Ponemon INSTITUTE

The State of IoT/OT Cybersecurity in the Enterprise

Sponsored by Microsoft

Independently conducted by Ponemon Institute LLC

Publication Date: November 2021

The State of IoT/OT Cybersecurity in the Enterprise

Presented by Ponemon Institute
November 2021

Part 1. Executive summary

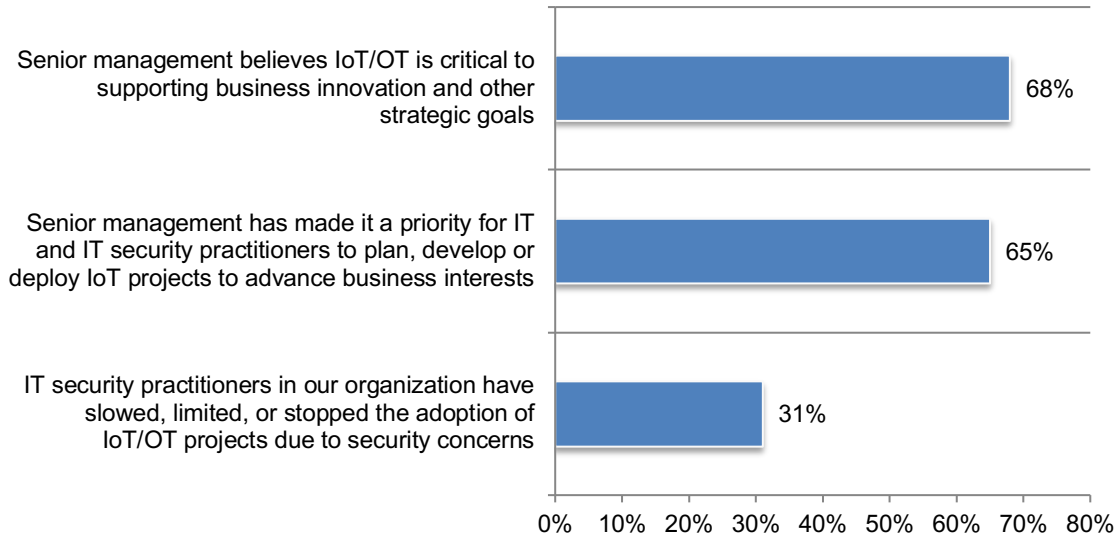
Sponsored by Microsoft and conducted by Ponemon Institute, the purpose of this study is to determine how effective organizations are in securing their Internet of Things (IoT) devices, including Enterprise Internet of Things (EIoT) and Industrial Internet of Things (IIoT) devices as well as their Operational Technology (OT) and Industrial Control Systems (ICS). Ponemon Institute surveyed 615 IT and IT security practitioners in the United States who are knowledgeable about the state of cybersecurity in their organizations.

As shown in this research, organizations are increasingly relying upon these devices to optimize their operations and the number of IoT and OT endpoints is growing dramatically. Industry analysts estimate that CISOs will soon be responsible for an attack surface three times larger than just a few years ago. Further, these devices are typically unmanaged and don't support agents leaving their security posture unknown and often insecure (e.g. security baselines unimplemented, unpatched and unmonitored). Finally, these devices are often invisible to IT security teams because they often lack the tools to discover and inventory such IoT and OT devices.

IoT/OT adoption is critical to ongoing business success. Advancing IoT/OT projects is a top priority even with concerns about the security. Sixty-eight percent of respondents say senior management believes IoT/OT is critical to supporting business innovation and other strategic goals as shown in Figure 1.

Sixty-five percent of respondents say senior management has made it a priority for IT and IT security practitioners to plan, develop or deploy IoT projects to advance business interest. As a possible consequence of senior management's push for deployment, few IT security practitioners (only 31 percent of respondents) are willing to slow, limit or stop the adoption of IoT/OT projects due to security concerns, which are described in more detail in the report.

Figure 1. Perceptions about the importance of IoT/OT to achieving business innovation
Strongly agree and Agree responses combined



Following is a summary of the findings that cover the following topics: the ineffectiveness of current security practices, vulnerability of IoT/OT devices, the risky exposure of IoT/OT devices, the threat landscape and the willingness to pay more for IoT devices and solutions in order to improve IoT/OT security.

IoT/OT devices are vulnerable. These devices are not designed with security in mind such as PC's and mobile devices are.

- Sixty percent of respondents say IoT/OT devices are one of the least secured part of their organizations' IT/OT infrastructure.
- Fifty-five percent of respondents do not believe IoT/OT devices have been designed with security in mind and 11 percent of respondents do not know.

The risky exposure of IoT/OT devices. The least secure devices on the typical network can be reached by attackers from the internet.

- Eighty-eight percent of respondents say their organizations' enterprise IoT devices are connected to the internet (e.g., for cloud printing services).
- Fifty-six percent of respondents say their organizations' OT devices are connected to the internet for such purposes as to enable remote access.
- Fifty-one percent of respondents say the OT network is connected to corporate IT (business) network (e.g., for SAP, remote access, etc.).

Lack of visibility is a key security challenge in the IoT/OT environment. Organizations struggle to get a view of what devices exist on their network and if they are being secured and monitored. Forty-seven percent of respondents say their organizations primarily use manual processes to identify and correlate compromised IoT/OT devices to the attacks.

- Twenty-nine percent of respondents say their organizations have a complete inventory of their IoT/OT devices. According to these respondents, organizations have an average of 9,685 devices.
- Barriers to ensuring the security of IoT devices are the lack of visibility of assets and vulnerabilities. Sixty-one percent of respondents have low or average confidence in the ability to identify whether IoT devices are compromised.
- Forty-two percent of respondents lack visibility of vulnerabilities. Seventy percent of respondents have low or average confidence in the security of their organizations' IoT devices and 64 percent of respondents have low or average confidence that IoT devices are patched and up to date.
- On a positive note, 67 percent of respondents say senior management considers improving IoT/OT security is top priority over the next 12 to 24 months.

The threat landscape defined. The volume of attacks against IoT/OT devices are increasing.

- Thirty-five percent of respondents say in the past two years their organizations experienced a cyber incident where an IoT device was used by an attacker to conduct a broader attack.
- Thirty-nine percent of respondents experienced a cyber incident in the past two years where an IoT device was the target of the attack itself.

- Fifty percent of respondents say the volume of attacks against IoT/OT devices have increased significantly (26 percent) or increased (24 percent).

- Sixty-three percent of respondents say the volume of attacks will significantly increase (36 percent) or increase (27 percent).

Organizations are willing to spend more on IoT devices and solutions to Improve the security of the IoT/OT environment. Devices are being designed to be more secure. According to a special analysis, respondents would be willing to spend more if the security of these devices would improve, especially for industrial IoT devices (an average of 37 percent more) and industrial IoT solutions (an average of 41 percent more).

Part 2. Key findings

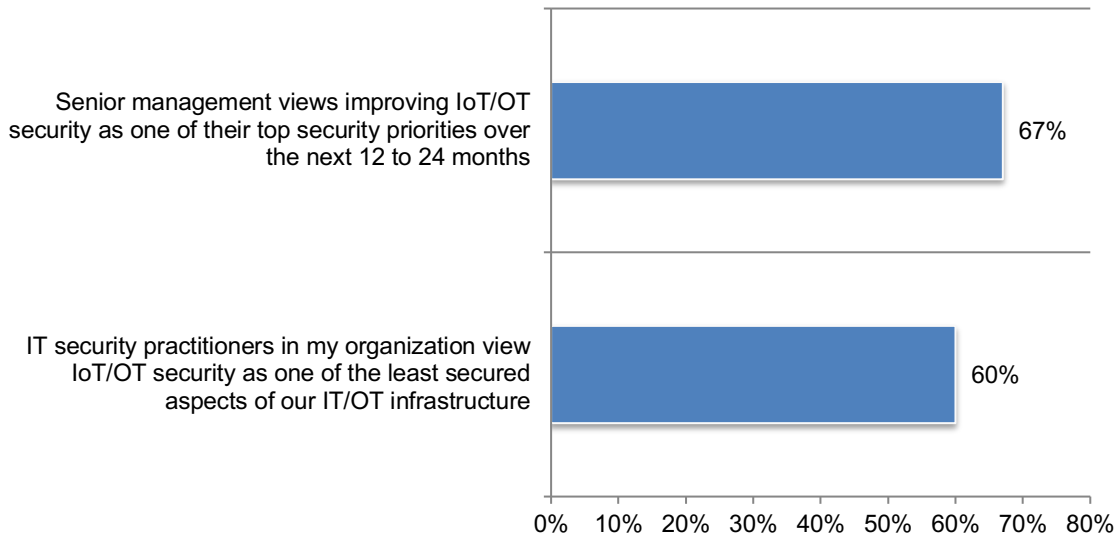
In this section, we provide a deep dive into the research. The complete findings are presented in the Appendix of this report. We have organized the report according to the following topics.

- IoT/OT devices are important to business innovation and profitability but create security risks
- The barriers and challenges to securing IoT/OT devices
- How much more would organizations spend on IoT/OT devices if they become more secure?
- Industry differences

IoT/OT devices are important to business innovation and profitability but create security risks

Senior management and IT security practitioners agree the insecurity of IoT/OT devices is posing risks to the organization. According to Figure 2, 60 percent of respondents say IoT/OT is one of the least secured aspects in the IT/OT infrastructure. As discussed previously, the importance of IoT/OT devices to the future of organizations has been established and, on a positive note, 67 percent of respondents say senior management views improving IoT/OT security as one of their top security priorities over the next 12 to 24 months.

