Overexposed and underprepared

The state of OT cybersecurity for energy and related industries



SIEMENS energy

Rapid digital innovation is reshaping industries around the world



Artificial intelligence advances mean new data centers hunger for electricity. Attackers apply the new power of generative AI to discovering and exploiting digital vulnerabilities. Energy companies have digitized operational technologies (OT) across new and legacy infrastructure, and now can leverage digital controls to optimize for emissions, efficiency, financial performance, and further automation.

Whether these changes will lay foundations for future prosperity or sow the seeds of future crisis is largely up to the public and private sector leaders charged with understanding and adapting to these new realities. Siemens Energy and the Ponemon Institute sought to survey critical industries that rely on digitized OT about the cyber threats they experience and the tools and techniques they deploy to make their organizations more resilient.

We found that these organizations – manufacturing, oil and gas, electricity, utilities, and petrochemical industries – see frequent, often sophisticated cyberattacks against OT systems. These industries share the difficult challenge of protecting productivity by staying ahead of attackers.

We believe that by building awareness, covering common blind spots, and sharing best practices, we can strengthen resilience within these industries. We can ensure that as innovation continues, we reap the benefits of increased productivity, and ward off the risks of increased threats.

Leo Simonovich
VP and Global Head
Industrial Cyber and Digital Security Systems
Siemens Energy

We believe that by building awareness, covering common blind spots, and sharing best practices, we can strengthen resilience within these industries.

About Ponemon Institute and Siemens Energy

Ponemon Institute

The Ponemon Institute conducts independent research on privacy, data protection and information security policy. Our goal is to enable organizations in both the private and public sectors to have a clearer understanding of the trends in practices, perceptions and potential threats that will affect the collection, management and safeguarding of personal and confidential information about individuals and organizations. Ponemon Institute research informs organizations on how to improve upon their data protection initiatives and enhance their brand and reputation as a trusted enterprise.



In addition to our research, Ponemon Institute provides strategic consulting to private and public sector organizations interested in establishing or enhancing their privacy, data protection, and security practices. To ensure that their goals are achieved, organizations engage us to assess their practices and conduct workshops and training programs.

Ponemon Institute is the parent organization of the Responsible Information Management (RIM) Council. The RIM Council draws its name from the practice of Responsible Information Management, an ethics-based framework and long-term strategy for managing personal and sensitive employee, customer and business information.

