FORTINET

REPORT

State of Operational Technology and Cybersecurity Report

Table of Contents

Executive Summary

Operational technology (OT) is vital to public safety and economic well-being, controlling the equipment that runs the world's manufacturing plants, power grids, water utilities, shipping lines, and more.

The rise of OT began in the early decades of the 20th century as electrically powered machines and controls replaced steam-powered and muscle-powered equipment. OT predates the rise of information technology (IT) by many decades, and traditionally, OT and IT networks have been separated by an air gap. Recently, however, IT-based technologies such as sensors, machine learning (ML), and big data are being integrated with OT networks to create new efficiencies and competitive advantages. This increases the digital attack surface and the risk of intrusion.

To explore the state of cybersecurity in OT environments, Fortinet surveyed plant operations and manufacturing leaders (plant operations leaders) at large manufacturing, energy and utilities, healthcare, and transportation organizations. The survey revealed insights that include:

1. **The impact of cyberattacks on OT environments is broad and deep.** About 74% of OT organizations have experienced a malware intrusion in the past 12 months, causing damages to productivity, revenue, brand trust, intellectual property, and physical safety.

2. **A lack of cybersecurity contributes to risk.** 78% have only partial centralized visibility on the cybersecurity of their OT environments. 65% lack role-based access control, and more than half do not use multi-factor authentication or internal network segmentation.

3. **Improving the OT security posture is constrained by the need to keep up with rapid change and a lack of staff resources.** Nearly two-thirds (64%) of OT leaders say that keeping pace with change is their biggest challenge, and almost half (45%) are limited by a shortage of skilled labor.

4. **A focus on cybersecurity is increasing in OT organizations.** 70% plan to roll OT cybersecurity under the CISO in the next year (only 9% of CISOs oversee OT security currently), and 62% of cybersecurity budgets are being increased.

This report reviews survey results, including:

- Challenges that plant operations leaders perceive in securing their OT environments
- The type and impact of intrusions they are experiencing
- How they manage cybersecurity
- What security gaps they face
- How they measure their success

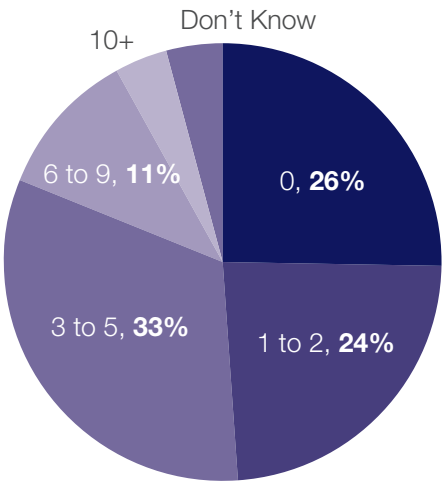
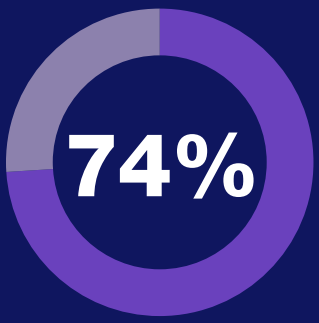
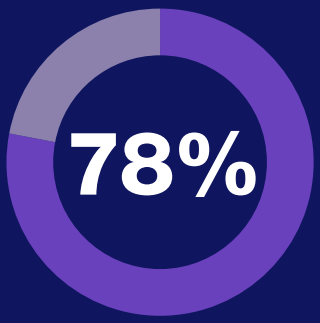


Figure 1. Number of Intrusions in Past 12 Months

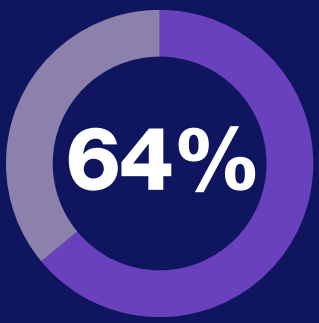
Infographic: Key OT Cybersecurity Findings



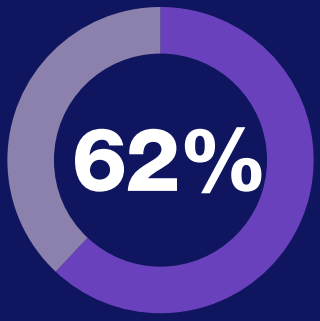
of OT organizations surveyed were breached in the past 12 months, resulting in data loss, operational disruptions or outages, and/or brand degradation.



have limited centralized cybersecurity visibility.



struggle to keep up with change.



are increasing their cybersecurity budgets.

