2021 STATE OF INDUSTRIAL CYBERSECURITY

The Risks Created by the Cultural Divide Between IT & OT Teams

Sponsored by Dragos, Inc.
Independently conducted by Ponemon Institute LLC
Publication Date: November 2021

Ponemon Institute© Research Report

The 2021 State of Industrial Cybersecurity

The Risks Created by the Cultural Divide Between the IT & OT Teams

Presented by Ponemon Institute, November 2021

Part 1. Executive Summary

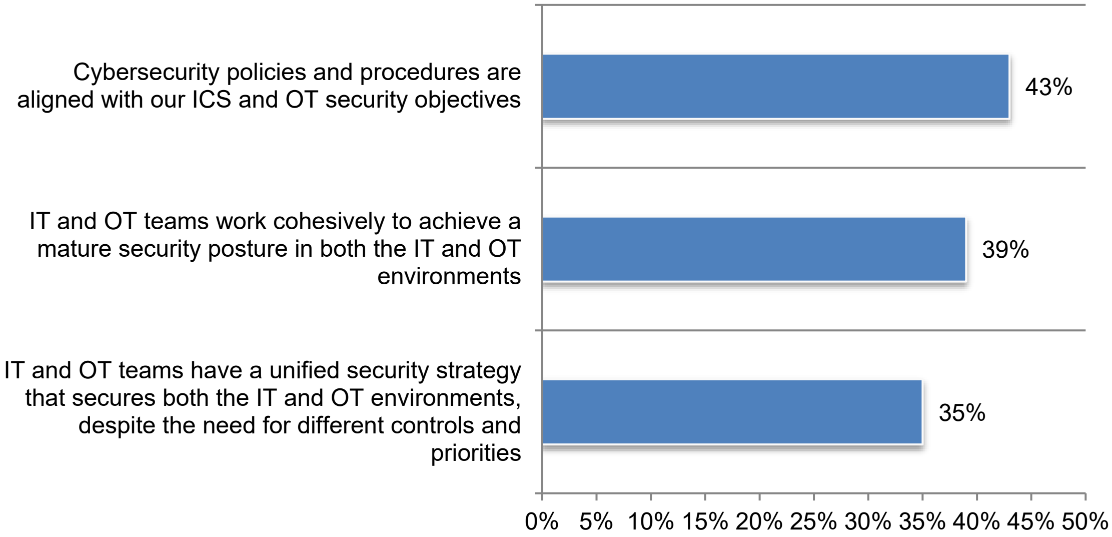
A primary challenge to improving the security of organizations' Industrial Control System (ICS) and Operational Technology (OT) environments, as revealed in this research, is the need to overcome the cultural and technical differences between OT and IT teams. Ideally, organizations should work toward establishing a unified IT and OT approach to addressing the threats and closing the gaps in security that leave organizations vulnerable to cyber attackers. Sponsored by Dragos, Ponemon Institute surveyed 603 IT, IT security and OT security practitioners at the C-level, managerial and director level in the United States. All are familiar with cybersecurity initiatives and ICS and OT security practices within their organizations.

In the context of this research, OT represents the programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). Examples include industrial control systems (ICS), building management systems, safety control systems, and physical access control mechanisms.

ICS encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system components such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components that act together to achieve an industrial objective.

The cultural divide between IT and OT teams affects the ability to secure both the IT and the ICS/OT environment. According to Figure 1, because of the lack of alignment between an organization's cybersecurity policies and procedures with OT and ICS security objectives, only 35 percent of respondents say their IT and OT teams have a unified security strategy that secures both the IT and OT environments, despite the need for different controls and priorities. Only 39 percent of respondents say IT and OT teams work cohesively to achieve a mature security posture in both the IT and OT environments.

Figure 1. Perceptions about IT and OT alignment
Strongly agree and Agree responses combined



The risks created by the cultural divide between the IT & OT Teams

- Fifty percent of respondents are optimistic about the future of their ICS/OT cybersecurity program. However, only 21 percent of respondents say their ICS/OT program activities have achieved full maturity and emerging threats drive priority actions. A fully mature program also means C-level executives and the board of directors are regularly informed about the efficiency, effectiveness, and security of the program. Twenty-nine percent of respondents say their organizations are in the late-middle stage which means C-level support, adequate budget, risk assessment and a cross-functional team of IT and OT SMEs work together cohesively.

- As the frequency and severity of attacks increase, organizations are struggling to keep ahead of these threats. Sixty-three percent of respondents say their organizations had an ICS/OT cybersecurity incident in the past two years.

- For the first time, this research calculates the cost of one cybersecurity incident in the ICS/OT environment. The average cost per cybersecurity incident is $2,989,550 (the calculation is shown in Table 1 of this report). An average of 316 days is spent to detect, investigate and remediate the cybersecurity incident. Based on the use of a threat hunting and incident response team that averages six IT and IT security personnel, it costs an average of $963,168 to detect, investigate and remediate the incident. The fixed costs including the replacement of equipment, downtime, legal and regulatory fines total $2,026,382. This equals the average total cost of $2,989,550.

- The majority of respondents say senior management lacks an understanding about the cyber risks in the ICS/OT environments. As a result, not enough resources are allocated to defend the ICS/OT environments. Paradoxically, according to 56 percent of respondents, the primary blocker for investing in ICS/OT cybersecurity is that ICS/OT cybersecurity is managed by the engineering department, which does not have security expertise followed by 53 percent of respondents who say ICS/OT security is managed by an IT department without engineering expertise.

- The Director/Manager of IT and the VP of Engineering are the functions most respondents in this study report to. However, by far the VP of Engineering is most accountable for the security of the ICS/OT program. Only 12 percent of respondents say the CISO is most accountable for the security of ICS/OT program. Further, only 35 percent of respondents say someone responsible for ICS and OT cybersecurity reports IT and cybersecurity initiatives to the board of directors. Of these respondents, 41 percent say such reporting takes place only when a security incident occurs.

- Only 38 percent of respondents say the security safeguards in place to protect the ICS and OT environments are covered during board meetings and only 36 percent of respondents say the effectiveness and efficiency of security programs and measures are presented.

- Cultural and technical differences must be overcome to have OT and IT teams work cohesively. The challenges often are not caused by a competition for budget dollars and new security projects (only 32 percent of respondents). Rather, it is the cultural and technical differences between traditional IT-specific best practices and what is possible in OT environments, such as patch management and unique requirements of industrial automation equipment vendors that cause conflicts between these two functions (50 percent and 44 percent of respondents, respectively).

- Only 46 percent of respondents say their organizations are effective in gathering intelligence about threats to the ICS/OT environment and 45 percent of respondents say their organizations are effective in discovering and maintaining an inventory of all devices attached anywhere on the OT network throughout the asset lifecycle.

Part 2. Key findings

In this section of the report, we provide an analysis of the research. The complete findings are presented in the Appendix of the report. We have organized the report according to the following topics.

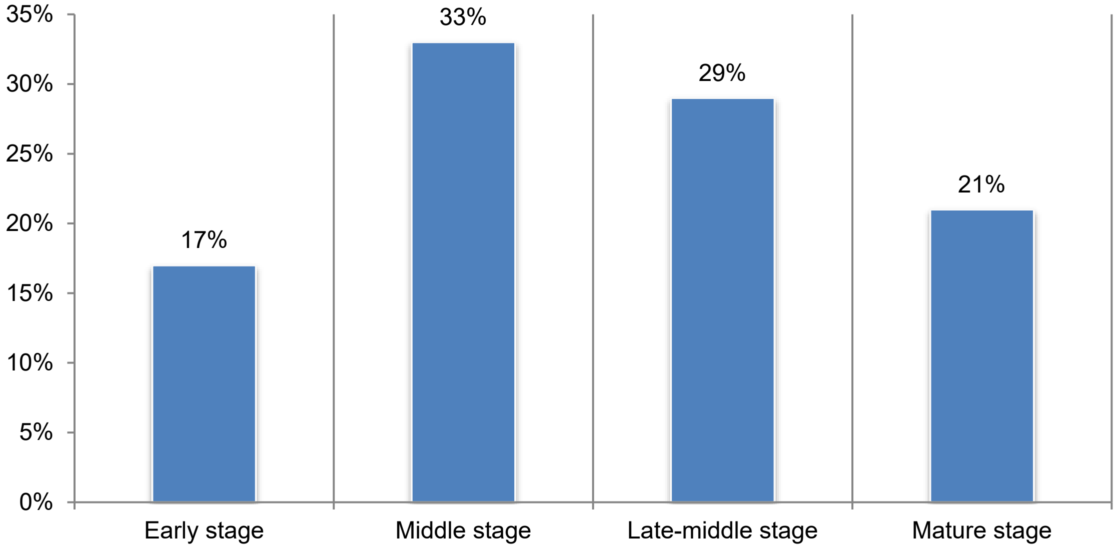
- The level of cybersecurity maturity for ICS/OT
- What does the organization have in place to secure the ICS/OT?
- OT cybersecurity investment, priorities and accountability
- The cause and consequences of an ICS and OT ransomware and cybersecurity incident

The level of cybersecurity maturity for ICS/OT

Fifty percent of respondents say their ICS and OT program activities are mature or in the late middle stage. In the context of this research, the four phases of maturity are described below. According to Figure 2, 50 percent of respondents say their organizations are stalled in the early (17 percent) or middle stage (33 percent), which means ICS and OT program activities have not been planned or deployed or only partially deployed. Only 21 percent of respondents say program activities are fully deployed and senior leadership is regularly informed about the efficiency, effectiveness and security of the program. Twenty-nine percent of respondents say their organizations are in the late-middle stage which means C-level support, adequate budget, risk assessment and a cross-functional team of IT and OT SMEs work together cohesively.

