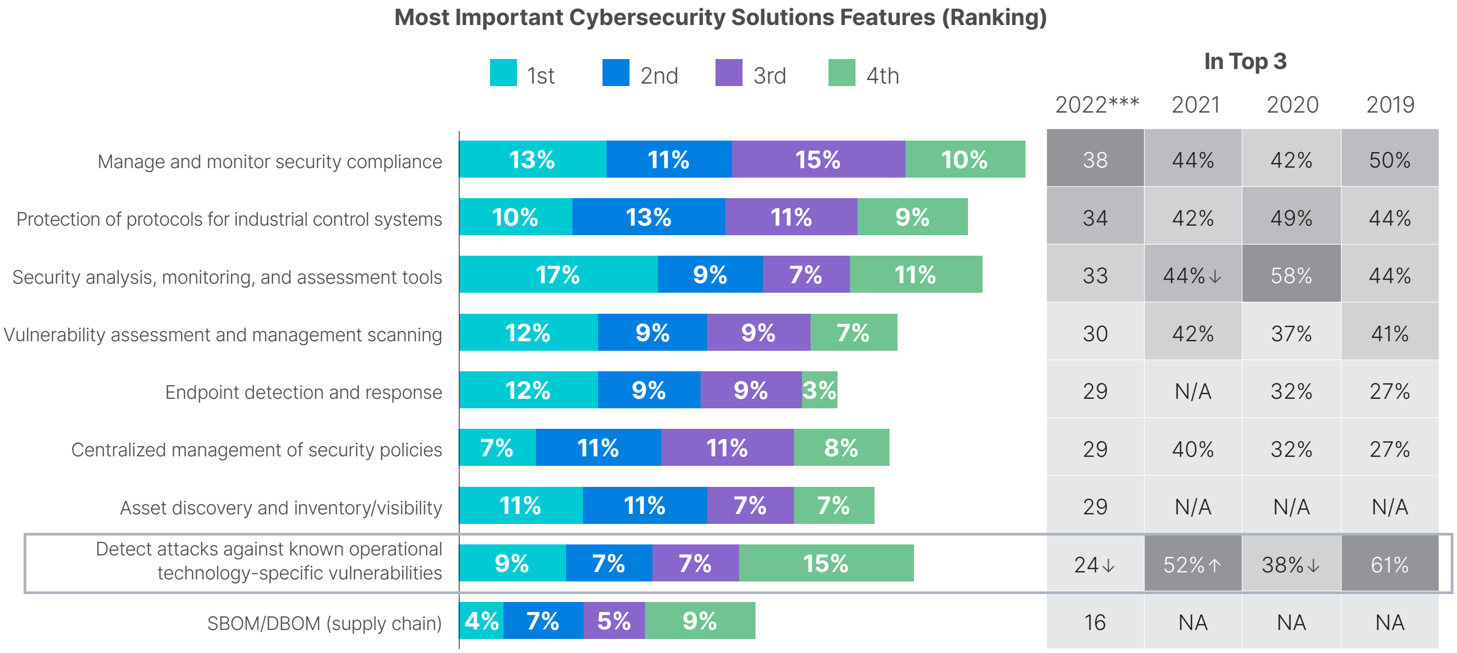


Figure 11: Level of concern about ransomware.

Ranking the importance of cybersecurity tools

Respondents were all over the map as to which features of cybersecurity solutions were most important for their organizations. Security analysis, monitoring, and assessment tools were most commonly cited as the most important—but only by a plurality of 17% (Figure 12). Overall, compliance management and monitoring solutions were the most commonly cited in the top three, and OT-specific protocol protection features ranked second.



	2022***	2021	2020	2019
Manage and monitor security compliance	38	44%	42%	50%
Protection of protocols for industrial control systems	34	42%	49%	44%
Security analysis, monitoring, and assessment tools	33	44%↓	58%	44%
Vulnerability assessment and management scanning	30	42%	37%	41%
Endpoint detection and response	29	N/A	32%	27%
Centralized management of security policies	29	40%	32%	27%
Asset discovery and inventory/visibility	29	N/A	N/A	N/A
Detect attacks against known operational technology-specific vulnerabilities	24↓	52%↑	38%↓	61%
SBOM/DBOM (supply chain)	16	NA	NA	NA

Figure 12: Ranking of most important cybersecurity solutions features.

Insight 3: Organizations report a gradually improving OT security posture, but more improvement is needed

As in past years, our survey asked respondents to self-report the level of OT security maturity their organizations have achieved, with a brief description for each of five maturity levels. Among all respondents, 84% have reached at least level 2, having established access and profiling (Figure 13). Half of respondents have reached at least level 3 by establishing predictive behavior, and 21% have reached level 4 with orchestration and automation.

This represents a marginal improvement over 2021, mostly through organizations moving from level 2 to level 3. The percentage of organizations achieving at least level 3 increased from 44% to 50% year over year.

Security incident response/ return to service time is a top-three OT success metric at 43% of organizations.

Analyzing the results by geography, a larger proportion of Latin America and APAC respondents have reached level 4. Meanwhile, in North America, more organizations have advanced past level 1, but fewer have achieved level 4, leaving more than 70% of organizations in the middle levels.

Unfortunately, only half of respondents say that their organization's OT security posture is a significant factor in its overall risk score (Figure 14)—although almost all other organizations include it as a moderate factor.

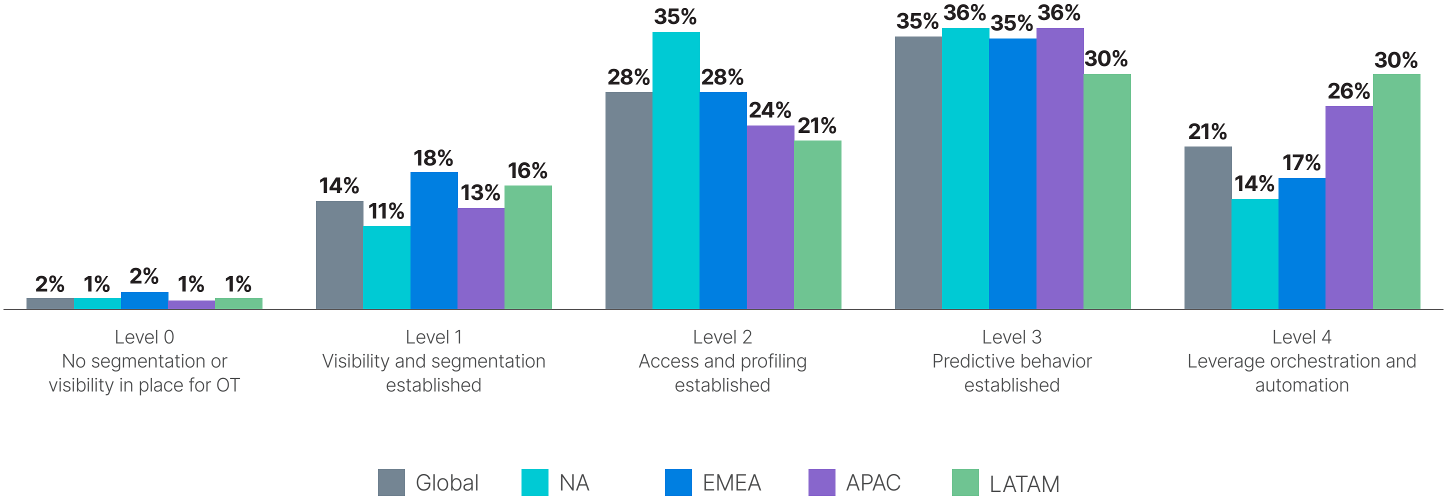


Figure 13: Maturity level of OT cybersecurity posture.

