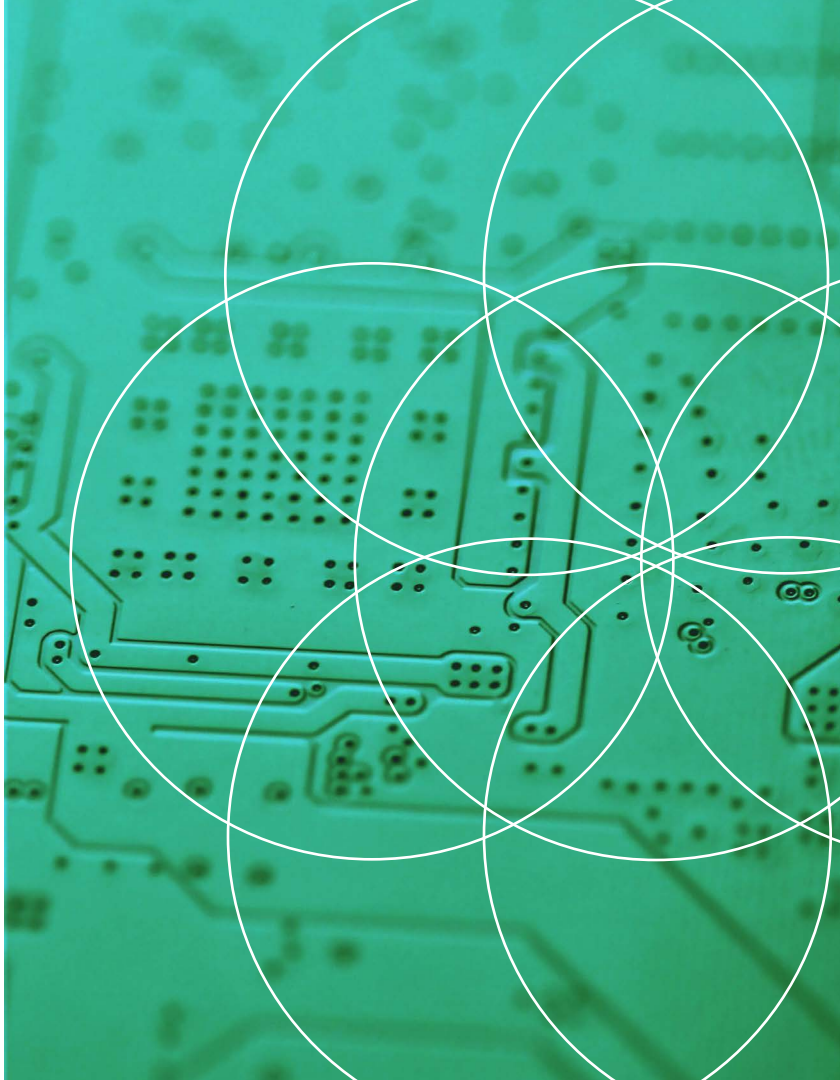
FORRESTER®

Apply Secure By Operations Principles To Safeguard Critical Infrastructure

Why Embedding More Robust Cybersecurity Practices Across Connected Operational Technology (OT) Is Vital

Get started →

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY SCHNEIDER ELECTRIC | JUNE 2025



Securing Connected OT Environments Requires Implementing Security Controls

For critical infrastructure operations teams, digital transformation has increased OT asset connectivity and, in turn, potential attack surfaces. As a result, teams can no longer rely solely on the security capabilities built into OT assets by technology providers during product development or on the implementation standards used by systems integrators during deployment (commonly known as “Secure by Design” principles). To block threat actors, “Secure by Operations” — a practice defined in this paper — maintains a cybersecurity posture across the OT asset lifecycle via secure implementation, configuration, and management, with clear roles for technology providers, integrators, and asset owners.

Schneider Electric commissioned Forrester Consulting to conduct a survey with 262 OT security decision-makers in critical infrastructure to explore how their organizations are securing their OT environments today.

Key Findings

Despite current measures, OT cyberattacks are common. Nearly all (91%) of respondents’ organizations experienced a breach from an OT cyberattack in the last 18 months — harming reputation and delivery of critical services.

Securing OT environments is challenging. Organizations lack the capabilities and expertise needed to maintain a secure environment across all interconnected assets and systems.