Breaches damaged

- Productivity (43%)
- Revenue (36%)
- Brand Reputation (30%)
- Business-Critical Data (28%)
- Safety at Risk (23%)

70% plan to **roll cybersecurity under the CISO** in the next year.

However, only 9% of CISOs currently oversee OT cybersecurity.

Compared with bottom-tier OT organizations (6+ intrusions in 12 months) top-tier OT security organizations (zero intrusions in 12 months) are:

100% more likely to use multi-factor authentication

94% more likely to use role-based access control

68% more likely to manage and monitor security events and perform event analysis

51% more likely to use network segmentation

46% more likely to schedule security compliance reviews

Methodology for This Study

The State of Operational Technology and Cybersecurity Report is based on a January 2019 survey of individuals who:

- Work at companies with more than 2,500 employees in the manufacturing, energy and utilities, healthcare, and transportation industries
- Have OT as their primary responsibility
- Have reporting responsibility for operations
- Are involved in cybersecurity purchase decisions

OT Operations Cybersecurity Insights

Insight: The Impact of OT Cyberattacks Is Broad and Heavy

Almost three-quarters (74%) of OT organizations experienced at least one malware intrusion in the past year, and half (50%) experienced 3 to 10 or more intrusions.

As Figure 2 shows, malware is the leading form of intrusion, followed by phishing (45%), spyware (38%), and mobile security breaches (28%).

The impact of breaches on OT organizations has been heavy, as shown in Figure 3.

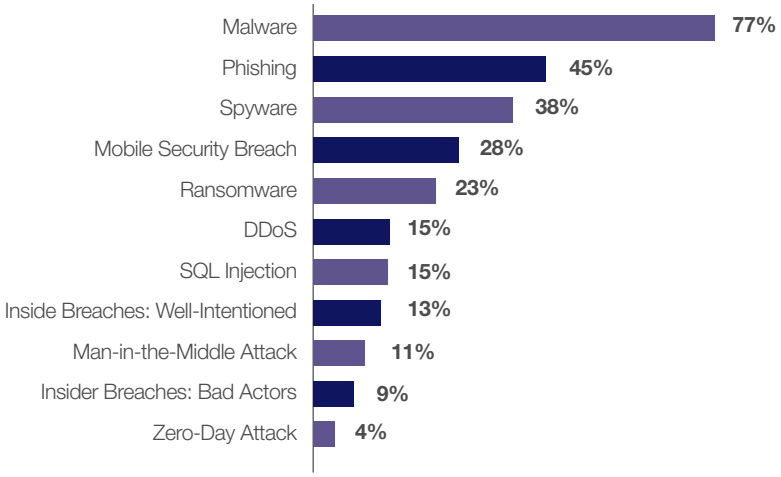


Figure 2. Type of OT Intrusion Experienced

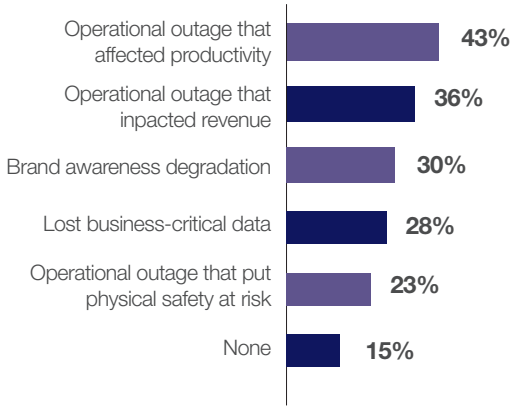


Figure 3. Impact of Breaches in OT Organizations

Insight: Lack of Cybersecurity Visibility Contributes to Risk

78% of organizations have only partial centralized cybersecurity visibility on OT operations, as shown in Figure 4.