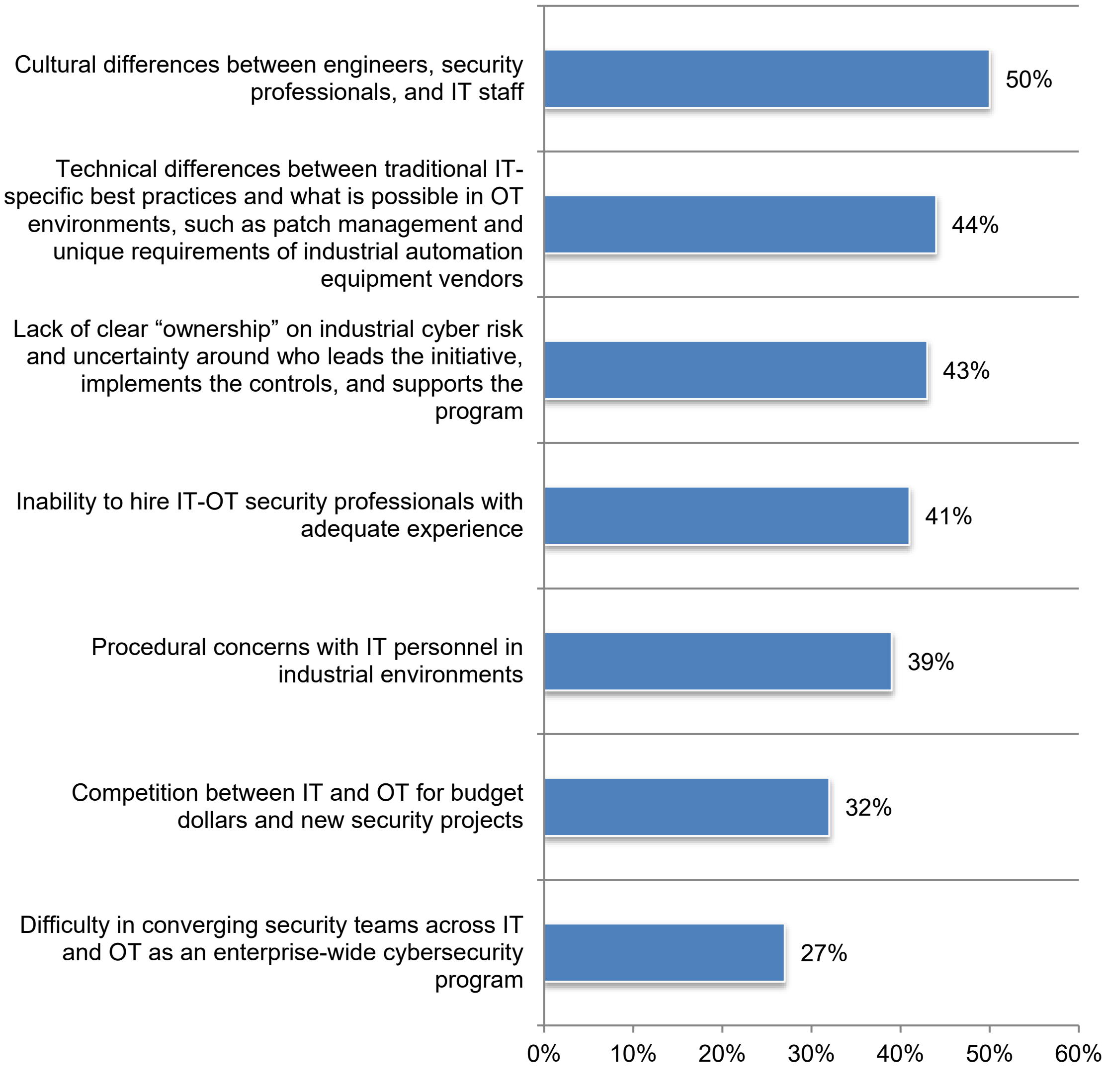
Early stage: Many ICS and OT program activities have not as yet been planned or deployed. Response to threats is reactive and ad hoc. Resources are not sufficient for staffing and investment in the program.
Middle stage: ICS and OT program activities are planned and defined but only partially deployed. Efforts are being made to establish security protocols, develop a workforce of SMEs, prioritize risks, increase investments, and take steps to have IT and OT work cohesively.
Late-middle stage: ICS and OT programs have C-level support and adequate budget. Risks are regularly assessed, and a cross-functional team of IT and OT SMEs work together cohesively.
Mature stage: ICS and OT program activities are fully deployed at target maturity states, emerging threats drive priority actions, and C-level executives and the board of directors are regularly informed about the efficiency, effectiveness, and security of the program.

Figure 2. What best describes the maturity of your organization's ICS/OT cybersecurity program?



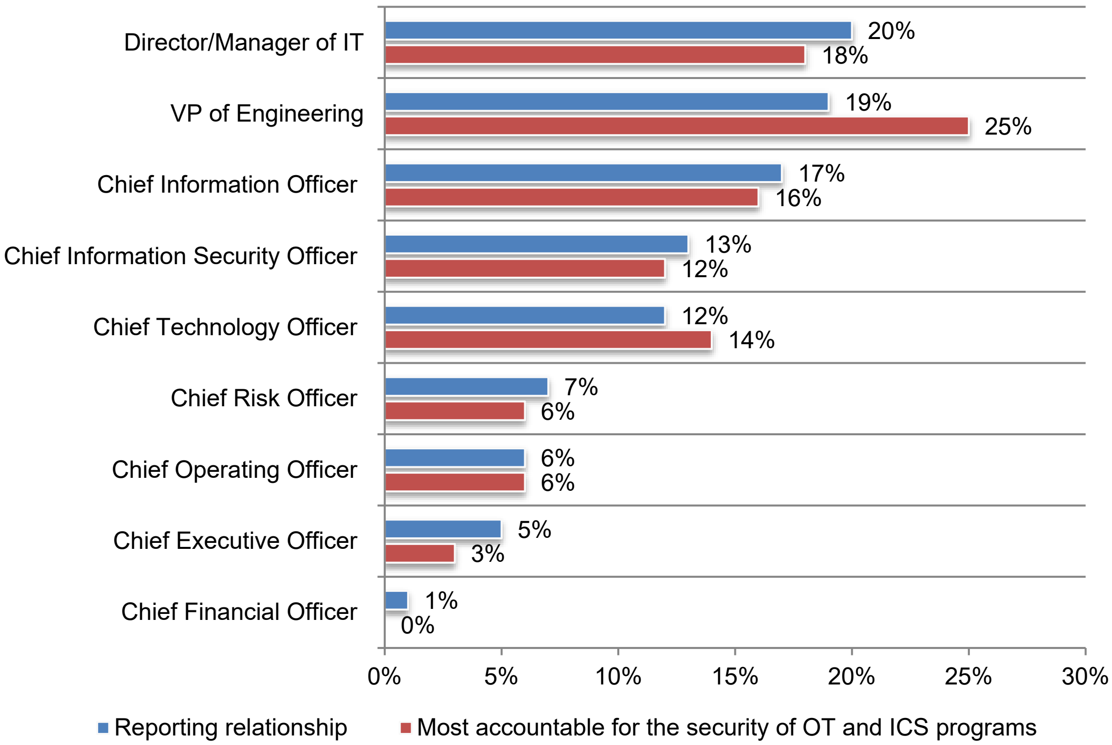
Cultural and technical differences must be overcome to have OT and IT work cohesively. The challenges of working cohesively often are not caused by a competition for budget dollars and new security projects (only 32 percent of respondents). Rather, it is the cultural and technical differences between traditional IT-specific best practices and what is possible in OT environments, such as patch management and unique requirements of industrial automation equipment vendors that cause conflicts between these two functions (50 percent and 44 percent of respondents, respectively), as shown in Figure 3. Also contributing to the cultural divide is the finding that 43 percent of respondents say there is a lack of clear "ownership" on industrial cyber risk and uncertainty around who leads the initiative, implements the controls and supports the program.

Figure 3. What are the primary challenges to having OT and IT work cohesively?
More than one response permitted



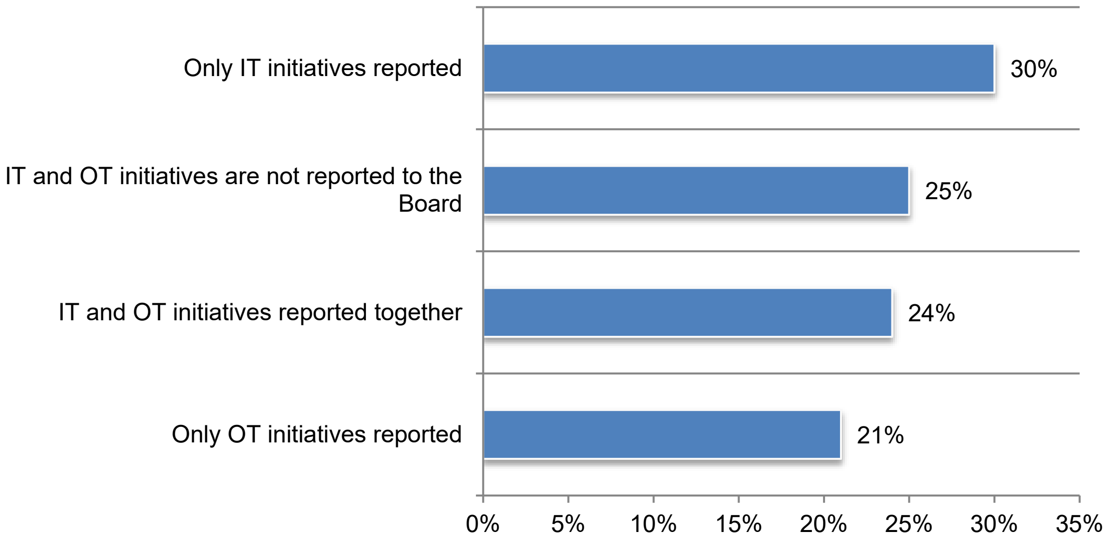
The Director/Manager of IT and the VP of Engineering are the functions most respondents report to, as shown in Figure 4. However, by far the VP of Engineering is most accountable for the security of the ICS/OT program. Only 12 percent of respondents say the CISO is most accountable for the security of ICS/OT program.

Figure 4. Reporting relationships and accountability



According to Figure 5, only 24 percent of respondents say IT and OT cybersecurity initiatives are reported to the board of directors. Twenty-five percent say these initiatives are **not** reported to the board.