For more information go to:
https://www.ponemon.org/

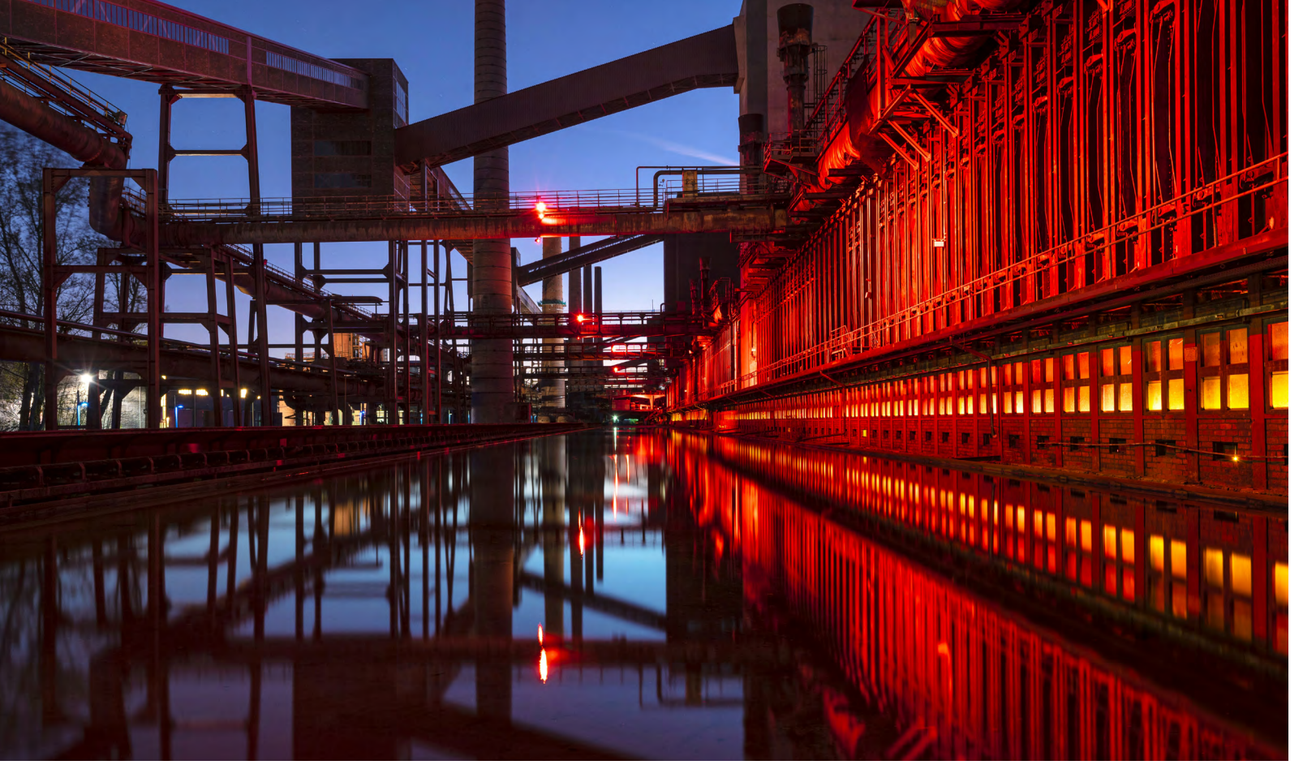


Siemens Energy

Siemens Energy is a global leader in energy technology and industrial cybersecurity. Established as a standalone entity in 2020, Siemens Energy combines over 150 years of expertise in power generation, transmission, and renewable energy technologies. The company operates across a diverse portfolio, including gas and steam turbines, wind power, grid solutions, and industrial cybersecurity.

At Siemens Energy, we recognize that industrial cybersecurity does more than reduce risks. Cybersecurity protects productive uptime and unlocks powerful, profitable efficiencies offered by digital controls for physical systems. We apply expertise in operational technologies to the challenges of securing digitized OT networks against evolving cyber threats. We help customers navigate the complex set of choices required for their organization's cybersecurity journey. We start with a risk-based strategy that assesses fundamentals, transforms an organization's response to the environment, and most importantly, builds capacity to monitor and respond to threats.

Headquartered in Munich, Germany, Siemens Energy operates in more than 90 countries, employing a diverse workforce dedicated to driving innovation and excellence. Through strategic partnerships and a customer-centric approach, Siemens Energy aims to empower the global energy transition, building secure, reliable, affordable, and sustainable infrastructure for future generations.



01 Foreword
Rapid digital innovation is reshaping industries around the world

02 About
About Ponemon Institute and Siemens Energy

05 Introduction
Today, networked digital devices control the physical systems across several key industries

06 Risk
OT environments remain exposed to cyber threat

09 Readiness
OT practitioners say cyber defenses don't measure up

12 Solution
Companies look to innovation to close OT cybersecurity gaps

15 Conclusion
There is a need for stronger OT cybersecurity for the surveyed industries

16 Survey methodology

Today, networked digital devices control the physical systems across several key industries

The productivity of industries like manufacturing, petroleum refining, utilities, oil and gas, and renewable power depends on securing these devices and networks against cyber threats. The same networked operational technology (OT) systems that makes these critical industries efficient to operate can inadvertently provide malicious attackers with easy targets.

This survey finds that around the world, OT systems in these critical industries are at risk. Organizations self-assess that they are underprepared for current and future threats. Known vulnerabilities exist in a majority of OT environments. 77% of organizations experienced a successful cyber incident in OT last year. It takes most organizations more than a month to detect cyber incidents, and an average of seven months to recover. Cybersecurity expertise is in short supply, while insider and third-party risks are top concerns.

Around the world, these critical industries are converging on several technologies and approaches aimed at enabling small teams to mitigate risks across their OT environments. A majority of organizations in these industries plan to invest in one or more new OT security technologies and services within the next 12 months.

Continuing to mature cybersecurity postures remains essential, because technology innovation continues to change the security landscape. Attackers develop new exploits. Businesses find new ways to integrate IT and OT. Developers build out new energy facilities to integrate wind, solar, biofuels, battery storage, hydrogen, liquified natural gas, and other emerging technologies. Artificial intelligence capabilities advance rapidly and are applied to new use cases, both constructive and malicious.