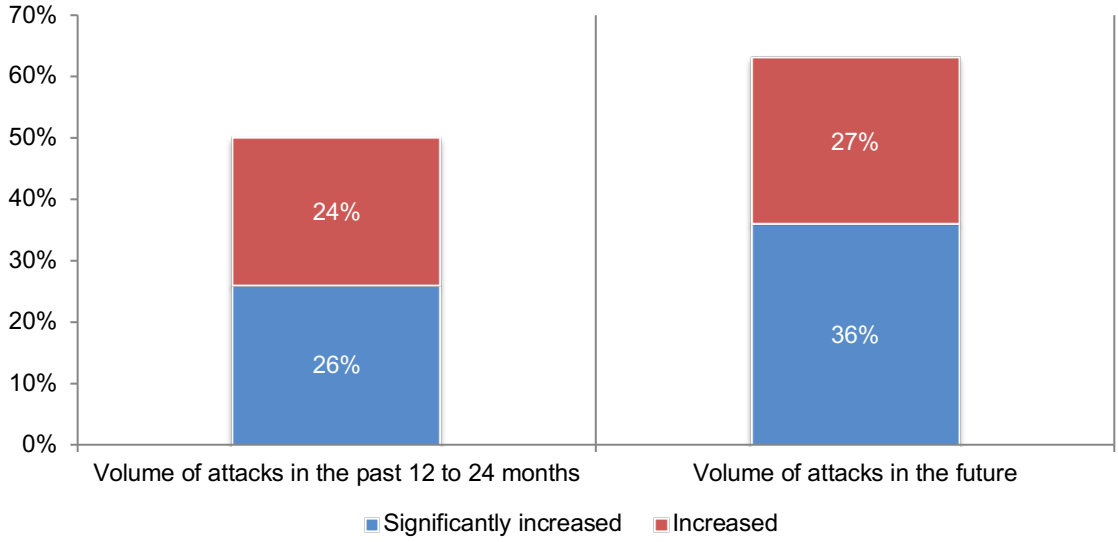
Figure 2. Perceptions about the current state of IoT/OT cybersecurity
Strongly agree and Agree responses combined



While a gap between productivity and security risk continues to grow. Our research suggest senior-level management recognize the need for a more robust IoT/OT infrastructure,

The volume of attacks against IoT/OT devices will increase. As shown in Figure 3, 50 percent of respondents say the volume of attacks against IoT/OT devices has increased significantly (26 percent) or increased (24 percent). In the future (2021 and beyond), 63 percent of respondents say the volume of attacks will significantly increase (36 percent) and increase (27 percent).

Figure 3. How has the volume of attacks changed in the past and will change?
Significantly increased and Increased responses presented

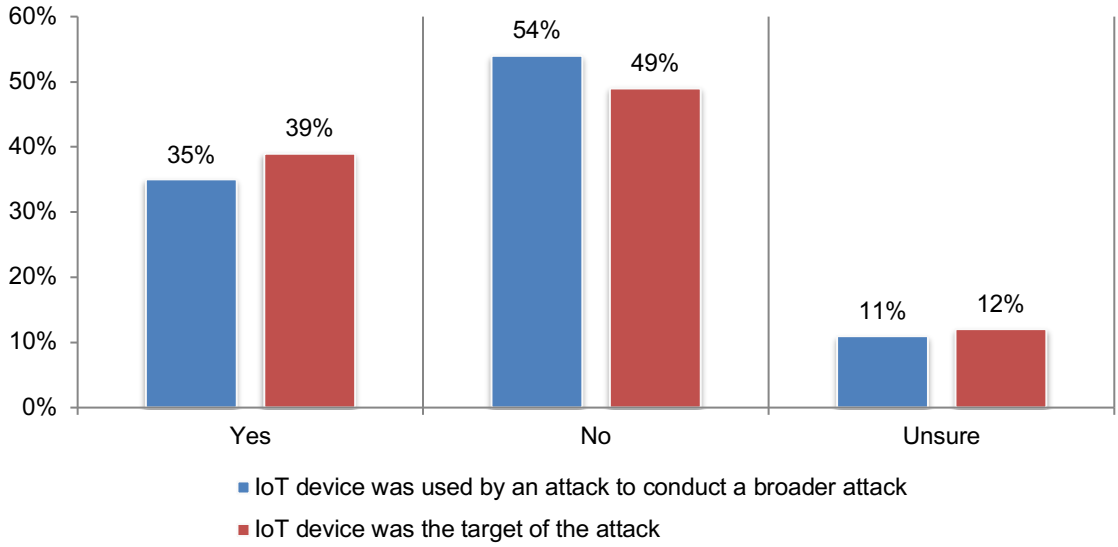


The main consequence of an increasing security risk in the IoT/OT infrastructure is the substantial rise in targeted attacks. Many of these attacks rely on leading-edged automation methods such as machine learning, orchestration and artificial intelligence.

Many cyber incidents involve IoT/OT devices. Forty-four percent of respondents say their organizations experienced a cyber incident in the past two years that involved an IoT/OT device. Contributing to security risks is the increasing reliance of edge devices. These devices can take the form of any small device with compute power near the end-user. Most IoT devices do not have much processing power and security features, leaving a vast number of vulnerable network entry points at the edge.

According to Figure 4, 35 percent of respondents say in the past two years their organizations experienced a cyber incident where an IoT device was used by an attacker to conduct a broader attack and 39 percent of respondents experienced a cyber incident in the past two years where an IoT device was the target of the attack itself.

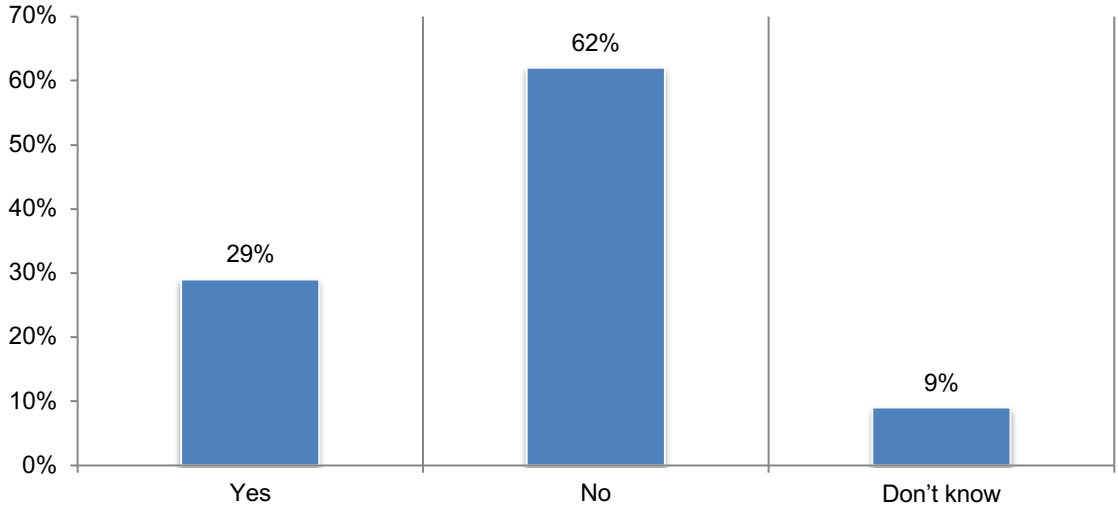
Figure 4. Types of cyber incidents organizations experienced in the past two years



The small footprint of IoT devices, such as surveillance video, lighting systems or local printers, present inherent limitations to built-in security at the device level.

Few organizations have an accurate asset inventory of their IoT devices in their security solutions. Only 37 percent of respondents are confident that their organizations have an accurate asset inventory of IoT devices in their security solutions. As shown in Figure 5, only 29 percent of respondents say their organizations have a complete inventory of its IoT/OT devices. If they do, organizations have an average of 9,685 devices.

Figure 5. Does your organization have a complete inventory of its IoT/OT devices?



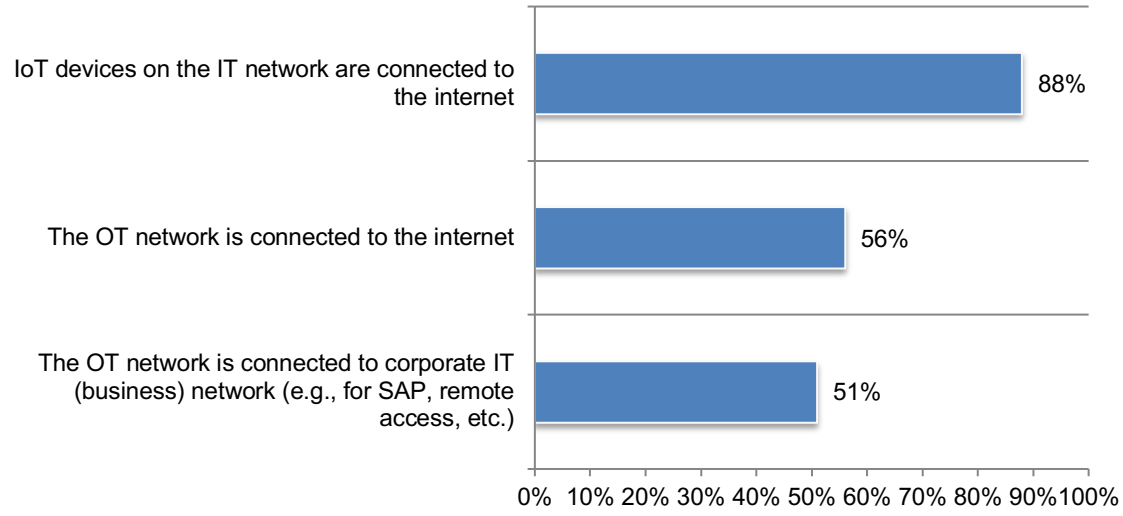
Our research presents the need for IoT/OT governance procedures such as the completion of an inventory process that lists the physical locations of all devices (including devices that are not connected to the Internet).

Organizations are vulnerable to attacks because IoT devices on IT networks and the OT networks are connected to the internet. As shown in Figure 6, 88 percent of respondents say their IoT devices are connected to the internet. These include such devices as smart TV, conferencing systems and printers connected to cloud printing services.

These devices are intended to improve ease of access and connection, rather than for security. It is recommended that IoT devices should be patched as soon as a vulnerability is identified. In addition, monitoring which devices interact and the movement of traffic between them will make it easier to detect abnormalities.

Fifty-six percent of respondents say the OT network and devices on the OT network are connected to the internet and 51 percent of respondents say their organizations' OT network is connected to their corporate IT network for SAP, remote access and more.