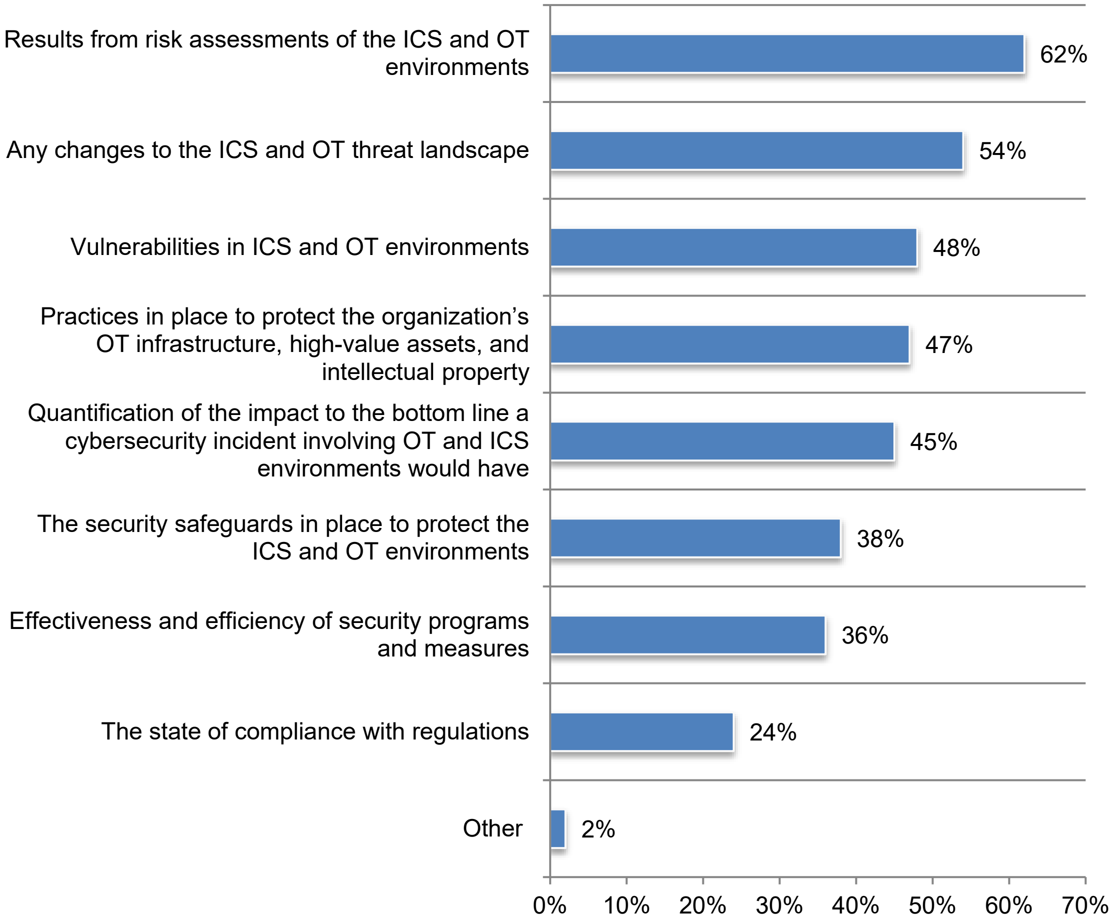
Figure 5. How are IT and OT cybersecurity initiatives reported to the board of directors?



Only 35 percent of respondents who are responsible for ICS and OT cybersecurity report to the board of directors. Of these respondents, 41 percent say such reporting takes place only when a security incident occurs. Fifty-nine percent say reporting takes place annually (17 percent of respondents), bi-annually (18 percent of respondents) or quarterly (24 percent of respondents).

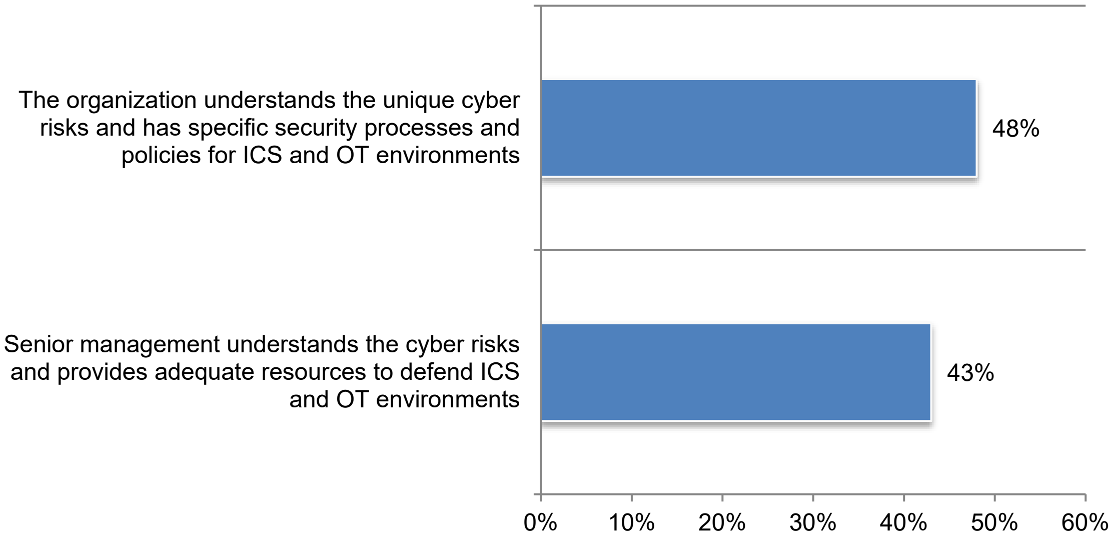
Figure 6 presents the topics covered during board meetings. As shown, the top two topics are the results of ICS and OT risk assessments (62 percent of respondents) and any changes to the ICS and OT threat landscape (54 percent of respondents). Less than half (48 percent) of respondents say vulnerabilities in ICS and OT environments are covered and only 47 percent of respondents say they discuss practices in place to protect the organization’s OT infrastructure, high value assets and intellectual property.

Figure 6. What topics are covered during the board meetings?
More than one response permitted



Many senior managers lack awareness of the risks and threats to the OT and ICS environments. As a result, resources to manage these risks are often inadequate. Less than half (48 percent) of respondents say their organizations understand the unique cyber risks and has specific security processes and policies for OT and ICS environments. Only 43 percent of respondents say senior management understands the cyber risks and provides enough resources to defend OT and ICS environments, according to Figure 7.

Figure 7. Perceptions about tone at the top
Strongly agree and Agree responses combined

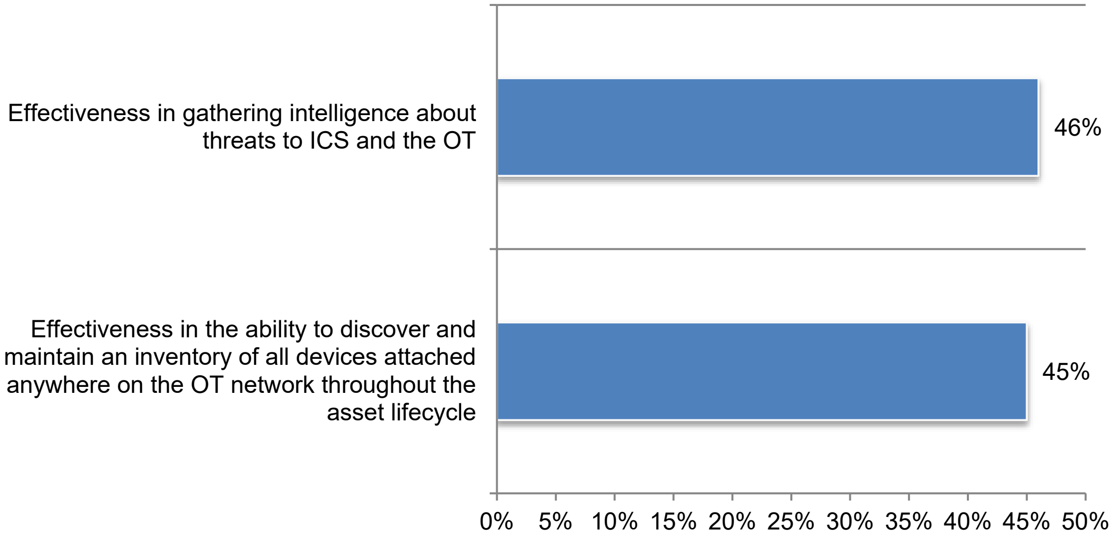


What does the organization have in place to secure the ICS/OT?

As the frequency and severity of attacks increase, organizations are struggling to keep ahead of these threats. Respondents were asked to rate the effectiveness of their intelligence gathering practices to understand threats to the ICS and OT environment, on a scale of 1 = not effective to 10 = highly effective.

As shown in Figure 8, only 46 percent of respondents say their organizations are very effective in gathering intelligence about threats to the ICS and OT. Only 45 percent of respondents say their organizations are very effective in the ability to discover and maintain an inventory of all devices attached anywhere in the OT network throughout the asset lifecycle.

Figure 8. Effectiveness in gathering intelligence about threats and ability to discover and maintain an inventory of all devices attached anywhere on the OT network throughout the asset lifecycle
On a scale of 1 = not effective to 10 = highly effective, 7+ combined responses



Business continuity and compliance risk from industry standards/regulations have financial consequences and are the top cybersecurity risks for organizations. According to Figure 9, only 35 percent of respondents say vulnerable equipment in OT networks is considered a top cybersecurity risk**.** Business continuity and interruption (44 percent of respondents) and compliance risk from industry standards/regulations (42 percent of respondents) are considered a cybersecurity risk. Only 28 percent of respondents say the increased attack surface with connectivity into the OT environment is a top cybersecurity risk.