This report provides insights drawn from surveys of cybersecurity professionals in manufacturing, petroleum refining, utilities, oil and gas, and renewable power organizations.

OT environments remain exposed to cyber threats

Estimating the risks posed by cyber threats requires understanding the frequency of attacks, their likelihood of success, and their impact when successful. Industry surveys like this one help assess the scale of these risks. Because responses are anonymized, respondents do not need to consider reputational risks to their organization when stating the number of cyber incidents or impacts their organizations experience.

Cyberattacks frequently target OT environments.

77%

of respondents report that within the past 12 months a security compromise resulted in the loss of confidential information or disruption to operations in the OT environment.

4% report 10 or more such attacks within the past 12 months.

52% say a successful cyber exploit on their organization's industrial control systems is likely in the next 12 months.

Looking only at reported cyberattacks likely underestimates the threat.

16% of cyberattacks on OT detected in the past 12 months required disclosure to regulators or the public.

When asked to estimate the share of cyberattacks on OT that go undetected, the **average response was 41%**.

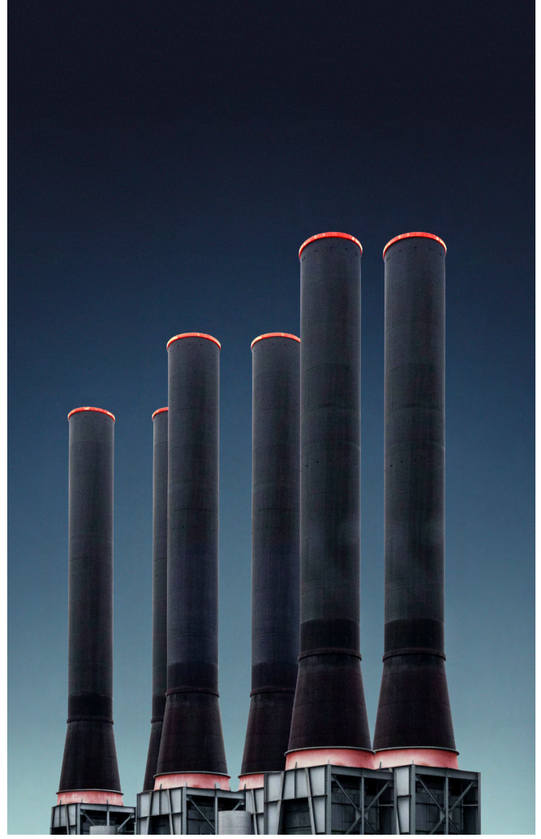
Cyberattacks against OT are a significant source of risk. Like attacks against IT, attacks on OT environments can result in the loss of information and disruption to normal workflows. Unlike most threats against IT, attacks against OT can create safety hazards. **46% of respondents say cyber threats present greater risk in the OT than the IT environment.**

Looking at the detected cybersecurity attacks on OT in the past 12 months

29% compromised OT equipment.

28% compromised one or more user accounts.

24% required halts to OT workflows.



When asked to identify the top cybersecurity threats to critical operations, respondents cite malicious insiders and third-party mistakes, closely followed by DNS-based denial of service attacks, insecure web applications, viruses and other malware, negligent insiders, insecure endpoints, watering hole attacks, and AI misuse.

26% of detected cybersecurity attacks on OT in the past 12 months involved one or more third-party vendors or contractors.

46 %

of respondents say it is likely that a successful cyber exploit against their company will cause a plant shutdown.

In 2021, a cyber attack prompted a shutdown of the Colonial Pipeline. Operators did not have the visibility needed to quickly determine whether their OT equipment had been affected by the attack. Approximately 45% of all liquid fuel to the U.S. Atlantic Coast could not move for six days, leading to fuel shortages, price shocks, and a state of emergency affecting 17 U.S. states.