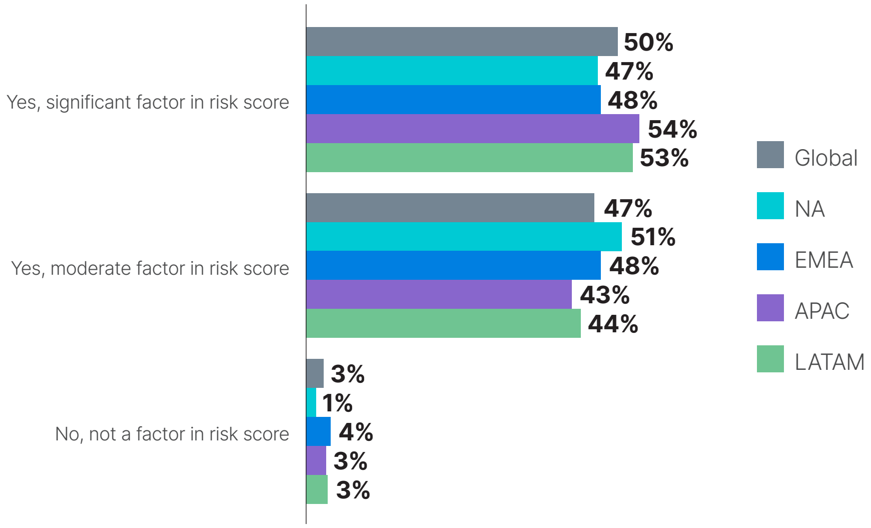


Figure 14: Importance of OT security posture in overall risk score.

Overall cybersecurity maturity

Respondents were also asked to rate the maturity of their overall cybersecurity program, including IT and OT. Here, respondents were more likely to have achieved level 3 (59%) but less likely to have achieved level 4 (16%, Figure 15). Again, Latin American and APAC companies show higher maturity while North American ones are lower overall. Larger organizations and those in the manufacturing sector are more likely to have higher maturity levels, as are organizations at which the top technology and security leaders have influence over cybersecurity decisions (Figure 16).

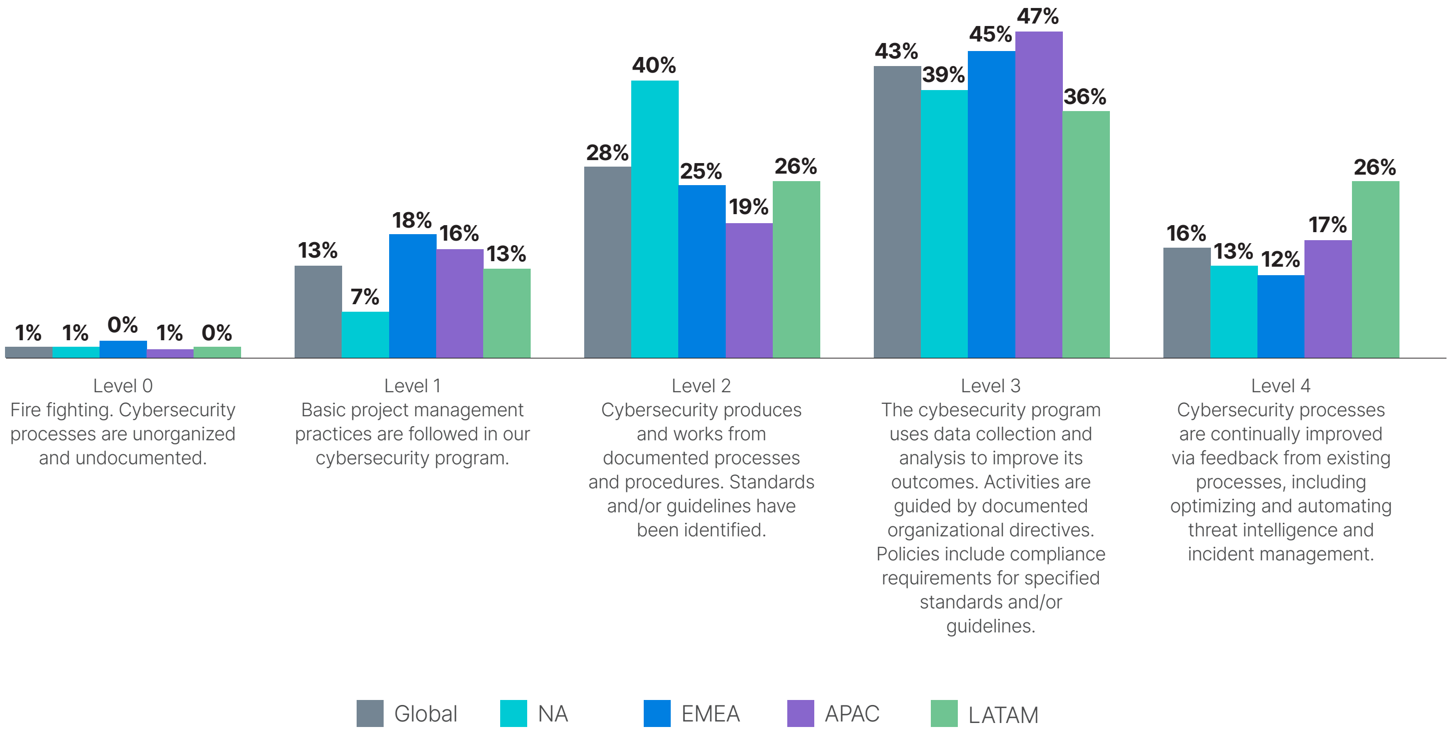
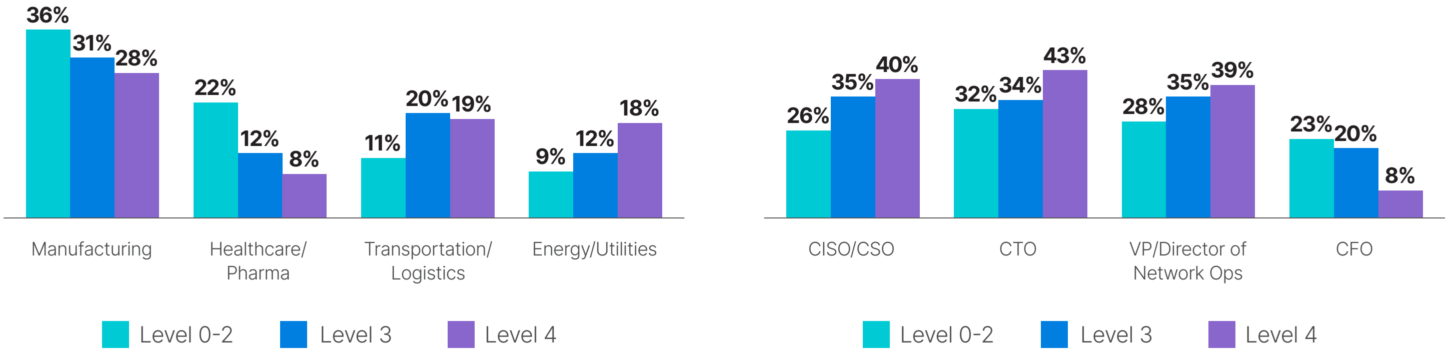


Figure 15: Maturity level of overall cybersecurity program.