Figure 6. OT network and device connections
Yes responses

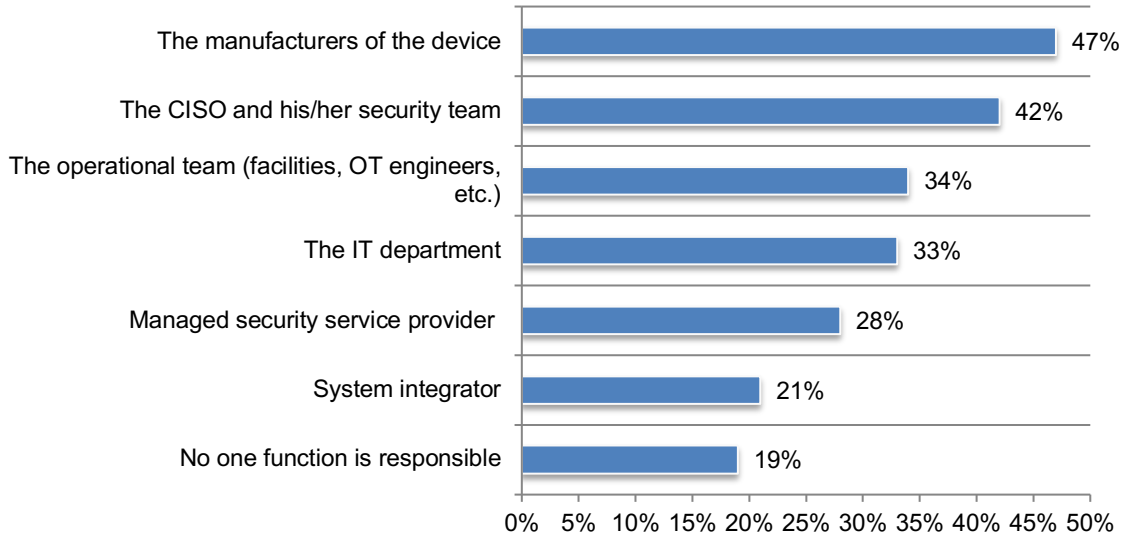


Results show that a source of significant vulnerabilities for many organizations is the connection of IoT devices operating in IT networks.

Organizations are relying upon manufacturers to secure IoT/OT devices. Fifty-five percent of respondents say they **do not believe** IoT/OT devices have been designed with security in mind and 11 percent of respondents say they **do not know**.

Yet, according to Figure 7 almost half (47 percent) of respondents are relying upon manufacturers to secure these devices. This is followed by assigning responsibility to the CISO and security team (42 percent).

Figure 7. Who secures IoT/OT devices within your organization?
More than one response permitted

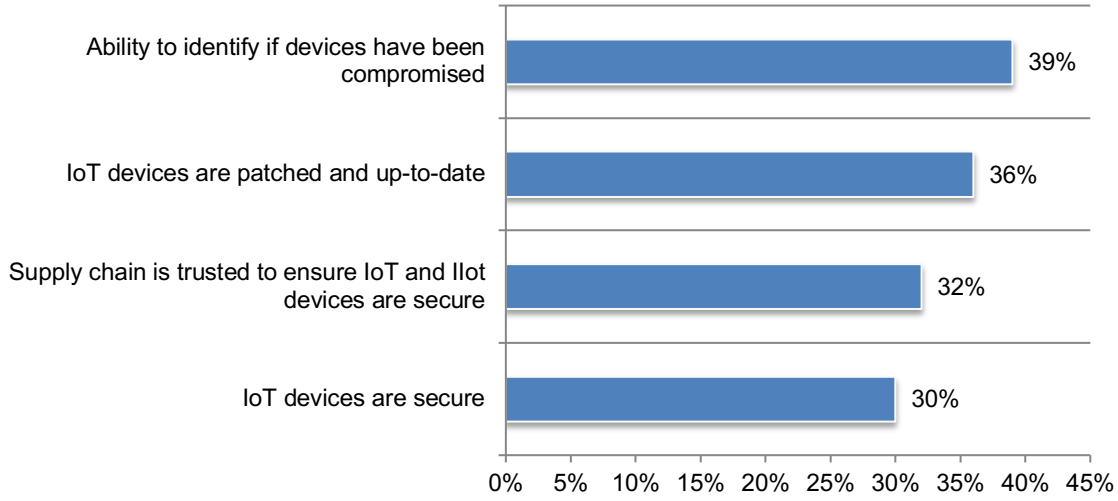


There is no clearly defined leader who has overall responsibility for ensuring the security of IoT/OT devices used throughout the organization. Ownership of this function is essential for establishing a strong IoT/OT governance and/or industrial control process.

There is a significant gap between the importance of IoT/OT devices and confidence in the security of these devices. Respondents were asked to rate the level of confidence in their organization's IoT/OT devices on a scale of 1 = no confidence to 10 = high confidence. Figure 8 presents the high confidence and very high responses (7+ on the 10-point scale).

As shown in Figure 8, only 30 percent of respondents have high or very high confidence that their IoT devices are secure, in their ability to identify if devices have been compromised (only 39 percent of respondents), IoT devices are patched and up-to-date (only 36 percent of respondents) and the supply chain is trusted to ensure IoT/OT devices are secure (32 percent of respondents).

Figure 8. Confidence in the security of IoT/OT devices
On a scale from 1 = no confidence to 10 = high confidence, 7+ responses presented



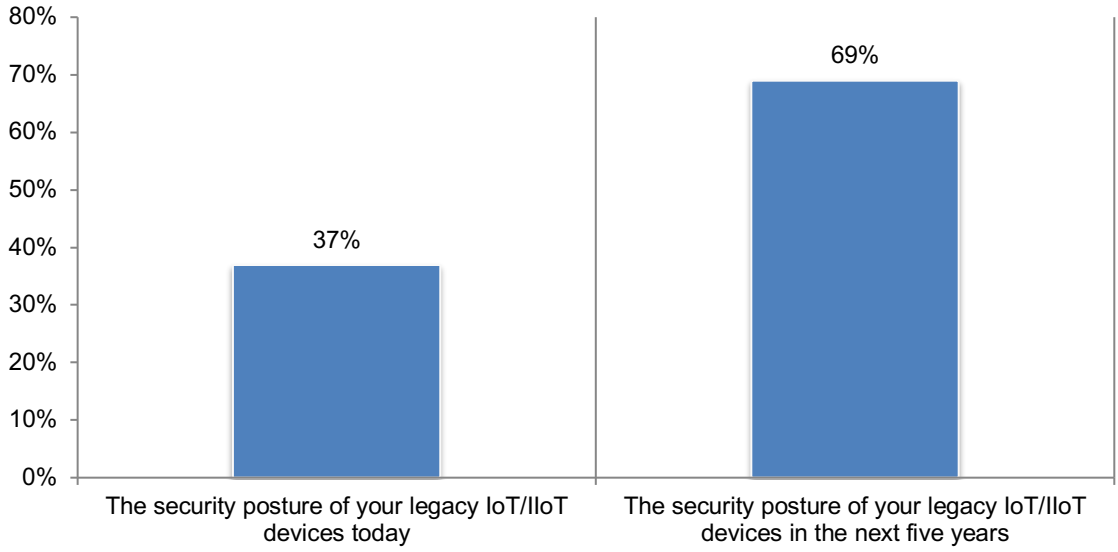
The lack of confidence in the security of IoT/OT devices is not surprising given the lack of strong governance and industrial control processes in many organizations.

The barriers and challenges to securing IoT/OT devices

While there are barriers and challenges to securing these devices, improvement in the IoT/OT security posture is expected to be achieved. As discussed previously, senior management recognizes the vulnerabilities of IoT/OT devices and is committed to making IoT/OT security a priority. Because of this commitment, respondents are optimistic that the security posture of IoT/OT devices will improve in the next five years, as shown in Figure 9.

Respondents were asked to rate the security posture of their organizations' legacy IoT/OT devices from a scale of 1 = not secure to 10 = highly secure. Figure 9 presents the security posture from secure to highly secure (7+ responses on the 10-point scale).

Figure 9. The security posture of legacy IoT/OT devices today and in five years
10-point scale from 1 = not secure to 10 = highly secure, 7+ responses presented

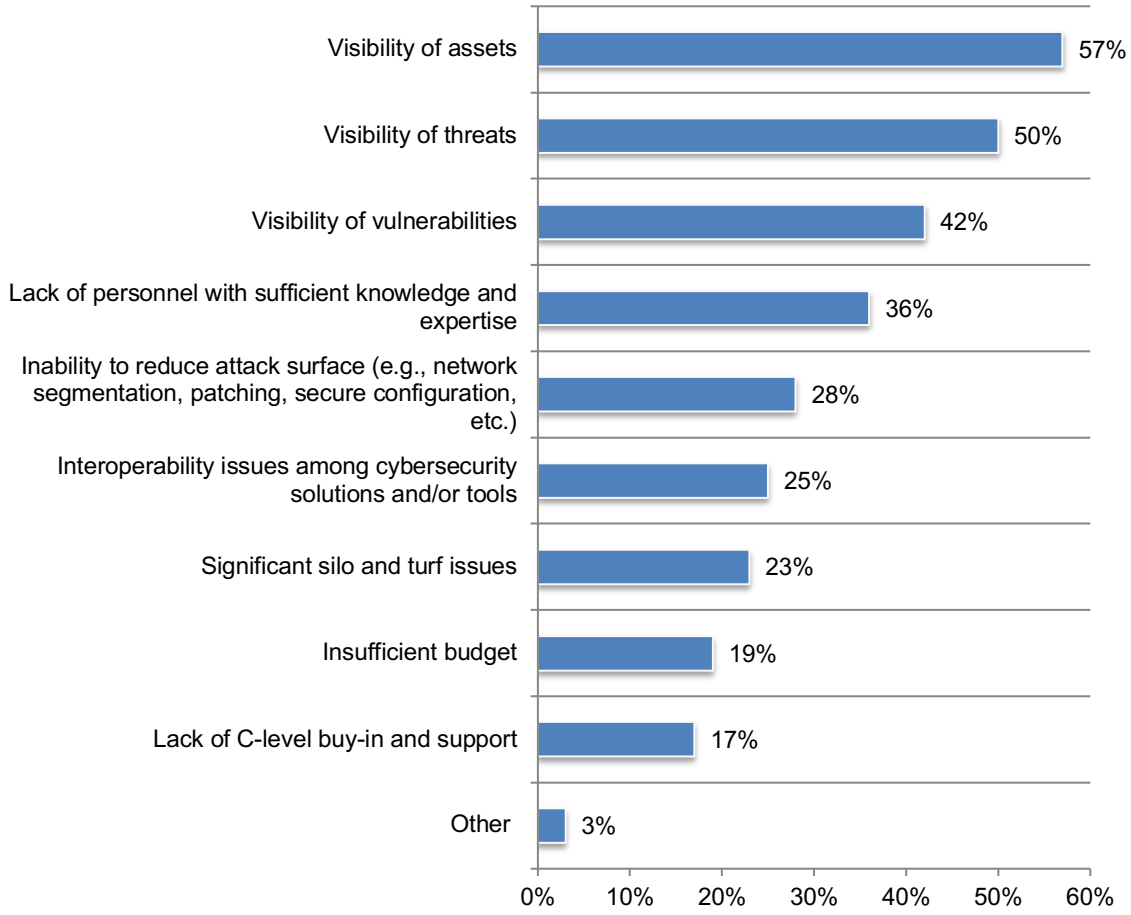


This figure paints a very positive picture about the state of IoT/OT security over the next five (5) years.