Case Study Colonial pipeline attack

Several potential vulnerabilities for OT environments are common:

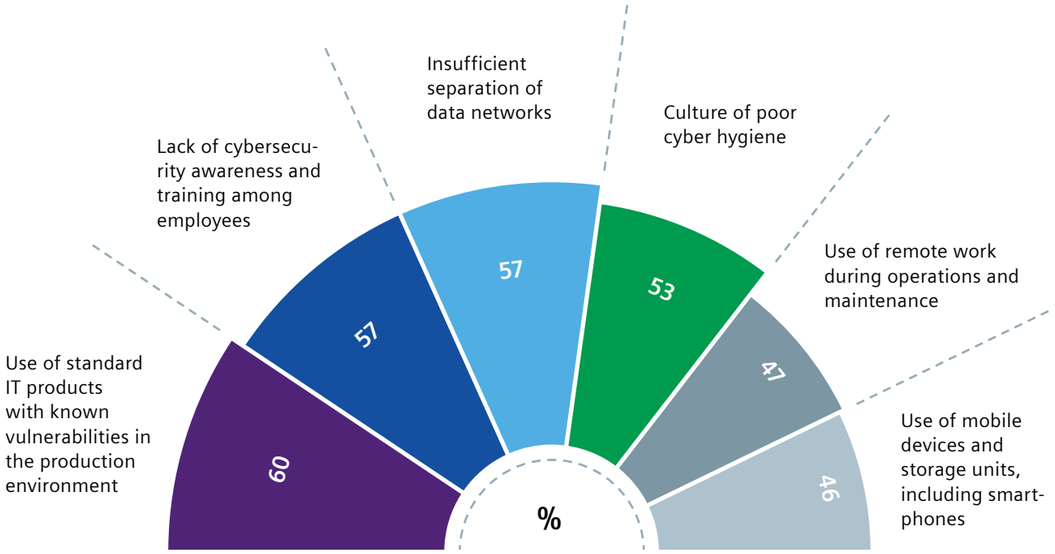


Figure 1 Reported common potential vulnerabilities for OT environments

Respondents say the top areas of vulnerability for OT are:

- Customer facing IT systems
- Blind spots in threat monitoring
- Industrial networks
- AI assets
- Changes to OT asset bases
- Lifecycle management
- Human-machine interfaces

In 2024, a faulty software update caused major outages in critical systems across several industries, costing U.S. Fortune 500 companies an estimated $5.4 billion. The error arose from incompatibility with an older data format, highlighting the impor-tance of comprehensive testing.

Case Study CrowdStrike software update incident

OT practitioners say cyber defenses don't measure up

Cybersecurity teams must defend their industrial infrastructure against global threats. Survey responses clearly show cybersecurity practi-tioners do not believe their industries have deployed mature cybersecurity.

Industry's self-assessment as unready aligns with the findings that most organizations experi-enced significant cyber incidents in the past year, and were slow to detect and recover from those cyber incidents.

Self-assessments reflect a lack of confidence in OT cybersecurity within organizations.

46% say their organization's industrial control systems protection and security is adequate.

51% say organization is effective in achieving compliance with security standards and guid-ance.

39% say their organization has the internal expertise to manage cyber threats in the OT environment.

49% say their organization's staffing level is adequate for OT cybersecurity.

Survey respondents were asked which descrip-tion best matched their organization's level of security, then provided with descriptions that map to the IEC 62443 standard's security levels.

