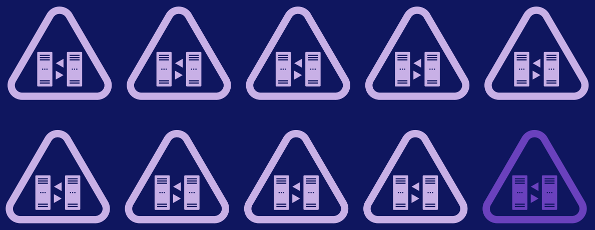
REPORT

2020 State of Operational Technology and Cybersecurity Report

Table of Contents

Infographic: Key Findings

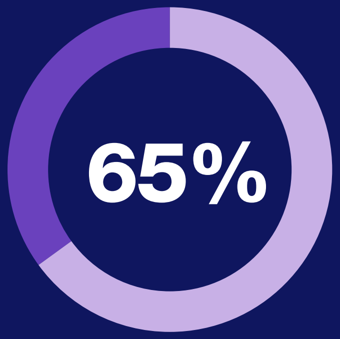
The 2020 State of Operational Technology and Cybersecurity Report from Fortinet finds that operational technology (OT) leaders are highly respected in their organizations, and that their teams are vital to their companies' bottom lines. Cybersecurity continues to be an integral part of their daily work—and that work continues to be a struggle.



9 out of 10

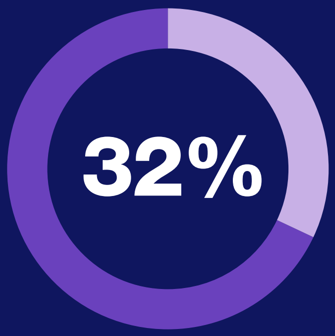
organizations **experienced at least one OT system intrusion** in the past year, up **19%** from 2019

65% had **3 or more intrusions**, up **18%** from 2019

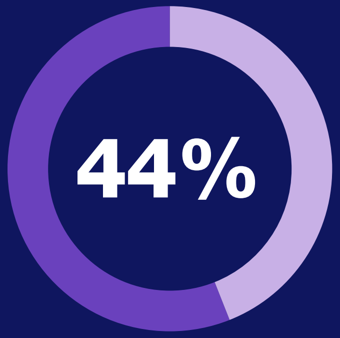


of OT leaders are responsible for embedding security within ops processes

But **78%** have placed OT security under the CISO, or will do so in the next year



have security vulnerabilities response time as a top-three measurement, down **12%** from 2019



do NOT track and report compliance with industry regulations

44% do NOT track and report compliance with security standards

Top-tier organizations are:

4X as likely to have centralized visibility in the SOC

133% more likely to track and report vulnerabilities found and blocked

2X as likely to currently have the CISO/CSO responsible for OT security

Get the full 2020 State of Operational Technology and Cybersecurity Report from Fortinet.

Executive Summary

The 2020 State of Operational Technology and Cybersecurity Report from Fortinet finds that operational technology (OT) leaders are highly respected in their organizations, and that their teams are vital to their companies' bottom lines. Cybersecurity continues to be an integral part of their daily work—and that work continues to be a struggle.

In fact, an April 2020 survey of OT leaders conducted by Fortinet indicates that, as a whole, organizations are moving in the wrong direction in terms of outcomes. Only 8% of respondents had seen no intrusions over the past 12 months, a decline of 18 percentage points compared with respondents to a similar survey a year ago. And the share of organizations experiencing three or more intrusions increased from 47% to 65% over that same period. These intrusions often impacted operational efficiency, revenue, and even physical safety.

A number of factors may play into this decline. OT systems are losing their air gaps and becoming increasingly interconnected with IT systems and the internet. Enterprise networks are becoming more complex, making holistic protection more difficult. And threat actors are using increasingly sophisticated tactics. But the research also shows a significant percentage of organizations have not extended some elements of basic security hygiene into their OT environments.

A deeper look into the data highlights this trend. We compared the practices of respondents who had seen no intrusions in the past year with those who had 10 or more intrusions, and found that "top-tier" OT leaders were significantly more likely to adhere to a number of best practices, including:

- Rolling the OT cybersecurity responsibility under the CISO—now or in the coming year
- Tracking and reporting basic cybersecurity metrics
- Being involved in cybersecurity purchase decisions
- Having OT activities be centrally visible
- Increasing security budgets

These best practices reflect a holistic approach to cybersecurity that enables OT leaders to keep up with industry changes, reduce time and increase productivity, and provide the best protection against threats and vulnerabilities.

Introduction

Operational technology (OT) is a vital component of a functioning economy. It makes it possible for the world's factories, energy production and transmission facilities, transportation networks, and utilities to function. Advances in technology have resulted in great improvements in operational efficiencies across the economy, and manufacturing and plant operations are no exception. Annual sales in OT hardware and software are projected to reach $40 billion by 2022 after growing by more than 6% annually over five years.[1]

Much of this new spending is related to the convergence of OT infrastructure such as supervisory control and data acquisition (SCADA) systems with IT networks to boost operational efficiency and profitability. Historically air gapped from the internet, OT systems now depend on information from IT systems and even public internet sites to effectively manage plant operations in real time.

But this improved agility comes at the cost of increased risk. While the biggest risk to an air-gapped OT system might come from software updates manually loaded from physical media, many of today's OT systems face all the threats that IT systems face. In addition, the attack surface for an OT system often includes Internet-of-Things (IoT) devices in remote locations, such as sensors attached to pipelines and water mains.