Figure 9. What are the top three cybersecurity risks for your organization?
Three responses permitted

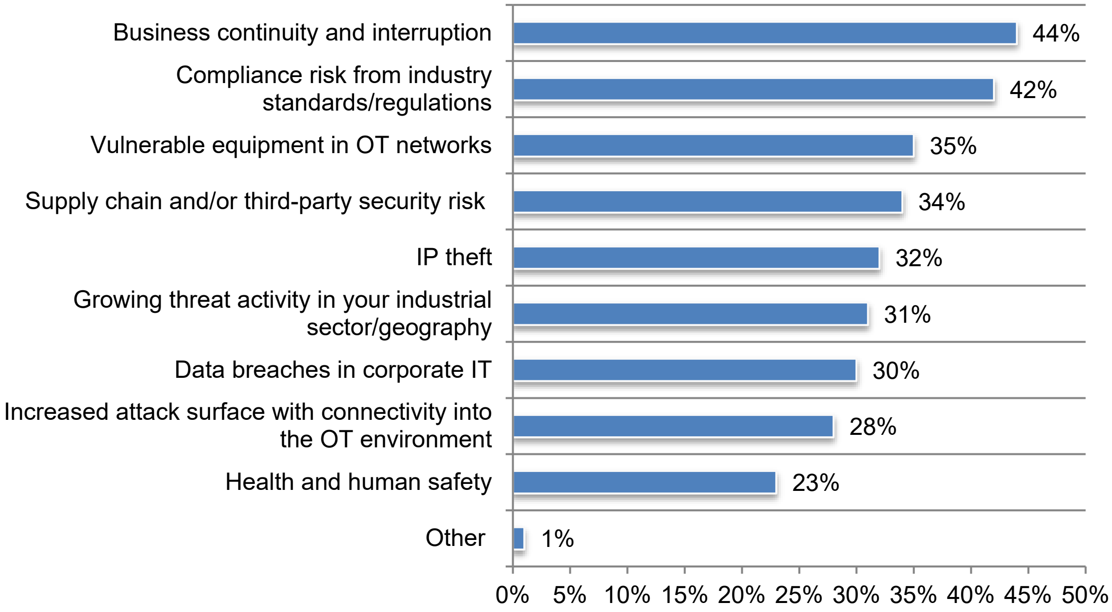


Figure 10 presents a list of capabilities used to secure the ICS/OT environment. As shown, more than half of respondents say their organizations use vulnerability assessments, where appropriate, including prior to commissioning new equipment (57 percent), managing USBs and maintenance laptops in the OT environment (55 percent), OT-specific network detection, including anomaly detection and industrial protocol analysis (52 percent) and physically locking and isolating sensitive equipment where possible (52 percent).

Figure 10. What capabilities are used to secure the ICS/OT environment?
More than one response permitted

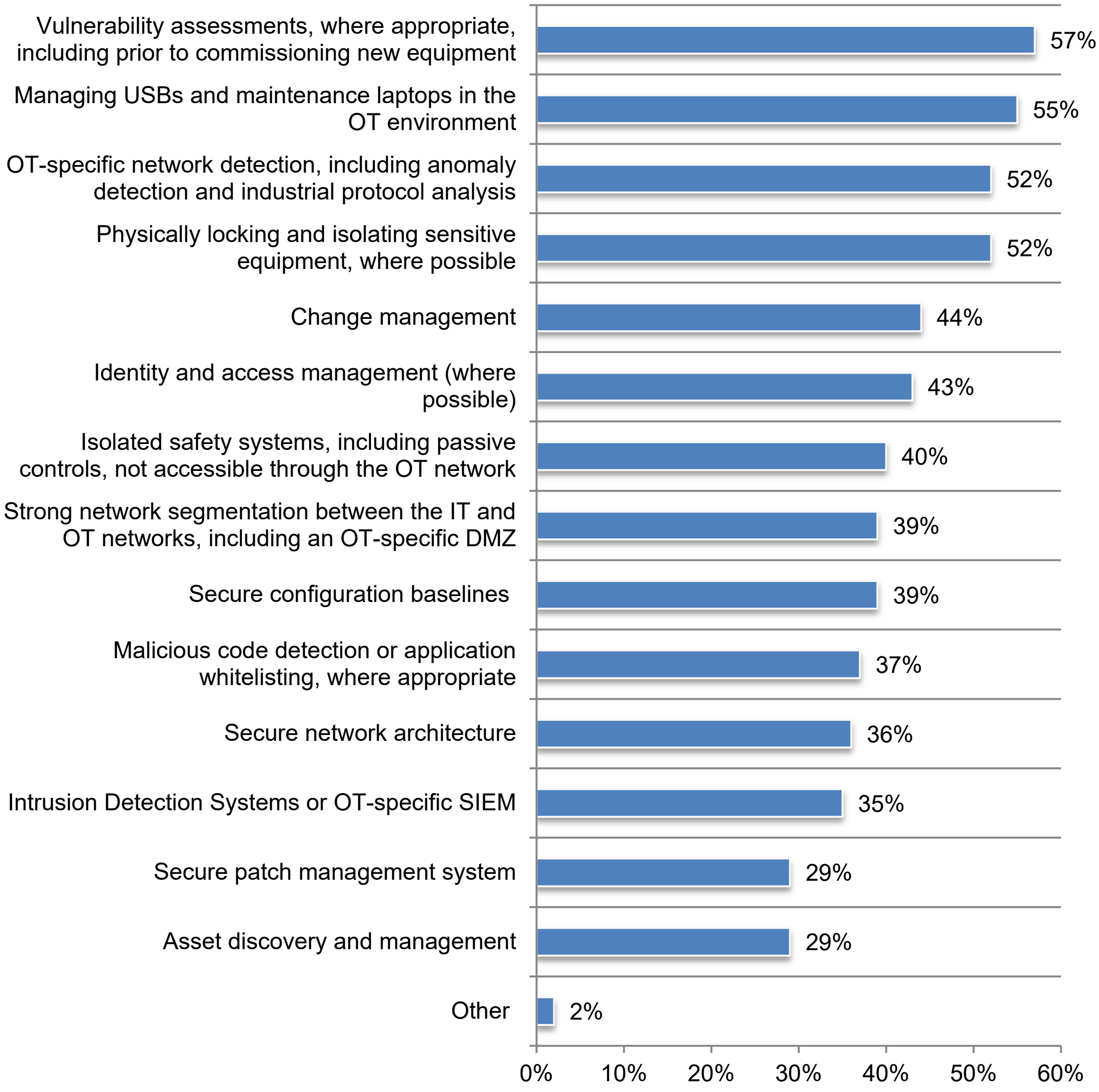
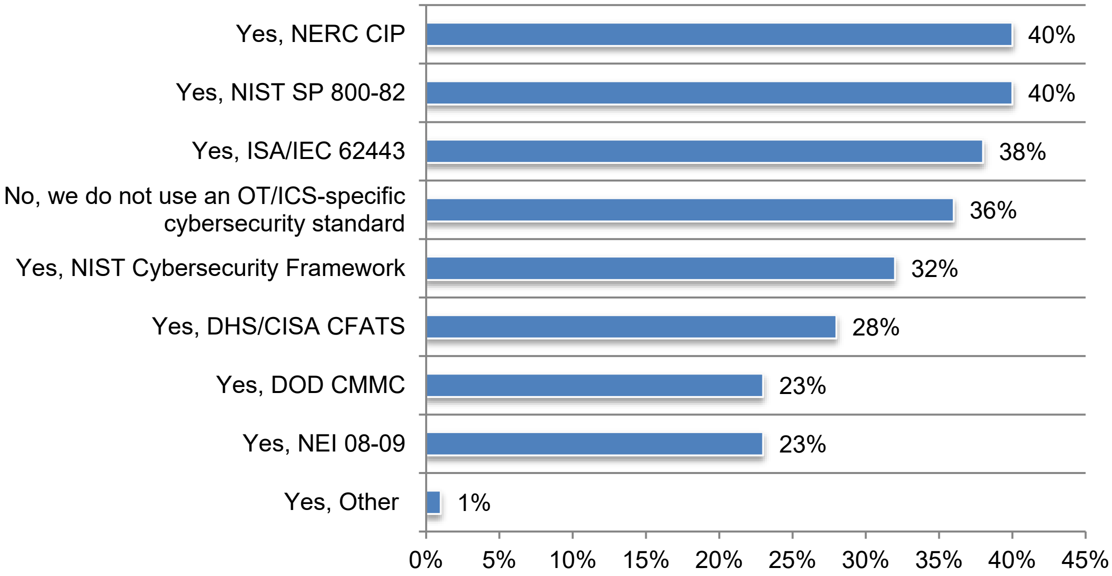


Figure 11 presents the ICS/OT specific cybersecurity standards organizations used to manage their security program. Thirty-six percent of respondents say their organizations do not use an ICS/OT-specific cybersecurity standard. The top two standards are NERC CIP and NIST SP 800-82, both 40 percent of respondents.

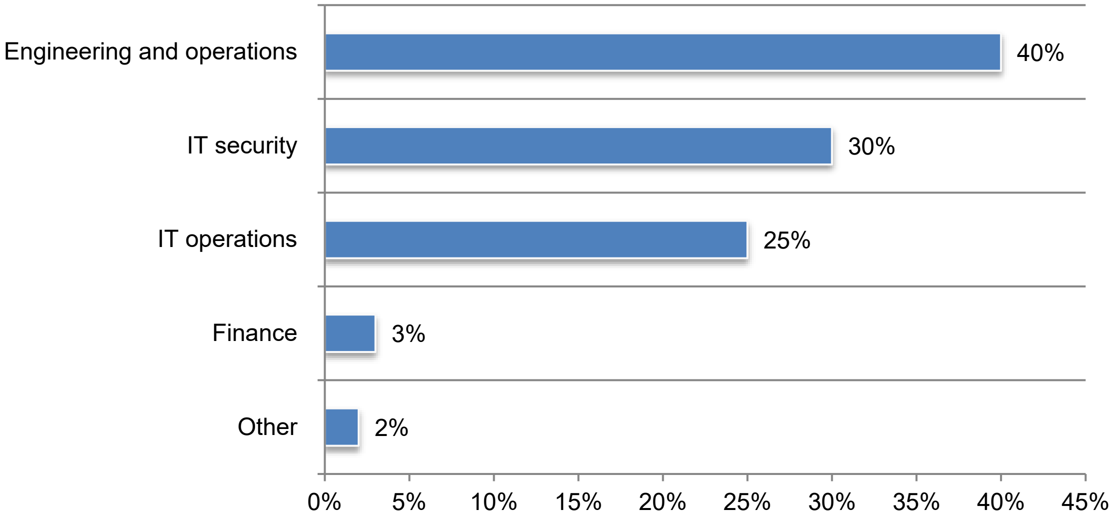
Figure 11. What ICS/OT-specific cybersecurity standards does your organization use to manage its security program?
More than one response permitted