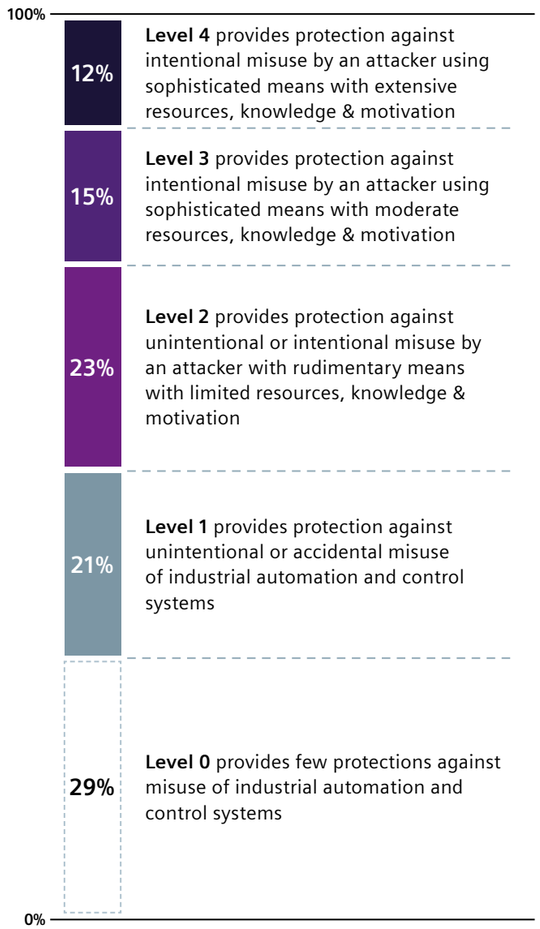


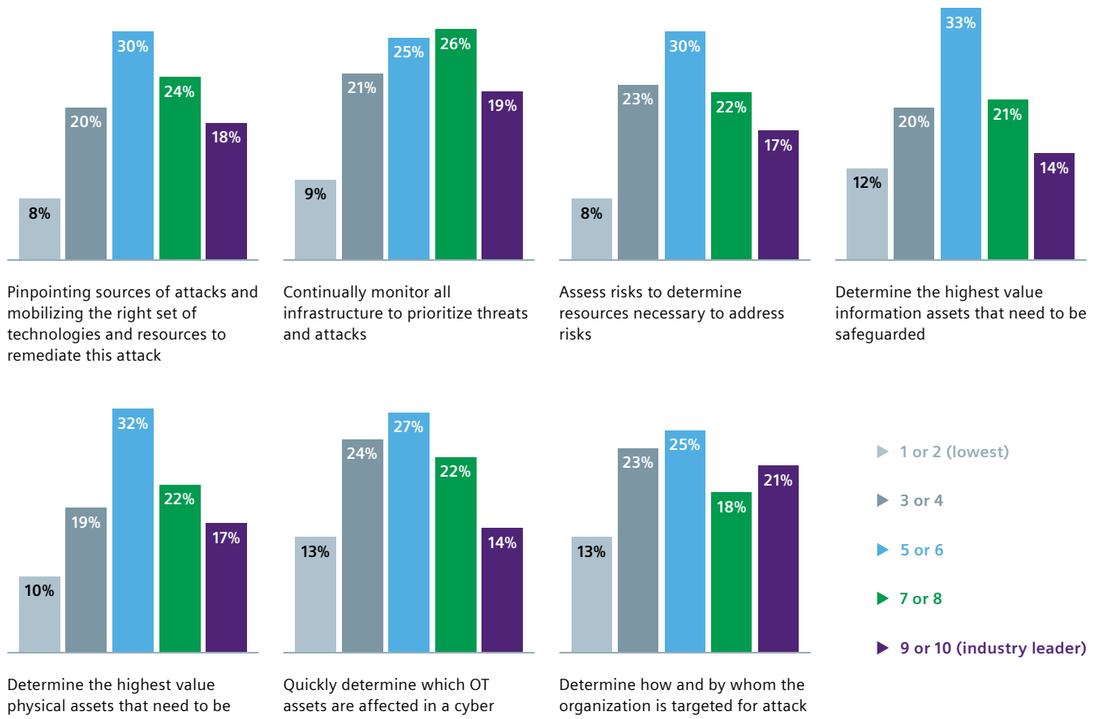
Figure 2 Organization's match of security levels for industrial cybersecurity (IEC 62443 standard)

At the same time, respondents indicate they believe their organizations are above average for their industries.

54% of respondents rate their organization as 7 or higher on a scale of 1-10, with 10 being industry leader in OT cybersecurity.

Across several capabilities critical for OT cybersecurity, respondents rated their organizations as moderately effective.

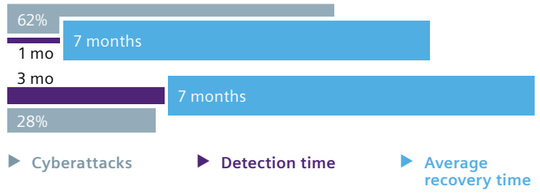
Figure 3 Reported ratings of OT cybersecurity capabilities on a scale of 1-10



Key cybersecurity performance measurements suggest the lack of confidence in OT cybersecurity is warranted. According to respondents:

62% of cyberattacks took more than 1 month to detect.