An increasingly advanced threat landscape compounds the risk, because OT leaders have to try to stay ahead of sophisticated adversaries using cutting-edge technology. Following security best practices takes time and energy some feel they do not have. Adaptability and flexibility are necessary traits for success, along with planning ahead to make sure productivity is not affected when employing best practices.

As organizations face increased threats and vulnerabilities, stagnant budgets, staffing shortfalls, and the continuing COVID-19 crisis, OT leaders will be tasked with adapting to meet these challenges. Following best practices could be the very thing that will allow them to do so with less frustration and time lost.

Methodology for This Study

This year's State of Operational Technology and Cybersecurity Report is based on a survey conducted in April 2020. The questions mirrored those asked in a similar survey a year earlier—the basis for the 2019 version of this report.[2] 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 last year's results, identifying several over-arching 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 no intrusions in the past 12 months—versus those that have seen more than 10 attacks in the same period.

> "Having to shift focus to develop cybersecurity solutions and ensure that I am following increased security best practices is hindering my ability to accomplish hourly and minute-based tasks."
> *–Survey Respondent, Manager of Manufacturing Operations, Manufacturing*

Insights for OT Security

As OT leaders fulfill their roles in cybersecurity, many are challenged by a lack of core protections; struggles with security measurements and analysis; and significant intrusions having a growing impact on their organizations.

Insight: OT Leaders Have Broad Responsibilities That Often Include Cybersecurity

OT leaders generally report to high-ranking people in the organization, including vice presidents, chief operations officers, and even the CEO (Figure 1). They are routinely consulted on cybersecurity matters, with 80% regularly participating in cybersecurity decisions and half having final say in those decisions (Figure 2).

In addition to operations team supervision and managing production efficiency, embedding security within operations processes is a direct responsibility for 64% of OT leaders (Figure 3). Nearly three-quarters (71%) are regularly involved in IT cybersecurity strategy, up from 56% in 2019 (Figure 5). This would seem to indicate that security would be a top success measurement. However, only one-third of OT leaders list it as a top-three success measurement and just over half as a top-five success measurement (Figure 4).

OT leaders will likely always have aspects of cybersecurity on their plates; the clear trend is still toward OT security being placed beneath the CISO. The CISO manages security matters for OT systems at 22% of organizations this year, up from 18% last year. And a staggering 61% of respondents say that they expect OT security responsibilities to be transferred to the CISO's team in the coming year. If those changes occur as expected, the CISO's team will manage OT security at 83% of organizations by next year. This likely reflects the increasing risk of connected OT systems and the critical nature of such infrastructure for business continuity.

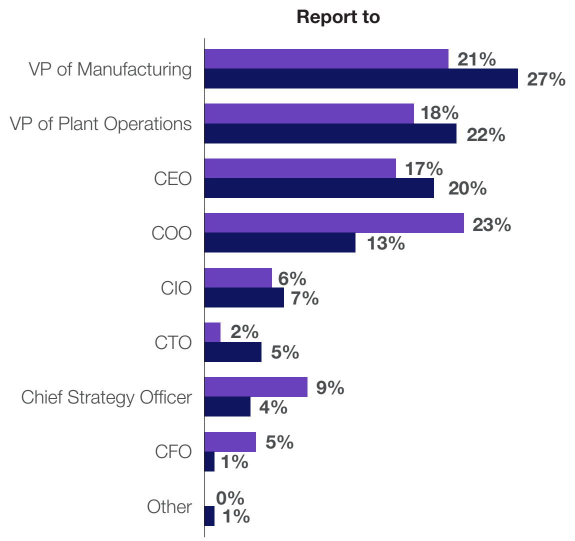


Figure 1: OT leaders' direct supervisor.

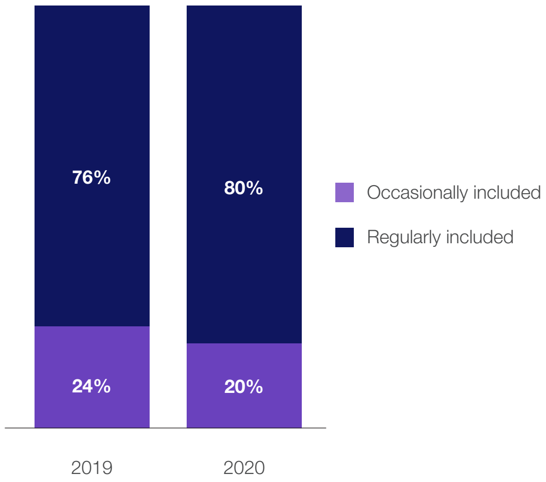


Figure 2: OT leaders' involvement in cybersecurity purchase decisions.

