Second Annual Study on The Internet of Things (IoT): A New Era of Third-Party Risk

Sponsored by Shared Assessments

Independently conducted by Ponemon Institute LLC

Publication Date: March 2018

SFG | SHARED ASSESSMENTS
The Trusted Source in Third Party Risk Management

Second Annual Study on The Internet of Things (IoT): A New Era of Third-Party Risk

Ponemon Institute: March 2018

Part 1. Introduction

With the proliferation of IoT devices in the enterprise, managing third-party risks to sensitive and confidential data has become a herculean task. As revealed in *The Second Annual Study on the Internet of Things (IoT): A New Era of Third-Party Risk,* companies are deeply concerned that failure to prevent a data breach or cyber attack due to an unsecured IoT device would have catastrophic consequences.

In the context of this research, IoT is defined as the network of physical objects or "things" embedded with electronics, software, sensors and network connectivity, which enables these objects to collect, monitor and exchange data. Examples of IoT devices in the workplace include network-connected printers and building automation solutions.

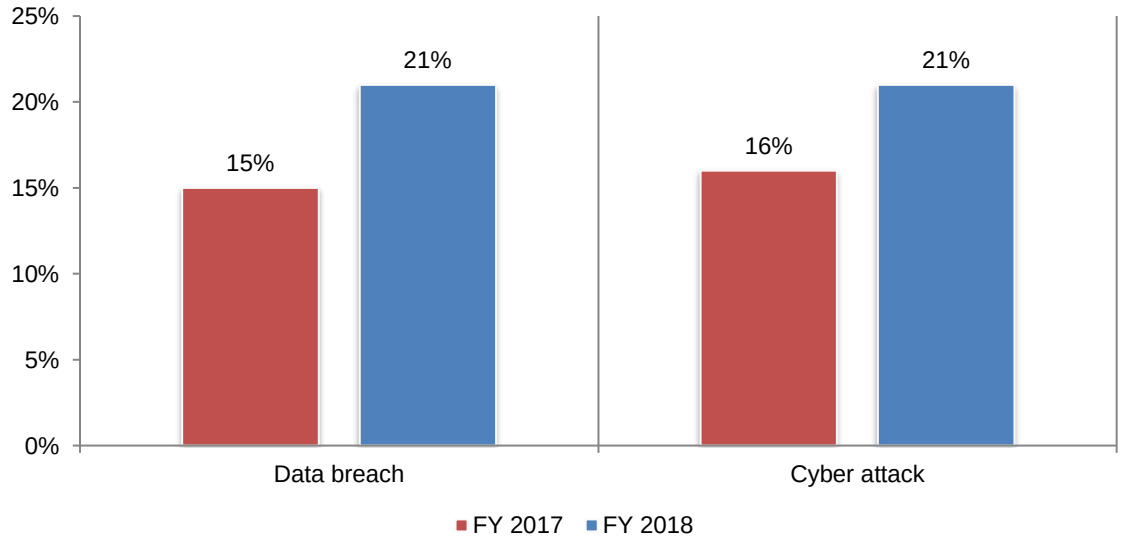
This is the third Third-Party Risk study sponsored by Shared Assessments and conducted by Ponemon Institute. Responses from 605 individuals who participate in corporate governance and/or risk oversight activities, and are familiar with the use of IoT devices in their organization are included in this study.

This year's study shows that while there have been some advances in third-party risk focused on IoT devices and applications from 2017, risk management in this area is still at a relatively low level of maturity.

As shown in Figure 1, worries about a potential breach or cyber attack have become a reality. Respondents who report their organization experienced a data breach **specifically because of unsecured IoT devices or applications** increased from 15 percent to 21 percent. Cyber attacks increased from 16 percent to 21 percent of respondents.

Figure 1. Has your organization experienced a data breach or cyber attack caused by unsecured IoT devices or applications in the past 12 months?