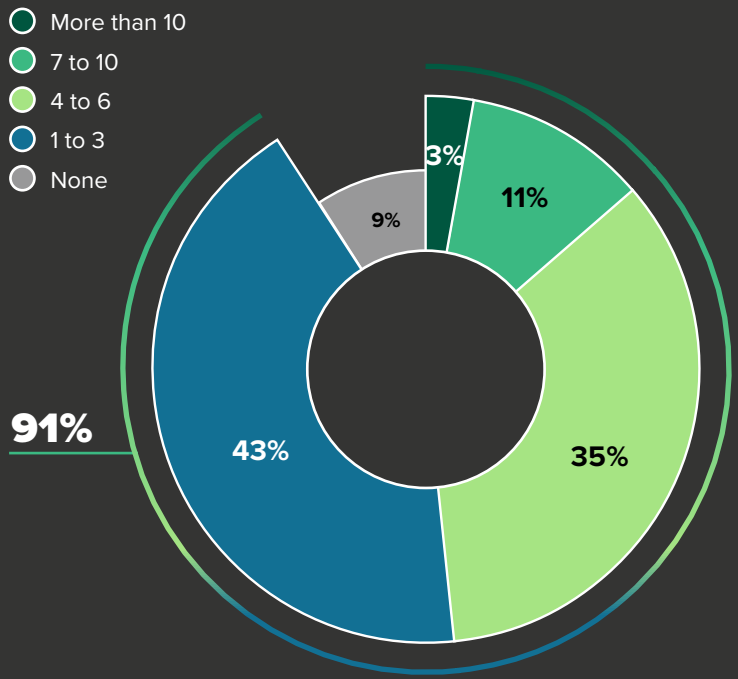
Secure by operations can improve OT security. Capabilities for continuous OT monitoring and patching, along with tapping into the right expertise for execution/oversight, can improve security postures.

Despite Security Practices In Place, OT Cyberattacks Are A Common Occurrence

Even though technology providers are adopting Secure by Design concepts (e.g., building security requirements into products, conducting regular prerelease security testing, and creating secure deployment guidelines), cyberattacks continue to wreak havoc on critical infrastructure organizations.

In fact, 91% of survey respondents reported that their organization experienced at least one breach or failure from a cyberattack impacting its OT systems over the last 18 months. While Secure by Design practices focus on incorporating security protections into OT assets and systems during product design, they do not protect the operational environments that connect the many different types of OT assets and systems being used at any one organization. This gap could allow bad actors to gain access to specific OT assets and systems within the compromised environment.

Frequency Of OT Cyberattacks Resulting In Breaches/Failures Within The Last 18 Months



Base: 262 OT cybersecurity decision-makers in critical infrastructure
Note: Percentages do not total 100 due to rounding.
Source: Forrester's Q2 2025 Critical Infrastructure OT Cybersecurity Survey [E-62864]

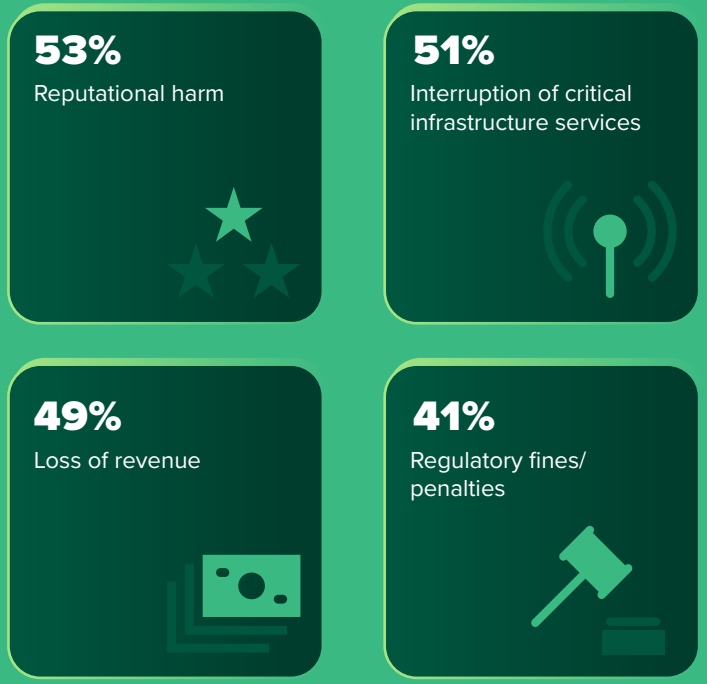
Critical Infrastructure Assets And Systems Are A Lucrative Target

Unfortunately, OT breaches and failures resulting from cyberattacks have significant negative consequences not only for the organization experiencing the attack, but also for the end users of critical infrastructure services and products.