% More Than 5,000 Employees		
21%	28%	41%

% Cybersecurity Aids/Impedes in My Success		
65%/4%	82%/6%	83%/11%
% Aids By Facilitating Security Standards		
40%	46%	58%

Figure 16: Selected demographics of respondents by maturity level of cybersecurity program.

Centralized visibility

The establishment of visibility of OT processes is included in level 1 in our OT security maturity matrix, but the granularity of that visibility can make a difference. While 98% of respondents claim at least level 1 in OT security maturity, only 74% say that more than three-quarters of their OT activities are visible by the security operations team (Figure 17). That figure is 77% in North America, an improvement over North American survey results from past years (Figure 18). However, the percentage of North American respondents who have 100% visibility seems to be in decline—from 23% in 2020 to 13% in 2022.

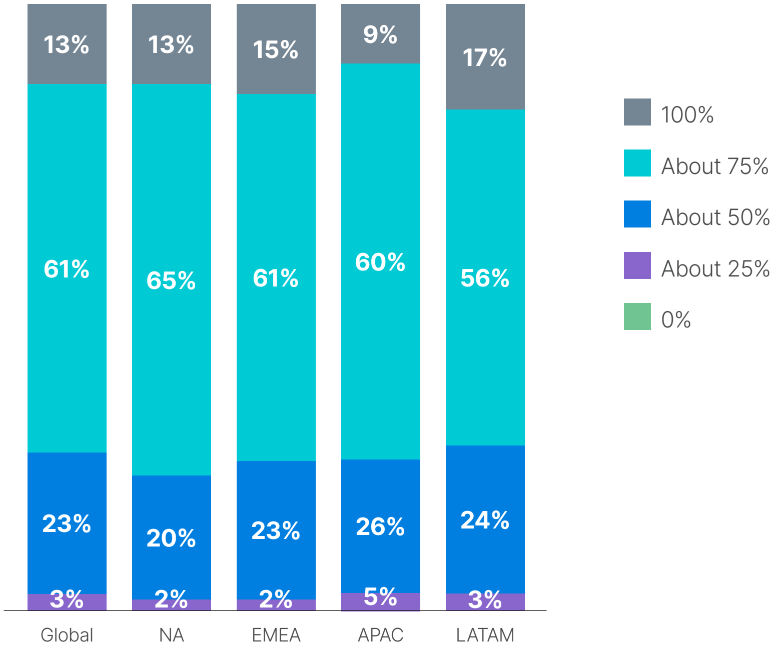


Figure 17: Visibility of OT activities by security operations.

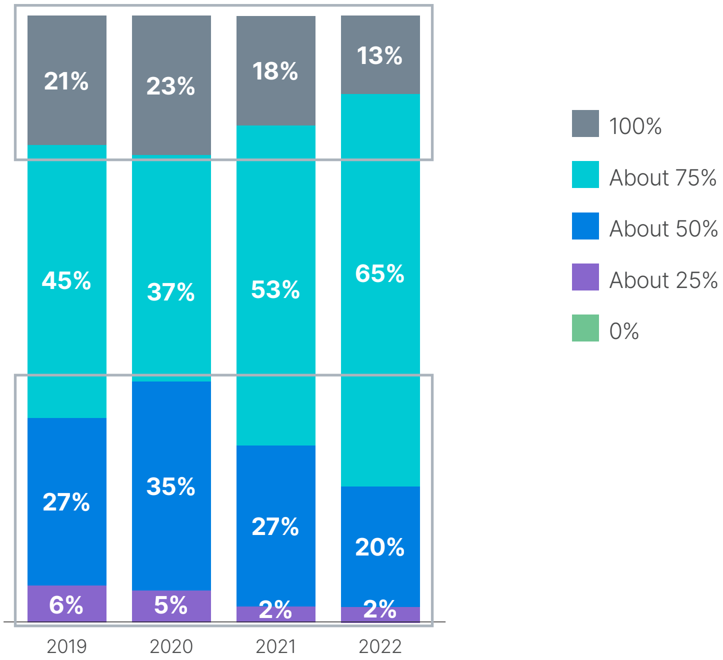


Figure 18: Visibility of OT activities by security operations, North America.

Insight 4: Organizations have diverse ways of addressing OT security, and many have security gaps

Because OT systems were often air-gapped from the internet in past years, the need to secure OT systems from IT threats is relatively new, and our survey found that security practices have not yet been standardized.

As we have discussed, one approach is to entrust OT security management to the SOC, which has fulfilled that function for IT systems for years. Almost all survey respondents have adopted this approach for at least some OT activities, but only 52% of organizations have managed to enable monitoring and tracking of *all* OT activities by the SOC team (Figure 19). This is essentially unchanged over the four years that we have conducted this survey. APAC companies are doing somewhat better in this regard, with 59% monitoring all activities from the SOC.

50% of organizations have achieved level 3 OT security maturity—up from 44% in 2021.

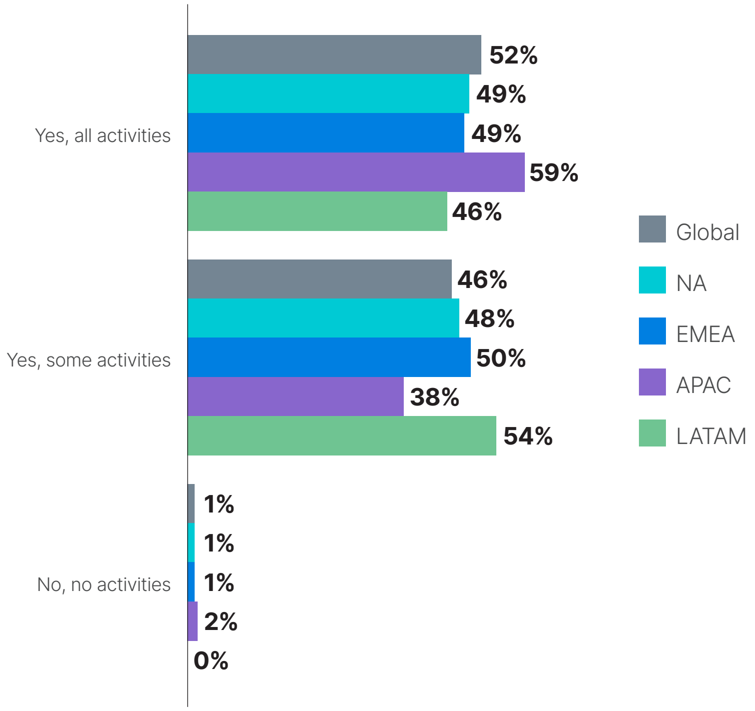


Figure 19: OT activities monitored and tracked by the SOC.

Metrics tracked and reported

When it comes to tracking and reporting security metrics, results are mixed. When presented with a list of basic cybersecurity measurements that arguably should be tracked at every organization, no more than 52% of respondents claimed to be tracking any of them (Figure 20).

Comparing the North American results with past years, the percentage that track and report several of the metrics declined significantly from 2021 (Figure 21)—including vulnerabilities found and blocked and intrusions detected and remediated.

Similar percentages of respondents report basic OT security information to executive management on a regular basis. Presented with a list that includes critical information like compliance reports, security assessments, and security compromises, no more than 53% reported any single item to executive management (Figure 22).