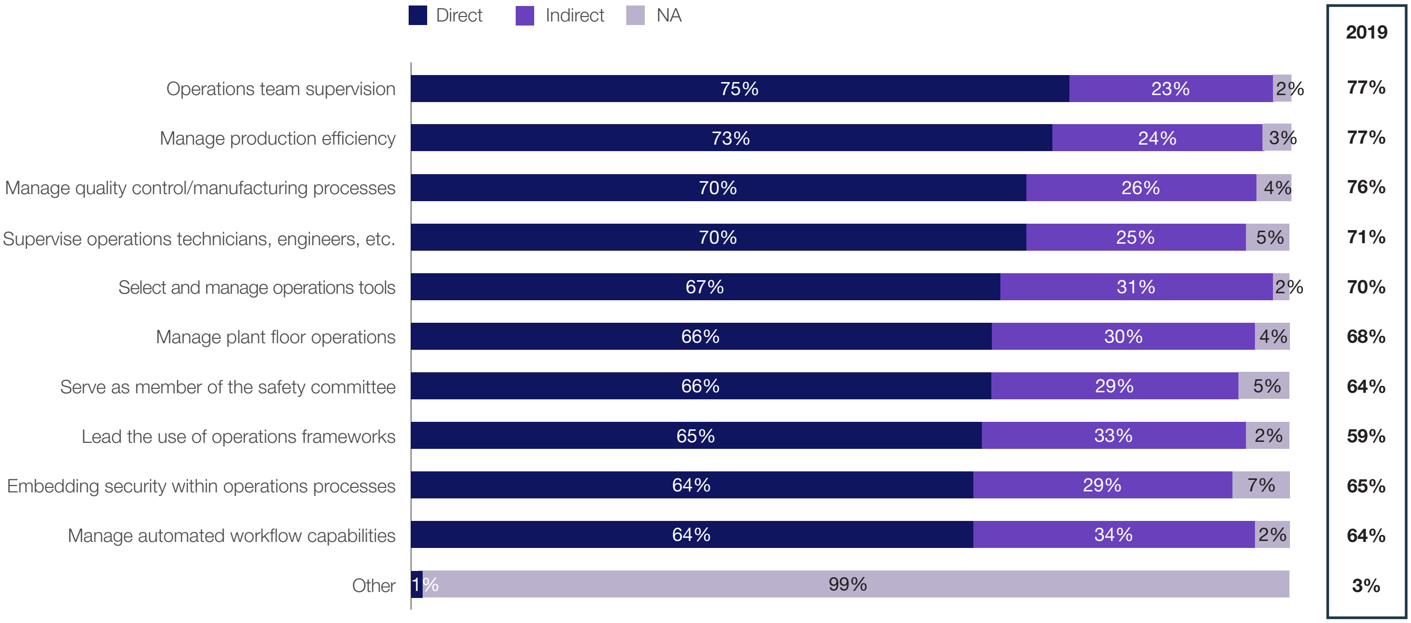


Figure 3: OT leaders' job responsibilities.

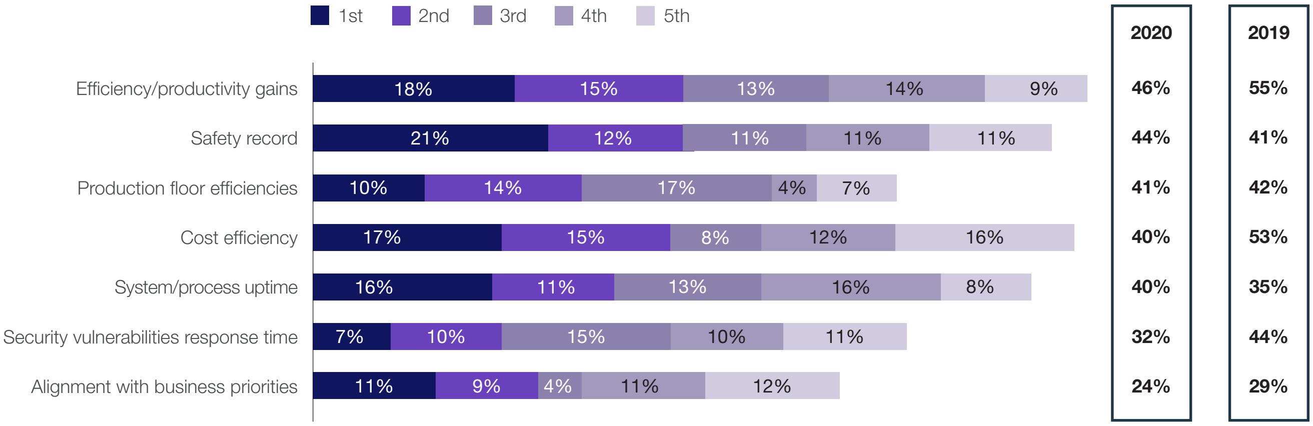


Figure 4: How OT leader success is measured (ranking).

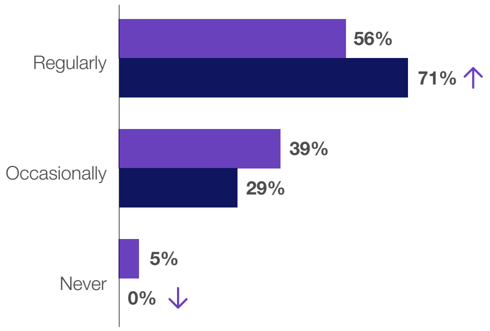


Figure 5: Involvement of OT leaders in IT cybersecurity strategy.

