REPORT

2021 State of Operational Technology and Cybersecurity Report

TABLE OF CONTENTS

Infographic: Key Findings

The 2021 State of Operational Technology and Cybersecurity Report from Fortinet finds that operational technology (OT) leaders continue to be involved in cybersecurity, but it remains a struggle. And over the past year, the pandemic only added to the security issues leaders had to face.

9 out of 10 organizations experienced at least one intrusion in the past year and 63% had 3 or more intrusions, which is similar to the results in 2020.

The most common intrusions were **malware at 57%** and **phishing at 58%,** which was up from **43%** last year.

42% experienced insider breaches, which is up from **18%** last year.

Compared with bottom-tier organizations, top-tier organizations:

Are more likely to use **orchestration and automation** and have **security tracking and reporting** in place.

Are more likely to have **100% centralized visibility** in their security operations center.

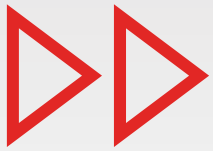
Were more prepared, earlier, to **accommodate work from home** driven by the pandemic.

Executive Summary

The 2021 State of Operational Technology and Cybersecurity Report from Fortinet finds that operational technology (OT) leaders continue to face cybersecurity challenges, some of which were exacerbated by the shift to work from home due to the pandemic. The pandemic also accelerated IT-OT network convergence for most organizations, which correlates to other CEO reports that indicate pandemic-related changes have accelerated digital transformation, putting organizations years ahead of where they would have expected to be at this point.[1,2]

Many organizations had to increase their technology budgets to accommodate the move to remote work. And as a result of the many changes brought about by the pandemic, many OT leaders are looking for new ways to streamline processes and reduce costs.

As noted in the 2020 report, the momentum for OT-IT network convergence was already happening pre-pandemic, but the effects of the pandemic accelerated digital transformation and increased the need for connectivity. Employees were required to work from home and OEMs and system integrators were hampered by their inability to travel to service equipment. Getting on-site became much more difficult, so the pandemic clearly increased the need for third-party secure remote access. Overcoming these challenges increased both costs and risks.



In a recent KPMG CEO survey, 80% of respondents suggested the pandemic had accelerated digital transformation, and 30% said that progress had put them years ahead of where they would have expected to be right now with one saying, "...we've seen 3 to 4 years of progress in just 3 to 4 months."[3]

In 2021, we saw a change in respondents away from Manager of Manufacturing to more VP and Director level. The responsibility for OT is shifting away from VP or Director of Network Engineering to CISOs and CIOs. Additionally, there were more security operations centers (SOCs) and significantly more network operations centers (NOCs) in place in 2021 than the prior year.

As we have in previous years, we also compared the practices of respondents who had seen zero intrusions in the past year with those who had 10 or more intrusions. We again found that "top-tier" OT leaders were significantly more likely to adhere to a number of best practices, including:

- Leveraging orchestration and automation and using predictive behavior
- Tracking and reporting the financial implications of cybersecurity to the business
- Reporting compliance with industry regulations and scheduled security assessments

Adhering to cybersecurity best practices helped top-tier OT organizations better withstand the technology changes, threats, and vulnerabilities that occurred during the pandemic.

Introduction

The operational technology (OT) market is expected to continue to grow through 2027 at a CAGR of 6.40%, which is no surprise because OT makes it possible for the world's factories, energy production and transmission facilities, transportation networks, and utilities to function.[4]

To boost operational efficiency and profitability, many OT companies have been integrating OT infrastructure such as supervisory control and data acquisition (SCADA) systems with IT networks. Competitive pressures are driving an urgency to reduce costs and increase efficiencies in a variety of ways, such as:

- Utilizing digital twins to reduce risks supporting asset performance management (APM)
- Increasing overall equipment effectiveness (OEE) to drive increased manufacturing yield
- Shifting from calendar-based to condition-based maintenance to minimize lost production associated with service outages
- Increasing asset availability and reliability
- Digitization of paper recordkeeping and service reports for service and maintenance activities

These and other digital transformation initiatives have led to innovations requiring new platforms and new ways for people to work than they have in the past. That change in workstyles was exacerbated with the sudden need for employees to work from home. Although the move to remote work is a significant example of digital transformation, the array of systems and processes affected as a business digitally innovates spans all of OT.

All the improved agility and efficiency that comes from OT-IT network convergence also comes with increased risks. The diminishing presence of the "air gap" between OT networks and IT systems means the OT infrastructure is subject to all of the threats that IT systems have traditionally faced. Worse, the attack surface for an OT system can comprise Industrial Internet of Things (IIoT) devices, which control critical systems that can have potentially dire health and safety consequences if they are breached.

A majority of OT leaders report the maturity of their security posture as at least Level 2 access, which means they have established visibility, segmentation, access, and profiling. At Level 2, they have complete role-based access and are working to achieve zero trust by enforcing multi-factor authentication. In fact, 99% of surveyed respondents were above Level 0, which means only 1% have absolutely no visibility or segmentation in place in OT.

Although progress is being made, there is room to grow. Most OT organizations are not leveraging orchestration and automation and their security readiness was further taxed by the COVID-19 crisis. OT-IT network convergence coupled with an ever-increasing advanced threat landscape and coping with pandemic-related issues made it even more difficult for OT leaders to stay ahead of adversaries. Although following security best practices takes time and money, those organizations that did were better able to withstand the changes brought about by the pandemic.

Methodology for This Study

This year's State of Operational Technology and Cybersecurity Report is based on a survey conducted from February 24 to March 1, 2021. The questions mirrored those asked in similar surveys in 2019 and 2020. Respondents work at companies involved in four industries: manufacturing, energy and utilities, healthcare, and transportation. All are responsible for some aspect of manufacturing or plant operations and occupied job grades ranging from manager to vice president. This study utilizes data from the survey to paint a picture of how operations professionals interact with cybersecurity in their daily work. The analysis looks at this year's data and compares it with results from prior years and identifies several overarching insights about the state of the industry. We then delve more deeply into the data, identifying best practices more commonly used by "top-tier" organizations—those who have experienced 0 intrusions in the past 12 months versus those that have seen more than 10 attacks in the same period.