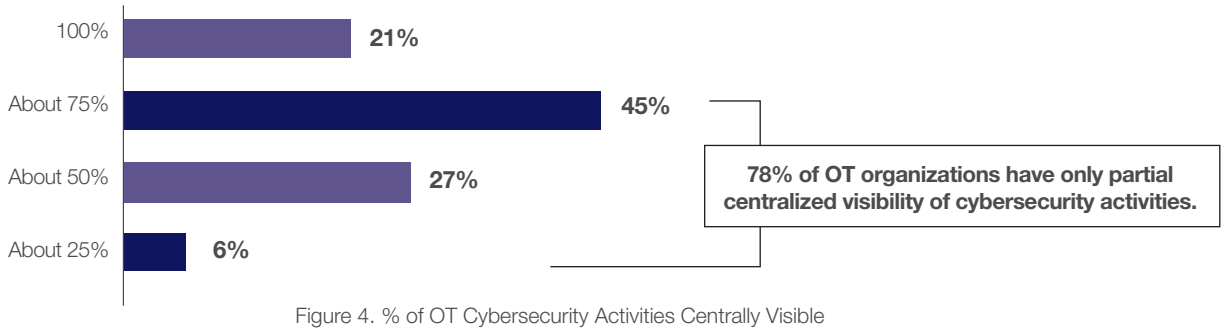


Figure 4. % of OT Cybersecurity Activities Centrally Visible

Insight: A Shortage of Skilled Labor Is a Major Inhibitor to Improving Cybersecurity

Nearly two-thirds of plant operations leaders (64%) say that keeping pace with change is their biggest challenge, followed by a broad set of additional challenges such as:

- Union relations (45%)
- Shortage of skilled labor (45%)
- Regulatory changes (44%)
- Availability and access to training (42%)
- Budgetary constraints (42%)

Further, a lack of skilled labor is a factor in the four biggest concerns plant operations leaders have about adding cybersecurity solutions:

- Create more complexity (53%)
- Require challenging adoption of security standards (45%)
- Require more operations staff (45%)
- Impede operational flexibility (44%)

However, despite a shortage of staff resources, OT organizations are determined to improve their security posture, according to additional data. Figure 5 shows the top concepts offered by plant operations leaders when asked what challenges are driving them to enhance cybersecurity.

Figure 5. Leading Challenges Driving Enhanced Cybersecurity

The question behind Figure 5 was “What are the top three challenges causing you to enhance or change your cybersecurity posture?” The more frequently a concept appeared in answers, the larger it appears above.

The most frequent security challenges that plant operations leaders expressed in Figure 5 are the ability to thwart hackers, safeguard a growing attack surface caused by digital transformation, maintain data security, and keep environments safe, productive, cost-efficient, and compliant—all while dealing with a skills shortage.

Insight: A Focus on Cybersecurity Is Increasing in OT Organizations

70% of surveyed organizations plan to roll OT cybersecurity under the CISO in the next year. Interestingly, only 9% of CISOs currently oversee OT cybersecurity. At present, the OT director/manager of Cybersecurity is responsible for cybersecurity in 50% of organizations, with another 24% indicating cybersecurity is under the charge of the VP/director of Networking Engineering and Operations.

Cybersecurity prioritization is evident in more than organizational restructuring of responsibilities. **62% of organizations say their cybersecurity budgets are increasing dramatically** this year, while 38% are maintaining their current cybersecurity budgets. OT organizations are making security risk a critical focus: 94% of survey respondents indicate they make OT security posture a significant or moderate factor in the broader risk score that the CISO shares with executive leadership and the board of directors.

Insight: OT Environments Are Complex to Protect

The OT environments that respondents are working to safeguard are complex. They consist of a widespread number of OT devices, from fewer than 50 to more than 500, as shown in Figure 6.