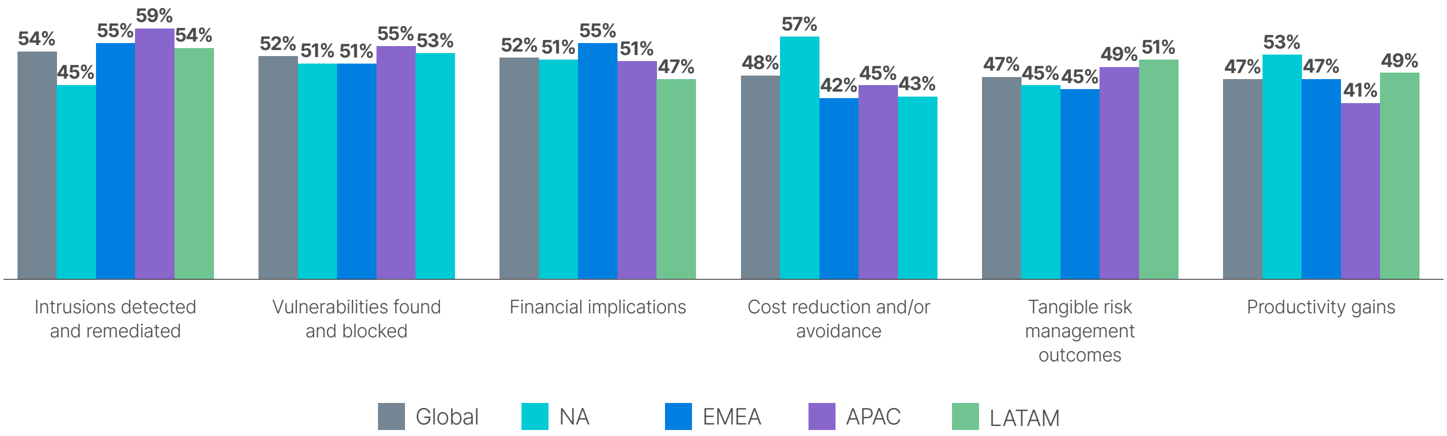


Figure 20: Cybersecurity measurements tracked and reported.

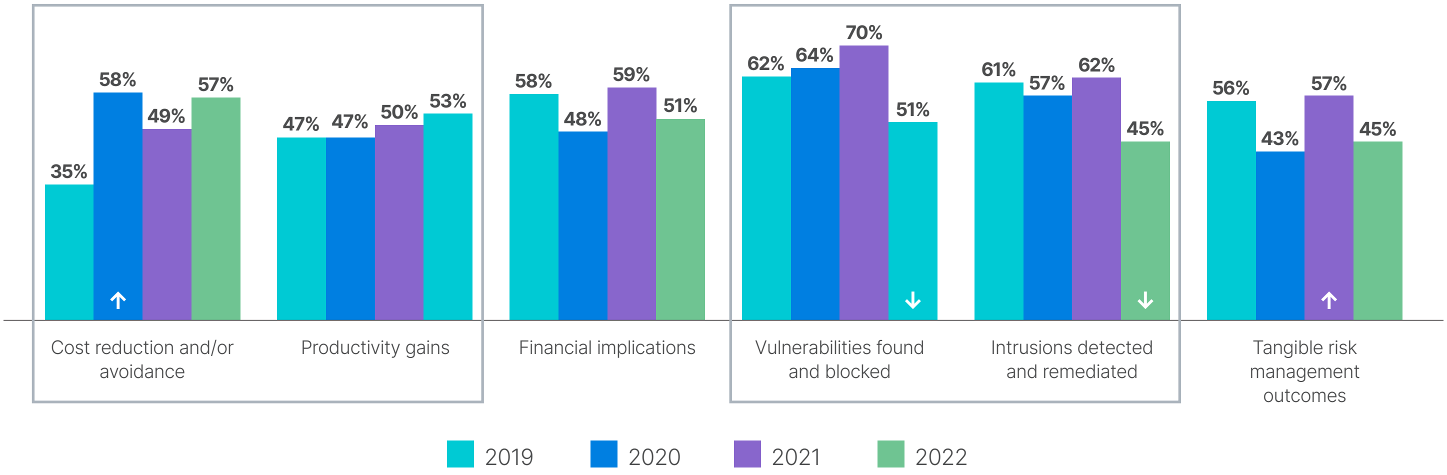


Figure 21: Cybersecurity measurements tracked and reported, North America.

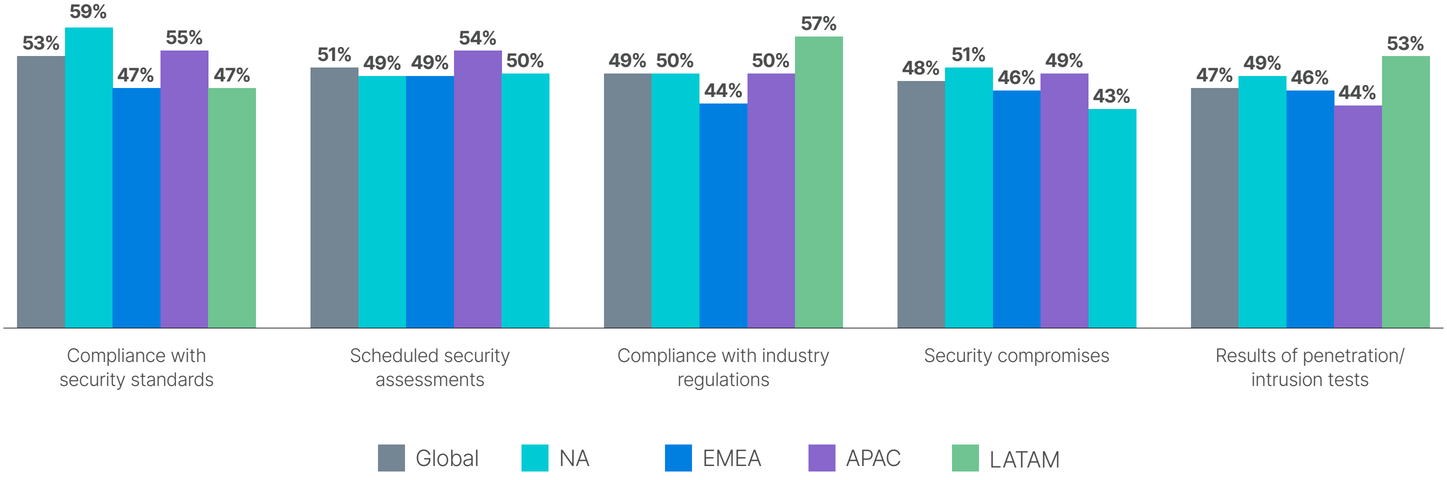


Figure 22: OT cybersecurity issues reported to executive management.

Security features in use

Respondents gave diverse answers regarding the tools and security features they use to secure their OT systems. Presented with a rather comprehensive list of tools and processes, no single feature is used by more than 47% of respondents (Figure 23). Solutions included for the first time this year include secure remote access (41%); security orchestration, automation, and response (SOAR; 37%); and the use of threat intelligence (36%).

This "some of the above" approach reflects an aspect of security that in many ways is still in its infancy, with different organizations trying different approaches. One practice that is clearly declining in popularity is the use of the network operations center (NOC) for management of OT security (Figure 24). Interestingly, North American respondents tended to use fewer of the listed features and practices overall.

No more than 47% of organizations use any single OT security tool or approach.