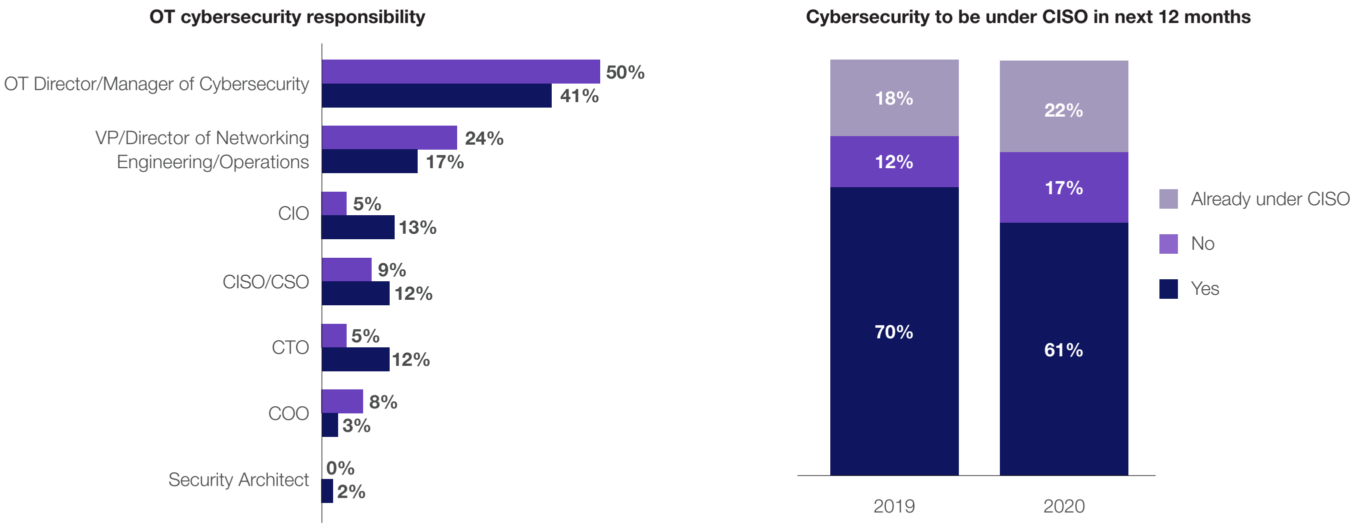


Figure 6: Cybersecurity responsibility now and in the next 12 months.

Insight: Many OT Infrastructures Still Lack Core Cybersecurity Protection

Although OT leaders have a number of cybersecurity and security features in place, many are lacking in key areas. For example, while security information and event management (SIEM) solutions are the most commonly cited security feature, nearly four in 10 still lack this tool (Figure 7). Nearly half lack a technical operations center (TOC) and a security operations center (SOC), with more than half lacking a network operations center (NOC). Of those who do have a SOC, 77% do not have all OT activities centrally visible by the security operations team (Figure 8). Features that enable zero-trust access are also lacking at many organizations, including internal network segmentation (47%), network access control (59%), and multi-factor authentication.

Fortunately, 58% of organizations are seeing their budgets increase in 2020, although only 13% expect a dramatic increase (Figure 9). Of some concern are the 15% of organizations seeing their security budgets decrease, up 10% over the year before. Although the question was not asked, it is possible these reductions may be connected to revenue losses and global business closures because of COVID-19.

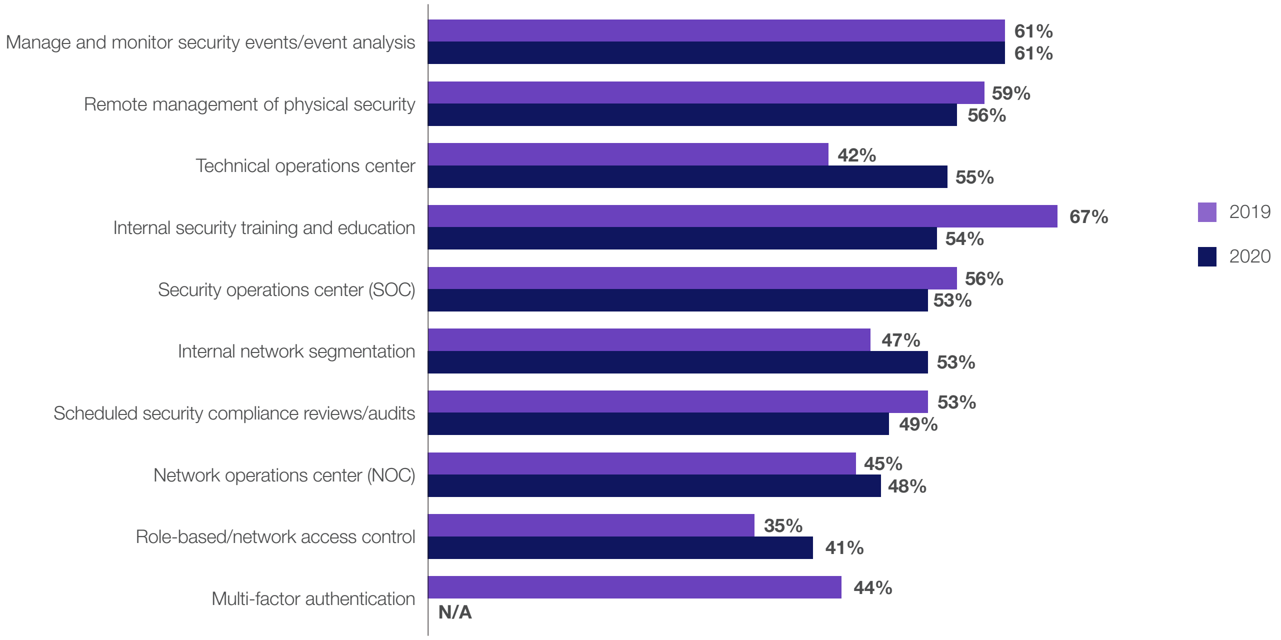


Figure 7: Cybersecurity and security features in place.