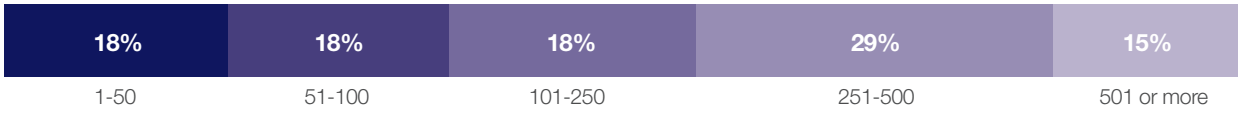


Figure 6. Number of OT Devices in Operation

Most organizations get their devices from 2 to 4 vendors, as shown in Figure 7.

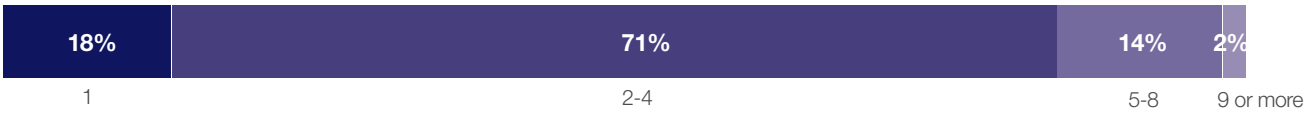


Figure 7. Number of Vendors Used for OT Devices

The most-used OT vendors in this survey are Honeywell, Siemens, and Emerson, as shown in Figure 8.

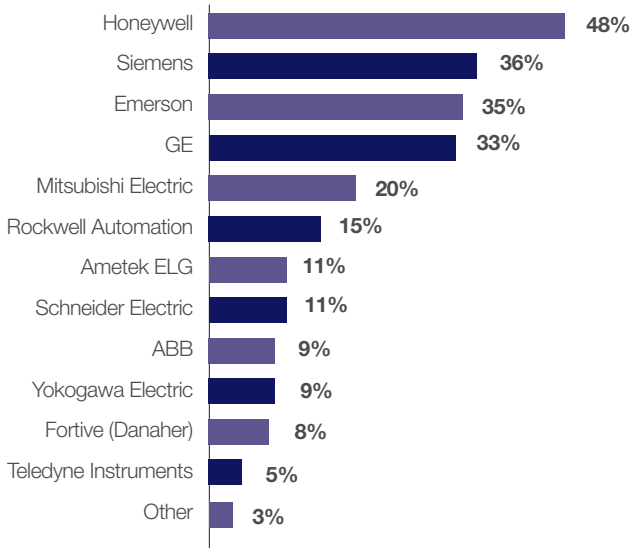


Figure 8. Vendors Used for OT Devices

Insight: Plant Operations Leaders Are Influential in Improving Cybersecurity

As OT organizations strengthen the cybersecurity of their environments, plant operations leaders are actively involved in the choices being made. More than three-fourths (76%) report they are regularly included in cybersecurity decisions, and nearly half (45%) have final say in OT decisions. Almost all are regularly (56%) or occasionally (39%) involved in the development of their organization's IT cybersecurity strategy.

It is interesting to note that a secure and stable environment is essential to the top three success metrics by which plant operations leaders are judged: maximizing productivity (55%), minimizing cost (53%), and reducing security vulnerabilities response time (44%).

It may be surprising that "reducing security vulnerabilities response time" is the third most important success metric. But imagine how quickly a cyberattack can disrupt a facility such as a factory, utility, or railroad, damaging productivity, revenue, and safety. A stable and resilient environment is also critical to plant operations leaders' top three direct job responsibilities: managing production efficiency (77%), supervising the operations team (77%), and managing quality control and manufacturing processes (76%).

> ***"The threat of a cyberattack is weighing us down, and we are investing in how to prevent it."***
>
> – Manager of Plant Operations, Manufacturer

Given their focus on stability and resilience, it is more obvious why 76% of plant operations leaders are actively involved in OT cybersecurity decisions. This task will take more time because OT cybersecurity spending is projected to rise 50% to $18.05 billion in 2023, up from $12.22 billion in 2017.[1]

There are a number of cybersecurity deficiencies that OT teams need to address, as the next section identifies.

Insight: OT Security Gaps Exist in Access Control, Authentication, Segmentation, and More

Figure 9 shows the percentage of responding OT organizations that do not have the key cybersecurity capabilities listed.