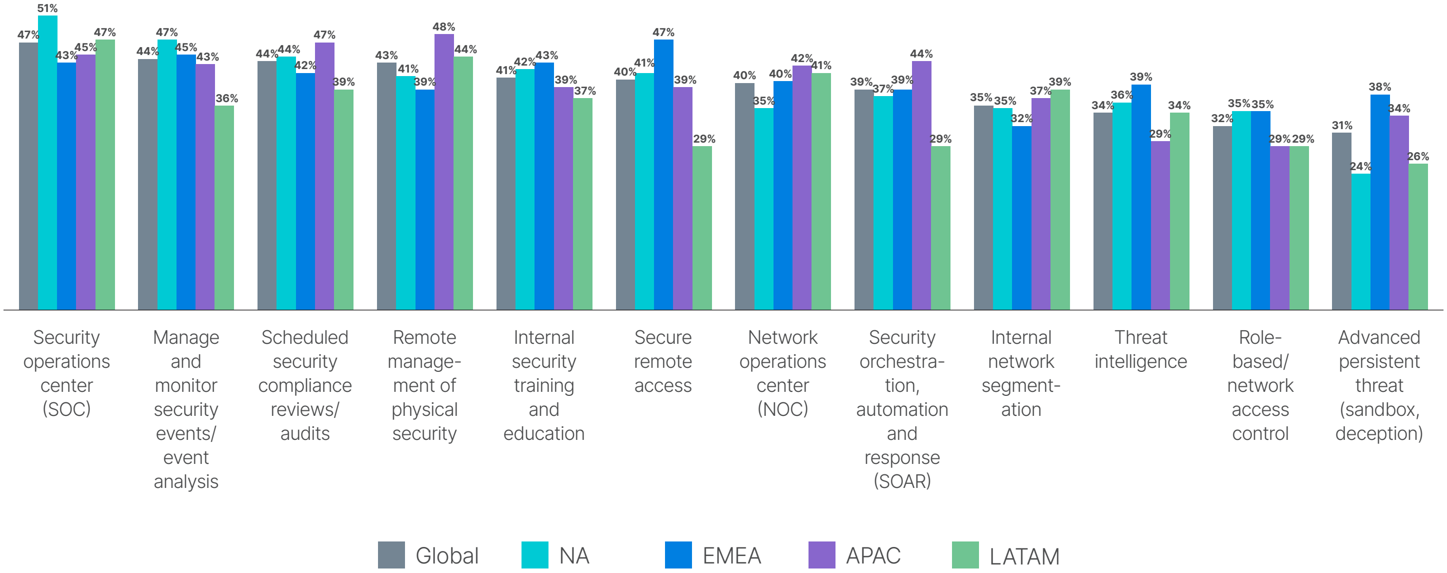


Figure 23: Cybersecurity and security features in place.

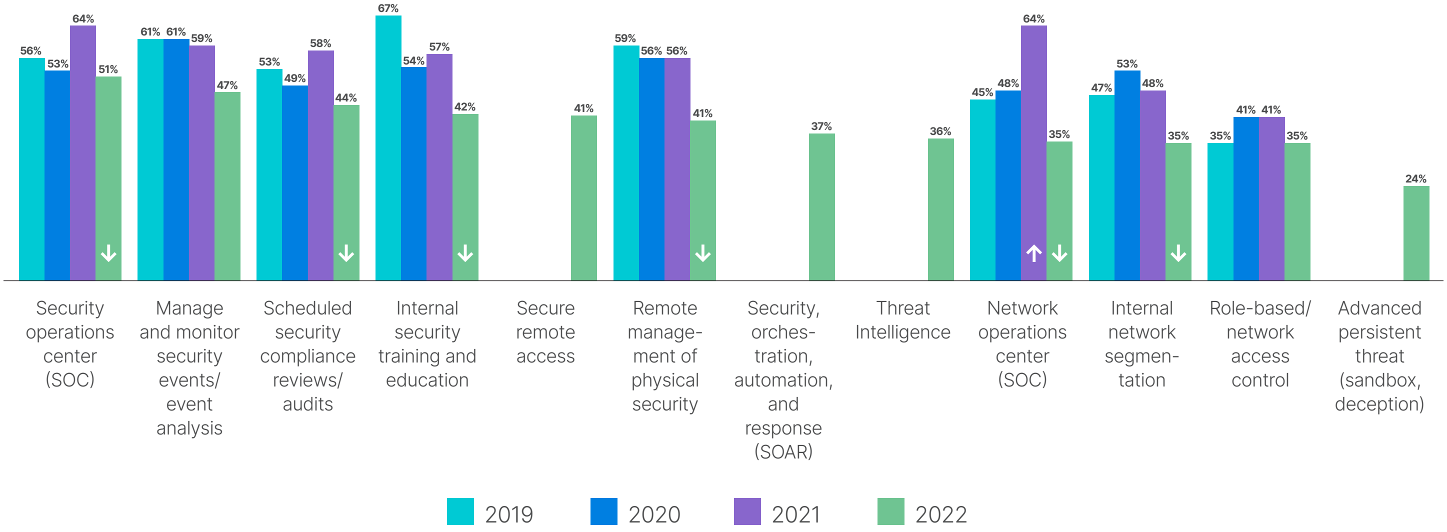


Figure 24: Cybersecurity and security features in place, North America.

Complexity of security systems and perception of efficacy

Complexity is one issue that can impede OT security. A vast majority of organizations use between two and eight different vendors for their OT devices and have between 100 and 10,000 devices in operation (Figure 25). Only 7% of organizations have been successful in reducing the number of vendors to one.

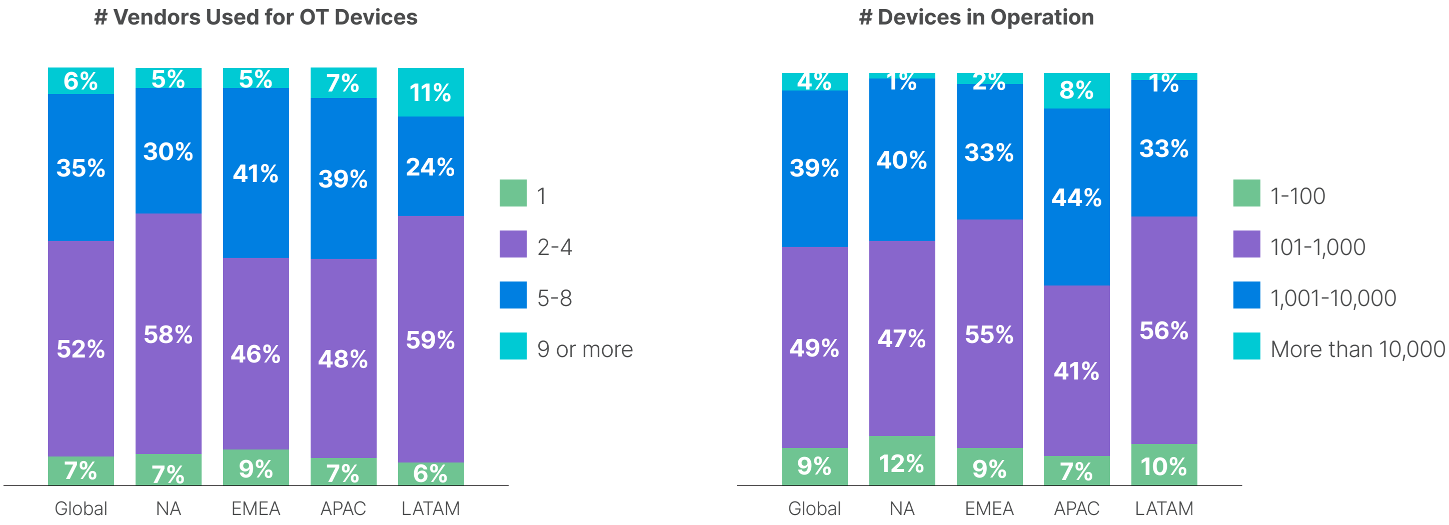


Figure 25: OT vendors and OT devices in use.