Lack of visibility is the primary barrier to ensuring the security of IoT/OT devices. According to Figure 10, 57 percent of respondents say the lack of visibility of their organizations' assets is affecting the security of IoT/OT devices. Organizations are also operating in the dark because of not having visibility of threats (50 percent of respondents) and visibility of vulnerabilities (42 percent of respondents).

Other barriers are a lack of personnel with sufficient knowledge and expertise (36 percent of respondents), interoperability issues among cybersecurity solutions (25 percent of respondents) and silo and turf issues (23 percent of respondents).

Figure 10. What are the primary barriers to ensuring the security of IoT and IIoT devices?



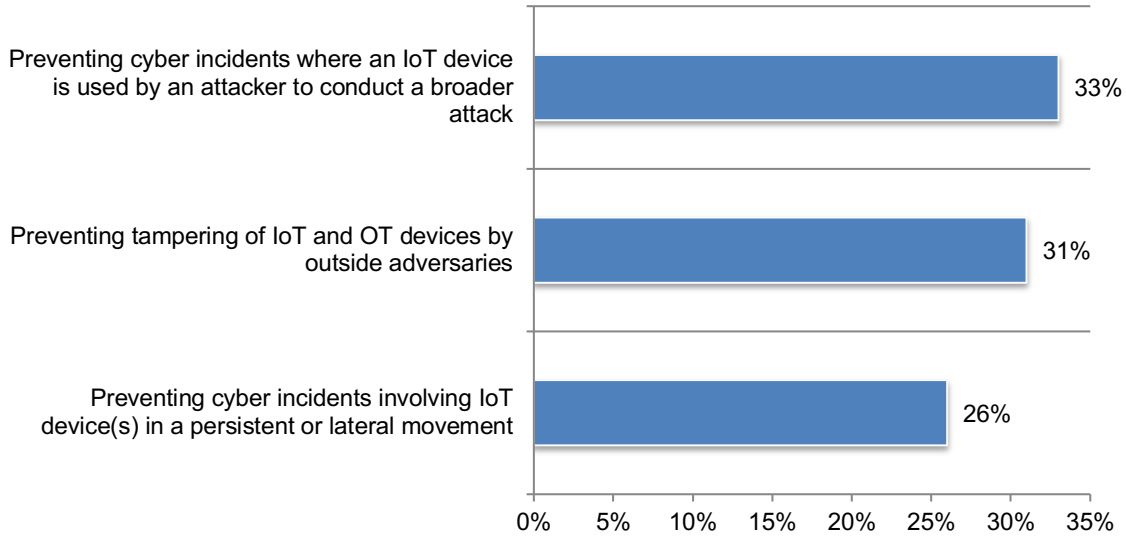
Our research shows the importance of visibility in the IoT/OT infrastructure in order to improve governance and control processes within my organization.

Organizations are ineffective in preventing cyberattacks against IoT/OT devices. Respondents were asked to rate the effectiveness of their organizations in preventing cyber incidents on a scale from 1 = not effective to 10 = highly effective. Figure 11 presents the 7+ responses on the 10-point scale (high to very high effectiveness).

As shown in Figure 11, only 33 percent of respondents rate the prevention of cyber incidents where IoT devices are used by an attacker to conduct broader attacks as high or highly effective, preventing the tampering of IoT and OT devices by outside adversaries (only 31 percent of respondents) and preventing cyber incidents involving IoT devices in a persistent or lateral movement (only 26 percent of respondents).

Figure 11. Effectiveness in organizations' ability to prevent cyber incidents involving IoT devices

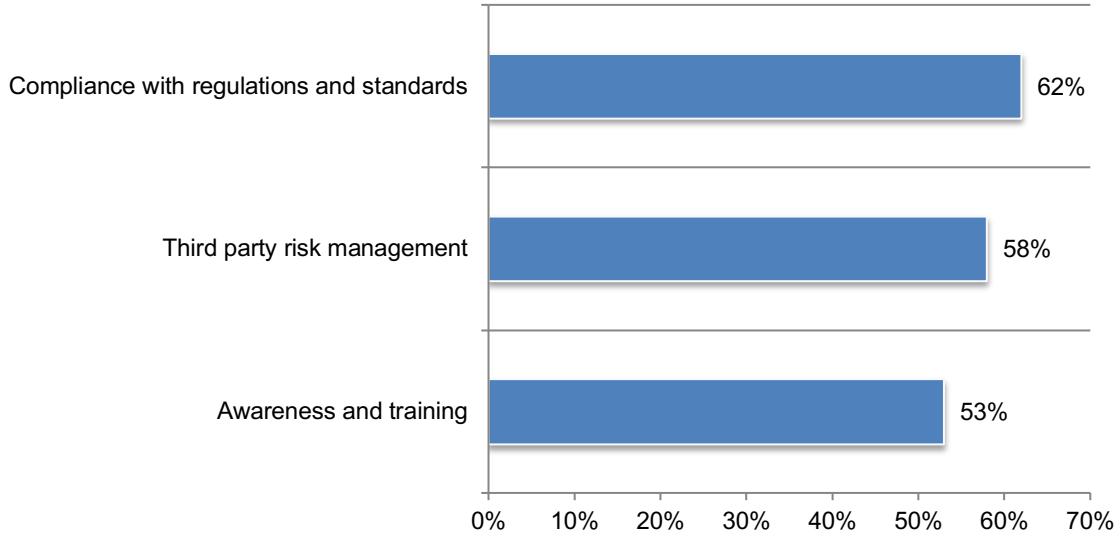
On a scale from 1 = not effective to 10 = highly effective, 7+ responses presented



The above figure shows the lack of effectiveness with respect to preventing cyber incidents, tampering of IoT devices deducting outside adversaries.

Organizations believe they are effective in achieving compliance with regulations. Respondents were asked to rate the effectiveness in meeting various features of their IoT/OT security program on a scale of 1 = not effective to 10 = very effective. The highly effective features (7+ responses) are shown in Figure 12. According to respondents, organizations are most effective in achieving compliance with regulations and standards (62 percent), third-party risk management (58 percent) and awareness and training (53 percent).

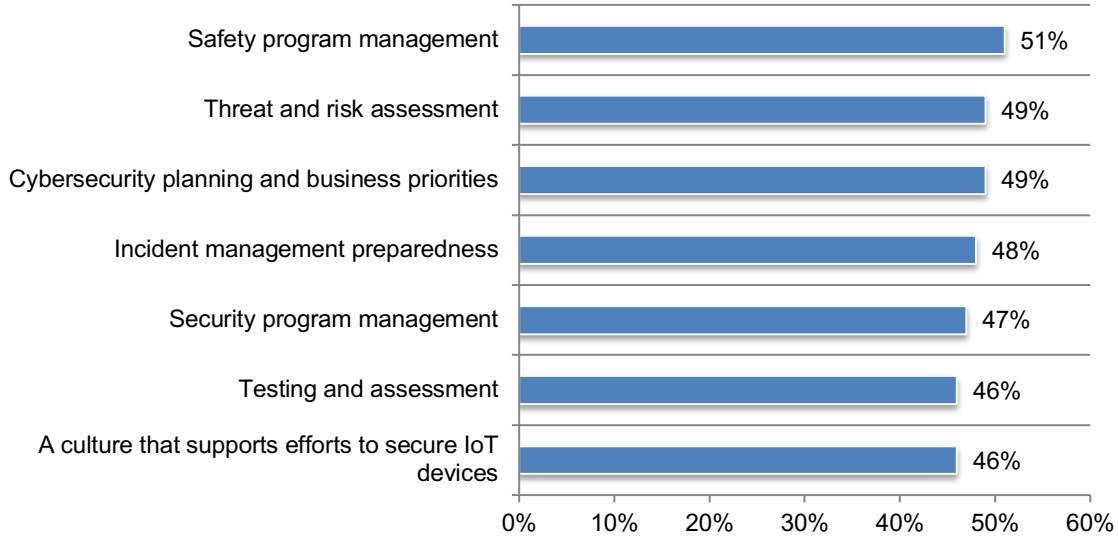
Figure 12. Effectiveness in meeting IoT/OT security program features
On a scale from 1 = not effective to 10 = very effective, 7+ responses presented



Organizations are generally positive with respect to meeting compliance requirements in the IoT/OT infrastructure.

Organizations are not effective in creating an effective IoT/OT security program. Respondents were asked to rate the effectiveness in achieving IoT security program features on a scale of 1 = not effective to 10 = very effective. Figure 13 presents the high effective or very effective respondents. As shown, most respondents are not confident in being effective in meeting IoT/OT security program features.