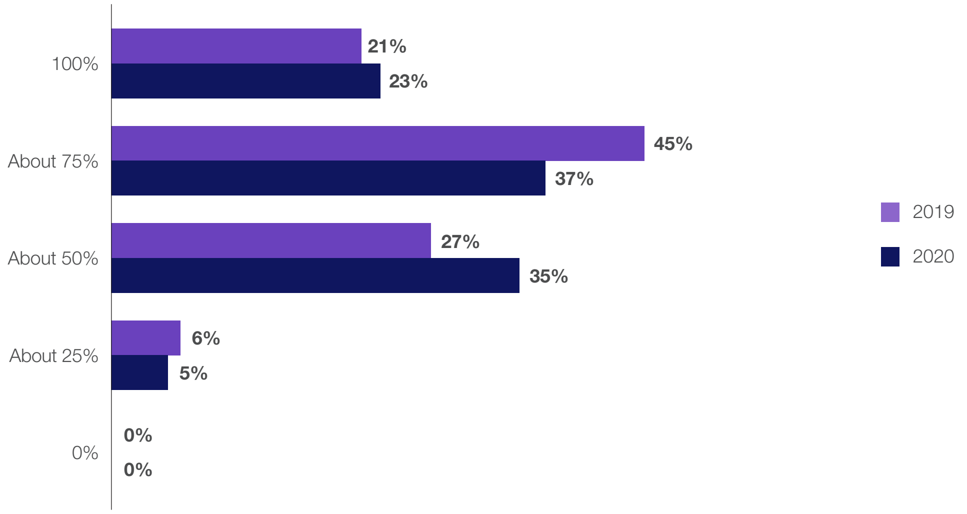


Figure 8: Percent of OT activities centrally visible.

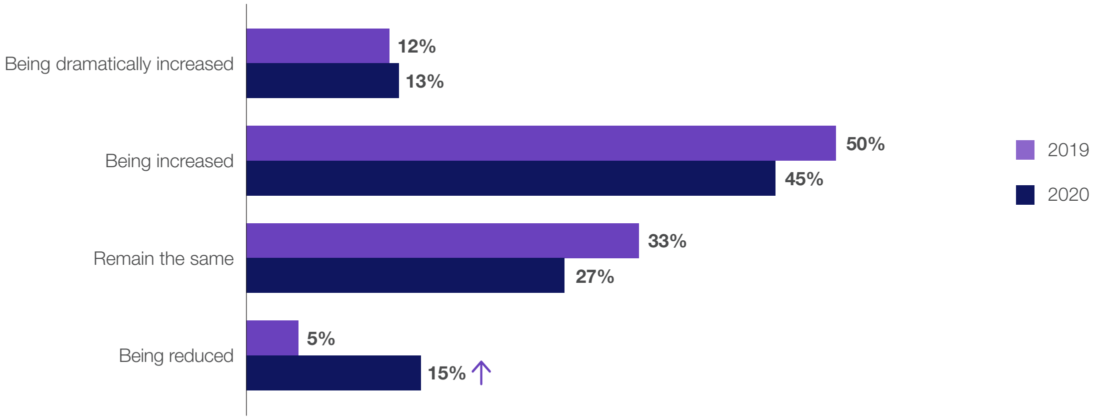


Figure 9: Security budget for 2020.

Insight: OT Leaders Still Struggle with Security Measurements and Analysis

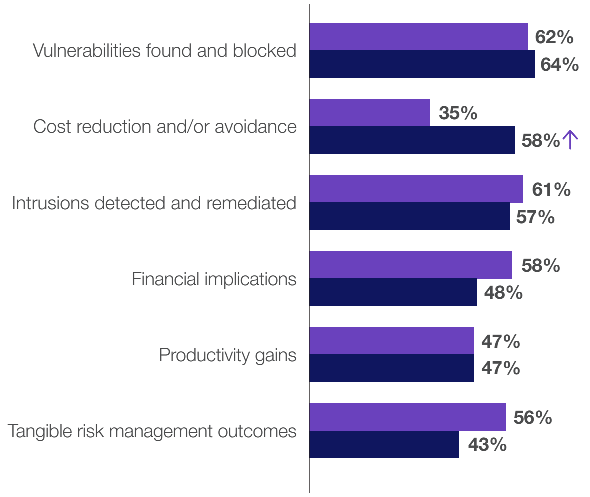
While some cybersecurity measurements are tracked and reported with some consistency, between 36% and 57% of organizations fail to measure each item on a list of standard metrics (Figure 10). Vulnerabilities (64%), intrusions (57%), and cost reduction resulting from cybersecurity efforts (58%) are tracked and reported most often, with tracking of cost reduction up 23% over last year. The least commonly reported metric is tangible risk management outcomes at 43%. This suggests that OT cybersecurity may not be fully integrated into enterprise-level considerations of risk.

