The 2020 Study on the State of Industrial Security.

Independently conducted by Ponemon Institute LLC.

www.tuv.com/fscs

Ponemon INSTITUTE

TÜVRheinland®
Precisely Right.

Table of Contents

Credits – Cybersecurity & Functional Safety
(c) TÜV Rheinland Industrial Services & Cybersecurity. All rights reserved TÜV Rheinland Industrial Services & Cybersecurity. Responsible in the terms of press law as well as service provider according to §6 of the media treaty and §6 of teleservice law is the operator of the website. TÜV Rheinland Group. p. 4: iStock-©4 PM production p. 6: iStock-©zorazhuang; p. 9: iStock-©PopTika; p. 12: iStock-©Goroden-koff; p. 15: iStock-©MNBB Studioi; p. 18: iStock-©Zapp2Photo

Dear Readers,

If your company becomes the victim of a cyberattack, the cyber attacker may have access not only to your IT network and systems also to your operational technology (OT). Is your company prepared for such an attack? Are your response plans for OT cybersecurity incidents practiced and do all parties involved know their roles and responsibilities? At TÜV Rheinland, we take the consequences of inadequate cybersecurity for the operational technology seriously. Following the good reception in 2019, we have decided to continue the Industrial Security Survey in 2020.

Recognizing digital challenges today. Securing the industrial future.

The Industrial Security Survey 2020 highlights the importance of tailoring cybersecurity policies and procedures to the specific requirements of operational technology. The results of the survey, executed by the renowned Ponemon Institute, uncover what challenges OT Managers around the world currently see coming for organizations and show once again how important it is to think about operational security holistically.

Now, more than ever, Industry requires new way of thinking and acting that recognizes the potential threats and effectively counters them. Cybersecurity is already an integral part of modern engineering and an indispensable prerequisite for industrial plant safety. There will be no safety without security. We look forward to working with you to bridging the gap between safe and secure operation. Securing today for a safer tomorrow.

PETR LÁHNER
EXECUTIVE VICE PRESIDENT
INDUSTRIAL SERVICES & CYBERSECURITY

Introduction.

TÜV Rheinland is pleased to present the findings from „The 2020 Study on the State of Industrial Security,” in cooperation with Ponemon Institute. The purpose of the research is to understand cyber risks across a broad spectrum of industries and the steps organizations are taking to reduce cyber risk in the operational technology (OT) environment.

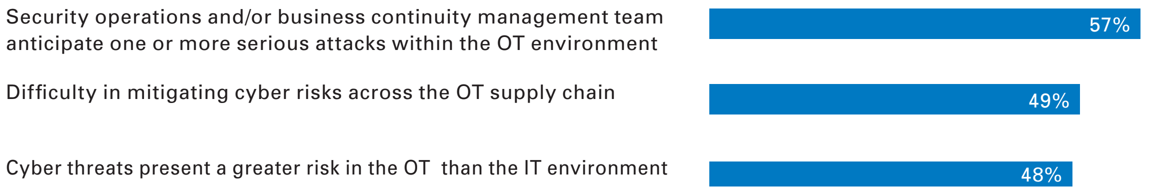
Ponemon Institute surveyed 2,258 cybersecurity practitioners in the following industries: automotive, oil and gas, energy and utilities, health and life science, industrial manufacturing and logistics and transportation. All respondents are responsible for securing or overseeing cyber risks in the OT environment and are aware of how cybersecurity threats could affect their organization.

In the context of this research, operational technology is the hardware and software dedicated to detecting or causing changes in physical processes through direct monitoring and/or control of physical devices. Simply put, OT is the use of computers to monitor or alter the physical state of a system, such as the control system for a power station. The term was established to demonstrate the technological and functional differences between traditional IT systems and industrial control systems environment.

THE OT ENVIRONMENT IS VULNERABLE TO CYBERATTACKS

As shown in Figure 1, 57 percent of respondents say their organizations' security operations and/or business continuity management teams believe there will be one or more serious attacks within the OT environment. Almost half (49 percent and 48 percent of respondents) say it is difficult to mitigate cyber risks across the OT supply chain and cyber threats present a greater risk in the OT than the IT environment.

FIGURE 1:
Perceptions about OT security risks[1]



[1] Strongly agreed and Agreed response combined

The following findings reveal the cybersecurity vulnerabilities in the OT environment.

OT AND IT SECURITY RISK MANAGEMENT EFFORTS ARE NOT ALIGNED

63 percent of respondents say OT and IT security risk management efforts are not coordinated, making it difficult to achieve a strong security posture in the OT environment. The management of OT security is painful because of the lack of enabling technologies in OT networks, complexity and insufficient resources.

ON AVERAGE, ORGANIZATIONS HAD FOUR SECURITY COMPROMISES THAT RESULTED IN THE LOSS OF CONFIDENTIAL INFORMATION OR DISRUPTION TO OT OPERATIONS

47 percent of respondents say OT technology-related cybersecurity threats have increased in the past year. The top three cybersecurity threats are phishing and social engineering, ransomware and DNS-based denial of service attacks. One-third of respondents say such exploits have resulted in the loss of OT-related intellectual property.

THE MAJORITY OF ORGANIZATIONS HAVE NOT ACHIEVED A HIGH DEGREE OF CYBERSECURITY EFFECTIVENESS

Less than half of respondents say they are very effective in responding to and containing a security exploit or breach (48 percent), continually monitoring the infrastructure to prioritize threats and attacks (47 percent) and pinpointing sources of attacks and mobilizing the right set of technologies and resources to remediate the attack (47 percent of respondents).

TO MINIMIZE OT-RELATED RISKS, ORGANIZATIONS NEED TO REPLACE OUTDATED AND AGING CONNECTED CONTROL SYSTEMS IN FACILITIES, ACCORDING TO 61 PERCENT OF RESPONDENTS

More than half (52 percent of respondents) say vulnerable software is creating risks in the OT environment. Risk management efforts are not coordinated making it difficult to achieve a strong security posture in the OT environment.

NOT ENOUGH EXPERTISE AND BUDGET ARE OFTEN CITED AS REASONS FOR NOT HAVING A STRONG SECURITY POSTURE IN THE OT ENVIRONMENT

Organizations represented in this research are spending annually an average of $64 million on cybersecurity operations and defense (OT and IT combined). An average of 26 percent of this budget (approximately $17 million) is allocated to the security of OT assets and infrastructure, while an average of 17 percent (approximately $10 million) is allocated specifically to OT cybersecurity. Respondents say their OT budgets are inadequate to properly execute their cybersecurity strategy.

ACCOUNTABILITY FOR EXECUTING A SUCCESSFUL CYBERSECURITY STRATEGY

Respondents were asked who is most accountable for executing a successful cybersecurity strategy. Only 20 percent of respondents say it is the OT security leader, followed by the Chief Information Officer/Chief Technology Officer (CIO/CTO) (18 percent), and finally, the IT security leader (17 percent).

ORGANIZATIONS ARE LAGGING BEHIND IN ADOPTING ADVANCED SECURITY TECHNOLOGIES

Only 38 percent of respondents say their organizations are using automation, machine learning and artificial intelligence (AI) to monitor OT assets. The majority of companies are not integrating security and privacy by design in the engineering of OT control systems.

Key findings.

In this section, we provide an analysis of the findings. The full audited findings are presented in the appendix of this report. The report is organized by the following topics.

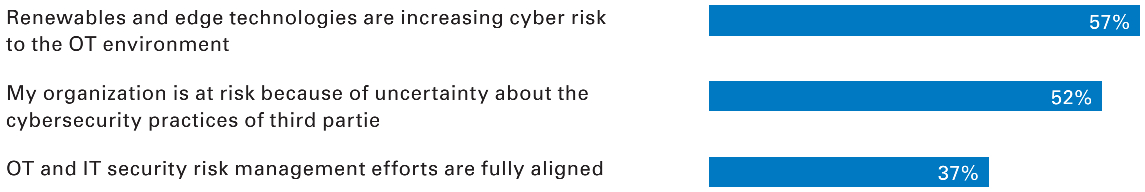
- Cyber risk in the OT environment
- Strategy and governance in the OT environment
- Steps taken to improve cybersecurity in the OT environment
- The state of industrial security varies among industries

Cyber risk in the OT environment.

EDGE TECHNOLOGIES AND THIRD PARTIES ARE CREATING RISKS IN THE OT ENVIRONMENT

According to Figure 2, the majority of respondents cite that renewables[1] and edge technologies are increasing cyber risk to the OT environment (57 percent). Also creating risk is the uncertainty about the cybersecurity practices of third parties (52 percent). Only 37 percent of respondents say their organizations OT and IT security risk management efforts are fully aligned. This lack of alignment by most organizations makes it difficult to achieve a strong security posture in the OT environment.

FIGURE 2:
Perceptions about the risks in the OT environment[2]



[2] Strongly agreed and Agreed response combined

[1] In the context of this research, we define renewables as technologies that enable organizations to create electricity, heat and fuel from renewable sources.