28% took more than 3 months to detect.



52% of organizations reported their average recovery time after detecting a cyberattack was 6 months or longer.

7 months

was the average recovery time after detection.

Practitioners are evenly divided when asked whether their organization's OT environment is more secure than five years ago:

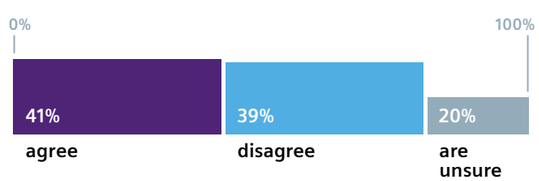


Figure 4 Is your organization's OT environment more secure than five years ago?

In some measures, a significant number of organizations have not yet caught up to industry best practices:

50% say IT and OT cybersecurity operations are aligned or fully aligned; 25% report little or no alignment.

51% say employees understand who is responsible and accountable for cybersecurity; 33% disagree and 16% are unsure.

Excluding budget and staffing constraints, organizations identified the top three OT cybersecurity challenges as:

- **Training**
- **Keeping pace with regulatory requirements**
- **Quantifying risk**

Taken together, these survey responses show a consensus that overall, OT cybersecurity is not mature. Most organizations have identified areas for improvement, both in terms of technology and in terms of business practices.

Companies look to innovation to close OT cybersecurity gaps

OT cybersecurity calls for a combination of technical capabilities, training, and implementation. All three must be sustained over time to keep up with emerging threats and changing asset bases.

For most organizations, maturing cybersecurity will require efficient use of the available resources. Cybersecurity staff, training, and expertise are frequently mentioned as constraints on OT cybersecurity.

62% of organizations have fewer than 10 employees devoted to OT cybersecurity.

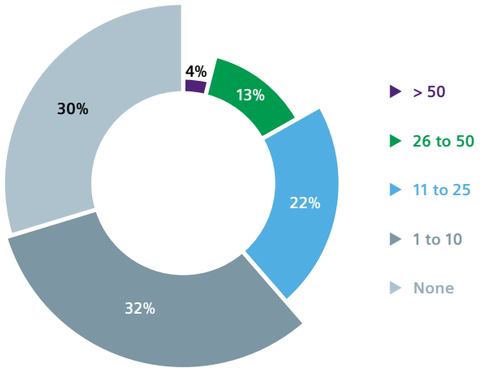


Figure 5 How many employees in your organization are dedicated to cybersecurity operations in the OT environment?

Responsibility for OT cybersecurity often rests with leaders who have a broader set of duties within their organization. The job titles deemed most responsible for ensuring cybersecurity objectives in the OT are:

- **Head, process engineering**
- **IT security leader**
- **Head, industrial controls**
- **Head, quality engineering**
- **CIO/ CTO**

The typical budget for IT and OT cybersecurity is between $6 and $25 million.

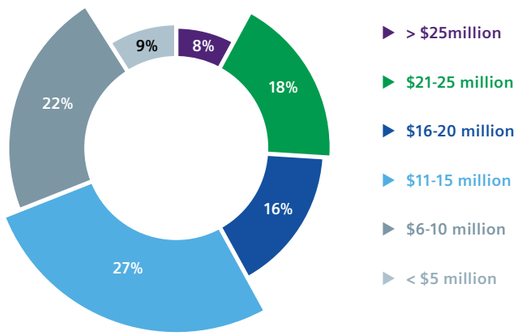


Figure 6 Total annual budget for cybersecurity operations and defense (OT and IT combined)

Most organizations allocate between 10 and 50% of the cybersecurity budget to OT.

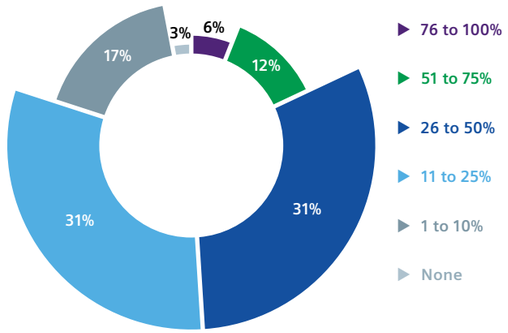


Figure 7 Percentage of total IT cybersecurity budget allocated to the security of OT assets and infrastructure

The most common services sought from managed security service providers are threat hunting, incident response, configuration management, software update and patch management, asset inventory, and anti-virus management, **closely followed by** network security monitoring, behavioral analytics, and security event monitoring.

in outside expertise for infrequent tasks like configuration, audit activities, and incident response.