Similarly, between 39% and 50% of organizations do not routinely share basic cybersecurity data with senior or executive leadership (Figure 11). Security compromises and compliance with security standards are shared the most often at 61% and 57%, respectively. This year saw a significant drop in reporting the results of penetration and intrusion tests, down 22% to 52%.

> "We need to have a solution that also covers remote employees and protects all company assets across the globe the same way."
> *– Survey Respondent, VP or Director of Plant Operations, Manufacturing*

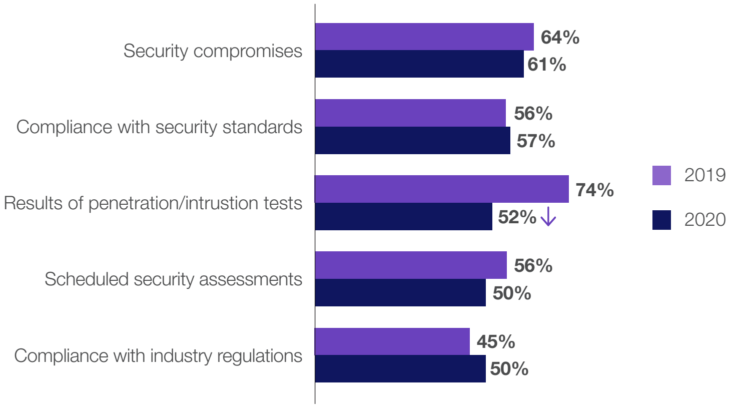
When asked which features in security solutions are most important to them, security analysis, monitoring, and assessment tools were most commonly cited, with 58% ranking this in the top 3 (Figure 12). This suggests that OT leaders see the need for a more strategic, data-driven approach to security. Interestingly, only 38% of respondents identified attack detection as one of the three most important features, down from 61% in 2019.

OT leaders continue to perceive that cybersecurity tools impede their work—and thus negatively impact their professional success. Respondents asserted that security solutions impede operational flexibility (53%) and create more complexity (50%; Figure 13).



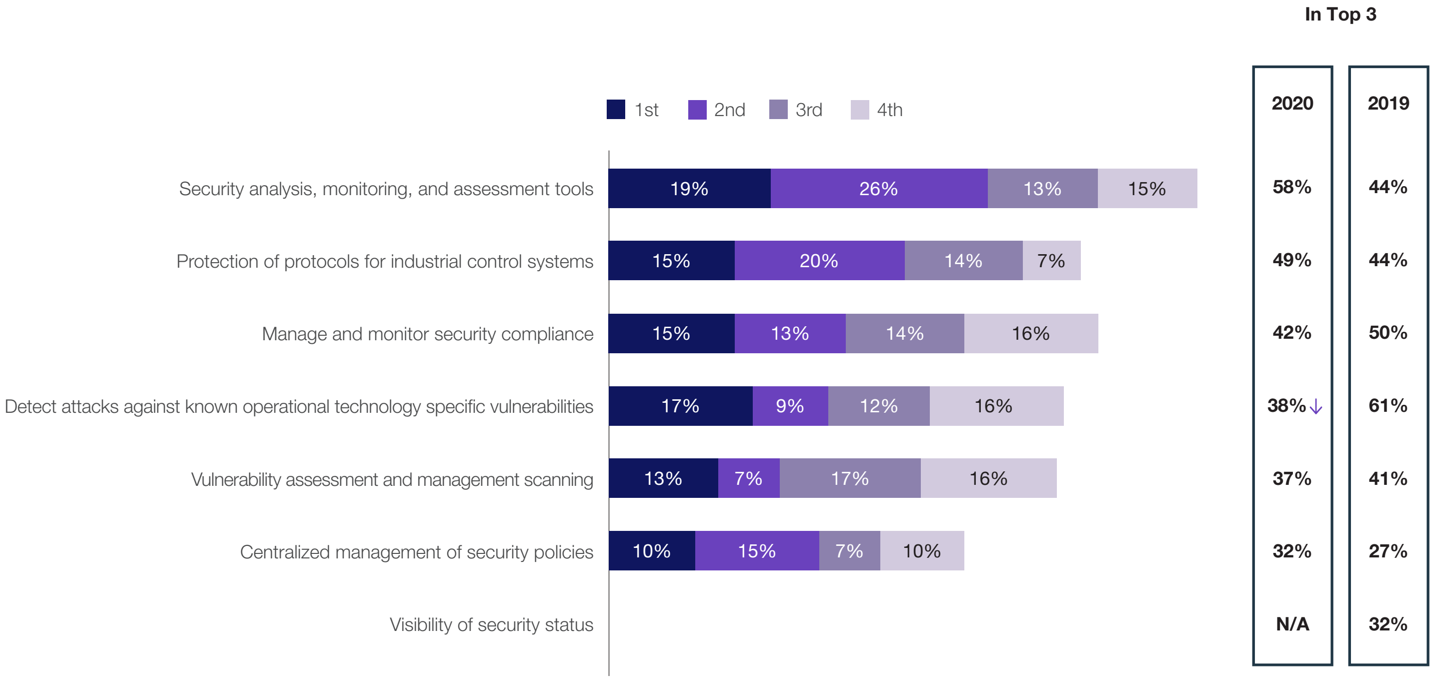
↑↓ Indicates significant difference from previous year at 95% CL

Figure 10: Types of cybersecurity measurements tracked and reported.