Insights for OT Security

As noted, OT leaders continued to struggle with changes related to OT-IT convergence. Additionally, the sudden need to increase budgets because of COVID-19 was a big part of the story in 2020. Leaders continued to face challenges related to security measurements and analysis and a significant number of intrusions, particularly from insider threats.

Insight 1: OT leaders continue to see significant intrusions that affect the organization. Outages that affect productivity and revenue continue, and the risks to physical safety are rising.

As a group, organizations represented by the OT leaders who participated in the survey have been largely unsuccessful at preventing cyber criminals from intruding their systems. Nine out of 10 organizations experienced at least one intrusion in the past year, which is almost identical to the results of last year's survey. Even though the pandemic was an unusual situation, a 90% rate of intrusion represents a significant problem that should concern OT leaders.

There was a significant change in insider breach instances, which have increased to 42%. Unlike unintentional security accidents, such as an employee who clicks a bad link, bad actors have malicious intent, which means OT leaders should carefully consider who has access to their systems. Additionally, with so many employees working from home, it is likely that the security issues related to home networks contributed to problems. For example, if virtual private network (VPN) filters are not adjusted correctly, phishing emails could pass through that would otherwise not get through on the corporate network. It also highlights the need for organizations to move toward a zero-trust model and away from a perimeter-based networking approach.

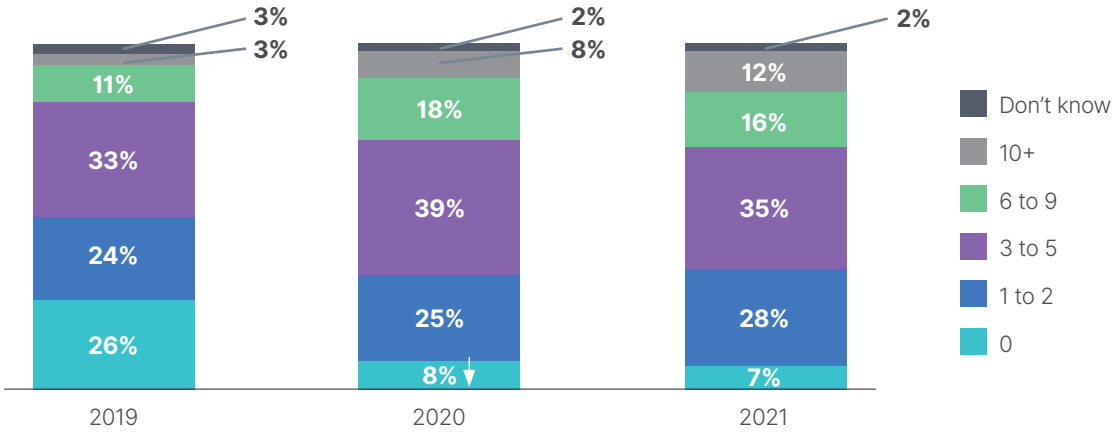


Figure 1: Number of intrusions in the past year.

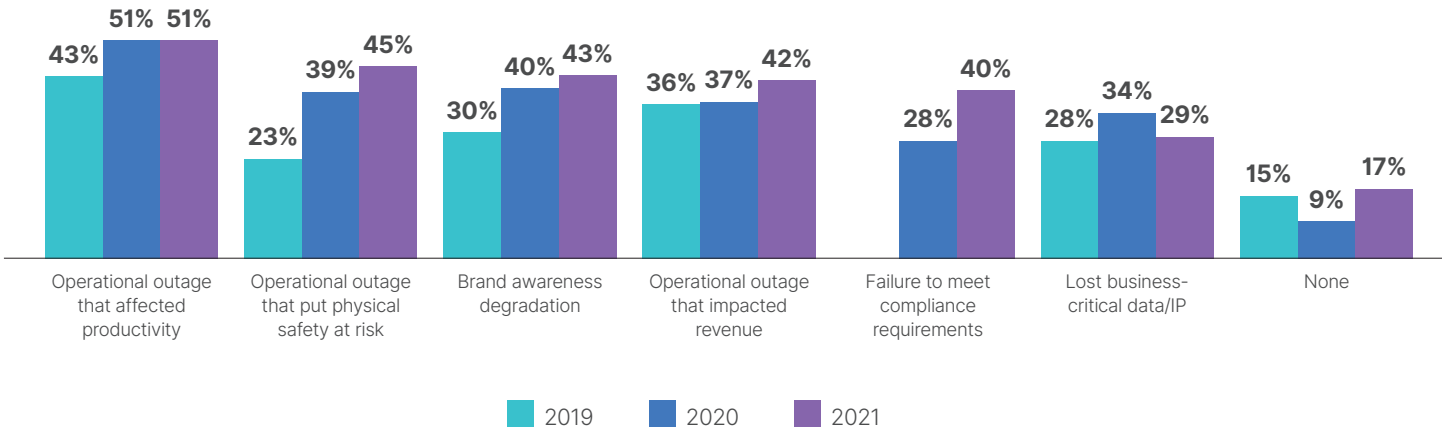


Figure 2: Impact on organization.

Insight 2: OT leaders were not prepared for changes related to the pandemic and had to quickly increase budgets and change processes.

With the exception of a small number of top-tier companies, OT leaders had to quickly increase spending to manage processes related to IT-OT network convergence and the need to support work from home. These two separate issues both affected technology budgets. SOCs and NOCs needed more staff and equipment because the pandemic accelerated digital transformation and increased the need for connectivity for secure remote access. Employees needing to work from home and OEMs and system integrators were hampered by their ability to travel. In the past, OEM technicians could get on a plane and work on-site to service equipment, but tightening corporate travel policies and government-imposed travel lockdowns during the pandemic hampered the ability to travel to the site. The pandemic accelerated the need for third-party secure remote access because technical staff could not be on-site doing work in person.