Insight 5: most organizations still experience multiple intrusions annually

Every year, we ask respondents one simple question about their security outcomes: How many intrusions they have experienced over the past 12 months. In 2022, three-quarters of respondents admitted to at least three intrusions, 19% had more than six, and 7% had more than 10 (Figure 26). Only 6% of respondents reported having no intrusions in 12 months.

Looking at the North American results of this question over four years, things are not getting any better overall, with about the same percentage having three or more intrusions since 2020 (Figure 27). One small consolation is that the percentage of North American respondents that had 10 or more intrusions declined from 12% to 5% year over year.

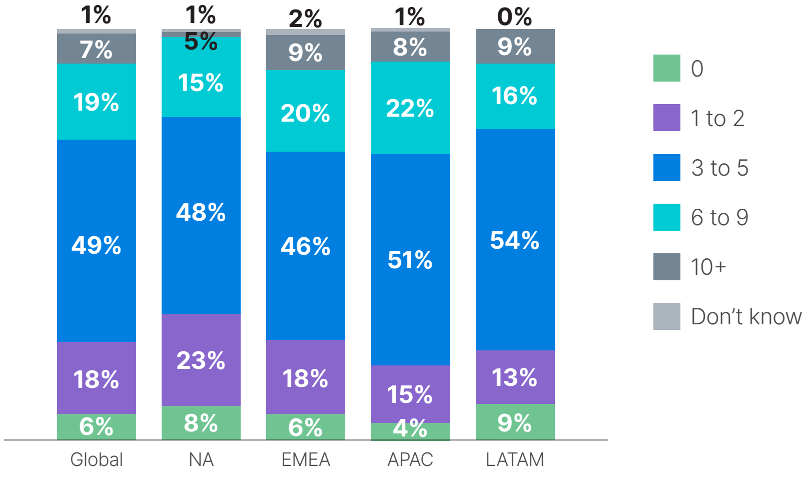


Figure 26: Number of intrusions in the past year.

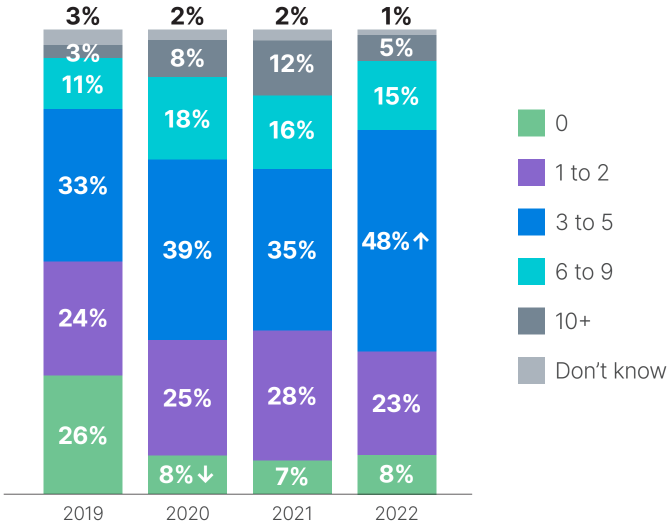


Figure 27: Number of intrusions in the past year, North America.

Types of attacks

Respondents experienced a wide variety of attack types—not surprising given the number of intrusions. A total of eight attack types impacted at least one-quarter of respondents apiece, with malware and phishing topping the list by hitting more than 40% of organizations (Figure 28). Ransomware hit fewer than one-third of organizations overall, but 44% of Latin American companies. And fewer Latin American respondents experienced phishing than in the other regions. Looking at the North American results over four years, malware and malicious insider breaches showed declines this year (Figure 29).

While the overall number of intrusions is remarkably similar regardless of the reported level of security maturity—likely because more mature organizations are able to detect a larger percentage of intrusions that occur. But looking at this by attack type, it becomes clear that more mature organizations have less problem with insider threats, while detecting more attacks from the outside (Figure 30).

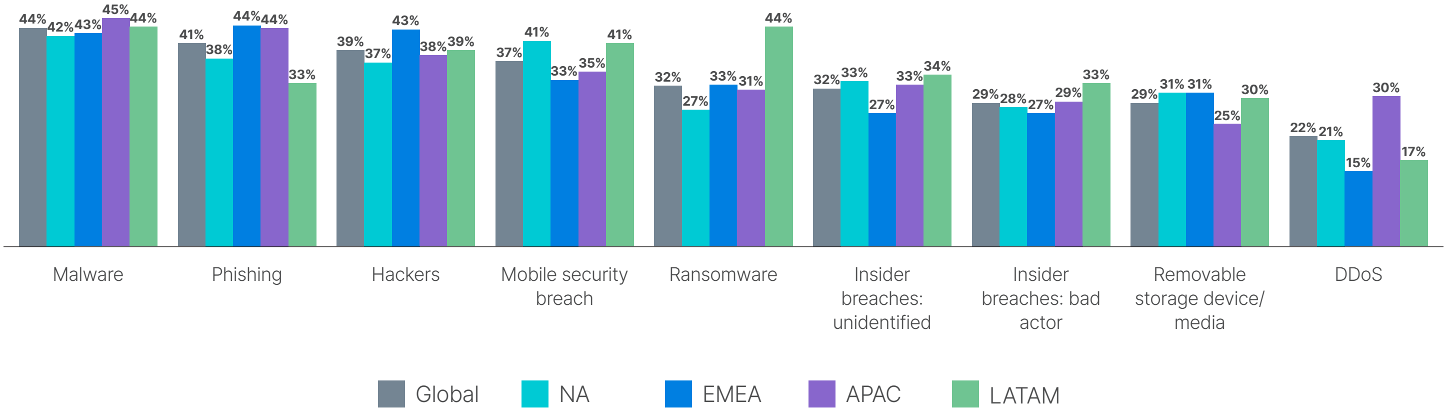


Figure 28: Types of intrusions experienced.

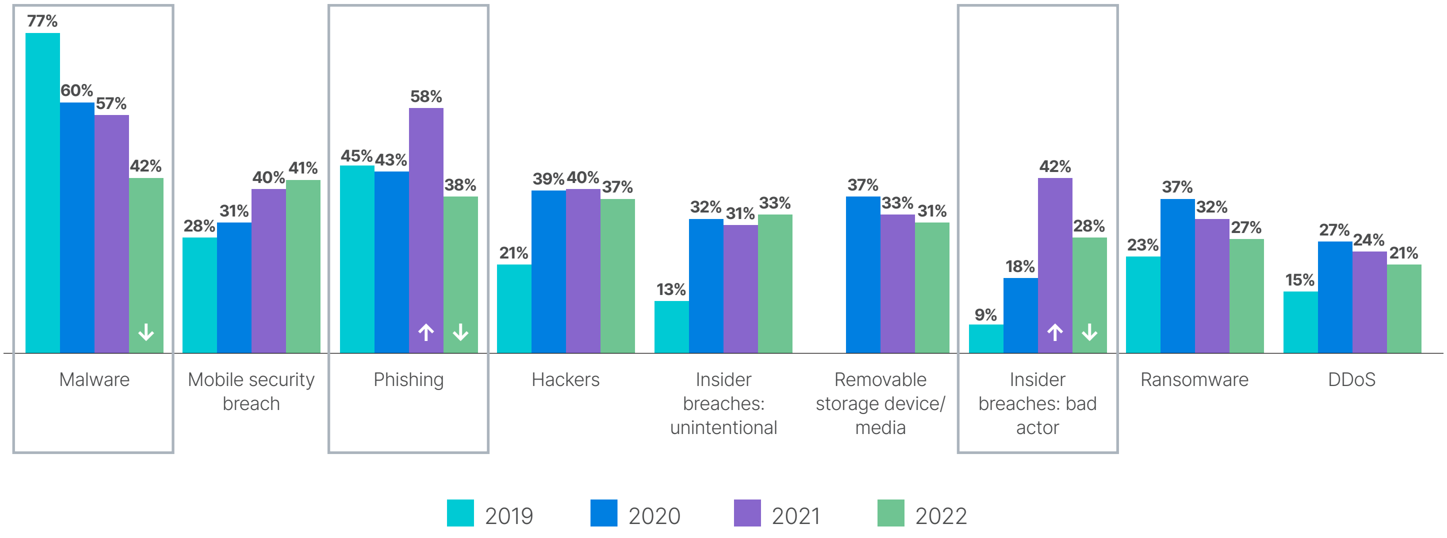


Figure 29: Types of intrusions experienced, North America.