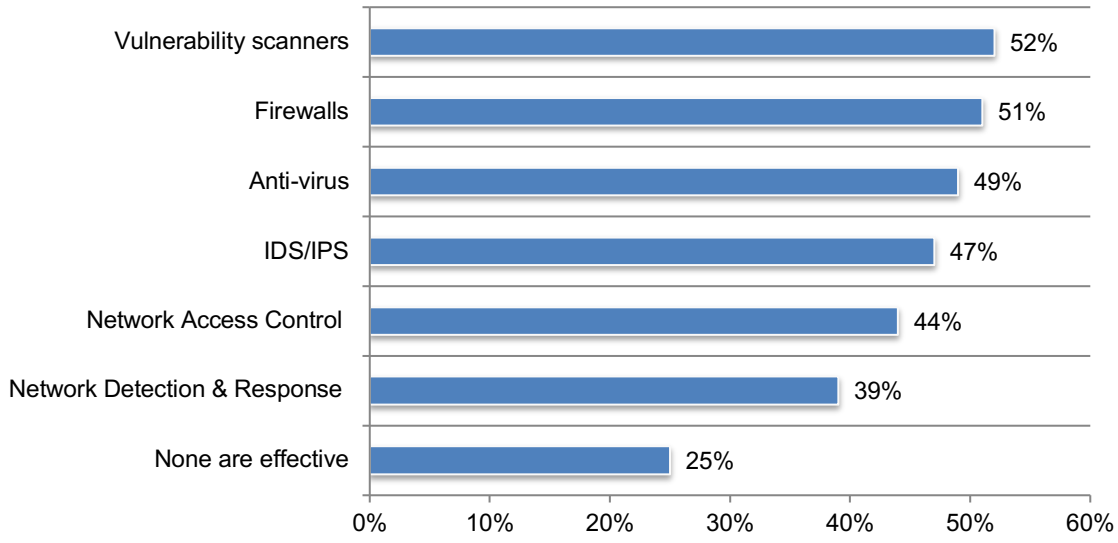
Figure 13. Following are features that relate to creating an effective IoT security program and their ability to be high or highly effective
On a scale from 1 = not effective to 10 = very effective, 7+ responses presented



The main features of a highly effective IoT security program include safety, threat assessment and other business priorities.

Network detection and response (NDR) solutions are shown to effectively secure IoT/OT devices, yet only 39 percent of respondents say their organizations are deploying them. Figure 14 presents security tools that can be used to secure devices. Fifty-two percent of respondents say their organizations use vulnerability scanners, 51 percent of respondents rely upon firewalls and 49 percent of respondents use anti-virus technologies. Many of these solutions are not applicable to securing devices, which indicates organizations are not mature in understanding how to achieve better security.

Figure 14. Which of the following existing security tools in the market can be used to effectively secure IoT/OT devices?
More than one response permitted



Our research suggests that organizations are using conventional IT security tools rather than OT-specific tools and applications to protect IoT devices and OT infrastructure.

How much would organizations spend on a more secure solution?

How valuable is a solution that would increase an organization's security posture in the IoT/OT environment? In this research, a second survey was conducted to determine how much more organizations would pay if they were assured that greater security would be achieved in the IoT/OT environment.

We surveyed individuals on four different scenarios as shown below to determine the average premium in percentage that organizations would pay to enhance their security posture. The four scenarios are as follows.

- How much more would you be willing to pay for an Enterprise IoT device that was designed to be as secure as a mobile device?
- How much more would you be willing to pay for an Enterprise IoT security solution that provides protection, detection and response capabilities that has the same level of efficacy as those that are available for traditional endpoints?
- How much more would you be willing to pay for an industrial IoT (OT/ICS) device that was designed to be as secure as a mobile device?
- How much more would you be willing to pay for industrial IoT (OT/ICS) security solution that provides protection, detection and response capabilities that has the same level of efficacy as those that are available for traditional endpoints?

In Table 1, the results are presented in four quartiles. Each quartile represents the average amount of premium in percentage respondents would be willing to pay. The research is divided between enterprise and industrial IoT. As shown, respondents will pay a higher average premium for industrial than enterprise: 23 percent and 32 percent premiums for enterprise vs. 37 percent and 41 percent for industrial.

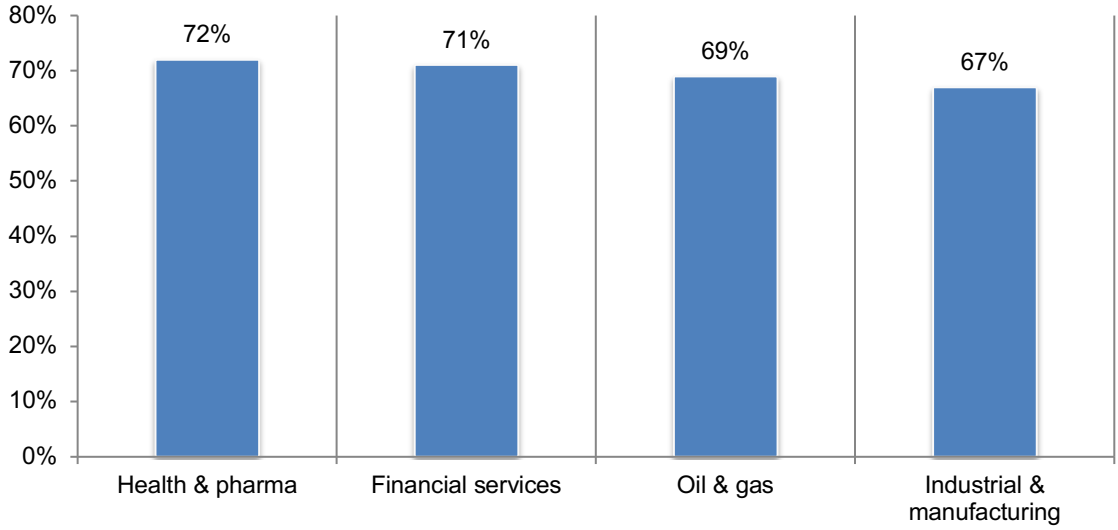
Table 1. How much are you willing to pay?	Enterprise IoT device	Enterprise IoT solution	Industrial IoT device	Industrial IoT solution
First quartile	19%	21%	24%	28%
Second quartile	20%	26%	29%	31%
Mean, median, mode	23%	32%	37%	41%
Third quartile	37%	42%	45%	50%
Fourth quartile	44%	50%	56%	62%
Difference	25%	29%	32%	34%

Industry differences

In this section, we provide findings from respondents in the following industries. These include financial services (92 respondents), oil & gas (55 respondents), industrial & manufacturing (74 respondents) and health & pharma (80 respondents).

All industries represented in this research are most likely to believe IoT/OT deployment is critical to their organizations' business goals. According to Figure 15, 72 percent of respondents in health & pharma and 71 percent of respondents in financial services say their organizations are committed to the deployment of IoT/OT devices.

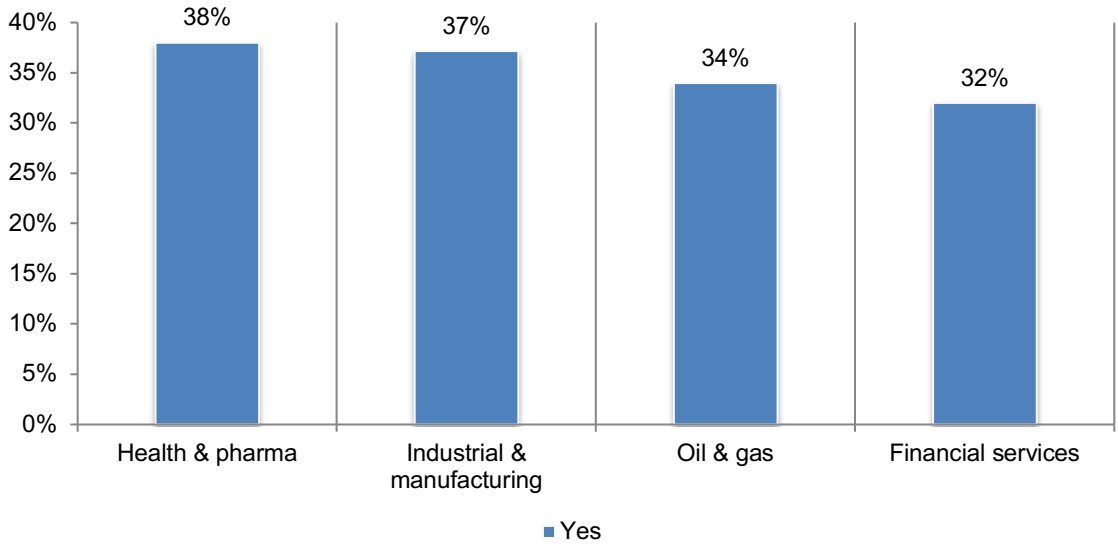
Figure 15. Senior management's perception about the importance of IoT/OT deployment
Strongly agree and Agree responses combined



The bar chart reveals that industry difference in the IoT/OT environment are only nominal (not statistically significant)

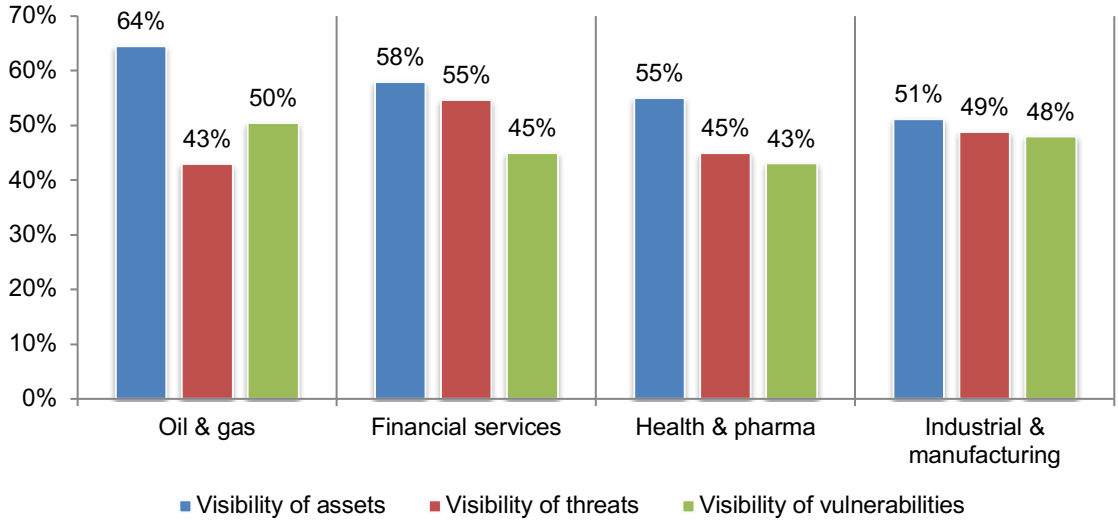
According to Figure 16, health & pharma and industrial & manufacturing are slightly more likely to have had a cyber incident in the past two years where an IoT device was used to conduct a broader attack.