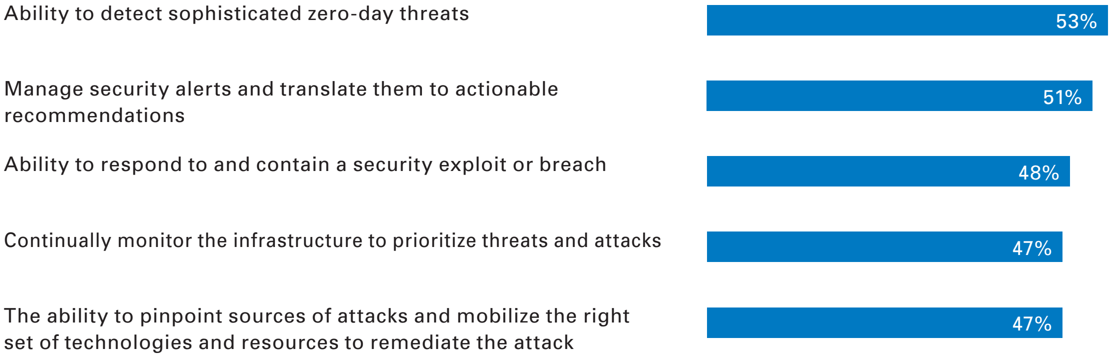
LESS THAN HALF OF RESPONDENTS HAVE CONFIDENCE IN THEIR ABILITY TO RESPOND TO AND CONTAIN A SECURITY EXPLOIT OR BREACH

In the past 12 months, organizations represented in this study had an average of four security compromises that resulted in the loss of confidential information or disruption to operations in the OT environment. One-third of respondents say such exploits have resulted in the loss of OT-related intellectual property, which are high-value information assets targeted by cyber criminals. It is critical for organizations to identify the risk and take steps to prevent the loss of these assets.

Respondents were asked to rate the effectiveness of mitigating cybersecurity risk on a scale of 1= low effectiveness to 10 = highly effective. Figure 3 presents high and highly effective responses (7+ on the 10-point scale) in completing tasks to reduce risk.

Less than half of respondents are confident in their ability to respond to and contain a security exploit or breach (48 percent), continually monitor the infrastructure to prioritize threats and attacks (47 percent) and pinpoint sources of attacks and mobilize the right set of technologies and resources to remediate the attack. More respondents rate their ability to detect sophisticated zero-day threats and manage security alerts and translate them into actionable recommendations, 53 percent and 51 percent of respondents respectively.

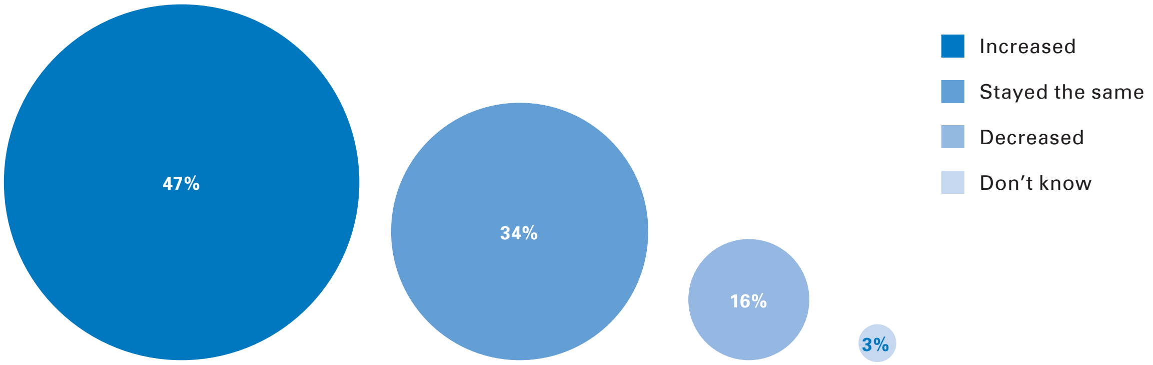
FIGURE 3:
Effectiveness in mitigating cybersecurity risk



OT TECHNOLOGY-RELATED CYBERSECURITY THREATS ARE WORSENING

As discussed previously, 57 percent of respondents expect one or more serious attacks within the OT environment. According to Figure 4, almost half of respondents say operational technology-related cybersecurity threats have increased in the past year.

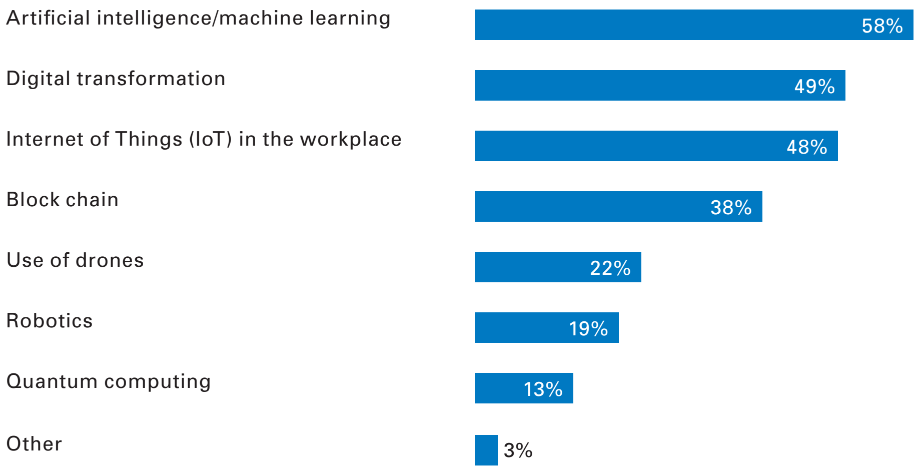
FIGURE 4:
How have the number of operational technology-related cybersecurity threats to your business changed in the past year?



DISRUPTIVE TECHNOLOGIES SUCH AS ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING ARE INCREASING THE RISK IN THE OT ENVIRONMENT

The adoption of artificial intelligence and machine learning can improve security in the OT environment. However, at the same time, 58 percent of respondents say these technologies increase risk. Almost half of respondents say digital transformation and IoT in the workplace are making the OT environment more vulnerable to cyber threats.

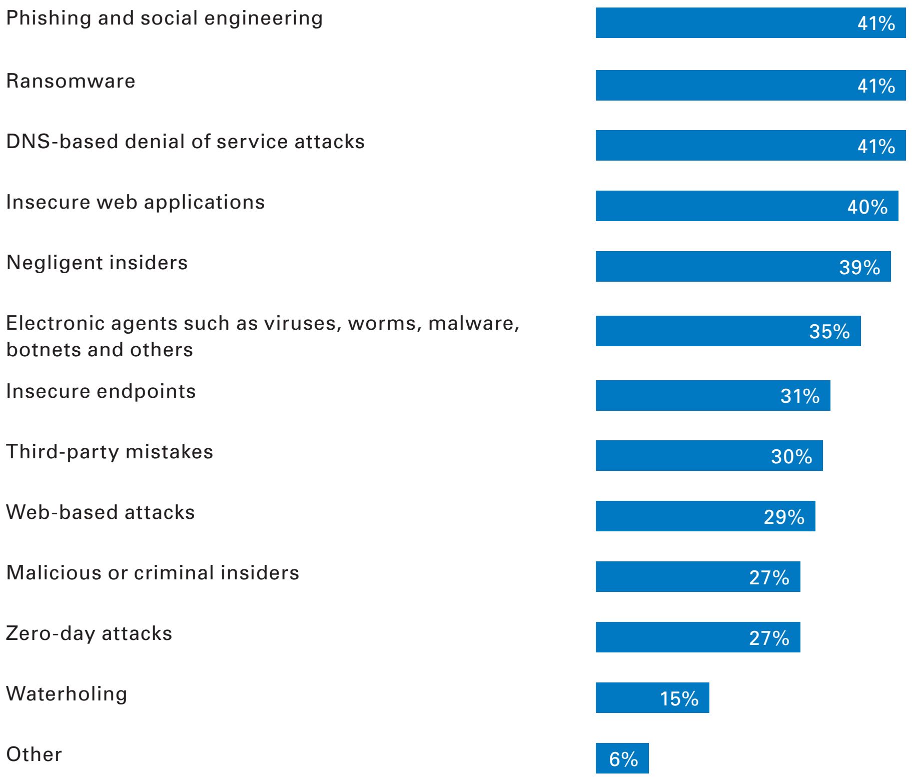
FIGURE 5:
Which of the following megatrends will increase risk to your organization?[1]



[1] More than one response permitted

The top three cybersecurity threats to the OT environment are phishing and social engineering, ransomware and DNS-based denial of service attacks (41 percent of respondents). Zero-day attacks and waterholing are not considered as great a threat.

FIGURE 6:
What are the top cybersecurity threats that may affect critical operations in the OT environment?[1]