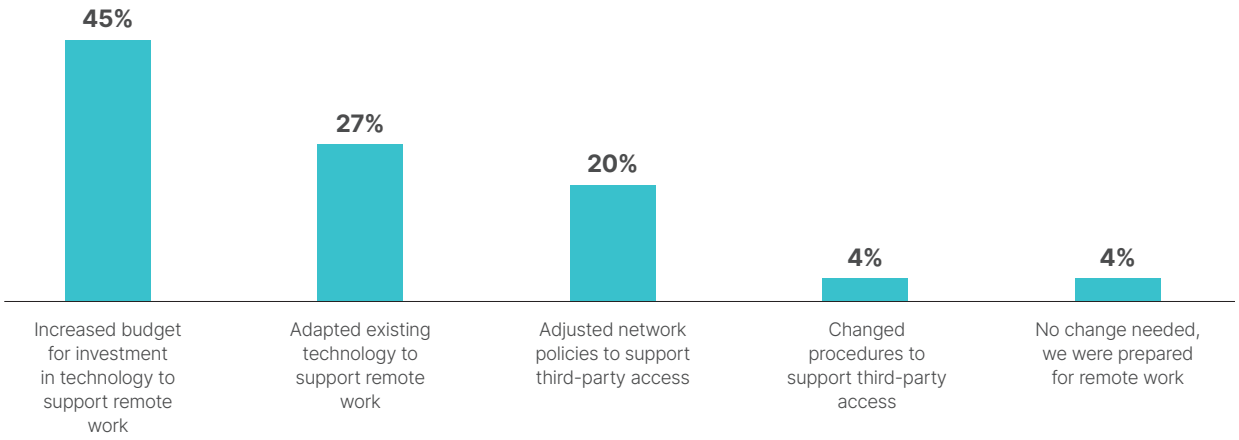


Figure 3: Biggest change to facilitate work from home.

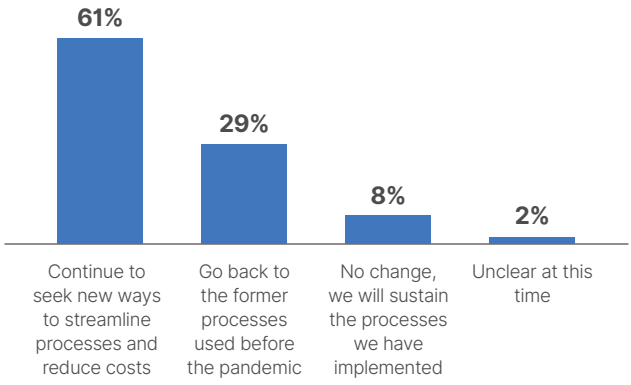


Figure 4: Post-pandemic work process adjustments.

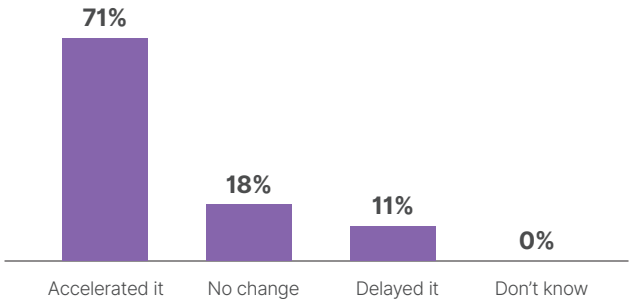
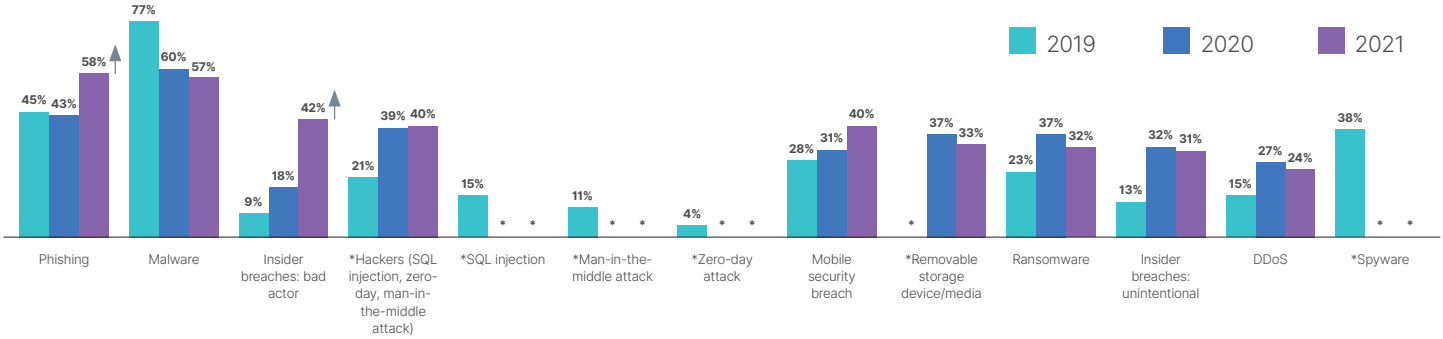


Figure 5: Pandemic impact on IT-OT convergence.

Insight 3: OT leaders faced a significant increase in insider threats and phishing. Malware continued to be a problem.

The survey showed significant growth in phishing attacks with 58% reporting this type of intrusion, up from 43% last year. The increase in phishing stems from attackers exploiting weaknesses related to the rapid changes to working that occurred at the beginning of 2020. No one was immune, and along with everyone else, OT organizations were affected.

Similarly, determining how to extend the workforce to the home affected organizations of all types, and OT was no exception. Bad actors targeted operational technology because they could exploit security weaknesses. And their success rates went up as they discovered a broad array of vulnerable attack surfaces. These numbers are not surprising because during periods of uncertainty and sudden change, exploits typically increase as attackers take advantage of new areas of risk. As employees continue to work remotely, it is clear that OT organizations need to extend zero trust to their endpoints to reduce the attack surface.



↑↓ indicates significant difference from previous year at 95% CL

*Answers adjusted in 2020: SQL Injection, Man-in-the-Middle Attack, Zero-Day Attack removed; Hackers (i.e., SQL Injection, Zero-Day Attack, Man-in-the-Middle Attack, etc.) added. Spyware removed. Removable Storage Device/Media added.