Figure 16. Did your organization experience a cyber incident in the past two years where an IoT device was used by an attacker to conduct a broader attack?
Yes responses presented



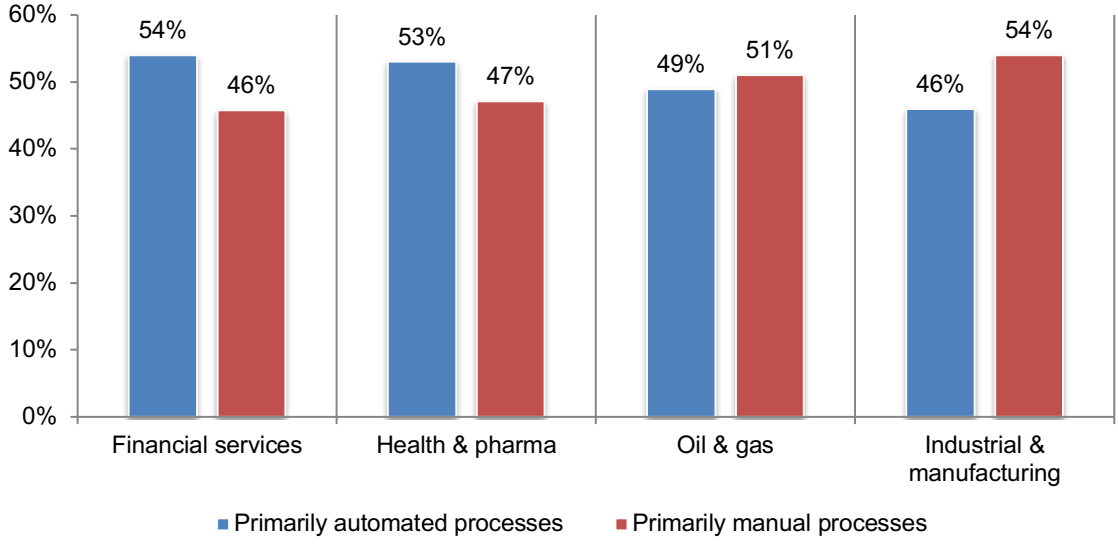
Visibility of assets, threats and vulnerabilities is critical to ensuring the security of IoT devices. Companies in the oil & gas industries are most likely to say the lack of visibility of their IoT assets (64 percent of respondents) followed by financial services (58 percent of respondents) is a barrier to ensuring the security of IoT devices**.** Health & pharma (43 percent of respondents) and financial services (45 percent of respondents) are less likely to say the lack of visibility of vulnerabilities is a barrier, as shown in Figure 17.

Figure 17. What are the top three barriers to ensuring the security of IoT devices?
Top three responses presented



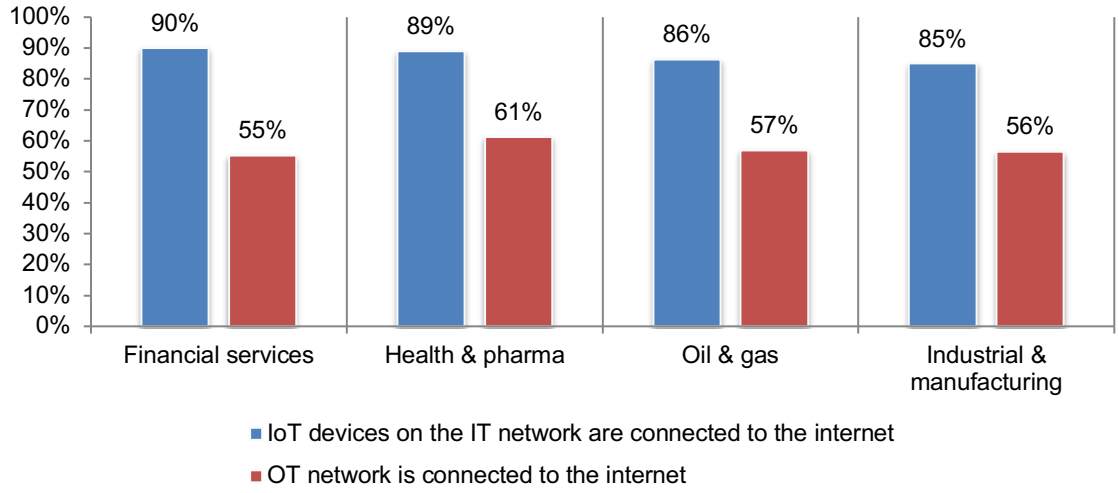
As shown in Figure 19, financial services (54 percent of respondents) and health & pharma (53 percent of respondents) are most likely to use automated processes to identify and correlate impacted IoT devices to the incidents and alerts raised by other security solutions such as SIEM and EDR. Companies in the industrial & manufacturing sector are most likely to rely upon manual processes.

Figure 18. What processes does your organization use to identify and correlate impacted IoT devices to the incidents and alerts raised by other security solutions such as SIEM and EDR?



Virtually every industry in this special analysis has IoT devices on the IT network connected to the internet, as shown in Figure 19. These connections are difficult to secure with traditional technologies. Moreover, the sheer volume of endpoints are a potential entry for attackers. The more devices connected, the more chance of a security incident.

Figure 19. The mythical airgap
Yes responses presented



Part 3. Methodology

A sampling frame of 17,003 IT and IT security practitioners in the United States who are knowledgeable about the state of cybersecurity in their organizations were selected as participants to this survey. Table 1 shows 672 total returns. Screening and reliability checks required the removal of 57 surveys. Our final sample consisted of 615 surveys or a 3.6 percent response.

Table 1. Sample response	Freq	Pct%
Sampling frame	17,003	100%
Total returns	672	4.0%
Rejected or screened surveys	57	0.3%
Final sample	615	3.6%

Figure 20 reports the respondent's organizational level within participating organizations. By design, more than half (54 percent) of respondents are at or above the supervisory levels. The largest category at 19 percent of respondents is manager.

Figure 20. Current position within the organization

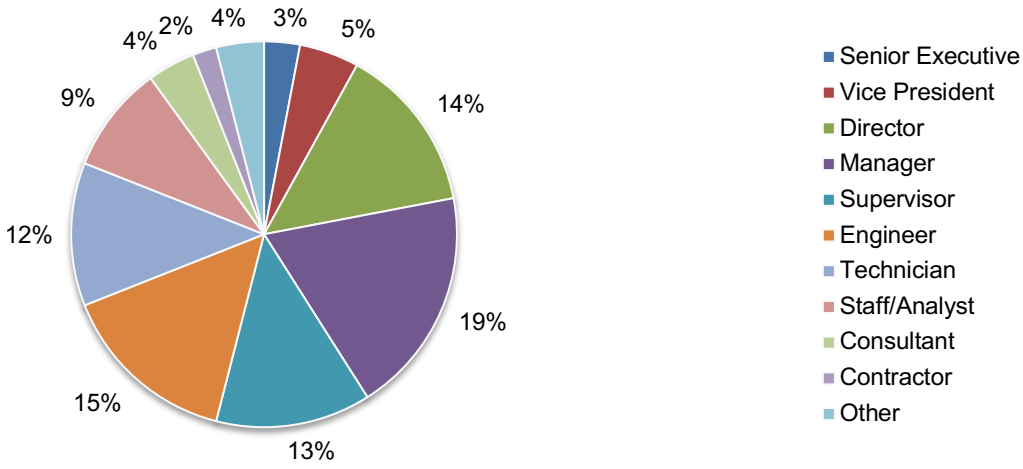


Figure 21 reports the primary person the respondent reports to within the organization. Twenty-six percent of respondents report to the chief information officer, 21 percent of respondents report to the chief information security officer and 10 percent of respondents report to the head of product engineering, as shown in Pie Chart 2.

Figure 21. Primary person respondent reports to within the organization

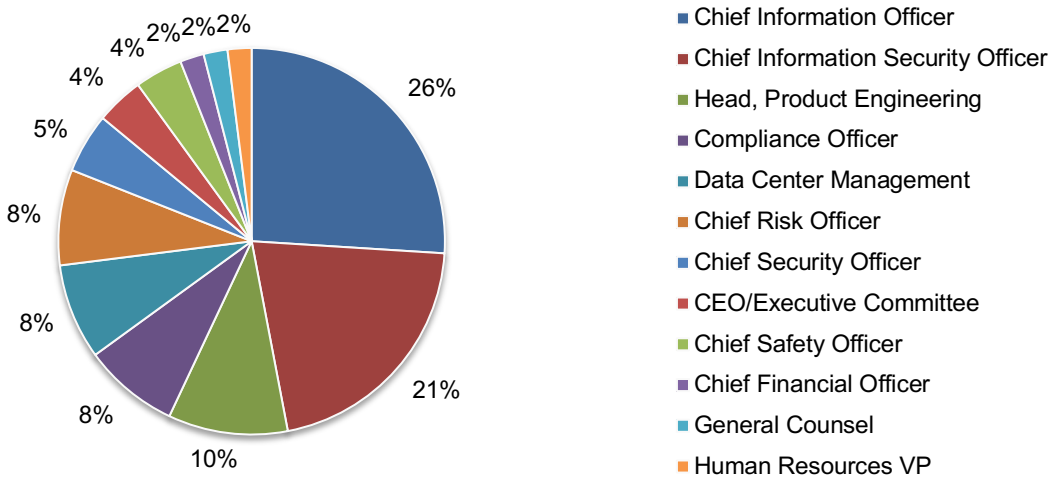
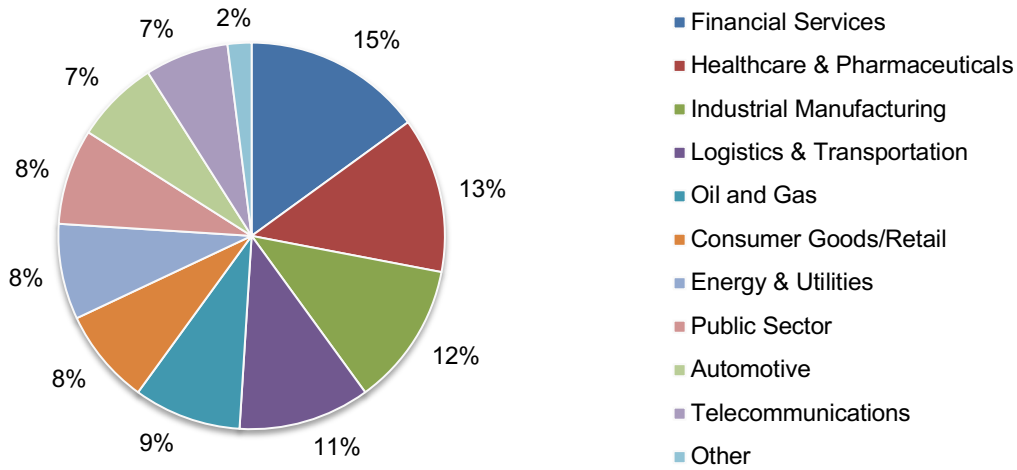