OT cybersecurity investment, priorities and accountability

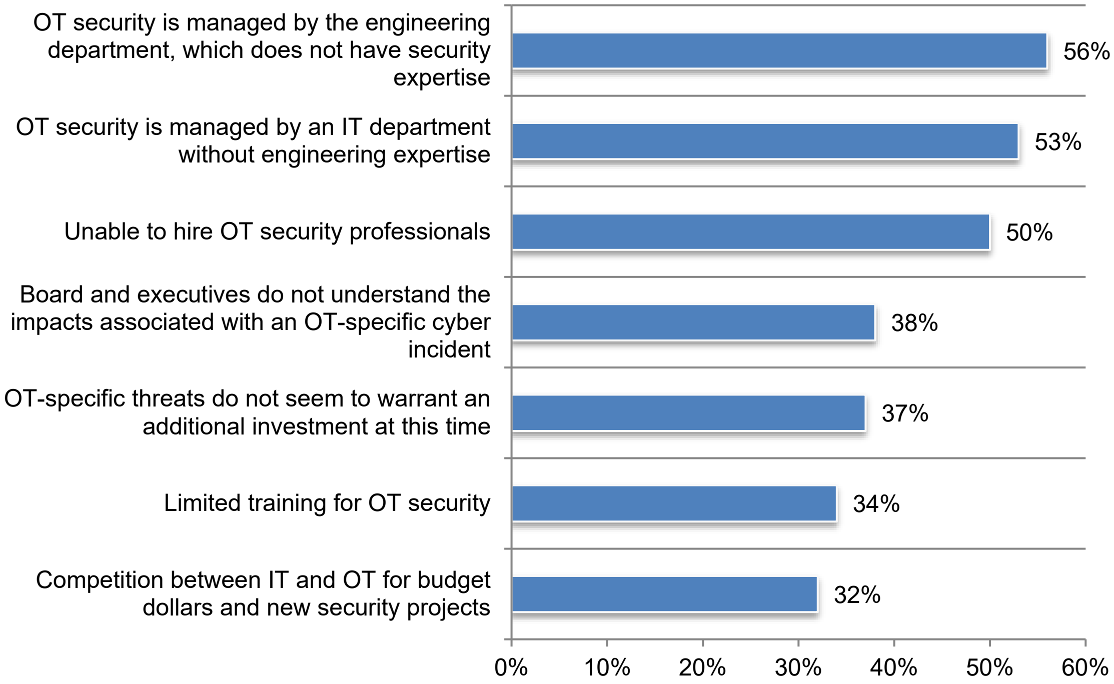
Engineering and operations is most responsible for the OT and ICS cybersecurity budget. As shown in Figure 12, 40 percent of respondents say engineering and operations controls the OT and ICS cybersecurity budget. As discussed previously, the VP of engineering is the person most respondents report to and who is accountable for the security of the OT and ICS environments. Only 30 percent of respondents say IT security is most responsible.

Figure 12. Which function is most responsible for the ICS and OT cybersecurity budget?



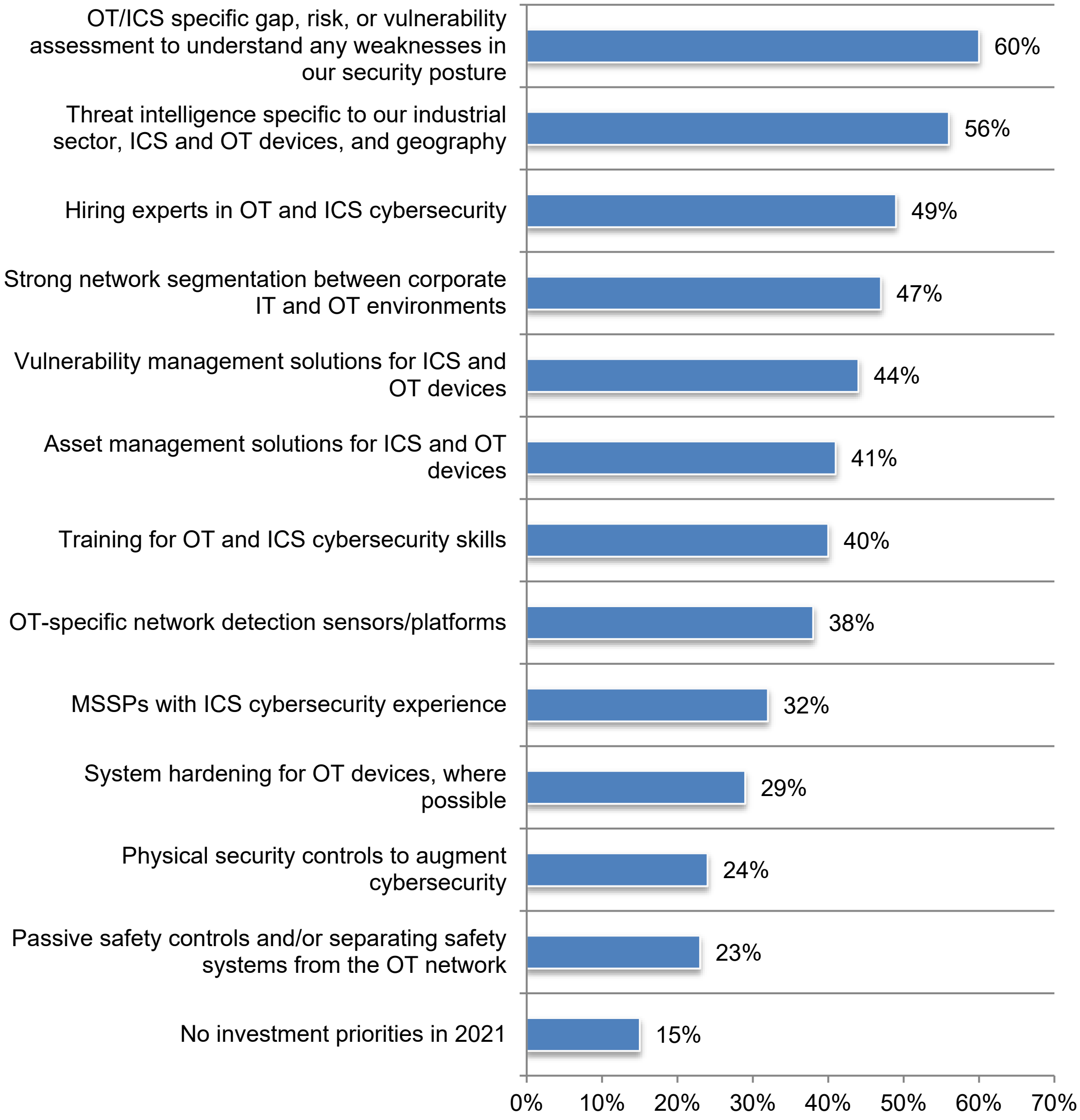
Accountability for the security of the ICS and OT environments is most often assigned to the VP of engineering and this function is most often considered a deterrent to investing in OT and ICS as shown in Figure 13. Fifty-six percent of respondents say the reason for blocking investments is that OT security is managed by the engineering department which does not have security expertise and 53 percent of respondents say OT security is managed by an IT department without engineering expertise.

Figure 13. What are the primary blockers for investing in ICS and OT cybersecurity?
Three responses permitted



Organizations are focused on making investments to improve the cybersecurity posture of ICS and OT environments. Figure 14 presents a list of investment priorities for 2021. As shown, the focus is on understanding weaknesses in the security posture (60 percent of respondents). Contributing to the security posture is gathering threat intelligence specific to their industry, ICS and OT devices and geography and hiring experts in OT and ICS cybersecurity (56 percent and 49 percent of respondents, respectively).

Figure 14. What are your organization's top three investment priorities for ICS and OT cybersecurity in 2021?
More than one response permitted



The cause and consequence of an ICS and OT ransomware and cybersecurity incident

In the context of this research, ransomware is a sophisticated piece of malware that blocks the victim's access to files. While there are many strains of ransomware, they generally fall into two categories:

Crypto ransomware encrypts files on a computer or mobile device making them unstable. Crypto ransomware essentially takes the files hostage, demanding a ransom in exchange for the decryption key needed to restore the files. **Locker ransomware** is a virus that blocks basic computer functions, essentially locking the victim out of their data and files located on the infected device. Instead of targeting files with encryption, cybercriminals demand a ransom to unlock the device.

A **cybersecurity** incident is defined as a violation or imminent threat or violation of computer and document security policies, acceptable use policies or standard security practices. An incident can involve the theft or misuse of both electronic/digital and paper documents that contain sensitive or confidential information.

Twenty-nine percent of respondents say their organization experienced a **ransomware attack** in the past two years. Of these respondents, 51 percent say their organizations paid an average ransom of more than $500,000.

Negligent insiders are most likely to cause a cybersecurity incident. Sixty-three percent of respondents say their organizations experienced an ICS/OT cybersecurity incident. Of these respondents, 47 percent of respondents say it was caused by a negligent insider followed by 41 percent of respondents who say it was a maintenance event or related issue, as shown in Figure 15.

Figure 15. What caused the cybersecurity incident?
More than one response permitted

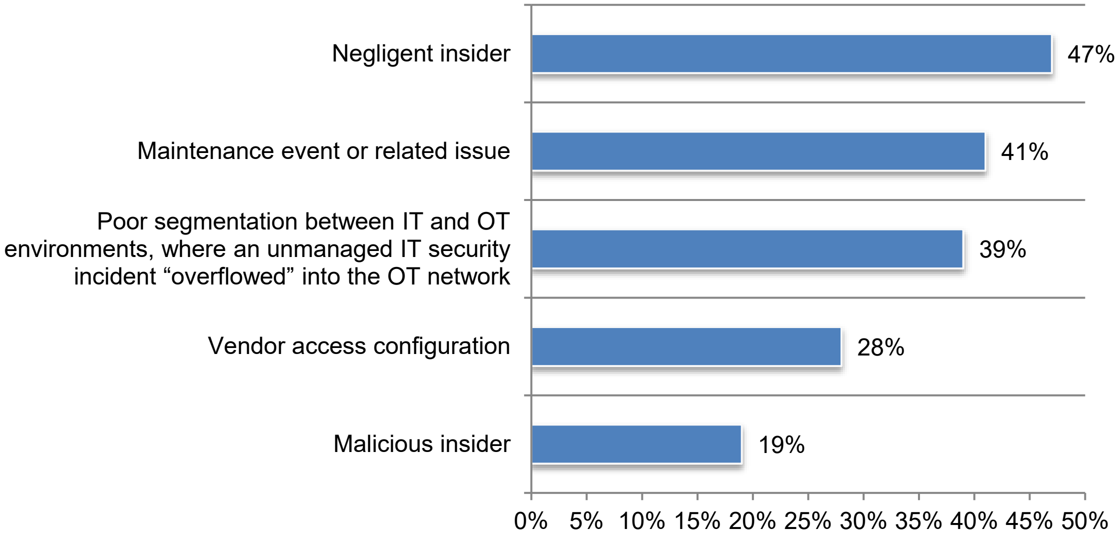


Table 1 shows the average time and cost to detect, investigate and remediate a cybersecurity incident in the ICS and OT environment. As discussed, 63 percent of respondents experienced an ICS/OT cybersecurity incident in the past two years. The average cost per cybersecurity incident for organizations represented in this research is $2,989,550.