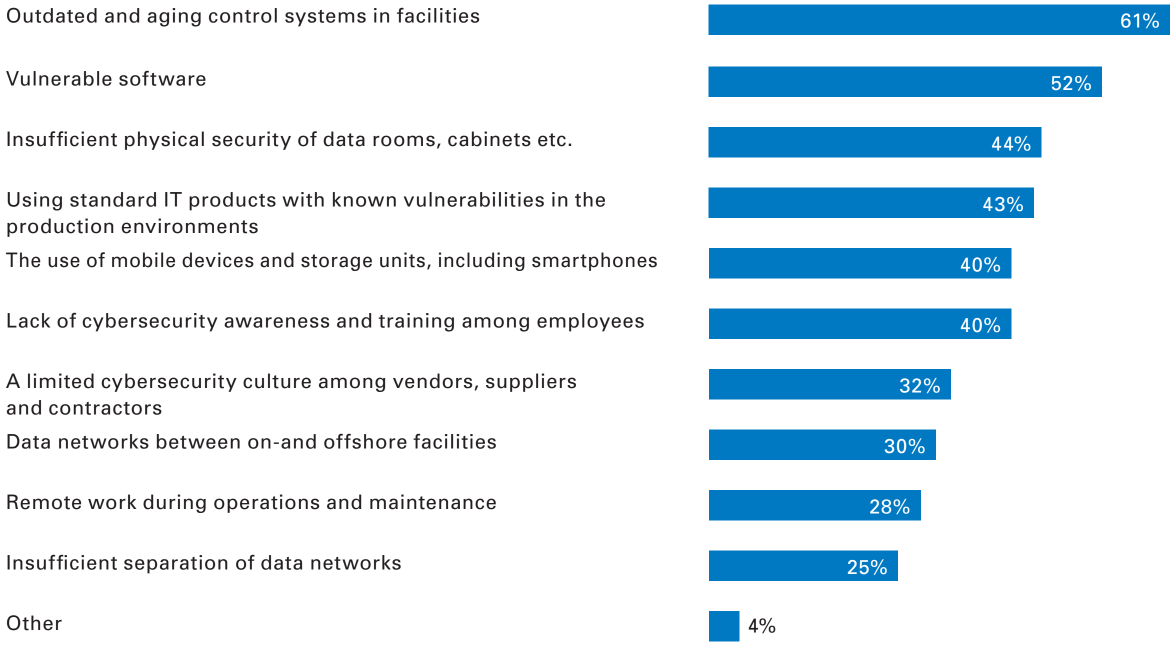
[1] Four responses permitted

OUTDATED AND AGING CONNECTED CONTROL SYSTEMS IN FACILITIES ARE THE BIGGEST BARRIER TO REDUCING OT-RELATED RISKS

According to Figure 7, 61 percent of respondents say the condition of their control systems makes reducing OT-related risks difficult. More than half of respondents (52 percent) say vulnerable software is a barrier.

FIGURE 7:

What are the top barriers to minimizing OT-related risk in your organization?[1]

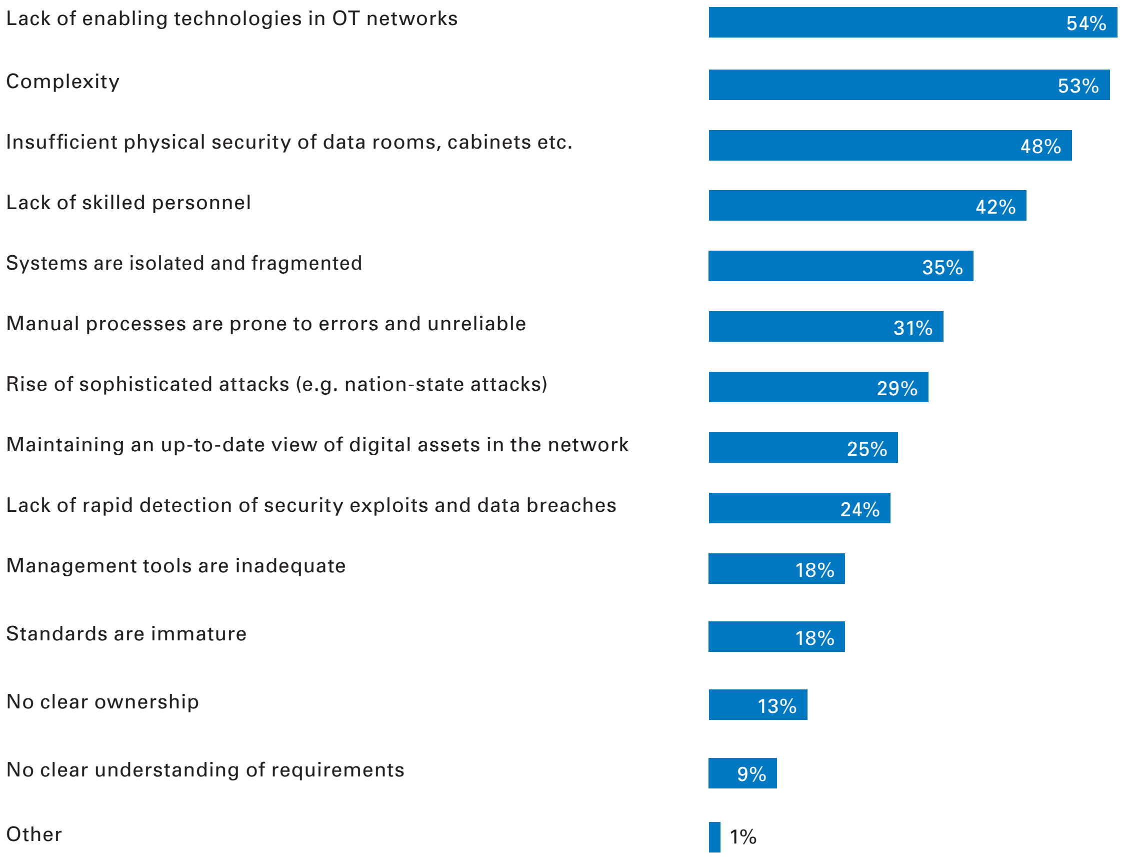


[1] Four responses permitted

THE MANAGEMENT OF OT SECURITY IS PAINFUL

76 percent of respondents say the overall "pain" associated with managing cybersecurity within the OT environment is severe. Reasons for the pain are shown in Figure 8. The lack of enabling technologies in the OT networks and complexity are top two sources for this pain.

FIGURE 8:
What makes the management of OT security painful?[1]



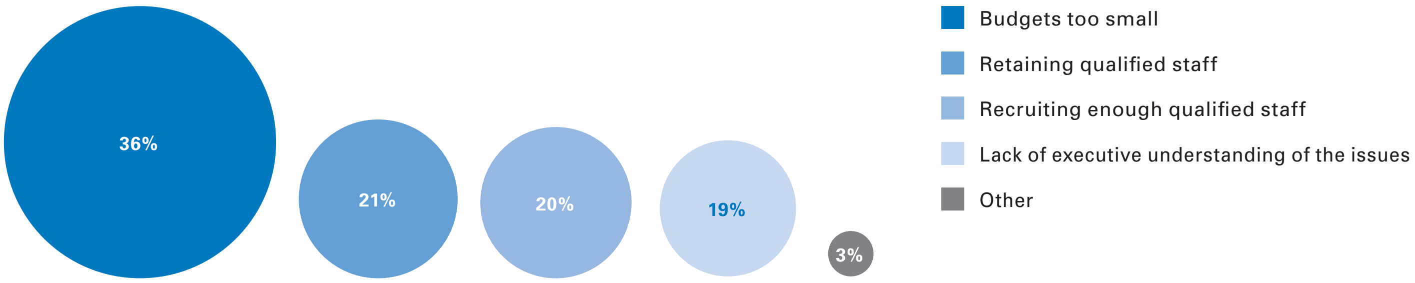
[1] Four responses permitted

Strategy and governance in the OT environment.

OT CYBERSECURITY STRATEGIES LACK AN ADEQUATE BUDGET

Organizations represented in this research are spending an average of $64 million annually on cybersecurity operations and defense (OT and IT combined). An average of 26 percent of this budget (approximately $17 million) is allocated to the security of OT assets and infrastructure and an average of 17 percent or approximately $10 million is allocated specifically to OT cybersecurity. As shown in Figure 9, respondents say their OT budgets are inadequate to properly execute their cybersecurity strategy.

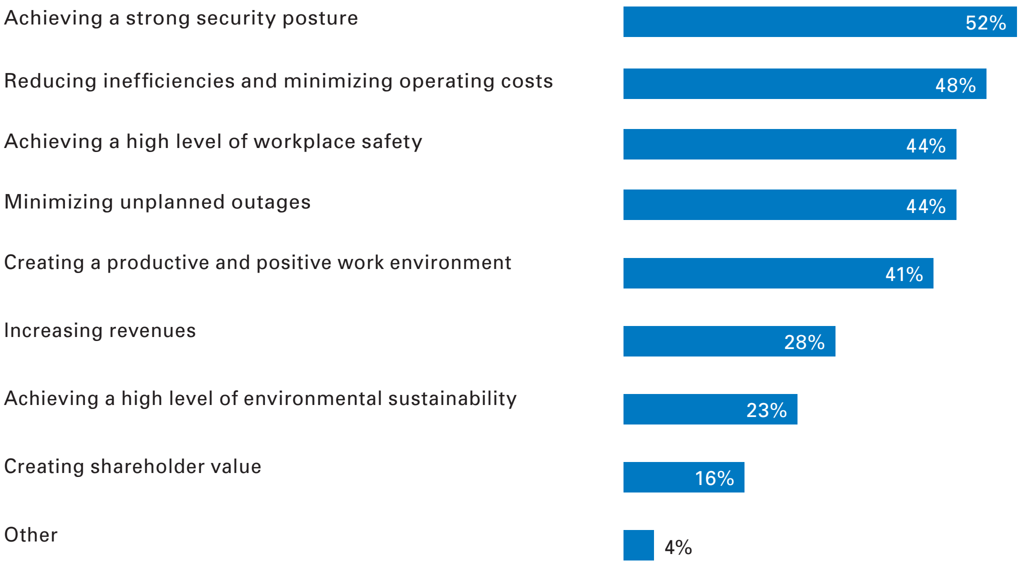
FIGURE 9:
Within your OT cybersecurity strategy, what area provides the most complex challenge?



THREATS TO THE OT ENVIRONMENT ARE INCREASING AND ORGANIZATIONS ARE MAKING THE ACHIEVEMENT OF A STRONG SECURITY POSTURE A PRIORITY

As shown in Figure 10, 52 percent of respondents recognize the importance of security as a top OT priority. However, as discussed previously, outdated and aging facilities, software vulnerabilities and inadequate budgets are a deterrent to achieving this goal. Also budget related is the priority of reducing inefficiencies and minimizing operating costs (48 percent of respondents).