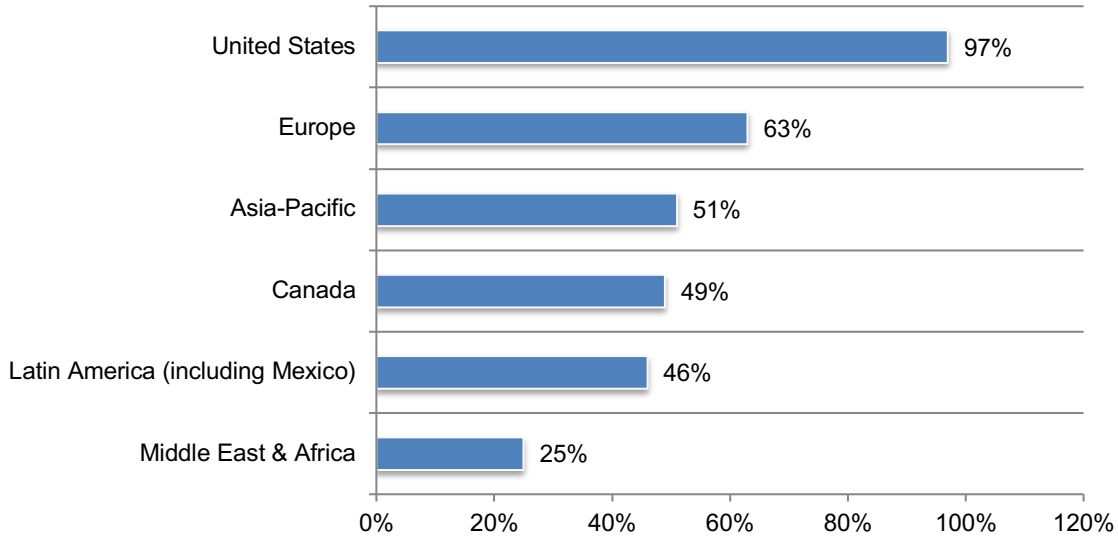
Figure 22 reports the industry focus of respondents' organizations. This chart identifies financial services (15 percent) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by healthcare and pharmaceuticals (13 percent of respondents), industrial manufacturing (12 percent of respondents), logistics and transportation (11 percent of respondents) and oil and gas (9 percent of respondents).

Figure 22. Primary industry focus



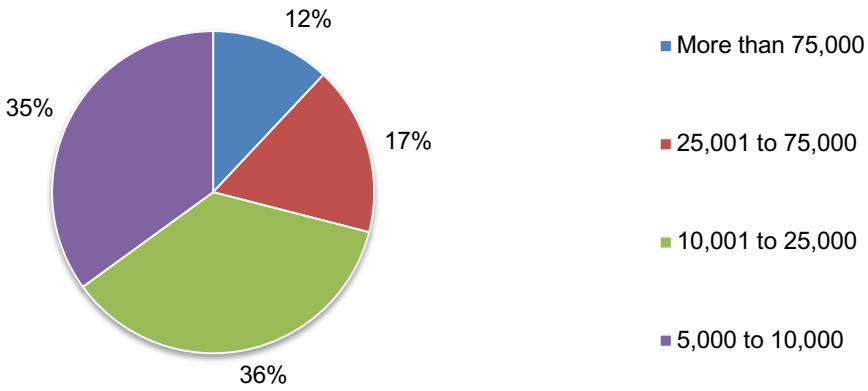
When asked where the employees are located, 97 percent of respondents identified the United States, 63 percent of respondents identified Europe, 51 percent of respondents identified Asia-Pacific, 49 percent of respondents identified Canada, 46 percent of respondents identified Latin America and 25 percent of respondents said their organization has employees in the Middle East and Africa.

Figure 23. Location of employees
More than one response permitted



As shown in Figure 24, 35 percent of respondents are from organizations with a global headcount of between 5,000 to 10,000, 36 percent of respondents are from organizations with a global headcount of between 10,000 and 25,000 and 29 percent of respondents are from organizations with more than 25,000 employees.

Figure 24. 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 and IT 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.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to al survey questions. All survey responses were captured in May 2021.

Survey response	Freq
Total sampling frame	17,003
Total returned surveys	672
Rejected surveys	57
Final sample	615
Response rate	3.6%

Part 1. Screening questions

S1. How familiar are you with the cybersecurity initiatives within your company today?	Pct%
Very familiar	45%
Familiar	34%
Somewhat familiar	21%
No knowledge (Stop)	0%
Total	100%

S2. How familiar are you with the use of enterprise IoT devices in your organization?	Pct%
Very familiar	39%
Familiar	36%
Somewhat familiar	25%
No knowledge (Stop)	0%
Total	100%

S3. How familiar or aware are you with OT/ICS/IIoT in your organization?	Pct%
Very familiar	41%
Familiar	32%
Somewhat familiar	27%
No knowledge (Stop)	0%
Total	100%

Part 2. Attributions

Please express your opinion about each one of the following statements using the agreement scale below each item. **Strongly agree and Agree responses combined.**	Pct%
Q1. Senior management believes IoT/OT is critical to supporting business innovation and other strategic goals.	68%
Q2. Senior management has made it a priority for IT and IT security practitioners to plan, develop or deploy IoT projects to advance business interests.	65%
Q3. IT security practitioners in our organization have slowed, limited, or stopped the adoption of IoT/OT projects due to security concerns.	31%
Q4. IT security practitioners in my organization believe that existing IoT/OT security solutions are in their infancy when compared to endpoint protection platforms (EPP) and endpoint detection and response (EDR) solutions.	53%
Q5. IT security practitioners in my organization view IoT/OT security as one of the least secured aspects of our IT/OT infrastructure.	60%
Q6. Senior management views improving IoT/OT security as one of their top security priorities over the next 12 to 24 months.	67%

Part 2. The state of cybersecurity in industrial organizations

Q7a. How has the volume of attacks against IoT/OT devices in your organization changed in the past 12 to 24 months?	Pct%
Significantly increased	26%
Increased	24%
Stayed the same	25%
Decreased	18%
Significantly decreased	7%
Total	100%

Q7b. How will the volume of attacks against IoT devices in your organization change in 2021 and beyond?	Pct%
Significantly increase	36%
Increase	27%
Stay the same	18%
Decrease	13%
Significantly decrease	6%
Total	100%

Q8. Did your organization experience a cyber incident in the past two years where an IoT device was involved?	Pct%
Yes	44%
No	50%
Unsure	6%
Total	100%

Q9. Did your organization experience a cyber incident in the past two years where an IoT device was used by an attacker to conduct a broader attack?	Pct%
Yes	35%
No	54%
Unsure	11%
Total	100%

Q10. Did your organization experience a cyber incident in the past two years where an IoT device was the target of the attack itself?	Pct%
Yes	39%
No	49%
Unsure	12%
Total	100%

Q11. What processes does your organization use to identify and correlate impacted IoT devices to the incidents and alerts raised by other security solutions such as SIEM and EDR? Please select only one choice.	Pct%
Primarily manual processes	47%
Primarily automated processes	53%
Total	100%

Q12. Who is ultimately accountable for the security of IoT/OT devices? Please select your top two choices.	Pct%
CISO and the security organization	25%
Operational leaders such as VP/Operations or VP/Manufacturing (OT organization)	30%
Line of business manager	12%
Product developer/engineer	16%
Other (please specify)	2%
No one function is responsible	15%
Total	100%

Q13. What are the primary barriers to ensuring the security of IoT and IoT devices? Please select your top three choices.	Pct%
Visibility of assets	57%
Visibility of vulnerabilities	42%
Visibility of threats	50%
Inability to reduce attack surface (e.g., network segmentation, patching, secure configuration, etc.)	28%
Lack of personnel with sufficient knowledge and expertise	36%
Lack of C-level buy-in and support	17%
Insufficient budget	19%
Significant silo and turf issues	23%
Interoperability issues among cybersecurity solutions and/or tools	25%
Other (please specify)	3%
Total	300%

Q14. Using the following scale from 1 = no confidence to 10 = high confidence, how confident are you that your IoT devices are secure?	Pct%
1 or 2	19%
3 or 4	30%
5 or 6	21%
7 or 8	18%
9 or 10	12%
Total	100%
Extrapolated value	4.98

Q15. Using the following scale from 1 = no confidence to 10 = high confidence, how confident are you in your organization's ability to identify if devices have been compromised?	Pct%
1 or 2	22%
3 or 4	28%
5 or 6	11%
7 or 8	18%
9 or 10	21%
Total	100%
Extrapolated value	5.26