48% of organizations participate in at least one cyber threat intelligence sharing effort.

63% of organizations say security analytics are essential or important to achieving a strong security posture.

Many organizations are responding to the scarcity of OT cybersecurity expertise by outsourcing.

Organizations seek cybersecurity technologies and services that amplify the impact of small teams. This includes automating routine tasks, leveraging process data resources for analysis, and bringing

45%

of organizations already outsource OT security operations, and a further 26% would consider outsourcing.

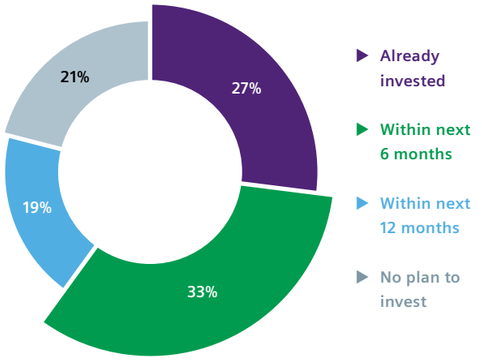


Figure 8 Planned timeline for next investment in OT security technology

Respondents ranked the top technologies and managed services most important to strong cybersecurity in OT as:

1. Patch & vulnerability monitoring
2. Managed anti-virus
3. Managed detection and response applications or services
4. Backup and restore capabilities in the cloud
5. Backup and restore capabilities on premises
6. Firewall audits
7. PLC integrity/data monitoring
8. OT Cloud
9. Purpose-built OT cybersecurity monitoring services
10. AI or machine learning for OT cybersecurity

A majority of organizations in these critical industries are investing in improving OT cybersecurity using technologies and managed services.

Given the identified lack of OT cybersecurity expertise within these critical industries, most organizations will need guidance when determining how best to advance their OT cybersecurity maturity.

52% of organizations consider cyber risks and secure by design principles when adopting new OT technologies and practices.

OEMs are the most trusted source of OT cyber expertise.

Figure 9 Who does your organization trust most to provide OT cyber expertise?

Conclusion

Overall these survey results describe an industry aware that OT cybersecurity must mature to meet evolving threats – and actively pursuing the needed improvements.

There is a need for stronger OT cybersecurity for the surveyed industries. Within their resource constraints, these industries are pursuing OT cybersecurity solutions that close vulnerabilities and skills gaps.

The surveyed industries report routinely high cyber threats and vulnerability to those threats. More than three-quarters experienced a significant cyber incident in the past year. Most expect to see an attack in the upcoming year. Respondents indicate their organizations lack adequate OT cybersecurity and lack internal OT cybersecurity expertise. Demand for expertise outstrips training pipelines.

Combining the perceived top threats and vulnerabilities with the technologies and services identified as important to OT cybersecurity suggest four broad priorities for solutions:

Security posture: This includes the overarching network architecture, correct the configuration of assets and security controls, and the timely deployment of patches, software, antivirus, and other measures needed to maintain security once it is established at a given level.

Visibility: This includes the ability to collect and analyze sufficient data to detect cyber threats and vulnerabilities in every part of the OT environment, as well as the ability to quickly determine the health of a given asset. Visibility may include data collected from outside the OT environment, such as cyber threat intelligence.

Resilience: This includes incident response, backup and restore capabilities, OT cloud solutions, and other solutions that enable continued productivity when cyber incidents have been detected.

Mitigating insider threats: Addressing posture, visibility, and resilience are often necessary but not sufficient to address the insider and third-party risks named as top concerns. Organizations should consider how their technology stack addresses identity, how to apply principles of least privilege, and whether to seek additional solutions to address insider threats. Solutions may include managed identity and privileged access controls, behavioral analytics, or other controls designed to detect and prevent malicious uses of authorized accounts.