Yes responses reported



Most salient trends

The Awareness of IoT Risk Is Increasing at a Faster Rate than the Maturity of Practices

While organizations' monitoring of their third-parties' IoT devices is increasing, the gains are still at a very low level. Only 29 percent of survey respondents say their organizations actively monitor the risk of IoT devices used by third parties. That being said, more companies (28 percent) are considering IoT related risk to be part of the third-party due diligence process. Further, the evaluation and inclusion of third-party IoT security risks as part of onboarding remains very low with only 26 percent of respondents in 2018.

Concerns have increased that a security incident related to unsecured IoT devices could be catastrophic. Ninety-seven percent of respondents say it is likely that a data breach or cyber attack related to unsecured IoT devices could be catastrophic for the organization.

In the next 24 months, more respondents believe their organizations will have a data breach and cyber attack caused by unsecured IoT devices or applications. This year, 81 percent of respondents say a data breach caused by unsecured IoT devices was likely, and the likelihood of a cyber attack such as a denial of service increased to 82 percent.

The number of IoT devices in the workplace will increase significantly. Forty-four percent of respondents say their organizations keep an inventory, and the average number of devices in the workplace is 15,874. This number is expected to increase to an average of 24,762.

More organizations consider IoT devices to be endpoints. Sixty percent of respondents say their organizations consider IoT devices to be endpoints to their networks or enterprise systems. However, most rely on contractual clauses and policies with third parties to control or disable IoT devices and applications that pose a risk.

Risk Management Practices Focused on IoT Are Uneven

Most organizations highlight the importance of a strong tone at the top, but indicate that it is not possible to determine whether third-party safeguards are sufficient. Sixty-six percent of respondents indicate the most important governance practice is a strong tone at the top. However, 58 percent of respondents indicate that it is not possible to determine if IoT and third-party safeguards are sufficient.

Most organizations rely on contract clauses and policies to mitigate third-party IoT risk, but fewer than half can monitor third-party contract compliance. Fifty-three percent of respondents say they rely on contractual agreements, and 46 percent of respondents indicate they have a policy in place to disable IoT devices that pose a risk. Only 26 percent indicate the use of a third party IoT assessment technique to identify and mitigate that risk.

Most organizations are not keeping an inventory of managed IoT devices or applications. Fifty-six percent of respondents do not inventory their IoT devices. The primary reason, according to 88 percent of respondents, is no centralized control over IoT devices and applications in the workplace. Sixty-four percent of respondents do not keep an inventory of IoT applications, mainly because of a lack of centralized control over these applications. Fewer than 20 percent of survey respondents say their organizations can identify a majority of the IoT devices.

More companies have a third-party risk management program. Sixty percent of respondents, say their companies have a third-party risk management program. Forty-two percent of these respondents say the program is part of their companies' enterprise risk management program, but only 29 percent of respondents say their organizations actively monitor the risk of IoT devices used by third parties.

The Gap between Internal and Third Party IoT Monitoring Is Substantial

Monitoring the risk of IoT devices used in the workplace increases. Fifty percent of respondents say their organizations monitor the risk of IoT devices inside of their organizations, up six percent from 2017. However, only 29 percent of respondents say their organizations monitor the risk of IoT devices used by third parties.

More organizations are applying third-party risk management practices to prevent security incidents. While not as prevalent as they should be**,** risk management practices such as requiring third parties to identify IoT devices connected to their network increased to 46 percent of respondents from 41 percent of respondents in 2017.

Most organizations indicate that new techniques are required to monitor IoT risks both internally and at their third parties. Seventy-one percent of respondents indicate the drive for innovation requires new approaches to IT risk management strategies and tactics.