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

Figure 11: Types of OT cybersecurity issues reported.



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

Figure 12: Most important security solutions features (ranking).

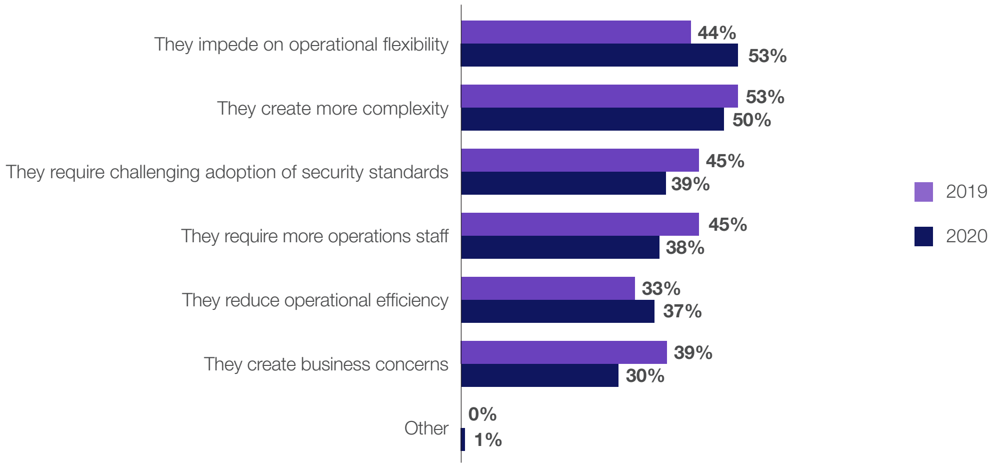


Figure 13: How cybersecurity solutions can negatively impact OT professionals' success (in top 3).

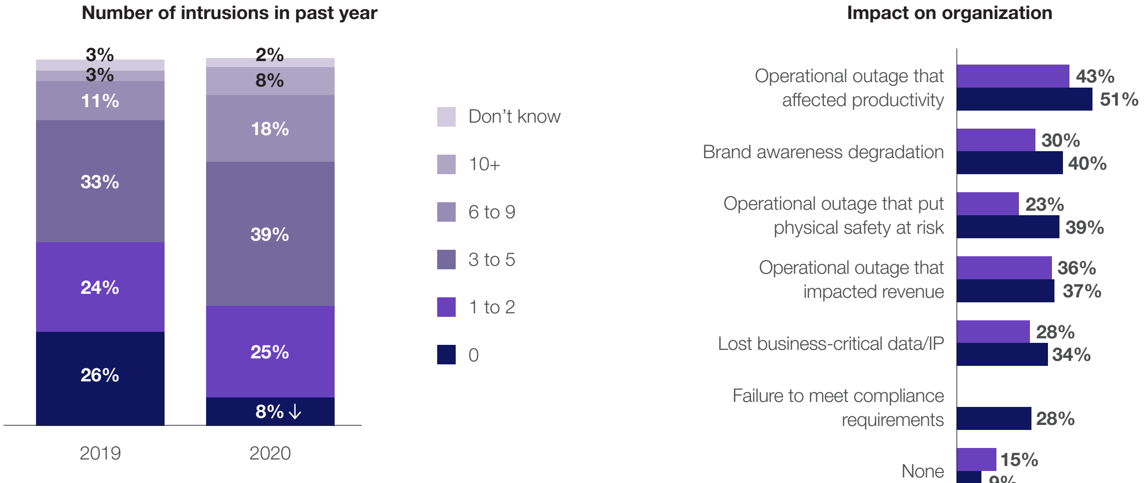
Insight: Most OT Leaders See Significant Intrusions, and These Have a Growing Impact

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, with 72% experiencing three or more and 26% experiencing six or more (Figure 14). Only 8% of organizations had no intrusions over 12 months. This figure compares with 26% of respondents who reported no intrusions in 2019, suggesting that the problem may be growing at some organizations.

The impact of these intrusions was not trivial. More than half of respondents reported an intrusion that affected productivity, while 37% saw operational outages impacting revenue. Nearly four in 10 (39%) reported that an intrusion put physical safety at risk—up from 16% last year. The latter is a real concern given the dangers inherent in industrial facilities.

> "Resources to deal with the attacks are becoming more challenging. Budgets need to expand to accommodate these newer, more sophisticated attacks."
> *–Survey Respondent, VP or Director of Plant Operations, Manufacturing*

Although the most common intrusions were malware (60%), phishing (43%), and hackers (39%), only hackers saw a significant increase in organizations affected over last year (Figure15). Ransomware and distributed denial-of-service (DDoS) attacks, as well as insider breaches (both unintentional and bad actor), also saw increases in the number of intrusions over last year.



↑ ↓ *Indicates significant difference from previous year at 95% CL*

Figure 14: Number of intrusions and the impact on organizations.