As shown in the table, an average of 316 days is spent to detect, investigate and remediate the cybersecurity incident. Based on the use of a threat hunting and incident response team that averages six IT and IT security personnel, it costs an average of **$963,168** to detect, investigate and remediate the incident. The fixed costs for the cybersecurity incident including the replacement of equipment, downtime, legal and regulatory fines total **$2,026,382.** This equals the average total cost of **$2,989,550.**

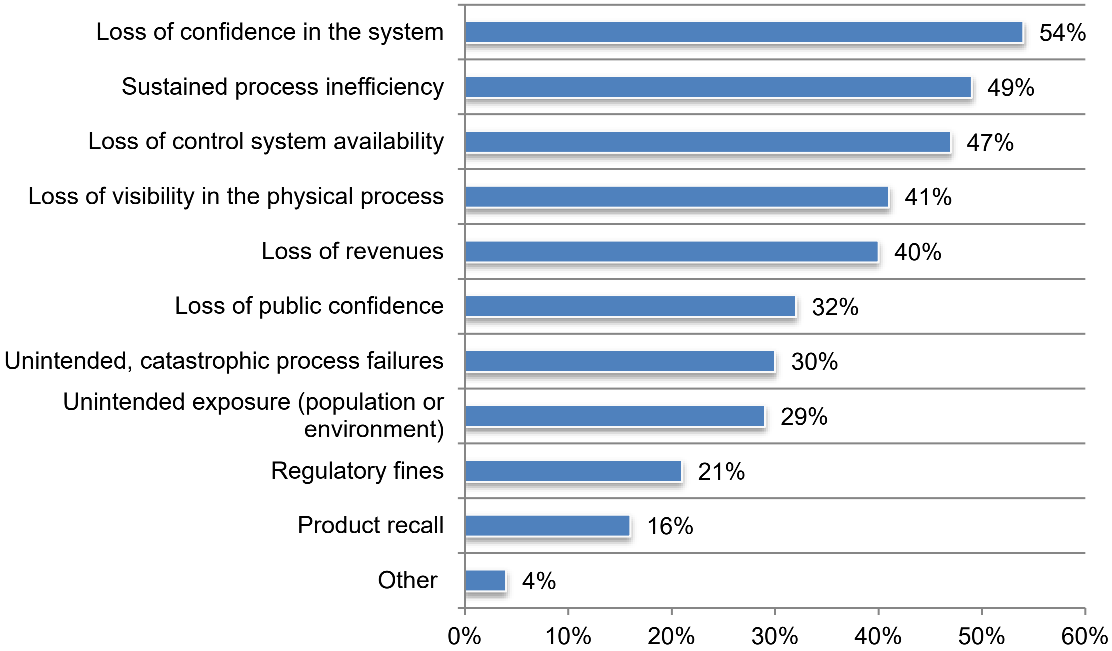
Table 1. The average time and cost to respond to a cybersecurity incident	**Cost calculations**
The average time to detect the cybersecurity incident	170 days
The average time to investigate the cybersecurity incident	66 days
The average time to remediate the cybersecurity incident	80 days
The average total days to detect, investigate and remediate the cybersecurity incident	316 days
The average **total hours** to remediate one cybersecurity incident (316 days x 8 hours per workday)	2,825 hours
The average cost **per team member** based on a $63.50* (hourly salary rate) x 2,825 hours	$160,328
The average total labor cost: $160,328 x 6 team members**	$963,168
The average fixed costs (includes equipment replacement, downtime, legal costs and regulatory fines)	$2,026,382
The average total cost ($963,168 + $2,026,382)	$2,989,550

*Average hourly fully loaded salary rate for IT and IT security personnel based on Ponemon Institute benchmark research

**Average number of IT & IT security personnel assigned to a threat hunting and incident response team based on Ponemon Institute benchmark research

Loss of confidence in the system was the number one consequence of the cybersecurity incident. As shown in Figure 16, 54 percent of respondents say confidence was lost in the system followed by sustained process inefficiency (49 percent of respondents) as a result of the cybersecurity incident.

Figure 16. What were the consequences of the cybersecurity incident?
More than one response permitted



Conclusion & recommendations

Based on the research, organizations can strengthen the cybersecurity posture of their ICS and OT environments by bridging the IT and OT cultural divide.

- Create cross-functional teams of IT and OT SMES to bridge the cultural divide. While there is a need for different controls and priorities, organizations should have a unified security strategy that secures both the IT and OT environments.
- A priority of these cross-functional teams should be to inform C-level executives and the board of directors about the efficiency, effectiveness and security of the ICS/OT cybersecurity program.
- According to the research, most organizations do not have regular meetings with the board to discuss such important topics as the security safeguards in place to protect the ICS and OT environments, the impact to the bottom line a cybersecurity incident would have and what practices are in place to protect the organization’s OT infrastructure, high value assets and intellectual property.
- The cross-functional teams should also create an incident response plan for responding to a cybersecurity incident and review the plan on a regular basis.
- Ensure there is enough budget and personnel to be able improve the ability to discover and maintain an inventory of all devices attached anywhere on the OT network throughout the asset lifecycle.

Other recommendations include the following

Because of the unique nature of OT security, an industrial cybersecurity program can't be a copy-and-paste of the IT cybersecurity program. ICS environments need cybersecurity strategies and tools tailored specifically to the different missions, challenges and threats faced by industrial organizations.

Make an OT Cybersecurity Roadmap: Effective industrial cybersecurity programs tend to be driven by threats and consequences to OT assets—prioritized by the business value of the asset and the likelihood of a given attack scenario.

Ideally, an organization should be able to gain visibility, control and minimum cybersecurity hygiene across the entire OT environment, but that takes time and money. In order to develop a solid cybersecurity roadmap that can incrementally phase in good cybersecurity practices, organizations should start first with a discovery process that gathers input from the board, executive stakeholders, and asset owners on the highest business priorities tied to OT processes and then survey the environment to understand all the OT assets in place and the priorities. The team then identifies and ranks the OT assets involved, based on business importance. From there the team should chart out the threat-driven and consequence-driven scenarios most likely to impact high-priority assets. The scenarios are defined as follows:

- Threat driven: These scenarios are those which threat intelligence reports have shown to impact organizations.
- Consequence driven: These scenarios are constructed by moving backwards from worst consequences of an attack that you would want to avoid in high-priority ICS environments and sketching out the common attack techniques that could be used to trigger them.

With these scenarios in mind, the team should examine existing controls and how they stack up against the tactics, techniques, and procedures (TTPs) used by attackers in each situation. Use this to identify gaps compared to an ideal set of controls and this provides the basis for setting out a roadmap. Don't try to boil the ocean, break it down into a multi-year plan for continuous improvement, prioritizing coverage and speed of investment based on that asset ranking gleaned from the stakeholders.

Get the Right Tools: Many IT detection and monitoring tools don't translate well to ICS environments. Often IT detection tools simply don't interface well with OT systems or are impractical when placed within an ICS environment. For example, endpoint protection won't work for PLCs.

What's more, the detection mechanisms and output are all based on IT-focused threats, so the context and correlation of what matters to OT operators will be missing. The machine learning models are not useful in ICS environments since they were designed and tuned for IT. Dragos experts are repeatedly called to incidents where they've found that Windows AV destroyed ICS applications because they looked odd to heuristics engines unaccustomed to the way ICS functions operate.

This is why an organization will need OT-specific cybersecurity tooling that can support the management of risks that matter most in industrial settings.

Skill Up: OT cybersecurity is a specialized endeavor. While the enterprise cybersecurity team may be able to take the lead on strategic planning—with heavy OT stakeholder collaboration—and even shoulder some of the day-to-day work, the team will need additional resources to execute on a plan. For many organizations, the best way to quickly build up the requisite skills will be by leveraging partners and third parties to bridge internal gaps, for example by putting a firm on retainer for rapid incident response.

The conversation should be ‘We’ve all bought into this together.’ You tie it to the business problem. Instead of it being some ephemeral problem, it’s based on real scenarios that either the threats have shown you or your people are concerned about, and so you’re able to present real information to the executives.

Part 3. Methodology

A sampling frame of 17,040 IT, IT security and OT security practitioners at the C-level, managerial and director level in the United States were selected as participants to this survey. All respondents are familiar with their organizations' cybersecurity initiatives and ICS and OT security. Table 2 shows 673 total returns. Screening and reliability checks required the removal of 70 surveys. Our final sample consisted of 603 surveys or a 3.5 percent response.

Table 2. Sample response	Freq	Pct%
Sampling frame	17,040	100%
Total returns	673	3.9%
Rejected or screened surveys	70	0.4%
Final sample	603	3.5%

Figure 16 reports the respondent's organizational level within participating organizations. By design, more than half (51 percent) of respondents are at or above the supervisory levels. The largest category at 23 percent of respondents is engineer.