Part 2. Key findings

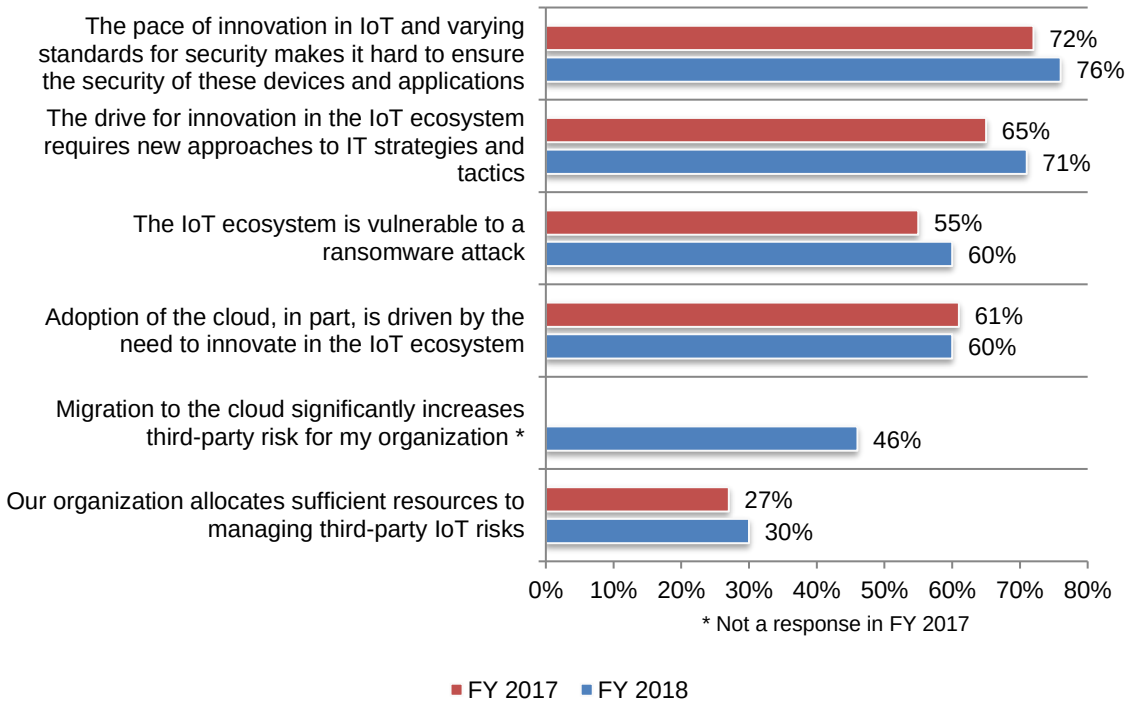
In this section, we provide an analysis of the research. The complete audited findings are presented in the Appendix of this report. We have organized the report according to the following topics:

The rise of IoT devices significantly increases third-party risk

IoT devices and applications are vulnerable to a ransomware attack. According to respondents, the average number of IoT devices in their organizations is expected to increase significantly in the next two years, from today's average of 15,874 to 24,762. With the plethora of unsecured IoT devices in the workplace, more respondents (60 percent of respondents vs. 55 percent in last year's study) believe the IoT ecosystem is vulnerable to a ransomware attack, as shown in Figure 2.

The pace of innovation in IoT and the varying standards for security among third parties make it difficult to ensure the security of these devices and applications, according to 76 percent of respondents, an increase from 72 percent. In addition, the drive for innovation requires new approaches to IT strategies and tactics, and 60 percent say adoption of the cloud is driven, in part, by the need to innovate in the IoT ecosystem.