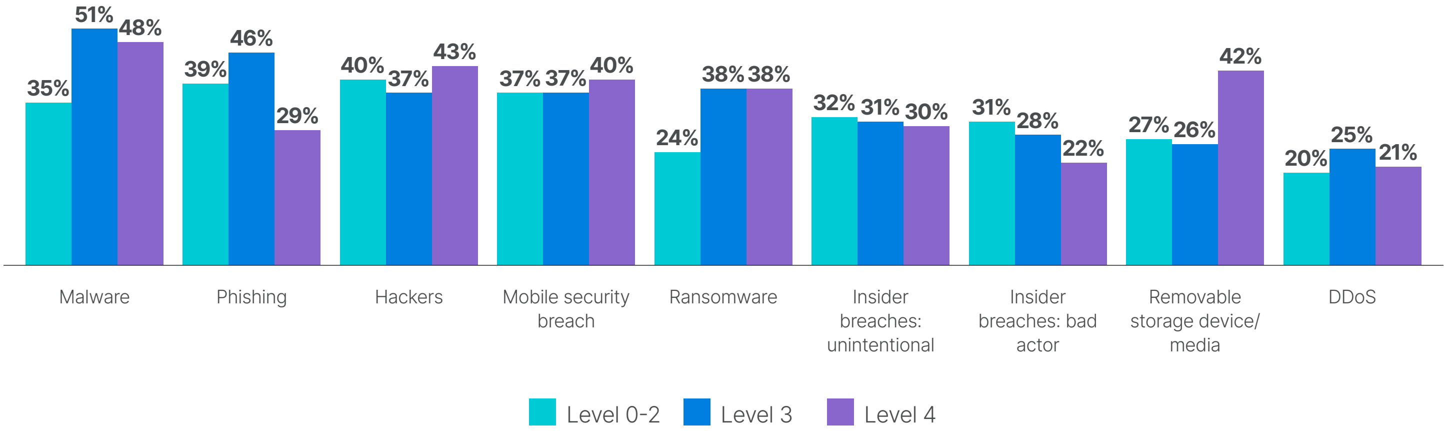


Figure 30: Types of intrusions experienced by reported security maturity level.

Impact of attacks

Interestingly, a slightly higher percentage of attacks impacted OT systems than IT systems (Figure 31), with 61% of intrusions impacting OT and 60% impacting IT. The business impacts of the intrusions were by no means trivial. Close to half of respondents suffered an operational outage that affected productivity, while more than one-third saw revenue, data loss, compliance, and brand-value impacts—and even threats to physical safety (Figure 32). And 90% of respondents admit that returning to service was a process that took hours or longer (Figure 33).

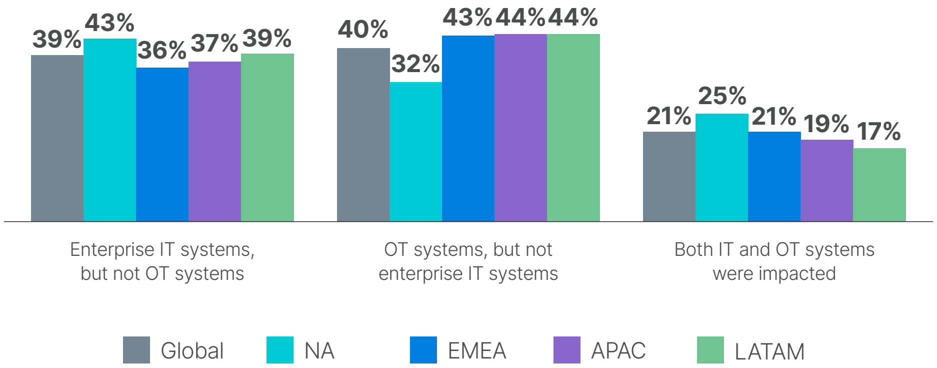


Figure 31: Environments impacted by intrusions.