Figure 16. Current position within the organization

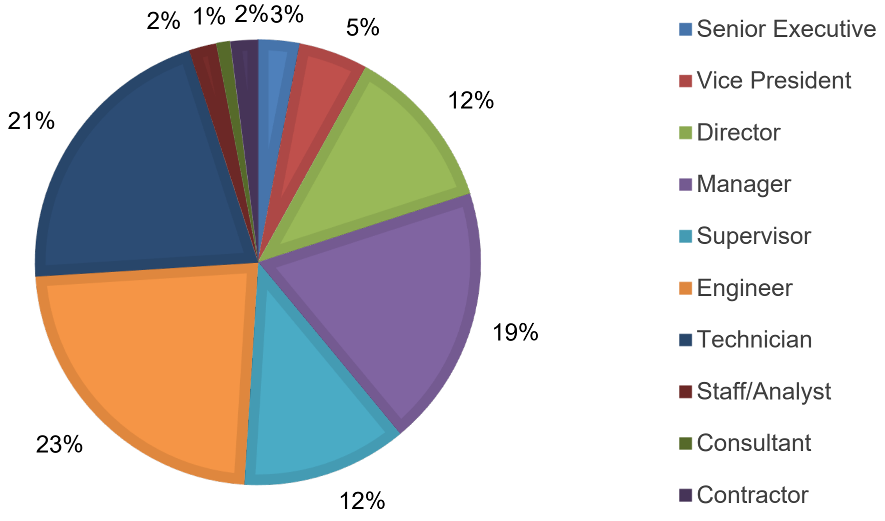
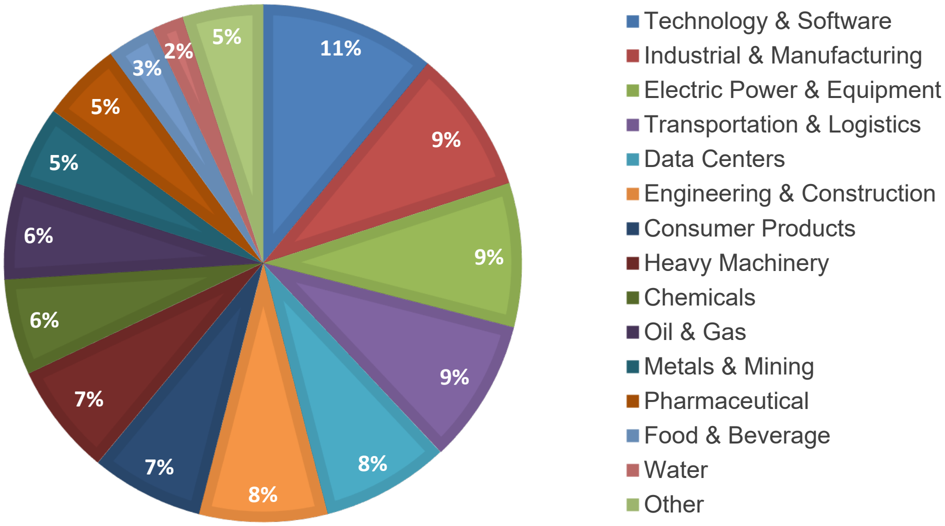


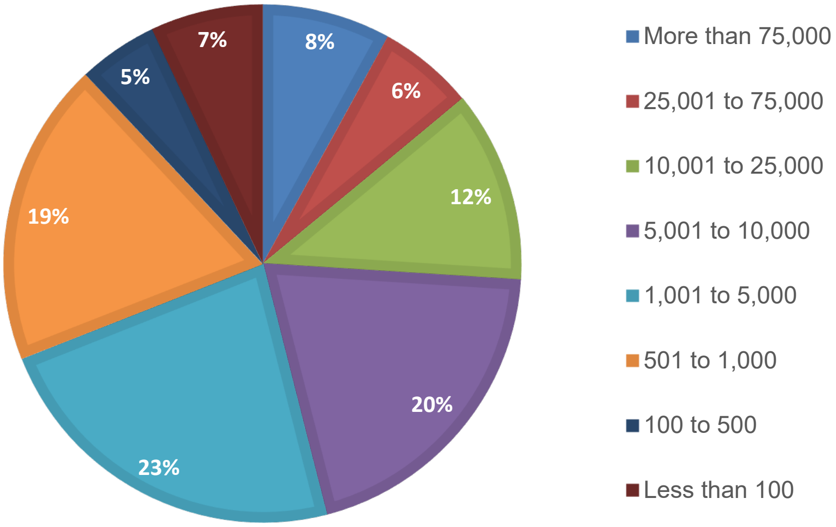
Figure 17 reports the industry focus of respondents' organizations. This chart identifies technology and software (11 percent of respondents) as the largest industry focus. This is followed by industrial and manufacturing, electric power and equipment, transportation and logistics, each at 9 percent of respondents.

Figure 17. Primary industry focus



As shown in Figure 18, 69 percent of respondents are from organizations with a global headcount of more than 1,000 employees.

Figure 18. Global full-time headcount



Part 4. Caveats to this study

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, IT security and OT security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

- 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.

Part 5. Appendix with the detailed audited findings

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in July 2021.

Survey response	Freq
Total sampling frame	17,040
Total returns	673
Rejected surveys	70
Final sample	603
Response rate	3.5%

Part 1. Screening questions

S1. How familiar are you with the cybersecurity initiatives within your organization today?	Pct%
Very familiar	41%
Familiar	34%
Somewhat familiar	25%
No knowledge (Stop)	0%
Total	100%

S2. How familiar are you with ICS and OT security in your organization?	Pct%
Very familiar	36%
Familiar	35%
Somewhat familiar	29%
No knowledge (Stop)	0%
Total	100%

S3. What is your role within your organization?	Pct%
C-level (CEO, CFO, CIO, CISO, COO, CRO, CTO)	30%
IT security manager/director	45%
OT security manager/director	25%
None of the above (Stop)	0%
Total	100%

Part 2. Background on ICS and OT Security

Q1. To whom do you report? Please select one top choice.	Pct%
Chief Executive Officer (CEO) (please proceed to Q3)	5%
Chief Financial Officer (CFO)	1%
Chief Information Officer (CIO)	17%
Chief Information Security Officer (CISO)	13%
Chief Operating Officer (COO)	6%
Chief Risk Officer (CRO)	7%
Chief Technology Officer (CTO)	12%
VP of Engineering	19%
Director/Manager of IT	20%
Other (please specify)	0%
Total	100%

Q2. If you don't report to the CEO, how many levels are you away from the CEO?	Pct%
1.0	17%
2.0	23%
3.0	25%
4.0	23%
4+	12%
Total	100%

Q3. Who is most accountable for the security of OT and ICS programs?	Pct%
Chief Executive Officer (CEO)	3%
Chief Financial Officer (CFO)	0%
Chief Information Officer (CIO)	16%
Chief Information Security Officer (CISO)	12%
Chief Operating Officer (COO)	6%
Chief Risk Officer (CRO)	6%
Chief Technology Officer (CTO)	14%
VP of Engineering	25%
Director/Manager of IT	18%
Other (please specify)	0%
Total	100%

Q4a. How are IT and OT cybersecurity initiatives reported to your Board of Directors?	Pct%
IT and OT initiatives reported together	24%
Only IT initiatives reported	30%
Only OT initiatives reported	21%
IT and OT initiatives are not reported to the Board	25%
Total	100%

Q4b. Do you or someone responsible for ICS and OT cybersecurity report to the Board of Directors?	Pct%
Yes	35%
No (please skip to Q5)	65%
Total	100%

Q4c. If yes, how often do you or someone responsible for ICS and the OT cybersecurity report to the Board of Directors?	Pct%
Annually	17%
Bi-annually	18%
Quarterly	24%
Only when a security incident occurs	41%
Total	100%

Q4d. What topics do you cover during the board meetings? Please check all that apply.	Pct%
Any changes to the ICS and OT threat landscape	54%
Vulnerabilities in ICS and OT environments	48%
Effectiveness and efficiency of security programs and measures	36%
Results from risk assessments of the ICS and OT environments	62%
Practices in place to protect the organization’s OT infrastructure, high-value assets, and intellectual property	47%
Quantification of the impact to the bottom line a cybersecurity incident involving OT and ICS environments would have	45%
The security safeguards in place to protect the ICS and OT environments	38%
The state of compliance with regulations	24%
Other (please specify)	2%
Total	356%

Attributions: Please express your opinion about each one of the following statements using the agreement scale below each item. **Strongly Agree and Agree response.**	Pct%
Q5. Senior management understands the cyber risks and provides adequate resources to defend ICS and OT environments.	43%
Q6. The company understands the unique cyber risks and has specific security processes and policies for ICS and OT environments.	48%
Q7. Our IT and OT teams work cohesively to achieve a mature security posture in both the IT and OT environments.	39%
Q8. Our IT and OT teams have a unified security strategy that secures both the IT and OT environments, despite the need for different controls and priorities.	35%
Q9. Our cybersecurity policies and procedures are aligned with our ICS and OT security objectives.	43%
Q10. Our organization has mechanisms in place to detect malicious communications in our OT systems.	34%
Q11. Digital transformation, or the trend towards the Industrial Internet of Things (IIoT), greatly expands cyber risk to the ICS and OT environment.	61%

Part 3. Maturity of the OT and ICS cybersecurity program

Q13. What best describes the maturity of your organization's ICS/OT cybersecurity program?	Pct%
Early stage: Many ICS and OT program activities have not as yet been planned or deployed. Response to threats is reactive and ad hoc. Resources are not sufficient for staffing and investment in the program.	17%
Middle stage: ICS and OT program activities are planned and defined but only partially deployed. Efforts are being made to establish security protocols, develop a workforce of SMEs, prioritize risks, increase investments, and take steps to have IT and OT work cohesively.	33%
Late-middle stage: ICS and OT program has C-level support and adequate budget. Risks are regularly assessed, and a cross-functional team of IT and OT SMEs work together cohesively.	29%
Mature stage: ICS and OT program activities are fully deployed at target maturity states, emerging threats drive priority actions, and C-level executives and the board of directors are regularly informed about the efficiency, effectiveness, and security of the program.	21%
Total	100%

Q14. Using the following 10-point scale, please rate the security posture of your organization's IT environment **today** from 1 = not secure to 10 = highly secure.	Pct%
1 or 2	12%
3 or 4	18%
5 or 6	15%
7 or 8	25%
9 or 10	30%
Total	100%
Extrapolated value	6.36

Q15a. Using the following 10-point scale, please rate the security posture of your organization's ICS and OT environments **today** from 1 = not secure to 10 = highly secure.	Pct%
1 or 2	12%
3 or 4	18%
5 or 6	15%
7 or 8	25%
9 or 10	30%
Total	100%
Extrapolated value	6.36

Q15b. Using the following 10-point scale, please rate the security posture of your organization's ICS and OT in the next **five years** from 1 = not secure to 10 = highly secure.	Pct%
1 or 2	5%
3 or 4	10%
5 or 6	16%
7 or 8	27%
9 or 10	42%
Total	100%
Extrapolated value	7.32