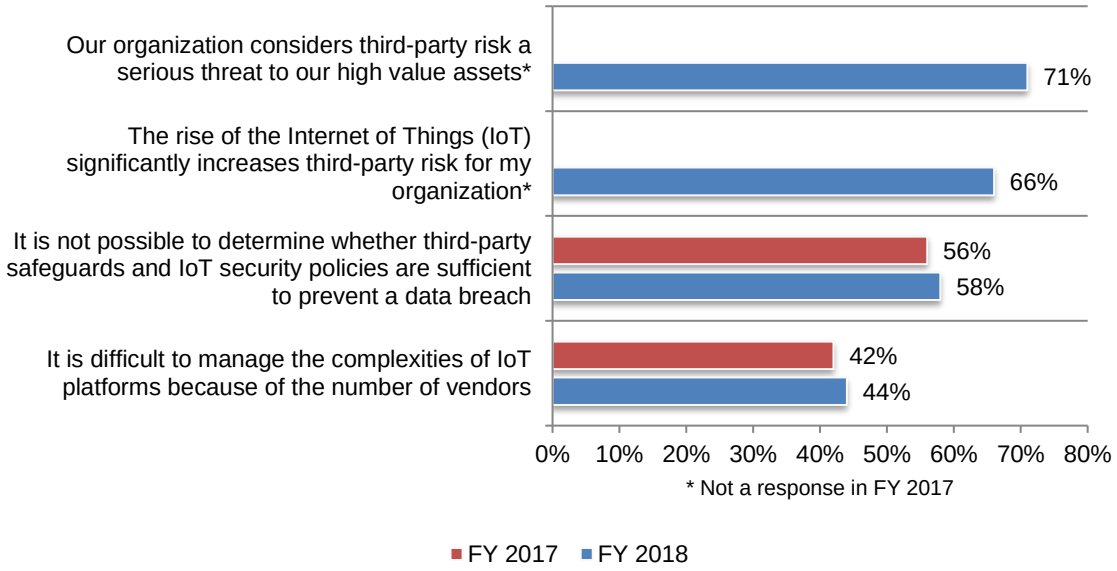
Figure 2. Perceptions about business innovation and IoT risks
Strongly agree and Agree responses combined



Third-party risk, especially to high-value assets, increases because of IoT. As shown in Figure 3, 71 percent of respondents say their organizations consider third-party risk a serious threat to their high-value assets and 66 percent of the respondents say the importance of the IoT ecosystem significantly increases third-party risk.

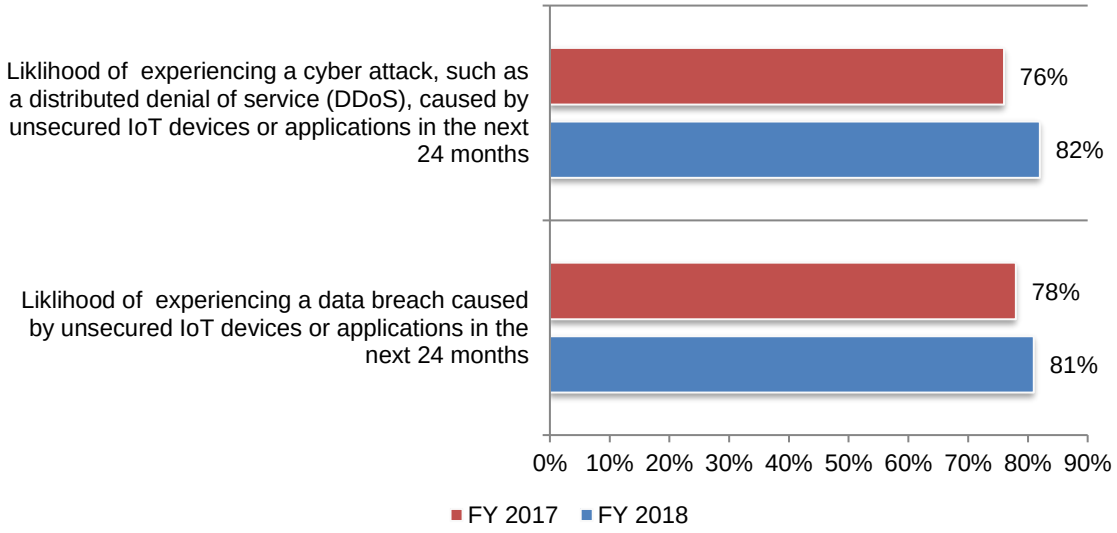
Fifty-eight percent of respondents say it is not possible to determine whether third-party safeguards and IoT security policies are sufficient to prevent a data breach. Forty-four percent of respondents say their organizations find it difficult to manage the complexities of IoT platforms because of the number of vendors.