Figure 6: Intrusion experienced.

Insight 4: OT leaders continue to struggle with security measurements and perceptions.

OT leaders are tracking and reporting cybersecurity measurements consistently with cost lower on the priority list than risk assessment and the implications to the business. Vulnerabilities (70%) and intrusions (62%) remain the top cybersecurity measurements that are tracked and reported, but tangible risk management outcomes have become more prevalent this year (57%). OT cybersecurity issues are reported to senior/executive leadership fairly evenly, although the results of penetration/ intrusion tests are not shared quite as much as the other issues.

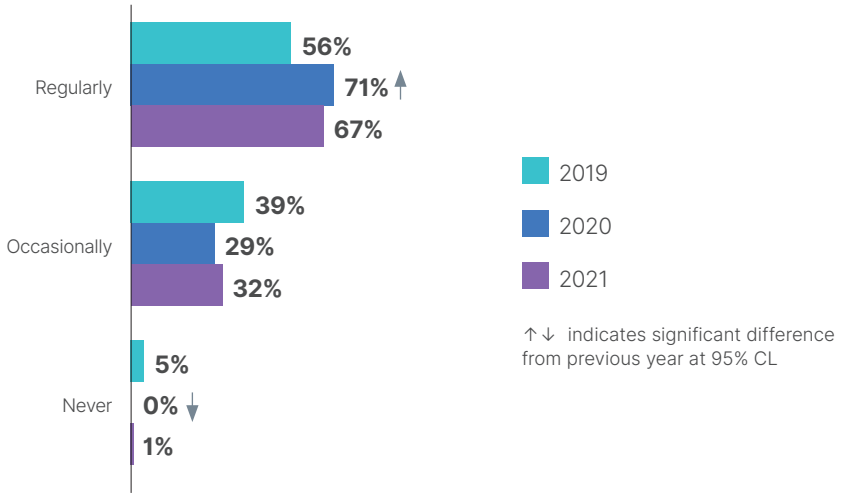
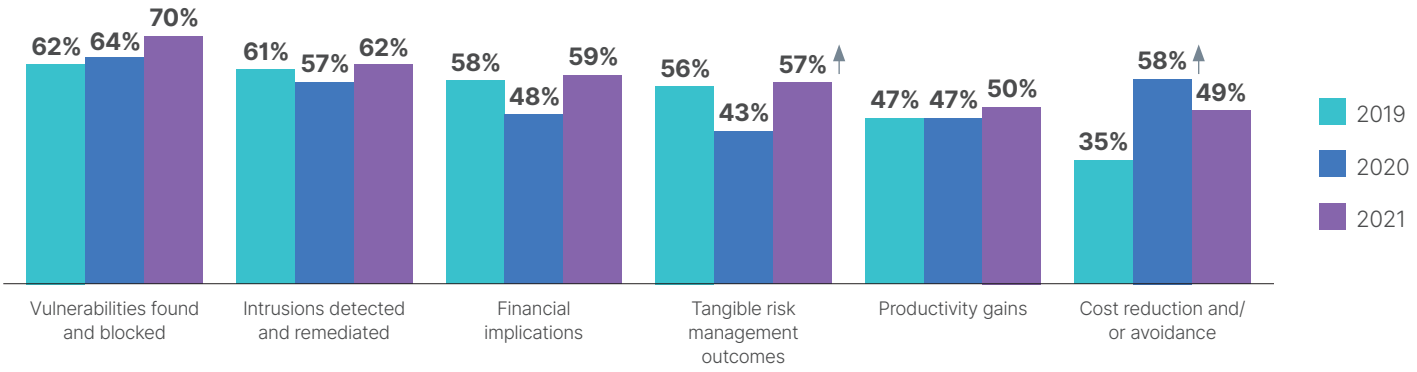
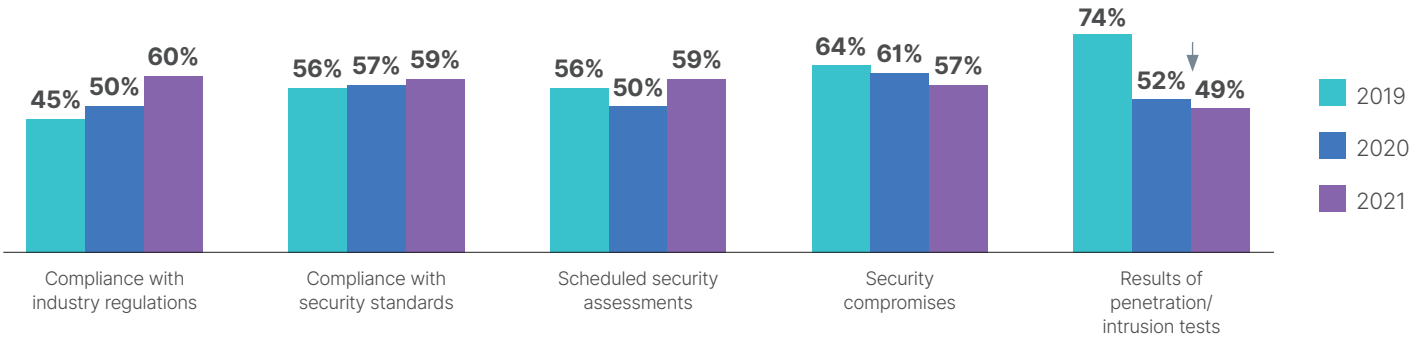


Figure 7: Involvement in IT cybersecurity strategy.