Q16. Using the following scale from 1 = no confidence to 10 = high confidence, how confident are you that you have an accurate asset inventory of your IoT/OT devices in your security solutions?	Pct%
1 or 2	16%
3 or 4	27%
5 or 6	20%
7 or 8	22%
9 or 10	15%
Total	100%
Extrapolated value	5.36

Q17. Using the following scale from 1 = no confidence to 10 = high confidence, how confident are you that IoT/)OT devices in your organization are patched and up-to-date?	Pct%
1 or 2	20%
3 or 4	29%
5 or 6	15%
7 or 8	21%
9 or 10	15%
Total	100%
Extrapolated value	5.14

Q18. Using the following scale from 1 = no confidence to 10 = high confidence, how confident are you that your organization's supply chain is trusted to ensure IoT and OT devices are secure?	Pct%
1 or 2	16%
3 or 4	29%
5 or 6	23%
7 or 8	22%
9 or 10	10%
Total	100%
Extrapolated value	5.12

Q19. Using the following scale from 1 = not effective to 10 = highly effective, please rate the effectiveness of your organization in preventing cyber incidents involving IoT/OT device(s) in a persistent or lateral movement.	Pct%
1 or 2	15%
3 or 4	31%
5 or 6	28%
7 or 8	15%
9 or 10	11%
Total	100%
Extrapolated value	5.02

Q20. Using the following scale from 1 = not effective to 10 = highly effective, please rate the effectiveness of your organization in preventing cyber incidents where an IoT/OT device is used by an attacker to conduct a broader attack.	Pct%
1 or 2	21%
3 or 4	27%
5 or 6	19%
7 or 8	20%
9 or 10	13%
Total	100%
Extrapolated value	5.04

Q21. Using the following scale from 1 = not effective to 10 = highly effective, please rate the effectiveness of your organization in preventing tampering of IoT and OT devices by outside adversaries.	Pct%
1 or 2	16%
3 or 4	33%
5 or 6	20%
7 or 8	23%
9 or 10	8%
Total	100%
Extrapolated value	5.00

Following are program features that relate to the effective security of your organization's IoT/OT devices. Please use the 10-point scale to rate your organization's effectiveness in meeting each program feature. 1=not effective to 10=very effective.

Q22. A culture that supports efforts to secure IoT and OT devices	Pct%
1 or 2	10%
3 or 4	18%
5 or 6	26%
7 or 8	26%
9 or 10	20%
Total	100%
Extrapolated value	6.06

Q23. Cybersecurity planning and business priorities	Pct%
1 or 2	13%
3 or 4	20%
5 or 6	18%
7 or 8	23%
9 or 10	26%
Total	100%
Extrapolated value	6.08

Q24. Threat and risk assessment	Pct%
1 or 2	12%
3 or 4	20%
5 or 6	19%
7 or 8	22%
9 or 10	27%
Total	100%
Extrapolated value	6.14

Q25. Security program management	Pct%
1 or 2	13%
3 or 4	21%
5 or 6	19%
7 or 8	22%
9 or 10	25%
Total	100%
Extrapolated value	6.00

Q26. Safety program management	Pct%
1 or 2	9%
3 or 4	20%
5 or 6	20%
7 or 8	26%
9 or 10	25%
Total	100%
Extrapolated value	6.26

Q27. Incident management preparedness	Pct%
1 or 2	12%
3 or 4	19%
5 or 6	21%
7 or 8	18%
9 or 10	30%
Total	100%
Extrapolated value	6.20

Q28. Awareness and training	Pct%
1 or 2	10%
3 or 4	23%
5 or 6	14%
7 or 8	25%
9 or 10	28%
Total	100%
Extrapolated value	6.26

Q29. Testing and assessment	Pct%
1 or 2	12%
3 or 4	24%
5 or 6	18%
7 or 8	15%
9 or 10	31%
Total	100%
Extrapolated value	6.08

Q30. Compliance with regulations and standards	Pct%
1 or 2	9%
3 or 4	11%
5 or 6	18%
7 or 8	27%
9 or 10	35%
Total	100%
Extrapolated value	6.86

Q31. Third party risk management	Pct%
1 or 2	13%
3 or 4	10%
5 or 6	19%
7 or 8	28%
9 or 10	30%
Total	100%
Extrapolated value	6.54

Part 3. Background on device cyber protection

Q32. What best describes the maturity of your organization's IoT/OT industrial controls program?	Pct%
Early stage – many industrial control program activities have not as yet been planned or deployed. Response to cybersecurity issues is reactive and ad hoc. Resources are not sufficient for staffing and administration of the program.	19%
Middle stage – industrial control program activities are planned and defined but only partially deployed. Efforts are being made to establish security protocols, business processes and workflows.	34%
Late-middle stage – industrial control program activities are deployed across the enterprise. The program has C-level support and adequate budget.	26%
Mature stage – industrial control program activities are fully deployed and maintained across the enterprise. C-level executives and board are regularly informed about the effectiveness of the program. Program activities are measured with KPIs.	21%
Total	100%

Q33a. Does your organization have a complete inventory of its IoT/OT devices?	Pct%
Yes	29%
No	62%
Don't know	9%
Total	100%

Q33b. If yes, how many IoT/OT devices does your organization have?	Pct%
Less than 1,000	12%
1000 to 5,000	23%
5,000 to 10,000	25%
10,000 to 25,000	24%
More than 25,000	11%
Do not know	5%
Total	100%
Extrapolated value	9,685

Q34. Which of the following existing security tools in the market can be used to effectively secure IoT/OT devices? Please check all that apply.	Pct%
Firewalls	51%
Anti-virus	49%
Vulnerability scanners	52%
Endpoint Protection Platforms (EPP)	34%
Endpoint Detection & Response (EDR)	32%
Network Detection & Response (NDR)	39%
Network Access Control (NAC)	44%
IDS/IPS	47%
None are effective	25%
Total	373%

Q35. Do you believe that existing IoT/OT devices have been designed with security in mind?	Pct%
Yes	34%
No	55%
Do not know	11%
Total	100%

Q36. Who secures IoT/OT devices within your organization? Please select all that apply.	Pct%
The manufacturers of the device	47%
System integrator	21%
Managed security service provider (MSSP)	28%
The IT department	33%
The CISO and his/her security team	42%
The operational team (facilities, OT engineers, etc.)	34%
No one function is responsible	19%
Total	224%

Q37. What are the top three IoT/OT security risks facing your organization? Please select only three responses.	Pct%
Compliance with industry standards/regulations	54%
Theft of sensitive IP such as proprietary formulas and manufacturing processes	57%
Production downtime resulting in revenue loss	43%
Safety and/or environmental incidents	38%
Brand impact	19%
Cost of breach recovery and response	28%
Supply chain risks	58%
Other (please specify)	3%
Total	300%

Q38a. Using the following 10-point scale, please rate the security posture of your organization's legacy IoT/OT devices **today** from 1 = not secure to 10 = highly secure	Pct%
1 or 2	20%
3 or 4	20%
5 or 6	23%
7 or 8	20%
9 or 10	17%
Total	100%
Extrapolated value	5.38

Q38b. Using the following 10-point scale, please rate the security posture of your organization's legacy IoT/OT devices in the next **five years** from 1 = not secure to 10 = highly secure	Pct%
1 or 2	10%
3 or 4	7%
5 or 6	14%
7 or 8	32%
9 or 10	37%
Total	100%
Extrapolated value	7.08

Q39. Is your OT network connected to your corporate IT (business) network (e.g., for SAP, remote access, etc.)?	Pct%
Yes	51%
No	49%
Total	100%

Q40. Is your OT network connected to internet (e.g., for remote access) or do you have any OT devices on the OT network that are connected to the internet?	Pct%
Yes	56%
No	44%
Total	100%

Q41. Do you have any IoT devices on your IT network that are connected to the internet (e.g., smart TV conferencing systems, printers connected to cloud printing services, etc.)?	Pct%
Yes	88%
No	12%
Total	100%

Part 4. Budget

Q42a. What range best describes your organization's annual IT operations budget in the current fiscal year?	Pct%
Less than $1 million	1%
$1 to $10 million	5%
$11 to $25 million	9%
$26 to $50 million	12%
$51 to $100 million	17%
$101 to $250 million	25%
$251 to $500 million	18%
More than $500 million	13%
Total	100%
Extrapolated value (US$ millions)	$ 208.33

Q42b. If yes, what percentage of your company's IT security budget is dedicated to securing IoT/IIoT/ICS devices.	Pct%
None	0%
Less than 1%	4%
Less than 5%	11%
Less than 10%	25%
More than 10%	60%
Total	100%
Extrapolated value	10%

Part 4. Your role and organization

D1. What organizational level best describes your current position?	Pct%
Senior Executive	3%
Vice President	5%
Director	14%
Manager	19%
Supervisor	13%
Engineer	15%
Technician	12%
Staff / Analyst	9%
Consultant	4%
Contractor	2%
Other	4%
Total	100%

D2. Check the **Primary Person** you or your IT security leader reports to within the organization.	Pct%
CEO/Executive Committee	4%
Chief Financial Officer	2%
General Counsel	2%
Chief Information Officer	26%
Chief Information Security Officer	21%
Compliance Officer	8%
Chief Safety Officer	4%
Chief Privacy Officer	0%
Human Resources VP	2%
Head, Product Engineering	10%
Chief Security Officer	5%
Data Center Management	8%
Chief Risk Officer	8%
Other (please specify)	0%
Total	100%

D3. What industry best describes your organization's industry focus?	Pct%
Automotive	7%
Consumer Goods / Retail	8%
Energy & Utilities	8%
Financial Services	15%
Healthcare & Pharmaceuticals	13%
Industrial Manufacturing	12%
Logistics & Transportation	11%
Oil and Gas	9%
Public Sector	8%
Telecommunications	7%
Other (please specify)	2%
Total	100%

D4. Where are your employees located? (Select all that apply)	Pct%
United States	97%
Canada	49%
Europe	63%
Asia-Pacific	51%
Middle East & Africa	25%
Latin America (including Mexico)	46%
Total	331%

D5. What is the worldwide headcount of your organization?	Pct%
Less than 5,000	0%
5,000 to 10,000	35%
10,001 to 25,000	36%
25,001 to 75,000	17%
More than 75,000	12%
Total	100%

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.