Figure 3. Why third-party risks increase
Strongly agree and Agree responses combined



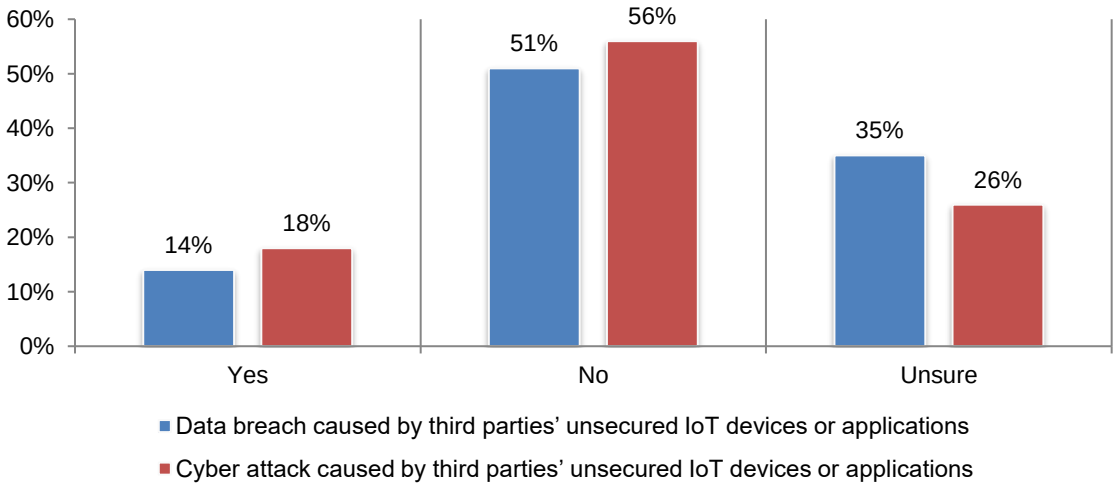
The likelihood of a data breach or cyber attack increases. As shown in Figure 4, 82 percent of respondents believe a cyber attack, such as a distributed denial of service (DDoS), is likely to occur, an increase from 76 percent of respondents in last year's study. Similarly, more respondents believe a data breach caused by unsecured IoT devices is likely.

Figure 4. How likely is a data breach or cyber attack caused by unsecured IoT devices or applications in the next 24 months?
Very likely, Somewhat likely and Likely responses combined



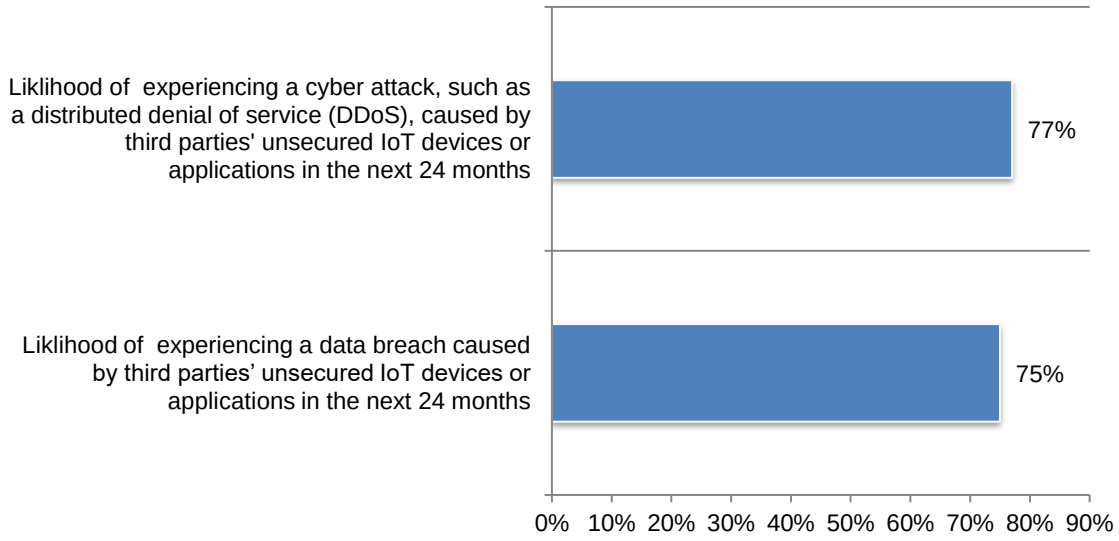
Many organizations in this research are uncertain whether a data breach or cyber attack caused by one of their third-parties' IoT devices occurred. As shown in Figure 5, 35 percent of respondents do not know if they were able to detect a third-party data breach and 26 percent of respondents are unsure their organization was affected by a cyber attack involving an IoT device.