FIGURE 10:
What are the top OT priorities for your organization?[1]



[1] Three responses permitted

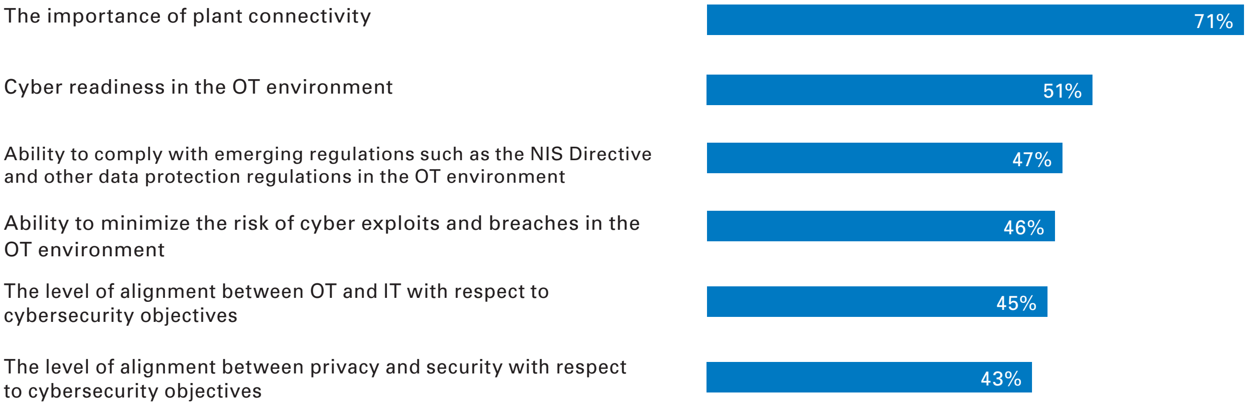
PLANT CONNECTIVITY IS THE MOST IMPORTANT FACTOR IN BEING READY FOR A CYBERATTACK

Respondents were asked to rate the importance, readiness and alignment of certain features in their cybersecurity strategy on a scale of 1 = low importance, readiness and alignment to 10 = high importance, high readiness and high alignment.

Figure 11 shows the 7+ responses (high and very high) on the 10-point scale. Just about half (51 percent of respondents) rate their cyber readiness in the OT environment as high or very high and only 46 percent of respondents rate their organizations' ability to minimize the risk of cyber exploits and breaches in the OT environment as very high. Plant connectivity is critical to achieving cyber readiness (71 percent of respondents). Resilient organizations would make plant connectivity an integral part of their cyber resilience strategy.

The findings also reveal the lack of alignment between OT and IT, as well as with the privacy function that may reduce cyber readiness. Only 45 percent of respondents say their organizations have a high level of alignment between OT and IT with respect to cybersecurity readiness. Similarly, only 43 percent of respondents rate the alignment between privacy and security with respect to cybersecurity objectives as very high. Less than half (47 percent of respondents) have a high level of ability to comply with emerging regulations such as the NIS[1] Directive and other data protection regulations in the OT environment.

FIGURE 11:
Perceptions about cyber readiness

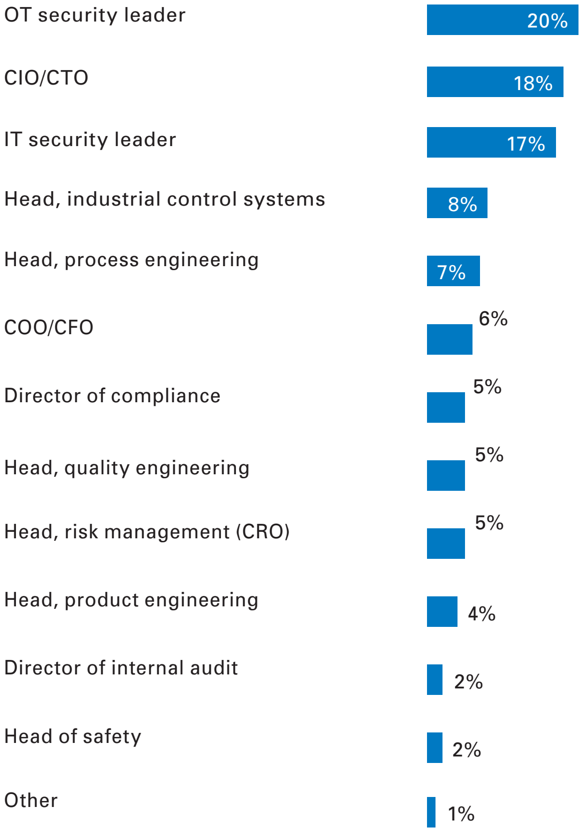


[1] (As part of the EU Cybersecurity strategy the European Commission proposed the EU Network and Information Security directive. The Network and Information Security directive (NIS Directive) is the first piece of EU-wide cybersecurity legislation.)

ACCOUNTABILITY FOR EXECUTING A SUCCESSFUL CYBERSECURITY STRATEGY

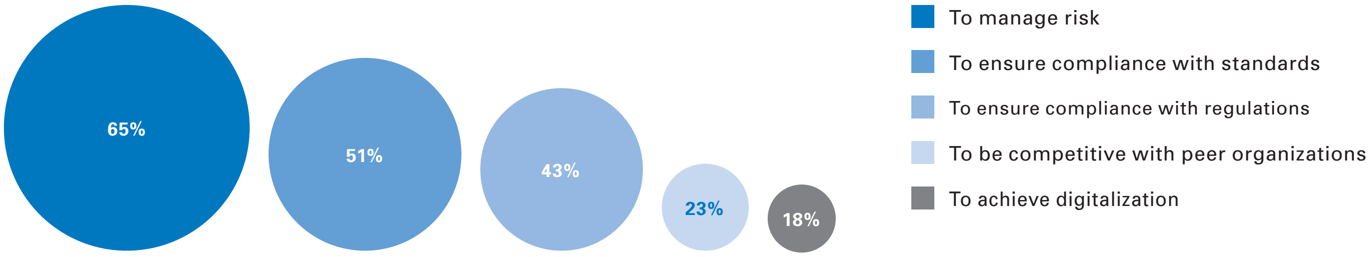
Respondents were asked who is most accountable for executing a successful cybersecurity strategy. Only 20 percent of respondents say it is the OT security leader followed by the CIO/CTO (18 percent) and the IT security leader (17 percent), as shown in Figure 12.

FIGURE 12:
Who is the primary person for ensuring cybersecurity objectives in the OT environment?



OT cybersecurity management programs are established to manage risk and ensure compliance with standards (65 percent and 51 percent of respondents, respectively), as shown in Figure 13.

FIGURE 13:
What best describes your organization's primary motivation for administering an OT cybersecurity program?[1]



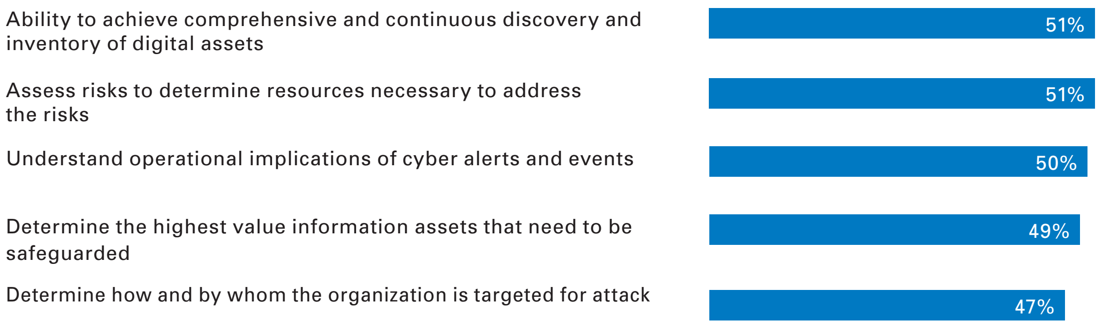
[1] Two responses permitted

ORGANIZATIONS ARE MOST EFFECTIVE IN THE DISCOVERY AND INVENTORY OF DIGITAL ASSETS AND ASSESSING RISKS

Respondents were asked to rate the effectiveness of their governance practices on a scale from 1 = low effectiveness to 10 = high effectiveness. Figure 14 presents the high effectiveness responses (7+). The findings reveal that half of respondents (51 percent) are very effective in achieving comprehensive and continuous discovery and inventory of digital assets and assessing risks to determine resources necessary to address the risks.

As discussed previously, one-third of respondents say their organizations high value IP data was stolen. Less than half of respondents (49 percent) say their organizations are very effective in determining the highest value information assets that need to be safeguarded. Only 47 percent of respondents say their organizations are very effective in determining how and by whom the organization is targeted for attack.