↑↓ indicates significant difference from previous year at 95% CL

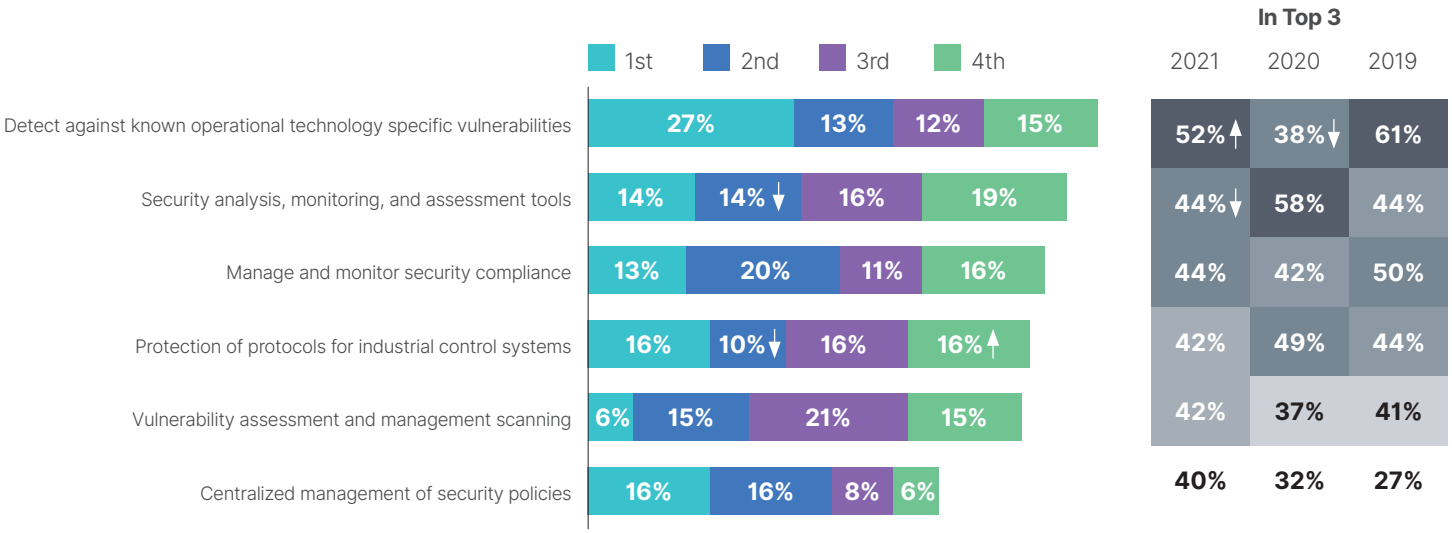
Figure 8: Cybersecurity measurements tracked and reported.



↑↓ indicates significant difference from previous year at 95% CL

Figure 9: Reported OT cybersecurity issues.

When asked which features in security solutions are most important to them, attack detection tools were most commonly cited, regaining the importance they lost in 2020 to become the most important security solution again in 2021. Security analysis, monitoring, and assessment tools were reported as significantly less important in 2021 than they were in 2020.



↑↓ indicates significant difference from previous year at 95% CL

Figure 10: Most important security solutions features (ranking).

In past years, respondents said cybersecurity solutions impeded operational flexibility, but in 2021, "creating business concerns" increased. Having a breach in the news is bad for business and it is likely that more cybersecurity education raised awareness and helped OT leaders see it as a necessary part of the strategy.

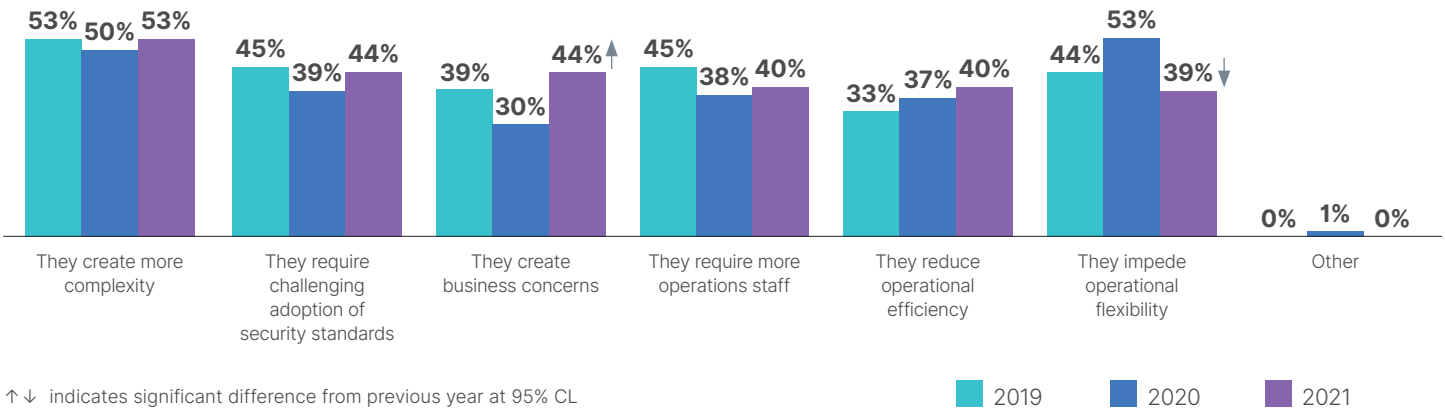


Figure 11: How cybersecurity solutions can negatively impact OT professional success (in top 3).

Best Practices of Top-tier Enterprises

In this year's survey, only 7% of OT leaders reported no intrusions, while 12% of respondents had 10 or more intrusions. We compared the survey responses from these two subsets—our "top-tier" and "bottom-tier" respondents. This analysis identified a number of best practices that top-tier OT leaders were more likely to employ.

1. Top-tier organizations are more likely to track and report financial implications.

As the old adage goes, what gets measured gets improved. Financial implications to security vulnerabilities were tracked and reported by 74% of top-tier organizations. They also track vulnerabilities found and blocked (74%) and tangible risk management outcomes (60%).