Figure 5. Has your company experienced a data breach or cyber attack caused by a third party's unsecured IoT devices?



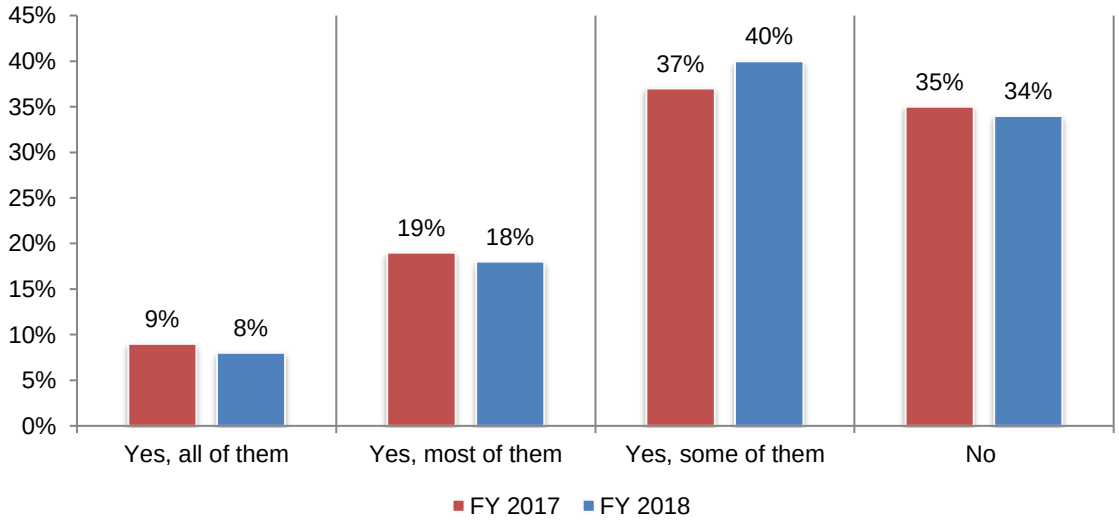
While many respondents do not believe they have experienced a data breach or cyber attack caused by a third party's unsecured IoT device, 77 percent of respondents believe such a cyber attack is likely, and 75 percent believe a data breach is likely.

Figure 6. How likely will your organization have a data breach or cyber attack caused by a third party's unsecured IoT devices?
Very likely, Somewhat likely and Likely responses combined



Similar to last year, most organizations represented in this research are not aware of all or most of the network of physical objects connected to the Internet. Figure 7 presents the trends in awareness about the network of physical objects connected to the Internet. In this year's study, 26 percent of respondents say their organizations know all (8 percent) or most (18 percent) of the physical objects, such as printers or building automation solutions, connected to the Internet. Thirty-four percent of respondentsss say their organizations have no understanding of which physical devices are connected to the Internet.

Figure 7. Are you aware of the network of physical objects that are connected?