Fifty-three percent of decision-makers at organizations that have experienced an OT breach/failure faced reputational harm, 51% saw an interruption of critical infrastructure services, 49% lost revenue, and 41% were subjected to regulatory fines and penalties. These consequences warrant additional actions by security leaders to reduce the number of breaches and failures experienced from OT cyberattacks — and minimize the impact to their business.

Impact Of OT Breaches/Failures Resulting From Cyberattacks

(Showing “Moderate negative impact” and “Significant negative impact”)



Base: 239 OT cybersecurity decision-makers in critical infrastructure who have experienced an OT cyberattack over the last 18 months
Note: Showing top four responses
Source: Forrester’s Q2 2025 Critical Infrastructure OT Cybersecurity Survey [E-62864]

However, OT Environments In Critical Infrastructure Remain Vulnerable

The majority of respondents in our survey recognize that more actions are needed to mitigate the consequences that OT cyberattacks can have on their organizations. More than 60% of OT leaders were concerned not only with their ability to protect their OT environments but also with their basic ability to detect compromised OT assets.

Furthermore, nearly three-quarters (71%) of respondents felt that their organization's current OT cybersecurity practices left their network of connected systems vulnerable to cybercriminals. To make matters worse, nearly two-thirds (64%) indicated that their organization lacked full visibility into all of its OT assets and systems.

Level Of Concern For The Lack Of Ability To Protect Against And Detect OT Cyberattacks

(Showing "Concerned" and "Very concerned")

68%

Protect:
Safeguards to manage cybersecurity risks are used

61%

Detect:
Possible cybersecurity attacks and compromises are found and analyzed

Current State Of OT Security

(Showing "Agree" and "Strongly Agree")

My organization's OT assets are a vulnerable entrance point for cyberattacks targeting its broader network of connected systems.

71%

My organization lacks full visibility into its network of connected OT assets and systems.

64%

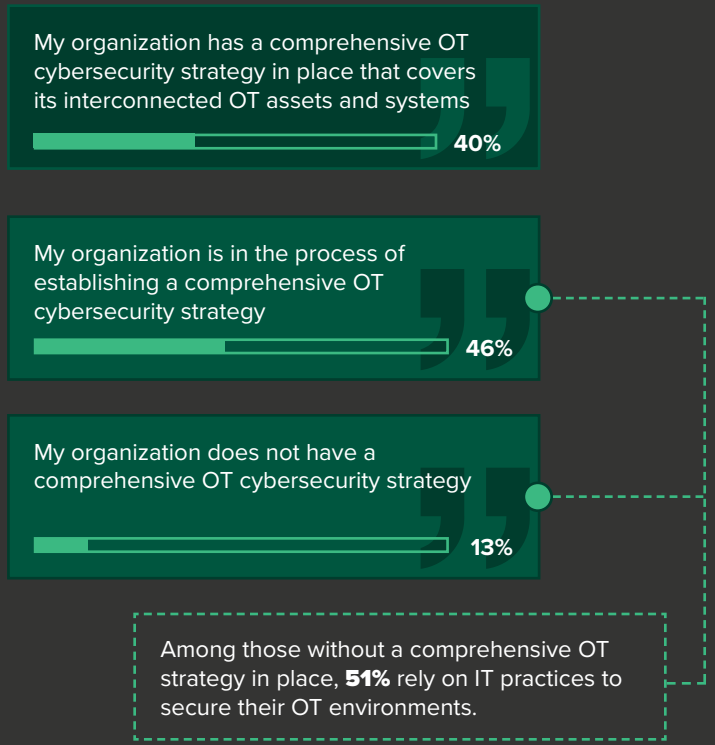
Base: 262 OT cybersecurity decision-makers in critical infrastructure
Note: Options are in order of NIST 2.0 Framework
Source: Forrester's Q2 2025 Critical Infrastructure OT Cybersecurity Survey [E-62864]