FIGURE 14:
Effectiveness in governance in the OT environment

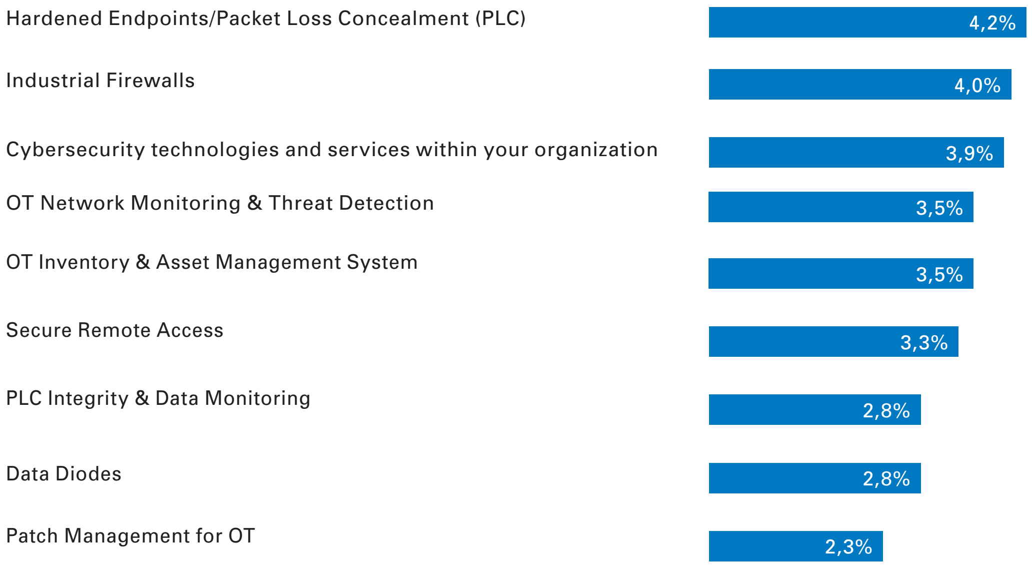


Steps taken to secure the OT environment.

THE TWO MOST EFFECTIVE TECHNOLOGIES TO IMPROVE SECURITY AND COMPLIANCE IN THE OT ENVIRONMENT ARE HARDENED ENDPOINTS/PLC AND INDUSTRIAL FIREWALLS

Figure 15 presents technologies and managed services used to reduce risk in the OT environment. Respondents were asked to rate these technologies or managed services on a scale of 1 = not effective to 5 very effective. While none were rated as very effective, the most effective are hardened endpoints/packet loss concealment (PLC) and industrial firewalls. OT network monitoring & threat detection and OT inventory and asset management systems are only somewhat effective.

FIGURE 15:
Effectiveness of technologies or managed services to foster security and compliance with standards

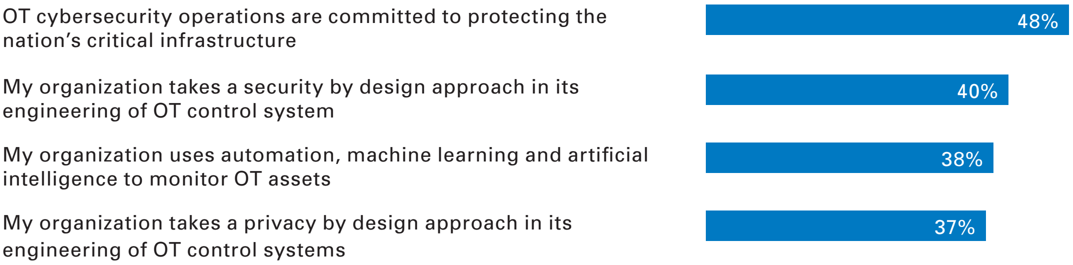


ORGANIZATIONS ARE LAGGING BEHIND IN ADOPTING ADVANCED SECURITY TECHNOLOGIES

Only 38 percent of respondents say their organizations are using automation, machine learning and artificial intelligence to monitor OT assets, as shown in Figure 16. The majority of companies are not integrating security and privacy by design in the engineering of OT control systems, only 40 percent and 37 percent of respondents say they are taking such steps, respectively.

FIGURE 16:

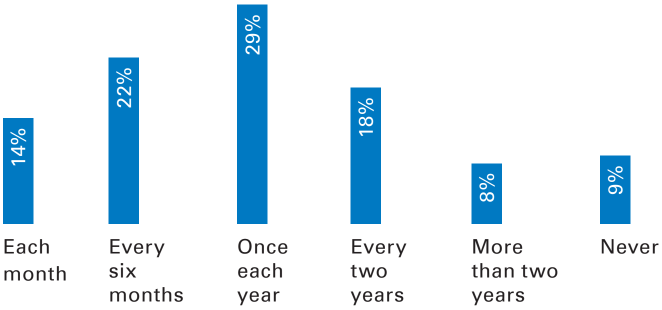
Perceptions about the use of technology to manage OT risk[1]



[1] Strongly agreed and Agreed response combined

FIGURE 17:

How often does your organization conduct comprehensive audits of its supply chain?



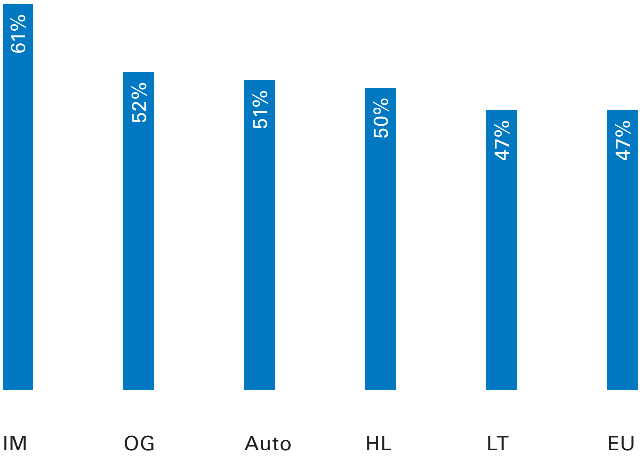
As discussed previously, almost half of respondents (49 percent) say that mitigating cyber risks across the OT supply chain is difficult. However, only 36 percent of respondents say their organization conducts a comprehensive audit of its supply chain each month or every six months.

The state of industrial security varies among industries.

INDUSTRIAL AND MANUFACTURING ORGANIZATIONS HAVE THE MOST DIFFICULTY IN MITIGATING CYBER RISKS, ACCORDING TO 61 PERCENT OF RESPONDENTS

In this section, we analyze the differences among the industries represented in this study: automotive (Auto, 346 respondents), oil and gas (OG 344 respondents), energy and utilities (EU, 319 respondents), health and life science (HL 462 respondents), industrial and manufacturing (IM 440 respondents) and logistics and transportation (LT 347 respondents). According to Figure 18, the majority of respondents in oil and gas, automotive and health and life science report difficulties according to 52 percent, 51 percent and 50 percent of respondents.

FIGURE 18:
My organization has difficulty in mitigating cyber risks across the OT supply chain[1]



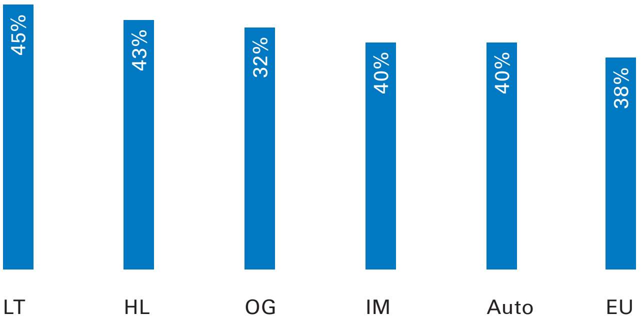
[1] Strongly agree and Agree responses combined

LOGISTICS AND TRANSPORTATION ORGANIZATIONS ARE MOST LIKELY TO USE SUCH ADVANCED TECHNOLOGIES AS AUTOMATION, MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE

45 percent of respondents in logistics and transportation say their organizations have adopted these technologies. Only 38 percent of respondents in energy and utilities organizations use these technologies, as shown in Figure 19.

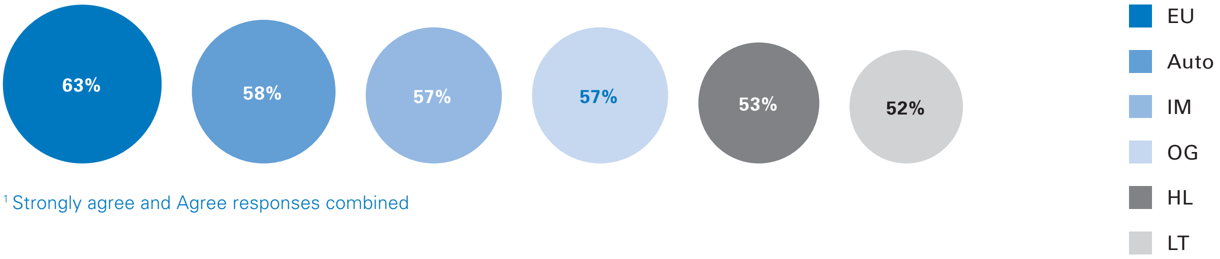
63 percent of respondents in energy and utilities say renewables and edge technologies are increasing cyber risk to the OT environment followed by automotive (58 percent), industrial and manufacturing (57 percent) and oil and gas (57 percent), as shown in Figure 20.

FIGURE 19:
My organization uses automation, machine learning and artificial intelligence to monitor OT assets[1]



[1] Strongly agree and Agree responses combined

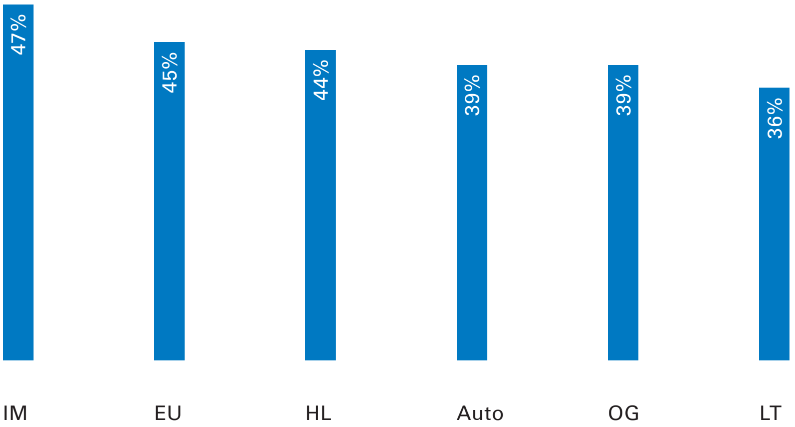
FIGURE 20:
Renewables and edge technologies are increasing cyber risk to the OT environment[1]



[1] Strongly agree and Agree responses combined

Industrial and manufacturing organizations are most likely to take a security by design approach, according to 47 percent of respondents. As shown in Figure 21, logistics and transportation is least likely to take this approach.