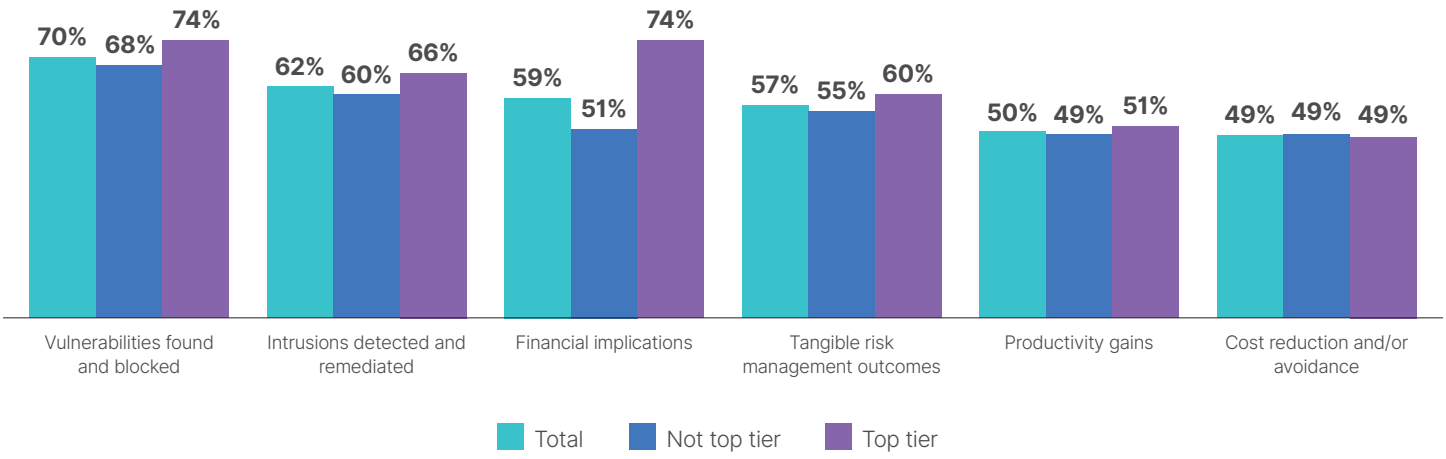


Figure 12: Cybersecurity measurements tracked and reported.

2. Top-tier organizations are more likely to report compliance with industry regulations and perform scheduled security assessments.

Compliance is increasingly a concern for an organization's top leaders, but if the reports must be prepared manually, at many OT organizations those reports are not likely to be performed more frequently than auditors demand. However, top-tier organizations are more likely to do these regular reports, suggesting that they have automated compliance reporting across the enterprise. With more of a real-time approach to reporting, they are better able to improve their security posture.

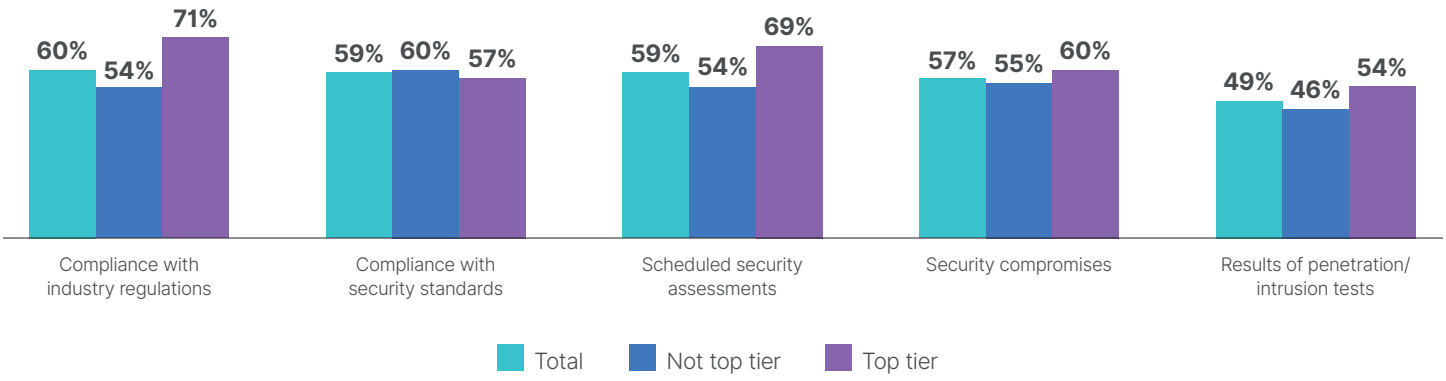


Figure 13: Reported OT cybersecurity issues.

3. Top-tier organizations are more likely to have 100% visibility into OT activities.

Centralized visibility is critical for effective security protection across the enterprise, and OT systems are no exception. Top-tier organizations are more likely to have full visibility.

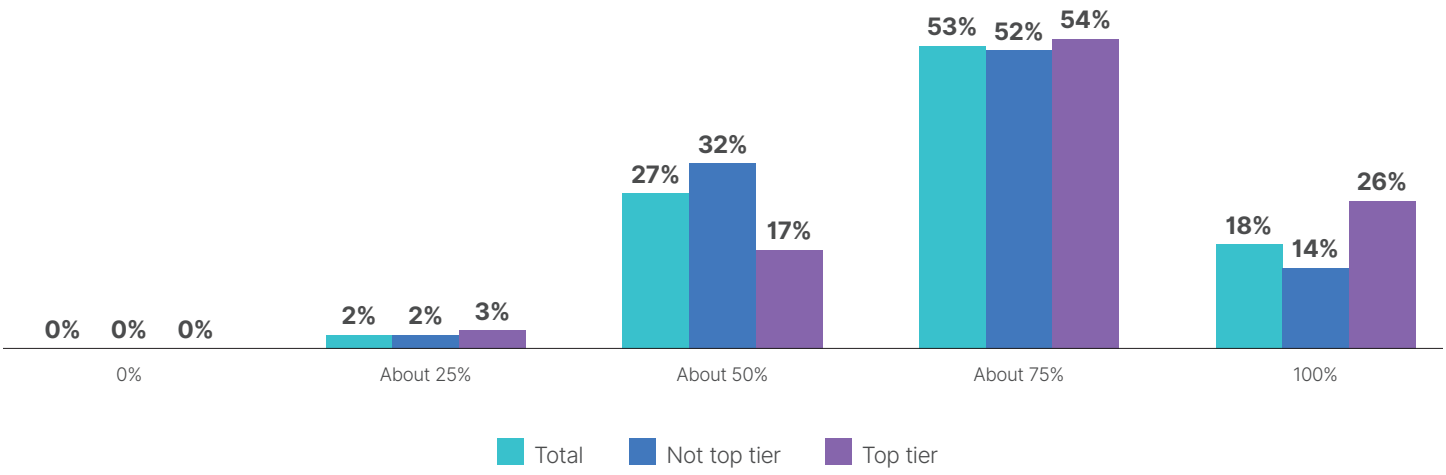


Figure 14: % of OT activities centrally visible.