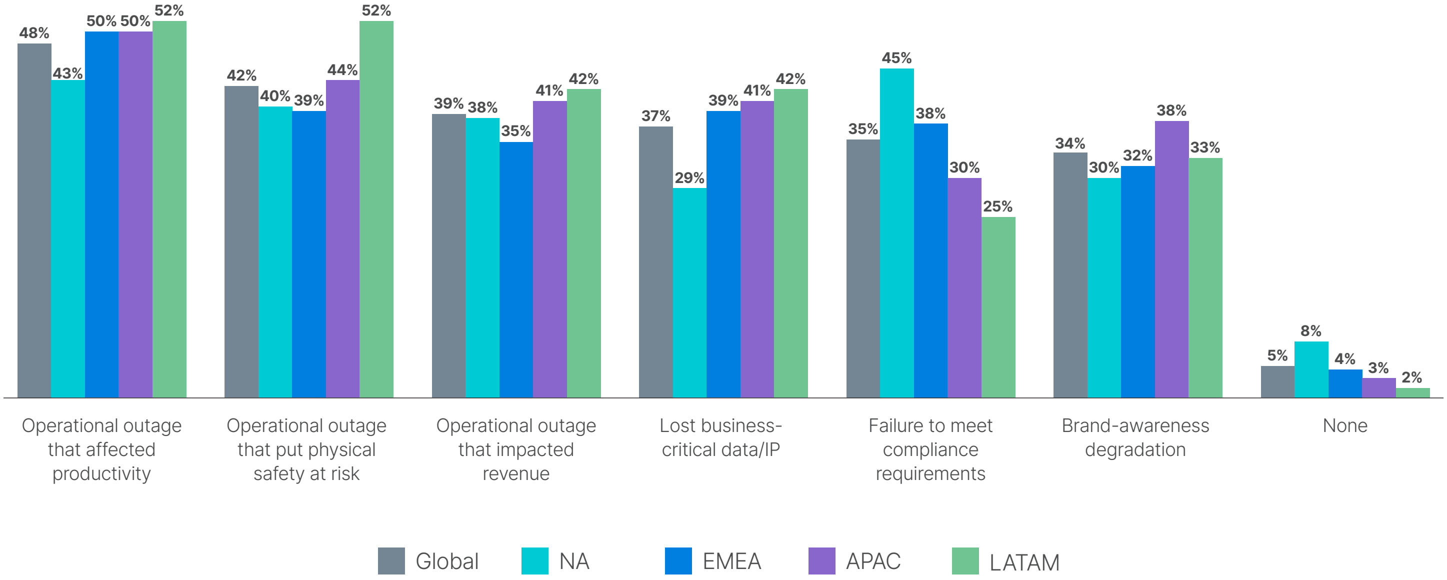
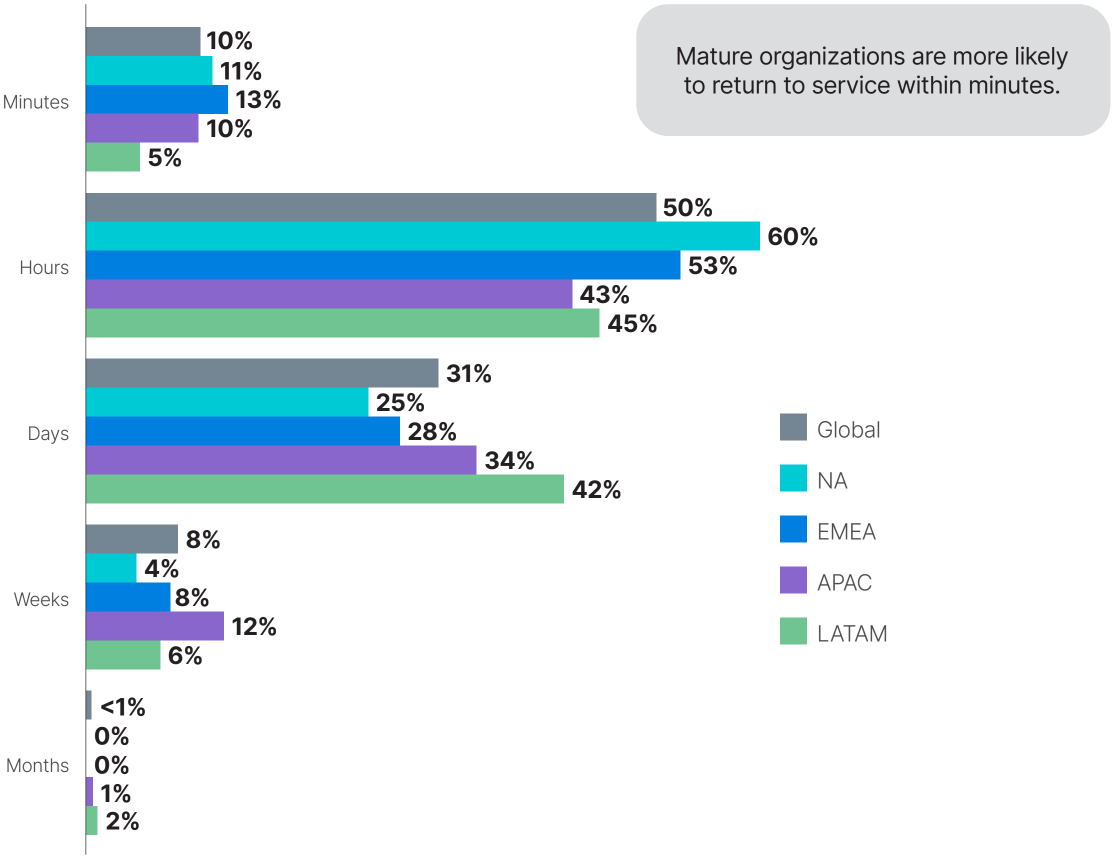


Figure 32: Organizational impacts of intrusions.



Mature organizations are more likely to return to service within minutes.

Figure 33: Longest return to service after an intrusion.

Best Practices of Top-Tier Organizations

Only 6% of organizations represented in this year's survey claim to have had no intrusions over the past 12 months, while 5% reported *more than 10 intrusions*. We compared the practices.

Only 6% of respondents could claim zero intrusions in the past year.

1. Top-tier organizations are 17% more likely to have all their OT activities centrally visible to cybersecurity operations.

Centralized, end-to-end visibility of all OT activities is key to ensuring their security, and this is definitely a work in progress at most organizations. Top-tier organizations are more than three times as likely to have achieved such visibility than their bottom-tier counterparts.

2. Top-tier organizations are 177% more likely to have security vulnerability response time as one of their top three success metrics.

As the old adage goes, "What gets measured gets improved," and responding quickly to OT security vulnerabilities is key to protecting these systems. The organizations with the best outcomes are nearly three times as likely to have this measurement as a prominent part of their performance review.

3. Top-tier organizations are 37% more likely to have role-based network access control technology in place.

Ensuring that only authorized parties can access specific systems is critical for securing any technology asset. When it comes to OT, people who need access to such systems have a relatively narrow range of job titles. Organizations that avoided intrusions last year are much more likely to have such controls in place.

4. Top-tier organizations are 48% more likely to report security compromises to senior/ executive leadership.

Items that are included in regular reports to executive leadership tend to remain at front of mind throughout the year. Organizations that keep top leaders apprised of security compromises tend to have fewer of them. Top-tier organizations tend to be more transparent with executive management.

5. Top-tier organizations are 32% more likely to have their SOC monitor and track OT security.

Security operations centers (SOCs) have existed for decades and have developed granular best practices for managing IT security. OT leaders who have avoided intrusions are more likely to have entrusted OT security to the same group.

6. Top-tier organizations are 44% more likely to track and report intrusions detected and remediated.

Understanding past attacks sharpens an organization's skills at thwarting future ones, and this starts with keeping records. Organizations that avoided intrusions are more likely to routinely report them when they do occur.

7. Top-tier organizations are infinitely more likely to use just one vendor for their IP-enabled OT devices.

Avoiding complexity in networking and systems is a good way to reduce the attack surface and improve the security posture. None of the organizations that experienced 10 or more intrusions were using just one vendor for their IP-enabled OT devices, while nearly one-third of top-tier organizations had achieved this.

Conclusion

The 2022 State of Operational Technology and Cybersecurity Report finds that OT security efforts at organizations around the world are making inadequate progress toward full protection of ICS and SCADA systems in the relatively new world of connected OT. The incremental progress that has been made in security maturity since last year has done little to move the needle on actual security outcomes. The result is that a vast majority of organizations still suffer intrusions—multiple times per year in most cases.

Given the geopolitical climate, governments around the world are warning that increased cyber attacks are likely on critical infrastructure and key economic assets. Industrial organizations across a broad spectrum of sectors will do well to quickly advance the maturity of their OT security efforts, leveraging predictive behavior, orchestration, and automation technologies to establish true zero-trust access and defend against threats coming from malicious and well-meaning insiders, external cybercriminals, and state-sponsored attackers.

Reference List

[1] Mayank Agrawal, et. al, "Industry 4.0: Reimagining Manufacturing Operations After COVID-19," McKinsey, July 29, 2020.

[2] "Global Threat Landscape Report, 1H 2021," Fortinet, August 2021.

[3] Clare Duffy, "Colonial Pipeline Attack: A 'Wake Up Call' about the Threat of Ransomware," CNN, May 16, 2021;
Liam Tung, "Ransomware: Meat Firm JBS Says It Paid Out $11m After Attack," ZDnet, June 10, 2021.

[4] "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure," CISA, April 20, 2022.

[5] Catherine Stupp, "Russian Cyberattacks Increase on Ukraine's Critical Infrastructure: Report," Wall Street Journal, April 5, 2022.

[6] Phil Muncaster, "Critical Infrastructure Firms See Cyber-Attacks Surge," InfoSecurity, May 10, 2022.

[7] Steven Webb, "IT/OT & OT Total Available Market Analysis," Westlands Advisory Research for Fortinet, March 2022.

[8] "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure," CISA, April 20, 2022.

June 2, 2022 11:21 AM

1578659-0-0-EN