Q16. How effective is your organization in gathering intelligence about threats to ICS and the OT? 1 = not effective to 10 = highly effective	Pct%
1 or 2	12%
3 or 4	22%
5 or 6	20%
7 or 8	25%
9 or 10	21%
Total	100%
Extrapolated value	5.92

Q17. How effective is your organization in its ability to discover and maintain an inventory of all devices attached anywhere on the OT network throughout the asset lifecycle? 1 = not effective to 10 = highly effective	Pct%
1 or 2	14%
3 or 4	17%
5 or 6	24%
7 or 8	19%
9 or 10	26%
Total	100%
Extrapolated value	6.02

Q18. What capabilities are used to secure your ICS/OT environment? Please select all that apply.	Pct%
Identity and access management (where possible)	43%
Asset discovery and management	29%
Secure configuration baselines	39%
Change management	44%
Secure network architecture	36%
Strong network segmentation between the IT and OT networks, including an OT-specific DMZ	39%
Physically locking and isolating sensitive equipment, where possible	52%
Managing USBs and maintenance laptops in the OT environment	55%
OT-specific network detection, including anomaly detection and industrial protocol analysis	52%
Vulnerability assessments, where appropriate, including prior to commissioning new equipment	57%
Isolated safety systems, including passive controls, not accessible through the OT network	40%
Malicious code detection or application whitelisting, where appropriate	37%
Intrusion Detection Systems or OT-specific SIEM	35%
Secure patch management system	29%
Other (please specify)	2%
Total	589%

Q19. Does your organization use an ICS/OT-specific cybersecurity standard to manage its security program? Please select all that apply.	Pct%
No, we do not use an OT/ICS-specific cybersecurity standard.	36%
Yes, NIST SP 800-82	40%
Yes, NIST Cybersecurity Framework	32%
Yes, ISA/IEC 62443	38%
Yes, NERC CIP	40%
Yes, NEI 08-09	23%
Yes, DHS/CISA CFATS	28%
Yes, DOD CMMC	23%
Yes, Other (please specify)	1%
Total	261%

Q20. Top three cybersecurity risks for your organization? Please select only three responses.	Pct%
Compliance risk from industry standards/regulations	42%
Data breaches in corporate IT	30%
IP theft	32%
Business continuity and interruption	44%
Health and human safety	23%
Supply chain and/or third-party security risk	34%
Growing threat activity in your industrial sector/geography	31%
Increased attack surface with connectivity into the OT environment	28%
Vulnerable equipment in OT networks	35%
Other (please specify)	1%
Total	300%

Q21. How effective is the working relationship between OT and IT? 1 = not effective to 10 = highly effective	Pct%
1 or 2	25%
3 or 4	27%
5 or 6	13%
7 or 8	15%
9 or 10	20%
Total	100%
Extrapolated value	5.06

Q22. What are the primary challenges to having OT and IT work cohesively? Please select only three responses.	Pct%
Cultural differences between engineers, security professionals, and IT staff	50%
Technical differences between traditional IT-specific best practices and what is possible in OT environments, such as patch management and unique requirements of industrial automation equipment vendors	44%
Procedural concerns with IT personnel in industrial environments	39%
Limited training for integrating IT and OT security practices	23%
Lack of clear "ownership" on industrial cyber risk and uncertainty around who leads the initiative, implements the controls, and supports the program	43%
Inability to hire IT-OT security professionals with adequate experience	41%
Competition between IT and OT for budget dollars and new security projects	32%
Difficulty in converging security teams across IT and OT as an enterprise-wide cybersecurity program	27%
Other (please specify)	1%
Total	300%

Part 4. Budget

Q23. What are the primary blockers for investing in ICS and OT cybersecurity? Please select only three responses.	Pct%
Competition between IT and OT for budget dollars and new security projects	32%
Board and executives do not understand the impacts associated with an OT-specific cyber incident	38%
OT security is managed by the engineering department, which does not have security expertise	56%
OT security is managed by an IT department without engineering expertise	53%
Limited training for OT security	34%
Unable to hire OT security professionals	50%
OT-specific threats do not seem to warrant an additional investment at this time	37%
Other (please specify)	0%
Total	300%

Q24. Which function is **most** responsible for the ICS and OT cybersecurity budget? Please select only one choice	Pct%
IT operations	25%
IT security	30%
Engineering and operations	40%
Finance	3%
Other (please specify)	2%
Total	100%

Q25. How would you describe the cybersecurity budget for ICS and OT? Please select one choice.	Pct%
More than adequate	14%
Adequate	41%
Inadequate	45%
Total	100%

Q26. What are your organization's top three cybersecurity investment priorities for ICS and OT cybersecurity in 2021? Please select only five responses.	Pct%
Hiring experts in ICS and OT cybersecurity	49%
Training for ICS and OT cybersecurity skills	40%
Strong network segmentation between corporate IT and OT environments	47%
OT-specific network detection sensors/platforms	38%
MSSPs with ICS cybersecurity experience	32%
System hardening for OT devices, where possible	29%
Physical security controls to augment cybersecurity	24%
Passive safety controls and/or separating safety systems from the OT network	23%
Asset management solutions for ICS and OT devices	41%
Vulnerability management solutions for ICS and OT devices	44%
Threat intelligence specific to our industrial sector, ICS and OT devices, and geography	56%
ICS and specific gap assessment, risk assessment, or vulnerability assessment to understand any weaknesses in our security posture	60%
No investment priorities in 2021	15%
Other (please specify)	2%
Total	500%

Part 5. The cost of an ICS and OT cybersecurity incident

Q27a. Did your organization experience a ransomware incident in the past two years?	Pct%
Yes	29%
No (please skip to Q30)	54%
Don't know (Please skip to Q30)	17%
Total	100%

Q27b. If yes, did you pay the ransom?	Pct%
Yes,	51%
No (please skip to Q30)	33%
Don't know (please skip to Q30)	16%
Total	100%

Q27c. If your organization paid the ransom, how much was it?	Pct%
Less than $100,000	33%
$100,001 to $250,000	15%
$250,001 to $500,000	11%
$500,001 to $1,000,000	21%
$1,000,001 to $1,250,000	9%
$1,250,001 to $1,500,000	7%
$1,500,001 to $2,000,000	3%
More than $2,000,000	1%
Total	100%
Extrapolated value	$ 519,450

Q28a. Did your organization experience an ICS/OT cybersecurity incident in the past two years?	Pct%
Yes	63%
No (please skip to Part 6)	20%
Don’t know (Please skip to Part 6)	17%
Total	100%

Q28b. What caused the ICS/OT cybersecurity incident? Please select all that apply.	Pct%
Negligent insider	47%
Malicious insider	19%
Maintenance event or related issue	41%
Vendor access configuration	28%
Poor segmentation between IT and OT environments, where an unmanaged IT security incident “overflowed” into the OT network	39%
Other (please specify)	0%
Total	174%

Q29. If yes, approximately, how long did it take to detect the cybersecurity incident?	Pct%
Less than 24 hours	9%
24 hours to 48 hours	5%
2 days to 7 days	8%
1 week to 4 weeks	23%
1 month to 6 months	23%
6 months to 12 months	20%
More than 12 months	12%
Total	100%
Extrapolated value (days)	170.05

Q30. Approximately, how long did it take to investigate the cybersecurity incident?	Pct%
Less than 24 hours	14%
24 hours to 48 hours	11%
2 days to 7 days	17%
1 week to 4 weeks	36%
1 month to 6 months	15%
6 months to 12 months	5%
More than 12 months	2%
Total	100%
Extrapolated value (days)	65.60

Q31. Approximately, how long did it take to remediate the cybersecurity incident?	Pct%
Less than 24 hours	13%
24 hours to 48 hours	13%
2 days to 7 days	16%
1 week to 4 weeks	30%
1 month to 6 months	18%
6 months to 12 months	7%
More than 12 months	3%
Total	100%
Extrapolated value (days)	80.46

Q32. What were the consequences of the cybersecurity incident? Please select all that apply.	Pct%
Loss of confidence in the system	54%
Loss of control system availability	47%
Loss of visibility in the physical process	41%
Loss of public confidence	32%
Loss of revenues	40%
Product recall	16%
Regulatory fines	21%
Sustained process inefficiency	49%
Unintended exposure (population or environment)	29%
Unintended, catastrophic process failures	30%
Other (please specify)	4%
Total	363%

Q33. What was the total cost of the ICS and OT security incident? Please take into consideration the following activities: detecting, investigating and remediation of the incident, including any equipment that needed to be replaced and any regulatory fines. All figures in $USD.	Pct%
Less than $50,000	12%
$50,000 to $100,000	30%
$100,001 to $250,000	12%
$250,001 to $500,000	23%
$500,001 to $1,000,000	10%
$1,000,001 to $5,000,000	6%
$5,000,001 to $10,000,000	4%
$10,000,001 to $100,000,000	2%
More than $100,000,000	1%
Total	100%
Extrapolated value	$ 2,989,550

Part 6. Your role and organization

D1. What organizational level best describes your current position?	Pct%
Senior Executive	3%
Vice President	5%
Director	12%
Manager	19%
Supervisor	12%
Engineer	23%
Technician	21%
Staff / Analyst	2%
Consultant	1%
Contractor	2%
Other	0%
Total	100%

D2. What industry sector best describes your organization's primary focus?	Pct%
Defense & Aerospace	1%
Industrial & Manufacturing	9%
Chemicals	6%
Consumer Products	7%
Data Centers	8%
Electric Power & Equipment	9%
Engineering & Construction	8%
Food & Beverage	3%
Heavy Machinery	7%
Metals & Mining	5%
Oil & Gas	6%
Pharmaceutical	5%
Technology & Software	11%
Transportation & Logistics	9%
Water	2%
Other (please specify)	4%
Total	100%

D3. Where are your employees located? (Select all that apply)	Pct%
United States	89%
Canada	63%
Europe	59%
Asia-Pacific	54%
Middle East & Africa	21%
Latin America (plus Mexico)	28%
Total	314%

D4. What is the worldwide headcount of your organization?	Pct%
Less than 100	7%
100 to 500	5%
501 to 1,000	19%
1,001 to 5,000	23%
5,001 to 10,000	20%
10,001 to 25,000	12%
25,001 to 75,000	6%
More than 75,000	8%
Total	100%

Please contact research@ponemon.org or call us at 800.887.3118 if you have any questions.

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.