FIGURE 21:
My organization takes a security by design approach in its engineering of OT control systems[1]

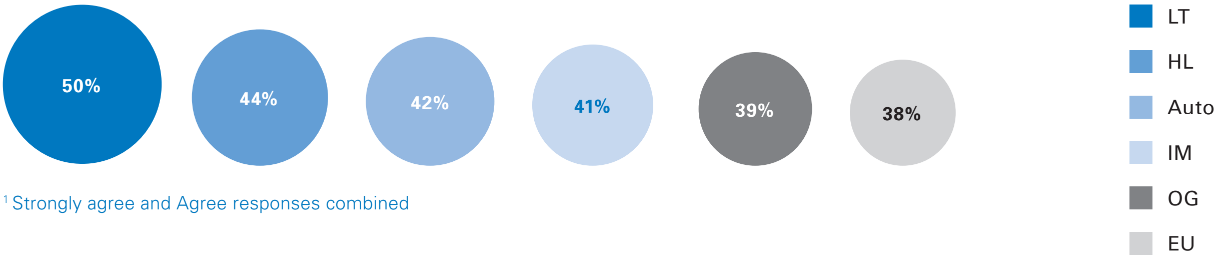


[1] Strongly agree and Agree responses combined

ORGANIZATIONS ARE UNDERSTAFFED TO SUPPORT ORGANIZATIONS' CYBERSECURITY OBJECTIVES OR MISSIONS IN THE OT ENVIRONMENT

As shown in Figure 22, only 39 percent of respondents in oil and gas and 38 percent of respondents in energy and utilities say their organization's staffing levels are adequate for meeting cybersecurity objectives in the OT environment.

FIGURE 22:
Is your organization's staffing level adequate for meeting cybersecurity objectives or mission in the OT environment?[1]



[1] Strongly agree and Agree responses combined

Methods.

A sampling frame of 60,706 IT and IT security practitioners in the following industries: automotive, oil and gas, energy and utilities, health and life science, industrial manufacturing and logistics and transportation were selected as participants to this survey. All respondents are responsible for securing or overseeing cyber risks in the OT environment and are aware of how cybersecurity threats could affect their organization. As shown in Table 1, 2,602 respondents completed the survey. Screening removed 344 surveys resulting in a final sample of 2,258 for a 3.7 percent response rate.

Table 1. Sample response	**Freq**	**Pct%**
Total sampling frame	60,706	100.0%
Total returns	2,602	4.3%
Rejected surveys	344	0.6%
Final sample	2,258	3.7%

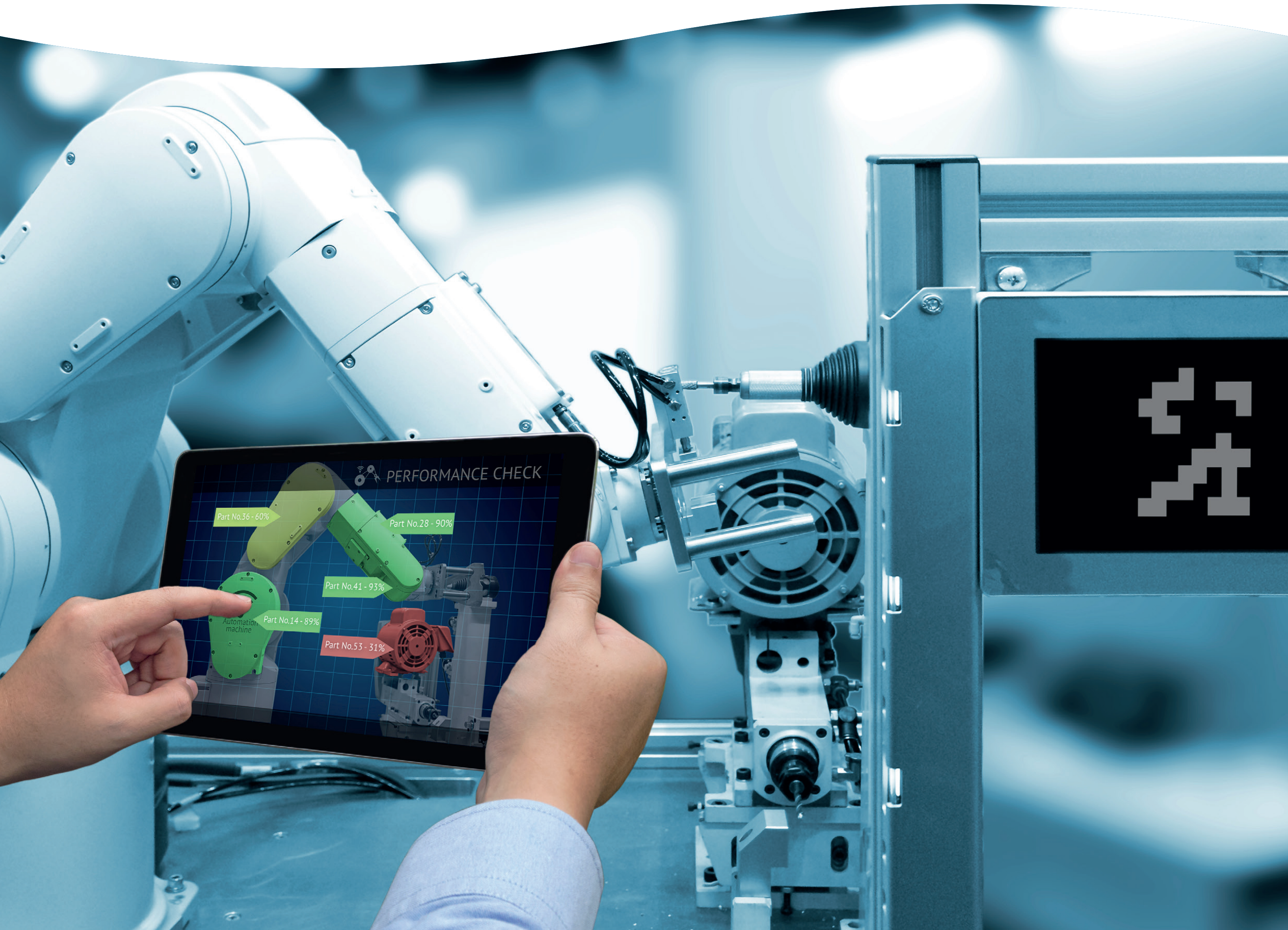


Chart 1 reports the current position or organizational level of the respondents. More than half of respondents (63 percent) reported their current position as supervisory or above and 31 percent of respondents are at the technician level.

CHART 1:
Distribution of respondents according to position level

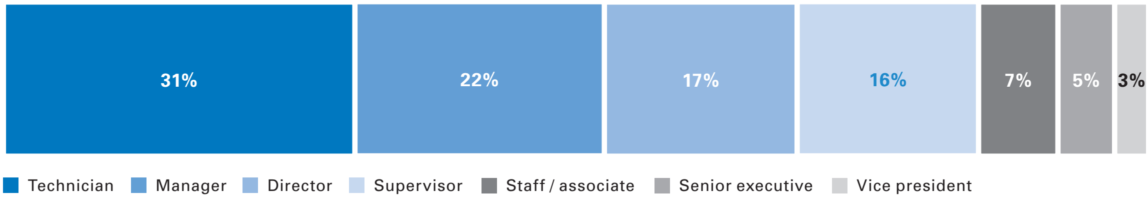
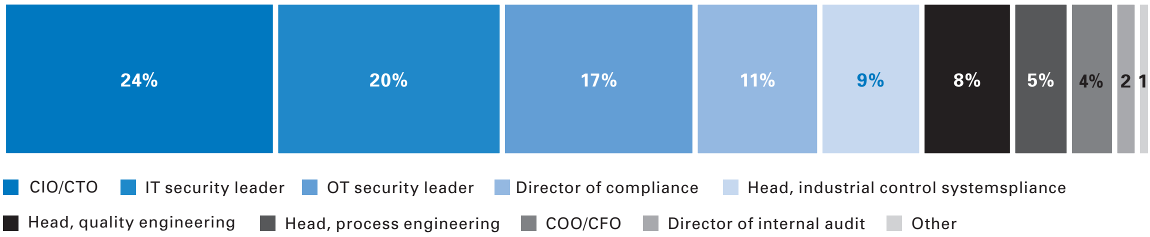


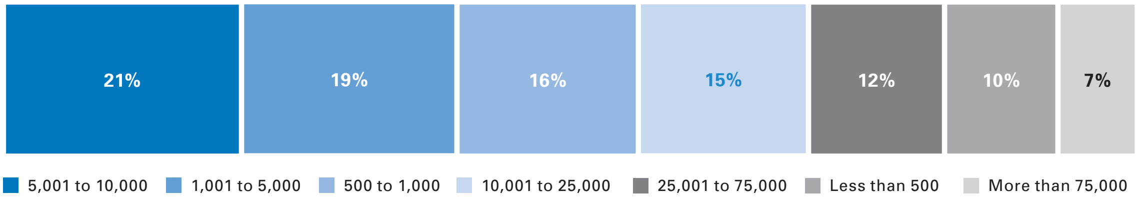
Chart 2 reveals that 24 percent of respondents report to the CIO/CTO, 20 percent of respondents report to the IT security leader, 17 percent of respondents report to the OT security leader, 11 percent of respondents report to the director of compliance and 9 percent of respondents report to the head of industrial control systems.