4. Top-tier organizations had less trouble facilitating work from home and some did not have to do anything at all.

To facilitate work from home, top-tier organizations were evenly spread among budget, technology, and network policy being the biggest changes they needed to make. And 11% reported that they did not need to make any changes at all because they were prepared for remote work.

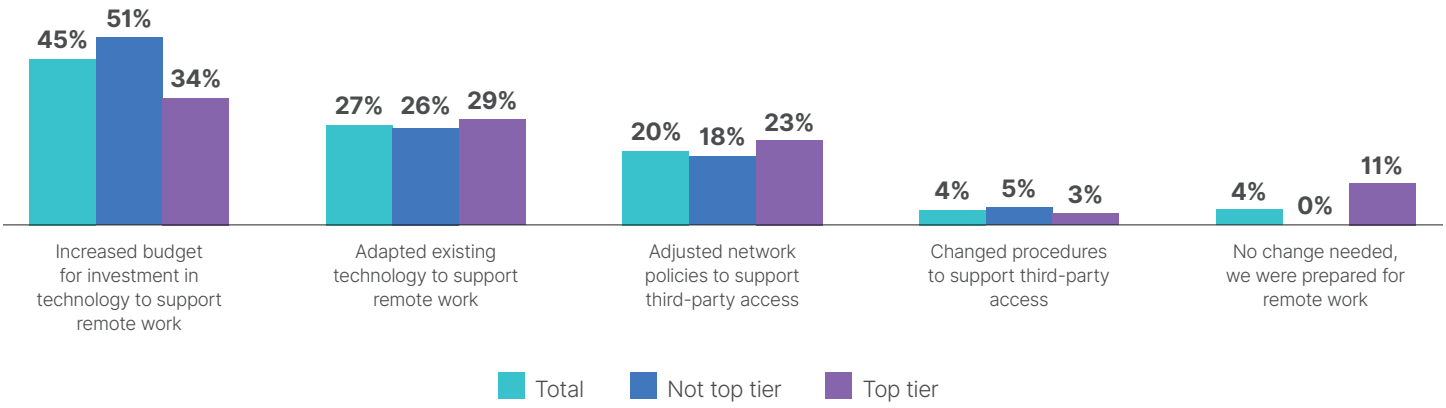


Figure 15: Biggest change to facilitate work from home.

5. Top-tier organizations are most likely to streamline processes and reduce costs post-pandemic.

The pandemic accelerated IT-OT network convergence for most OT organizations, but top-tier organizations were more likely to report that they will continue to seek ways to streamline processes and reduce costs post-pandemic (74%).

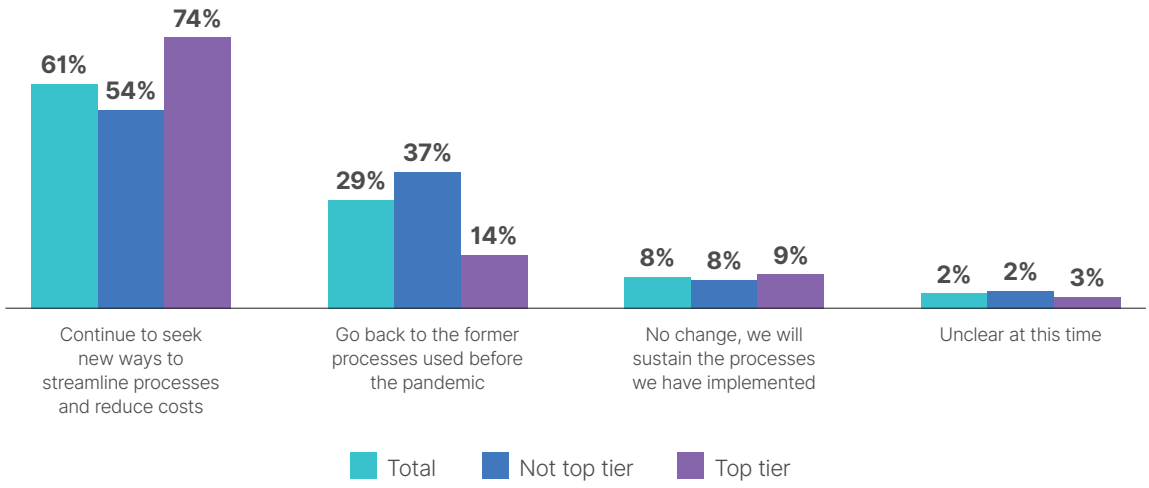


Figure 16: Post-pandemic work process adjustments.

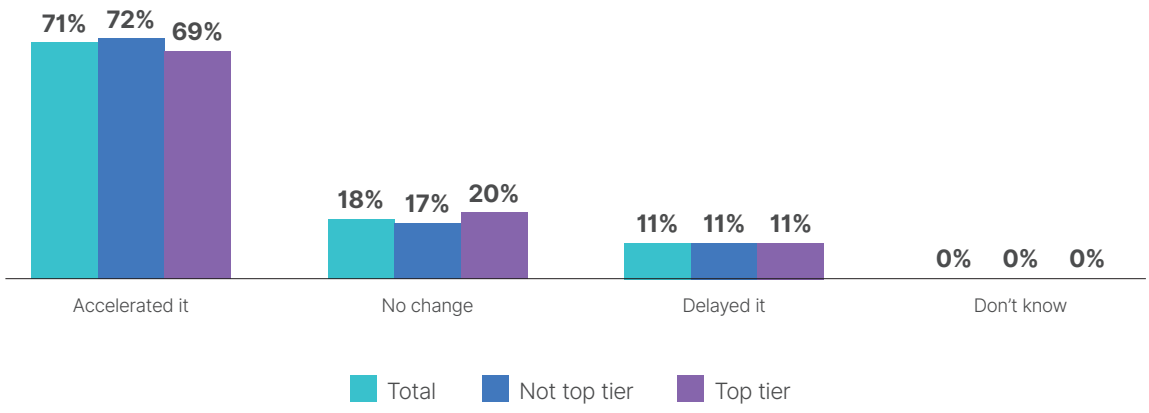


Figure 17: Pandemic impact on IT-OT convergence.