Survey methodology

The sampling frame is composed of 33,290 IT and OT security practitioners in the United States, European Union, Middle East, Asia Pacific and Americas. As shown in Table 1, 1,899 respondents completed the survey. Screening removed 197 surveys. The final sample was 1,702 surveys (or a 5.1 percent response rate).

Sixty-five percent of respondents reported their current position as supervisory or above and 31 percent of respondents reported their position is at the technician/staff level.

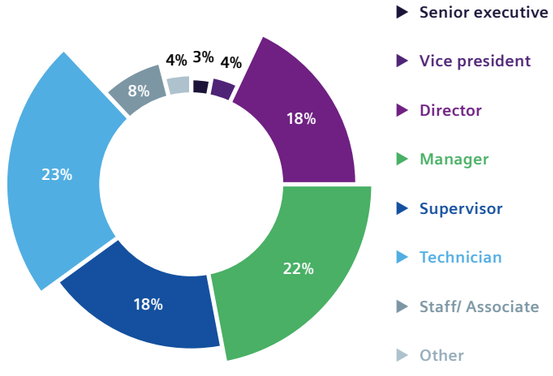


Figure 10 Distribution of respondents according to position level

When asked the title of the primary person to whom the respondent or their leader reports, nineteen percent of respondents identified the head, industrial control systems as the person to whom they report. Another 15 percent indicated they report directly to OT security leader, 14 percent of respondents report to the head, process engineering and 14 percent of respondents report to the head, quality engineering.

Small, medium and large organizations are included in the sample. 36 percent of responses came from organizations with a global full-time headcount less than 1,000 employees, 36 percent of respondents are from organizations with a global headcount of 1,000 to 10,000 employees and 37 percent of respondents are from organizations with a global headcount of more than 10,000 employees.

Table 1 Sample response

	United States	Europe	Middle East	Asia-Pacific	Americas	Global
Total sampling frame	12,390	6,224	4,851	5,480	4,345	33,290
Total returns	503	413	348	325	310	1,899
Rejected surveys	50	29	42	39	37	197
Final sample	453	384	306	286	273	1,702
Response rate	**3.7%**	**6.2%**	**6.3%**	**5.2%**	**6.3%**	**5.1%**

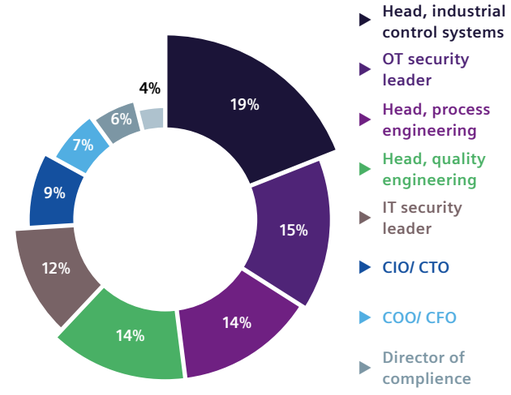


Figure 11 Distribution of respondents according to reporting channel

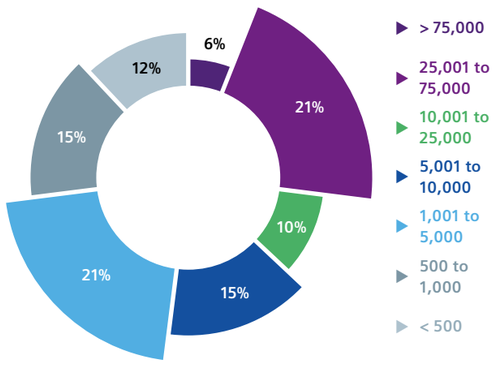


Figure 12 Distribution of respondents according to the full-time headcount of the global organization

Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or OT security practitioners in the United States, European Union, Middle East, Asia Pacific and Latin America. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a specified time period.

Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Published by

Siemens Energy Global GmbH & Co. KG
Otto-Hahn-Ring 6,
81739 München, Germany

For more information, please contact
Phone: +49 (89) 78050
E-mail:contact@siemens-energy.com

For the U.S. published by

Siemens Energy, Inc.
4400 N Alafaya Trail
Orlando, FL 32826, USA

For more information, please contact
Phone: +1 202-347-4378
E-mail: john.la-rue@siemens-energy.com

siemens-energy.com

© Siemens Energy, 2025

Siemens Energy is a trademark licensed by Siemens AG.