Most Cybersecurity Strategies Fail To Protect Operational Environments

Just 40% of respondents said that their organization had an OT cybersecurity strategy that secures all interconnected assets and systems. Among those without such a strategy, 51% said that their organization relied on IT practices to secure OT environments. But IT lacks a full understanding of how to secure OT assets/systems without affecting equipment performance or daily operations.[1]

Without a cybersecurity strategy that fully covers their OT environments, organizations remain at risk. For example, a misconfigured infrastructure control system can provide an entrance point for cybercriminals targeting connected assets. Recently, a nation-state attack on an Ireland water plant's pressure pump controller with an unsecured internet connection led to a deliberate shutdown and downstream water outages.[2]

Current OT Cybersecurity Strategies In Place Today



Base: 262 OT cybersecurity decision-makers in critical infrastructure
Source: Forrester's Q2 2025 Critical Infrastructure OT Cybersecurity Survey [E-62864]

Important OT Cybersecurity Capabilities Are Elusive For Many Organizations

Operations teams managing critical infrastructure are missing important OT cybersecurity capabilities needed to protect against and detect cyberattacks. Less than half of respondents indicated that their organization could monitor OT assets and systems 24/7 for cyberthreats, ensure the availability of security controls, conduct network segmentation, or restrict access to its OT systems for most or all of its assets. And just half indicated that their organization could manage security controls throughout the lifecycles of most or all of their assets and systems (e.g., deploying patches after asset/system commissioning).

The inability to deploy these OT cybersecurity capabilities across all assets and systems opens up organizations to significant operational fragility that can prevent threat vulnerability detection, lead to unnecessary risk exposure, and undermine operational resilience.

OT Cybersecurity Capabilities In Place Today

Base: 262 OT cybersecurity decision-makers in critical infrastructure
Note: Showing select responses; not showing "don't know"
Source: Forrester's Q2 2025 Critical Infrastructure OT Cybersecurity Survey [E-62864]

Organizations Need More Resources And Expertise To Improve OT Security

Not only do many operations teams lack the strategy and solution capabilities needed to protect their OT environments, but many also lack the expertise and staffing resources to implement and maintain a robust OT security posture. While this talent gap is well known in the cybersecurity industry, it is even more acute in the OT field.

To address these challenges, respondents indicated that the most important actions their organizations are taking to improve their cybersecurity postures are hiring and training dedicated internal OT cybersecurity resources and leveraging managed security service providers (MSSPs). MSSPs can help organizations augment their current security practices by providing solution capabilities, staffing, and expertise needed for securing/monitoring OT environments, maintaining compliance, and managing response and recovery services.[3]

Actions Organizations Are Taking/Planning To Take To Improve OT Cybersecurity Posture

Base: 262 OT cybersecurity decision-makers in critical infrastructure
Source: Forrester's Q2 2025 Critical Infrastructure OT Cybersecurity Survey [E-62864]

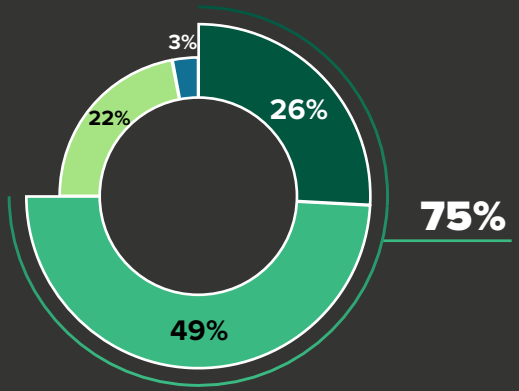
Implementing Secure By Operations Principles Can Help Improve OT Security

Critical infrastructure operations teams have a major need to improve their OT security postures. Most lack a cybersecurity strategy that accounts for their full environment of connected assets and systems. They also lack critical capabilities to improve their OT security (e.g., asset monitoring, network segmentation, access management, patching), as well as the staffing and expertise to implement and oversee these capabilities.

Secure by Operations principles can help by providing a guide for maintaining a secure, multitechnology landscape after initial deployment, including performing continuous monitoring and patching and tapping into the proper resources and expertise to ensure that OT equipment is integrated and operated securely. Three quarters of respondents said that adopting Secure by Operations principles was important or critical for their organization's ability to mitigate future OT cyberattacks.