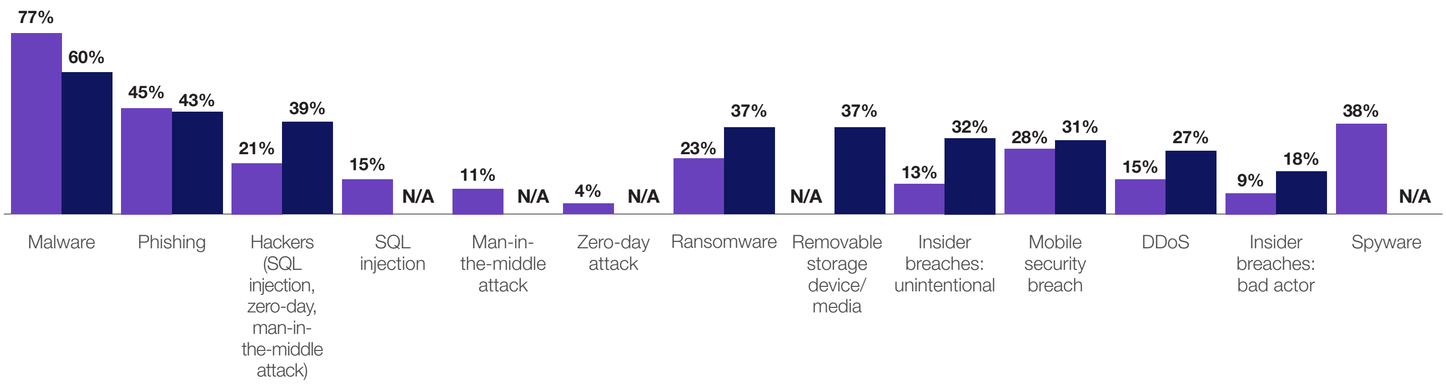


Figure 15: Types of intrusions experienced.

Best Practices of Top-tier Organizations

As discussed, only 8% of OT leaders reported no intrusions in the past year, while another 8% 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 *four times as likely* to have all their OT activities centrally visible to the security operations team.

Centralized visibility is critical for effective security protection across the enterprise, and OT systems are no exception. All top-tier respondents have achieved visibility for at least half of their OT activities, and half have achieved full visibility.

2. Top-tier OT leaders are *133% more likely* to track and report on vulnerabilities found and blocked.

Nearly half of data breaches were traced to software vulnerabilities this past year, compared with just 26% the year before.[3] Nearly all top-tier respondents track and report on vulnerabilities, but less than half of bottom-tier respondents adhere to this best practice.

3. Top-tier organizations are twice as likely to have the CISO or CSO currently responsible for OT security.

As OT becomes more connected, it is more important that the security of OT systems is a part of the larger cybersecurity infrastructure. Top-tier organizations are ahead of the curve on this. Fortunately, the majority of both top-tier and bottom-tier organizations plan to follow this best practice in the coming year if they are not already.

4. Top-tier OT leaders are 25% more likely to have direct responsibility for embedding security into OT processes.

When security is a part of the foundation of OT technology when it is deployed—rather than added on as an afterthought—it is more likely to be effective. More than half of top-tier OT leaders have direct responsibility for ensuring this best practice.

5. Top-tier organizations are 25% more likely to have a network operations center (NOC).

Centralized visibility and monitoring of network activity across IT and OT environments helps ensure both performance and security for business-critical OT systems, and top-tier organizations are more likely to have achieved this.

6. Top-tier OT leaders are 25% more likely to be measured by response time to security vulnerabilities.

As the old adage goes, what gets measured gets improved. More than half of top-tier respondents ranked response time to security vulnerabilities as either a first or second priority, while twice as many of the respondents who are not in the top-tier ranked it third, fourth, or fifth.

7.Top-tier OT leaders are 25% more likely to report on compliance with industry regulations to executive leadership.

Compliance is increasingly a concern for an organization's top leaders, but if the reports must be prepared manually, they likely get updates no more frequently than the auditors. Top-tier organizations are more likely to do these regular reports, suggesting that they have automated compliance reporting across the enterprise. This enables more of a real-time approach to reporting and better opportunities to improve.

Conclusion

While some organizations are managing the cybersecurity of their OT systems with considerable success, many more are struggling. This is clearly illustrated in the 19% decline in the percentage of organizations with no intrusions in their OT systems compared with last year.

The nature of the challenge is unique at each organization. Some are challenged by staffing—either a lack of people or inadequately trained team members. Some are challenged by inadequate tools to handle threats and vulnerabilities. Some are challenged by the cost of providing these things. Many are challenged by the frequency and number of threats and by the time required to maintain adequate security to manage them. All but a few had at least one intrusion in the past year, with many having more than one.

Those following the specific best practices identified in this report tended to see significantly fewer intrusions. These recommendations are not earth-shattering. Rather, they consist of many of the basic practices of security hygiene—taking a proactive approach to security, working toward centralized visibility and control, and tracking and reporting basic cybersecurity metrics. As OT systems lose their air gaps and become integrated with IT systems and with the internet, OT leaders will need to reinforce security awareness on their teams and bolster their systems with adequate security protection.

> "Zero-day attacks can hurt us tremendously, even when we have security measures in place. We have to always ensure we back up our data in real-time, so we never have to lose time and money."
> *–Survey Respondent, Head of Manufacturing/Plant Operations, Energy/Utilities*

[1] "Global Operational Technology Market—Industry Trends and Forecast to 2024," Data Bridge Market Research, October 2017.

[2] "State of Operational Technology and Cybersecurity Report," Fortinet, March 15, 2019.

[3] "2020 Data Breach Investigations Report," Verizon, May 2020.

FORTINET

www.fortinet.com

June 30, 2020 1:10 PM

report-2020-ot-cybersecurity

710343-0-0-EN