6. Top-tier organizations are more likely to have OT responsibility under the CIO.

In general, there is a trend of OT responsibility shifting away from VP or director of network engineering to CISOs and CIOs. Although OT directors tend to have ultimate responsibility for OT cybersecurity, regardless of the type of organization, top-tier organizations are more likely to have responsibility under the CIO (23%), and are less likely to plan to roll OT responsibility under the CISO.

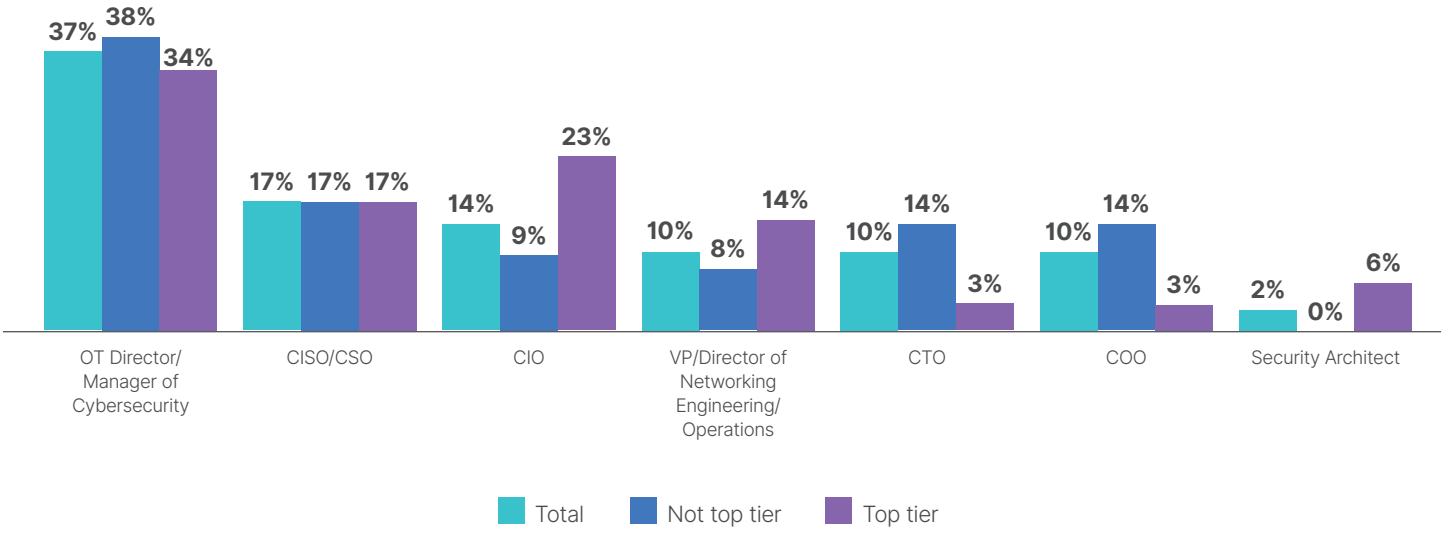


Figure 18: OT cybersecurity responsibility.

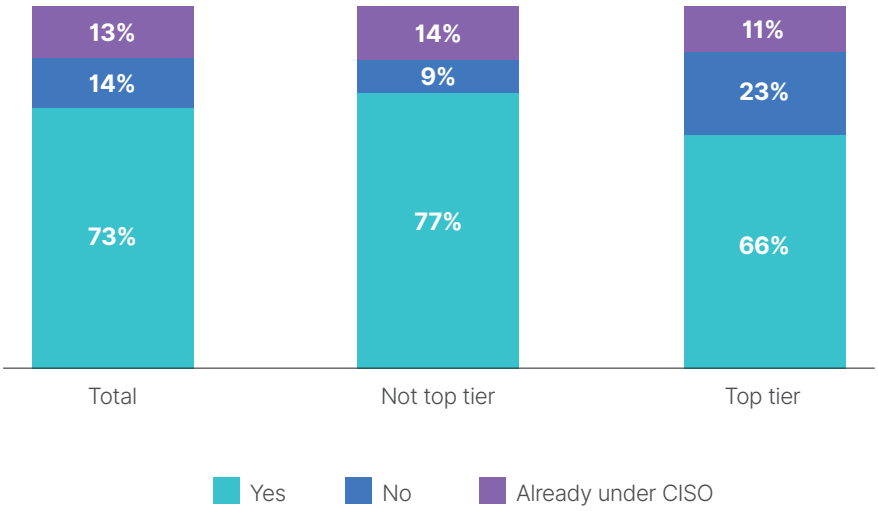


Figure 19: Cybersecurity to be under CISO in the next 12 months.

Conclusion

Risks continue to be high in companies that are charged with protecting OT environments, holding steady from last year. The results are not as bad as they could be considering the coincident of a global pandemic. If nothing else, the past year has reflected how important it is for organizations to continue proportional investment in security. Since OT networks are rarely air gapped from IT networks and connections to the internet, OT systems are more vulnerable. They face increasing risks from IT-borne and internet-borne attacks. And because of the increase in insider threats, OT organizations will need to continue to work to establish zero-trust access for remote users and focus on security awareness and training throughout the organization.

Reference List

[1] "KPMG 2020 CEO Outlook: COVID-19 Special Edition," KPMG International, September 2020.

[2] Thomas Menze, "The State of Industrial Cybersecurity in The Era of Digitalization," ARC Advisory Group, September 2020.

[3] "KPMG 2020 CEO Outlook: COVID-19 Special Edition," KPMG International, September 2020.

[4] "Global Operational Technology Market—Industry Trends and Forecast to 2027," Data Bridge Market Research, July 2020.

May 26, 2021 5:15 AM

956064-0-0-EN