Importance Of Secure By Operations Strategies For Mitigating Future OT Cyberattacks

- Critical
- Important
- Nice to have
- Not important
- Not at all important



Secure by Operations is the practice of maintaining cybersecurity throughout the operational lifecycle of industrial systems — beyond secure product design — by ensuring secure implementation, configuration, and continuous management of the environment. It emphasizes a collective and defined responsibility model among technology providers, systems integrators, and asset owners to uphold security controls and operational resilience.

Base: 262 OT cybersecurity decision-makers in critical infrastructure
Source: Forrester's Q2 2025 Critical Infrastructure OT Cybersecurity Survey [E-62864]

Secure By Operations Principles Are Expected To Drive Broad Organizational Benefits

Operational security decision makers expect to realize significant operational, financial, and end-user benefits by following Secure by Operations principles like monitoring and patching in their OT environments. Most respondents indicated that their organizations would see improved recovery times, reduced capex from longer OT asset lifespans, and improved company reputation.

Expected benefits also go beyond traditional security-related improvements; nearly half of respondents expected their organizations to see improved employee experience, operational efficiency, and compliance as well as reduced risk of operational interruptions.

Expected Benefits From Implementation Of Secure By Operations Practices

Base: 262 OT cybersecurity decision-makers in critical infrastructure
Note: Showing top responses
Source: Forrester's Q2 2025 Critical Infrastructure OT Cybersecurity Survey [E-62864]

Conclusion

The critical infrastructure sector has a significant opportunity to improve OT security by adopting Secure by Operations principles on top of existing Secure by Design practices. Our research yielded two key actions to take:

- **Emphasize collaboration and action across OT stakeholders.** Technology providers, systems integrators, and asset owners/operators must work closely to prevent sophisticated cyberattacks. Security capabilities built into OT assets by tech providers are still important for keeping OT assets safe — as are systems integrators for secure implementation.
- **Immediately engage partners to implement and advance Secure by Operations practices.** Maintaining a secure OT environment is hard. Partners like MSSPs provide expertise, capabilities, and technology to manage security and continuous monitoring.

Endnotes

[1] Source: The Forrester Wave™: Operational Technology Security Solutions, Q2 2024, Forrester Research, Inc., June 11, 2024.

[2] Source: Alexander Martin, Two-day water outage in remote Irish region caused by pro-Iran hackers, *The Record*, December 11, 2023.

[3] Source: Planning Guide 2023 Security And Risk, Forrester Research, Inc., August 23, 2022.

Resources

Related Forrester Research:

Top Recommendations For Your Security Program, 2025, Forrester Research, Inc., March 6, 2025.

The Operational Technology Security Solutions Landscape, Q1 2024, Forrester Research, Inc., February 6, 2024.

The Forrester Wave™: Operational Technology Security Solutions, Q2 2024, Forrester Research, Inc., June 11, 2024.

The Top Trends In Operational Technology (OT) Security, Forrester Research, Inc., February 22, 2023.

Related Blogs/Webinars:

Brian Wrozek, Putting The New Joint Cyber Defense Collaborative Priorities Into Action, Forrester Blogs

April 16, 2025, Top Recommendations For Your Security Program, 2025, Webinar.

Project Team:

Ben Anderson,
Market Impact Consultant

Contributing Research:

Forrester's Technology And Security research group

Methodology

This Opportunity Snapshot was commissioned by Schneider Electric. To create this profile, Forrester Consulting conducted an online survey of 262 operational technology security decision-makers. The custom survey began and was completed in April 2025.

ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute their specific priorities using a unique engagement model that ensures lasting impact. For more information, visit forrester.com/consulting.

© Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. [E-62864]

Demographics

GEOGRAPHY	
North America	44%
EMEA	33%
APAC	11%
South America	11%

INDUSTRY	
Critical infrastructure asset operator	35%
Critical infrastructure asset owner	29%
Critical infrastructure systems integrator	14%
Critical infrastructure OEM/manufacturer	13%
Critical infrastructure government authority	8%

COMPANY SIZE	
500 to 999 employees	28%
1,000 to 4,999 employees	35%
5,000 to 19,999 employees	22%
20,000 or more employees	14%

JOB TITLE	
C-level	12%
Vice president	23%
Director	29%
Manager	36%

Note: Percentages may not total 100 due to rounding.

FORRESTER®