CHART 2:
Primary person respondent reports to within the organization



As shown in Chart 3, more than half of respondents (55 percent) are from organizations with a global headcount of more than 5,000 employees.

CHART 3:
Global employee headcount



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 IT security practitioners in automotive, oil and gas, energy and utilities, health and life science, industrial manufacturing and logistics and transportation organizations. 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.

Appendix: Detailed Survey Results.

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured from December 8, 2019 to December 23, 2019.

Survey response	Total
Total sampling frame	60,706
Total returns	2,602
Rejected surveys	344
Final sample	2,258
Response rate	3.7%

PART 1. SCREENING QUESTIONS

S1. What best describes your organizations' primary industry sector?	Total
Automotive	346
Oil & Gas	344
Energy & Utilities	319
Health & Life Sciences	462
Industrial Manufacturing	440
Logistics & Transportation	347
None of the above (stop)	–
Total	2.258

S2. Does your job involve securing or overseeing cyber risks in the operational technology (OT) environment?	Total
Yes, full responsibility	35%
Yes, some responsibility	45%
No responsibility (stop)	22%
Total	100%

S3. What best defines your level of awareness about how cybersecurity impacts (or could impact) the state of cybersecurity within you company?	Total
High level of awareness	40%
Moderate level of awareness	36%
Low level of awareness	24%
No awareness (stop)	0%
Total	100%

PART 2. TRENDING QUESTIONS: Q1 TO Q10 ARE QUESTIONS USED TO TREND FY2019 TO FY2020

Q1. Have you ever conducted an operational technology cybersecurity risk assessment?	**Total**
Never	32%
Don’t know	5%
Yes, in the past year	29%
Yes, in the past 5 years	34%
Total	100%

Q2. Are you able to detect all the endpoints on your operational technology network?	**Total**
No	27%
Yes, automatically	37%
Yes, manually	32%
Don’t know	4%
Total	100%

Q3. In the past year, have you lost operational technology-related intellectual property (IP) as a result of data theft?	**Total**
No	40%
Don’t know	36%
Yes	24%
Total	100%

Q4. Do your customers explicitly ask you to demonstrate that you have taken steps to secure your OT network?	**Total**
No	63%
Yes, a few	24%
Yes, all of them	13%
Total	100%

Q5. Do you actively share operational technology threat-related intelligence with your peers?	**Total**
Yes	37%
No	44%
Occasionally, but nothing formal	13%
Don’t know	6%
Total	100%

Q6. Do you continuously monitor your operational technology network for cybersecurity threats?	**Total**
No	43%
Yes, but only ad hoc	19%
Yes, we have a solution that monitors the network 24/7	32%
Don’t know	5%
Total	100%

Q7. In the past year, has the number of operational technology-related cybersecurity threats to your business...	**Total**
Increased	47%
Decreased	16%
Stayed the same	34%
Don't know	3%
Total	100%

Q8. Approximately what percentage of your IT/OT budget do you allocate specifically to OT cybersecurity? (Chose closest value)	**Total**
1 to 5%	4%
6 to 10%	13%
11 to 15%	24%
16 TO 20%	31%
More than 20%	28%
Total	100%
Extrapolated value	17%

Q9. Within your OT cybersecurity strategy what area provides the most complex challenge?	**Total**
Retaining qualified staff	21%
Recruiting enough qualified staff	20%
Lack of executive understanding of the issues	19%
Budgets too small	36%
Other	3%
Total	100%

Q10. Do you assess or review cybersecurity issues when conducting safety-related assessments?	**Total**
No	27%
Yes	49%
Sometimes	19%
Don't know	4%
Total	100%

PART 3. STATE OF OT SECURITY: PLEASE RATE EACH ONE OF THE FOLLOWING 10 STATEMENTS USING THE SCALE PROVIDED BELOW EACH ITEM. STRONGLY AGREED AND AGREED RESPONSE COMBINED

	Total
Q11a. My organization has difficulty in mitigating cyber risks across the OT supply chain.	49%
Q11b. Cyber threats present a greater risk in the OT than the IT environment.	48%
Q11c. Renewables and edge technologies are increasing cyber risk to the OT environment.	57%
Q11d. My organization is at risk because of uncertainty about the cybersecurity practices of third parties.	52%
Q11e. In my organization, OT and IT security risk management efforts are fully aligned.	37%
Q11f. My organization's security operations and/or business continuity management team anticipate one or more serious attacks within the OT environment.	57%
Q11g. My organization uses automation, machine learning and artificial intelligence to monitor OT assets.	38%
Q11h. My organization's OT cybersecurity operations are committed to protecting the nation's critical infrastructure.	48%
Q11i. My organization takes a privacy by design approach in its engineering of OT control systems.	37%
Q11j. My organization takes a security by design approach in its engineering of OT control systems.	40%

PART 4. STRATEGY & GOVERNANCE IN THE OT ENVIRONMENT

Q12. What are the top OT priorities for your organization? Please select the top three.	**Total**
Creating shareholder value	16%
Minimizing unplanned outages	44%
Achieving a high level of workplace safety	44%
Increasing revenues	28%
Reducing inefficiencies and minimizing operating costs	48%
Achieving a high level of environmental sustainability	23%
Creating a productive and positive work environment	41%
Achieving a strong security posture	52%
Other (please specify)	4%
Total	300%

Q13. Using the following 10-point scale, please rate your organization's cyber readiness in the OT environment. 1 = low readiness to 10 = high readiness	**Total**
1 or 2	10%
3 or 4	11%
5 or 6	29%
7 or 8	25%
9 or 10	26%
Total	100%
Extrapolated value	6.45

Q14. Using the following 10-point scale, please rate your organization's ability to minimize the risk of cyber exploits and breaches in the OT environment. 1 = low ability to 10 = high ability	**Total**
1 or 2	10%
3 or 4	13%
5 or 6	31%
7 or 8	26%
9 or 10	20%
Total	100%
Extrapolated value	6.15

Q15. Using the following 10-point scale, please rate your organization's ability to comply with emerging regulations such as the NIS Directive and other data protection regulations in the OT environment. 1 = low and 10 = high.	**Total**
1 or 2	7%
3 or 4	13%
5 or 6	32%
7 or 8	29%
9 or 10	18%
Total	100%
Extrapoalated value	6.26

Q16. Please rate the importance of plant connectivity using the following 10-point scale from 1 = low importance to 10 = high importance.	**Total**
1 or 2	5%
3 or 4	8%
5 or 6	15%
7 or 8	31%
9 or 10	40%
Total	100%
Extrapoalated value	7.34

Q17. Using the following 10-point scale, please rate the level of alignment between OT and IT with respect to cybersecurity objectives from 1 = no alignment (completely separate) and 10 = full alignment.	**Total**
1 or 2	13%
3 or 4	17%
5 or 6	26%
7 or 8	27%
9 or 10	18%
Total	100%
Extrapoalated value	5.89

Q18. Using the following 10-point scale, please rate the level of alignment between privacy and security with respect to cybersecurity objectives from 1 = no alignment (completely separate) and 10 = full alignment.	**Total**
1 or 2	14%
3 or 4	17%
5 or 6	26%
7 or 8	21%
9 or 10	22%
Total	100%
Extrapolated value	5.92

Q19. Does your organization have an OT incident response plan?	**Total**
Yes	49%
No	51%
Total	100%

Q20. Who is the primary person for ensuring cybersecurity objectives in the OT environment? Please select one choice only.	**Total**
COO/CFO	6%
CIO/CTO	18%
IT security leader	17%
OT security leader	20%
Head, industrial control systems	8%
Head, process engineering	7%
Head, quality engineering	5%
Head, product engineering	4%
Head of safety	2%
Head, risk management (CRO)	5%
Director of compliance	5%
Director of internal audit	2%
Other (please specify)	1%
Total	100%

Q21. What best describes your organization's primary motivation for administering an OT cybersecurity program? Please select your top two choices.	**Total**
To manage risk	65%
To ensure compliance with regulations	43%
To ensure compliance with standards	51%
To be competitive with peer organizations	23%
To achieve digitalization	18%
Other (please specify)	0%
Total	200%

Q22. How many employees in your organization are dedicated to cybersecurity operations in the OT environment?	**Total**
None	14%
1 to 10	11%
11 to 25	32%
26 to 50	23%
51 to 100	10%
More than 100	10%
Total	100%
Extrapolated value	34.56

Q23. Is your organization's staffing level adequate for meeting cybersecurity objectives or mission in the OT environment?	**Total**
Yes	43%
No	58%
Total	100%

Q24. Please rate the overall "pain" associated with managing cybersecurity within the OT environment, where 1 = minimal pain to 10 = severe pain?	**Total**
1 or 2	4%
3 or 4	8%
5 or 6	12%
7 or 8	34%
9 or 10	42%
Total	100%
Extrapoalated value	7.56

Q25. If you rated overall pain at 6 or above, what makes the management of OT security painful? Please select the top four (4) reasons.	**Total**
No clear ownership	13%
Insufficient resources (time/money)	48%
Lack of skilled personnel	42%
No clear understanding of requirements	9%
Management tools are inadequate	18%
Systems are isolated and fragmented	35%
Standards are immature	18%
Manual processes are prone to errors and unreliable	31%
Maintaining an up-to-date view of digital assets in the network	25%
Lack of rapid detection of security exploits and data breaches	24%
Lack of enabling technologies in OT networks	54%
Complexity	53%
Rise of sophisticated attacks (e.g. nation-state attacks)	29%
Other (please specify)	1%
Total	400%