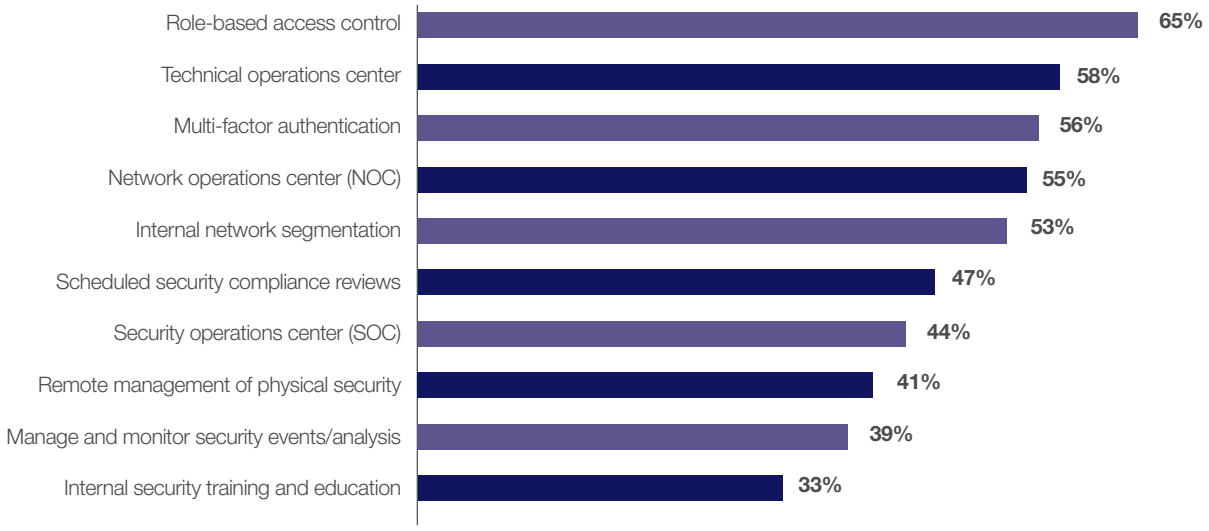


Figure 9. Percentage of OT Organizations That Lack Key Cybersecurity and Security Measures

The missing capabilities in Figure 9 cause a number of security gaps:

- **About two-thirds** (65%) of OT companies surveyed lack role-based access control, giving attackers more freedom to move within their OT environments.
- **Almost 6 in 10** (56%) OT organizations lack multi-factor authentication. A recent Verizon report finds that 81% of breaches began with lost or stolen credentials.[2] Many breaches into OT environments depend on spear phishing to obtain stolen credentials. (An estimated two dozen U.S. energy grid companies were breached using spear phishing and stolen credentials within the past two years per the *Wall Street Journal*, and attackers left malware in their OT environments that could be used for future sabotage.[3]) Multi-factor authentication makes the successful use of stolen credentials more difficult.
- **More than half** of organizations (53%) lack internal network segmentation. The National Institute of Standards and Technology (NIST) Cybersecurity Guidelines have called segmentation "one of the most effective architectural concepts that an organization can implement" to protect its OT environment.[4] Industry experts point out that many recent OT malware attacks could have been thwarted by segmentation, as it limits freedom of movement from one OT production network to another, and even within an OT production network.[5]
- **Almost half** (44%) do not have a security operations center (SOC) and more than half (55%) lack a network operations center (NOC), leading to reduced visibility and heightened risk. A SOC can more quickly detect, thwart, or minimize a breach. A NOC maximizes network throughput and availability. The SOC and NOC can be integrated to enhance results for both.[6]
- **Almost 4 in 10 organizations** (39%) do not manage, monitor, or analyze security events, making breaches difficult to discover. With most organizations now recognizing the inevitability of a successful intrusion, cyber resiliency—or incident response and event management—is critical in minimizing the impact of a breach.[7]
- Basic security practices remain a challenge for a significant number of organizations, with **one-third** (33%) admitting they do not have internal security training awareness programs and education. With insider threats comprising 30% of all breaches, this is a requisite for any organization—IT or OT.[8]

Best Practices of Top-Tier OT Security Organizations

26% of our respondents (the "top-tier" organizations) report **zero intrusions** within the past 12 months. On the other hand, 17% of our respondents (the "bottom-tier" organizations) had **six or more intrusions** in the past 12 months, and some did not even know how many intrusions they had. It is interesting to note the disparities between these two groups. They include:

1. **Top-tier organizations are 100% more likely than bottom-tier organizations to use multi-factor authentication,** making access with stolen credentials more difficult.