Q26. Who does your organization trust most to provide OT cyber expertise? Please select one choice.	**Total**
Consultants that specialize in OT	25%
Managed security service providers (MSSPs)	20%
Traditional IT companies	13%
Defense contractors	24%
Government	15%
Other (please specify)	3%
Total	100%

Q27. Does your organization transfer industrial security data off-premises for monitoring or forensic purposes?	**Total**
Yes	50%
No	50%
Total	100%

Q28. With respect to OT cybersecurity, where is your organization in making significant is investments today or in the near term? Please rank order the following five investment categories from 1 = largest to 5 = smallest investment category.	**Total**
Technologies	1.6
Personnel	2.3
Training	4.2
Compliance	4.8
Infrastructure	2.9

Q29a. Following are 8 technologies or managed services that seek to foster security and compliance with standards. For each technology or managed service listed, please check all used by your organization today or that you planned to be use within the next 12 months.	**Total**
OT Inventory & Asset Management System	46%
Industrial Firewalls	43%
Data Diodes	30%
Hardened Endpoints/PLC	54%
OT Network Monitoring & Threat Detectione	53%
Patch Management for OT	28%
Secure Remote Access	23%
PLC Integrity & Data Monitoring	32%
Total	309%

Q29b. For each item either used or planned to be used, indicate the effectiveness of each technology or managed service with respect to achieving a strong cybersecurity posture within your organization. Please use the following 5-point effectiveness scale: 1 = not effective, 2 = minimally effective, 3 = somewhat effective, 4 = effective, 5 = very effective.	**Total**
Cybersecurity technologies and services within your organization	3.9
OT Inventory & Asset Managemaent System	3.5
Industrial Firewalls	4.0
Data Diodes	2.8
Hardened Endpoints/PLC	4.2
OT Network Monitoring & Threat Detection	3.5
Patch Management for OT	2.3
Secure Remote Access	3.3
PLC Integrity & Data Monitoring	2.8
Average	3.4

Q30. How often does your organization conduct comprehensive audits of its supply chain?	**Total**
Each month	14%
Every six months	22%
Once each year	29%
Every two years	18%
More than two years	8%
Never	9%
Total	100%

PART 5. CYBER RISK IN THE OT ENVIRONMENT

Q31. Please rate your organization's effectiveness in completing each task using a 10-point scale below each item. 1 = low to 10 = high.	
Q31a. The ability to pinpoint sources of attacks and mobilize the right set of technologies and resources to remediate the attack	**Total**
1 or 2	10%
3 or 4	17%
5 or 6	26%
7 or 8	25%
9 or 10	22%
Total	100%
Extrapolated value	6.12

Q31b. Continually monitor the infrastructure to prioritize threats and attacks	**Total**
1 or 2	8%
3 or 4	16%
5 or 6	29%
7 or 8	25%
9 or 10	22%
Total	100%
Extrapolated value	6.24

Q31c. Assess risks to determine resources necessary to address the risks	Total
1 or 2	8%
3 or 4	12%
5 or 6	29%
7 or 8	25%
9 or 10	26%
Total	100%
Extrapolated value	6.50

Q31d. Determine the highest value information assets that need to be safeguarded	Total
1 or 2	12%
3 or 4	10%
5 or 6	29%
7 or 8	27%
9 or 10	22%
Total	100%
Extrapoalated value	6.24

Q31e. Determine how and by whom the organization is targeted for attack	Total
1 or 2	9%
3 or 4	16%
5 or 6	27%
7 or 8	22%
9 or 10	25%
Total	100%
Extrapoalated value	6.24

Q31f. Ability to respond to and contain a security exploit or breach	Total
1 or 2	11%
3 or 4	16%
5 or 6	24%
7 or 8	22%
9 or 10	26%
Total	100%
Extrapoalated value	6.22

Q31g. Ability to detect sophisticated zero-day threats	Total
1 or 2	8%
3 or 4	14%
5 or 6	26%
7 or 8	26%
9 or 10	27%
Total	100%
Extrapoalated value	6.50

Q31h.Ability to achieve comprehensive and continuous discovery and inventory of digital assets	**Total**
1 or 2	9%
3 or 4	14%
5 or 6	26%
7 or 8	27%
9 or 10	24%
Total	100%
Extrapolated value	6.37

Q31i. Manage security alerts and translate them to actionable recommendations	**Total**
1 or 2	13%
3 or 4	15%
5 or 6	22%
7 or 8	26%
9 or 10	25%
Total	100%
Extrapoalated value	6.21

Q31j. Understand operational implications of cyber alerts and events	**Total**
1 or 2	10%
3 or 4	11%
5 or 6	30%
7 or 8	24%
9 or 10	26%
Total	100%
Extrapoalated value	6.39

Q32. Which of the follow megatrends will increase risk to your organization?	**Total**
Digital transformation	49%
Use of drones	22%
Internet of Things (IoT) in the workplace	48%
Quantum computing	13%
Block chain	38%
Artificial intelligence/machine learning	58%
Robotics	19%
Other (please specify)	3%
Total	250%

Q33. What are the top cybersecurity threats that may affect critical operations in the OT environment? Check only the top four choices.	**Total**
DNS-based denial of service attacks	41%
Electronic agents such as viruses, worms, malware, botnets and others	35%
Insecure endpoints	31%
Insecure web applications	40%
Malicious or criminal insiders	27%
Negligent insiders	39%
Phishing and social engineering	41%
Ransomware	41%
Third-party mistakes	30%
Waterholing	15%
Web-based attacks	29%
Zero-day attacks	27%
Other (pleasea specify)	6%
Total	400%

Q34. What are the top barriers to minimizing OT-related risk in your organization? Please select your top four choices only.	**Total**
Lack of cybersecurity awareness and training among employees	40%
Remote work during operations and maintenance	28%
Using standard IT products with known vulnerabilities in the production environment	43%
A limited cybersecurity culture among vendors, suppliers and contractors	32%
Insufficient separation of data networks	25%
The use of mobile devices and storage units, including smartphones	40%
Data networks between on-and offshore facilities	30%
Insufficient physical security of data rooms, cabinets etc.	44%
Vulnerable software	52%
Outdated and aging control systems in facilities	61%
Other (please specify)	4%
Total	400%

PART 6. EXPLOITS & SECURITY BREACHES

Q35. How often has your organization suffered a security compromise that resulted in the loss of confidential information or disruption to operations in the OT environment over the past 12 months?	**Total**
None	21%
Once	29%
2 to 5	26%
6 to 10	15%
More than 10 incidents	8%
Total	100%
Extrapolated value	3.62

Q36. What percentage of all cyberattacks in the OT environment are detected?	**Total**
None	5%
1 to 10%	15%
11 to 25%	24%
26 to 50%	33%
51 to 75%	15%
76 to 100%	8%
Total	100%
Extrapolated value	34%

PART 7. OT SECURITY BUDGET

Q37. What is the total IT annual budget for cybersecurity operations and defense (OT and IT combined)?	**Total**
Less than $1 million	3%
$1 to $5 million	6%
$6 to $10 million	12%
$11 to $15 million	13%
$16 to $20 million	15%
$21 to $25 million	16%
$26 to $50 million	14%
$51 to $100 million	11%
$101 to $500 million	6%
More than 500 million	4%
Total	100%
Extrapolated value (US$ millions)	$64.0

Q38. What percentage of the total IT cybersecurity budget is allocated the security of OT assets and infrastructure?	**Total**
None	12%
1 to 10%	29%
11 to 25%	25%
26 to 50%	15%
51 to 75%	11%
76 to 100%	8%
Total	100%
Extrapolated value	26%

PART 8. YOUR ROLE & ORGANIZATION

D1. What organizational level best describes your current position?	**Total**
Senior executive	5%
Vice president	3%
Director	17%
Manager	22%
Supervisor	16%
Technician	31%
Staff / associate	7%
Other (please specify)	0%
Total	100%

D2. Check the Primary Person you or your supervisor reports to within the organization.	**Total**
OT security leader	17%
Head, industrial control systems	9%
Head, process engineering	5%
Head, quality engineering	8%
IT security leader	20%
COO/CFO	4%
CIO/CTO	24%
Director of compliance	11%
Director of internal audit	2%
Other (please specify)	1%
Total	100%

D4. What is the worldwide headcount of your organization?	**Total**
Less than 500	10%
500 to 1,000	16%
1,001 to 5,000	19%
5,001 to 10,000	21%
10,001 to 25,000	15%
25,001 to 75,000	12%
More than 75,000	7%
Total	100%

About Ponemon Institute.

Advancing Responsible Information Management
Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

www.ponemon.org

About TÜV Rheinland.

For more than 20 years, TÜV Rheinland's Cybersecurity business has been helping companies from various industries to use innovative technologies securely. Our experts have a high level of industry knowledge about cybersecurity. In an increasingly vulnerable world of networked systems and devices, our cybersecurity solutions aim to combine security and data protection.

Our team carries out cybersecurity tests, industrial security tests and data protection tests on the Internet of Things (IoT) and cloud infrastructures, among others. TÜV Rheinland runs a worldwide network of more than one hundred laboratories, which support manufacturers with a single source for their cybersecurity and data protection demands.

www.tuv.com/fscs

TÜV Rheinland i-sec GmbH
Am Grauen Stein
51105 Cologne
Germany
cybersecurity@tuv.com

tuv.com/fscs

TÜVRheinland®
Precisely Right.