2. **Top-tier organizations are 94% more likely than bottom-tier organizations to use role-based access control,** restricting a potential attacker's movement.

3. **Top-tier organizations are 68% more likely than bottom-tier organizations to manage and monitor security events and perform event analysis,** reducing risk from a breach by minimizing the time to detection.

4. **Top-tier organizations are 51% more likely than bottom-tier organizations to use network segmentation** to restrict a potential attacker's movement.

5. **Top-tier organizations are 46% more likely than bottom-tier organizations to schedule security compliance reviews** to strengthen security posture.

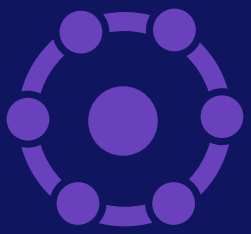
Conclusion: Cybersecurity is a Growing Requirement for OT Success

Risk is high in OT environments: Almost 8 out of 10 have been breached in the past year, with half reporting 3 to 10 or more breaches. Breach damages have been reported that affect productivity, revenue, brand trust, intellectual property, and physical safety. This study identifies factors that must be addressed to reduce risk, such as the fact that 78% of organizations lack complete, centralized cybersecurity visibility, 56% do not have multi-factor authentication, and 53% do not yet use internal network segmentation, a highly recommended OT best practice.[9]

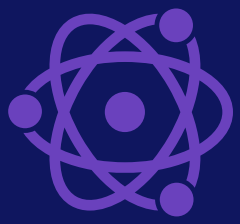
OT plant operations leaders indicate they are active and influential in evaluating cybersecurity solutions. They seek solutions that support their top goals of maximizing productivity while minimizing cost.

To address a lack of centralized visibility and a shortage of staff, OT organizations should heed the following recommendations:

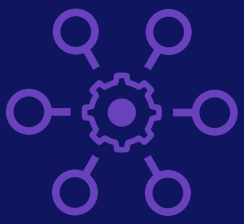
> ***"Security solutions need to act smarter and be more effective, often in the face of reduced budgets."***
>
> – VP of Manufacturing, Major Manufacturer



Seek security solutions that work together to provide broad visibility of the entire digital attack surface, spanning OT and IT environments.



Look for a security fabric-based approach that provides integrated protection across all devices, networks, and applications.



Search for automated security capabilities, with solutions that coordinate a response and use technologies such as machine learning.

Minimize risk with OT cybersecurity best practices such as network segmentation, multi-factor authentication, and role-based access control.

These cybersecurity approaches will improve an organization's security posture while helping to compensate for a shortage of skilled labor.

Reference List

[1] Industrial Control Systems (ICS) Security Market worth $18.05 billion by 2023," MarketsandMarkets, accessed February 25, 2018.

[2] 2017 Data Breach Investigations Report, Verizon, accessed November 30, 2018.

[3] Rebecca Smith and Rob Barry, "America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It," The Wall Street Journal, January 10, 2019.

[4] Keith Stouffer, et al., "Guide to Industrial Control Systems (ICS) Security," NIST, May 2015.

[5] Peter Newton, "Securing IIoT requires extra care. NAC and segmentation can help," TechTarget, September 28, 2018.

[6] "Bridging the NOC-SOC Divide," Fortinet, accessed March 5, 2019.

[7] Patrick Spencer, "Cyber Resilience Rises to the Forefront in 2019, According to New Scalar Security Study," Scalar Security Blog, February 20, 2019.

[8] "2018 Data Breach Investigations Report," Verizon, March 2018.

[9] Keith Stouffer, et al., "Guide to Industrial Control Systems (ICS) Security," NIST, May 2015.

FORTINET

www.fortinet.com

March 15, 2019 1:09 PM

report-state-of-operational-technology.indd

330327-0-0-EN