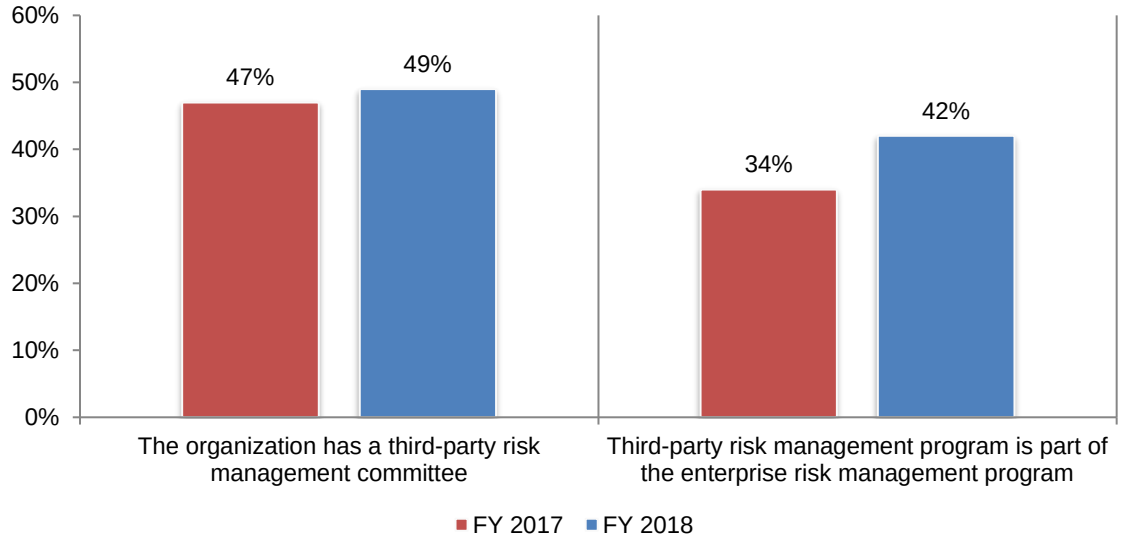


IoT risk management practices are uneven and most are ineffective

Many third-party management risk programs are ineffective. Sixty percent of respondents say their organizations have a third-party risk management program. Of these, only 28 percent of respondents rate their third-party risk management program as highly effective.

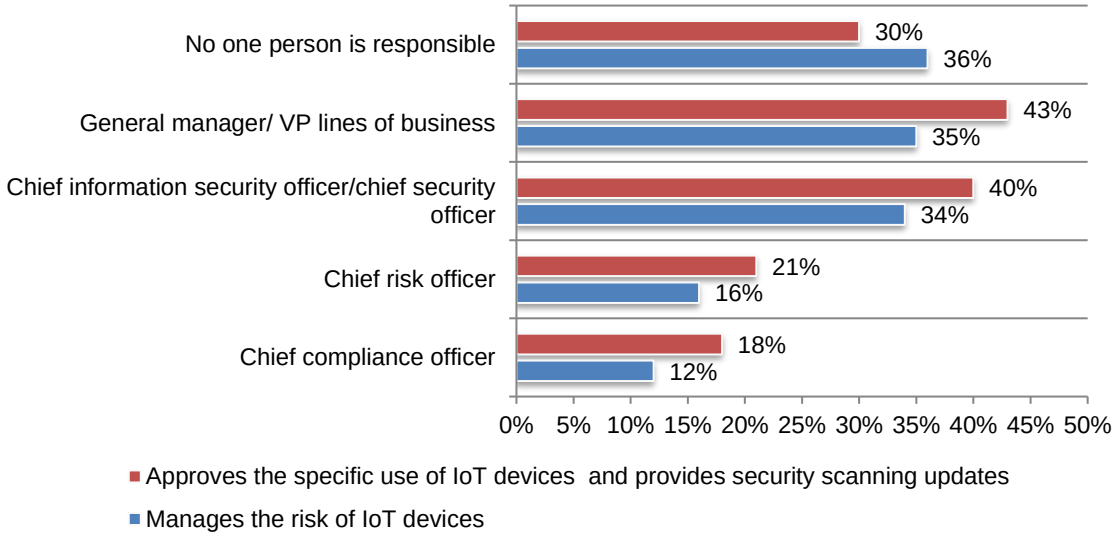
Trends in reasons for not achieving a high level of effectiveness are shown in Figure 8. Specifically, only 49 percent of those respondents that have a third-party management program have a third-party risk management committee, a slight increase from 47 percent of respondents in last year's research. More respondents in this year's study say their companies' third-party risk management program is part of their organizations' enterprise risk management program (an increase from 34 percent of respondents to 42 percent of respondents).

Figure 8. Why current third-party risk management programs are not ready for IoT
Yes responses reported



There is a gap between who approves the specific uses of IoT devices and those who manage the risk. As shown in Figure 9, while 43 percent of respondents say the general manager/VP lines of business is responsible for approving the use of IoT devices, only 35 percent of respondents say they are responsible for managing the risk.

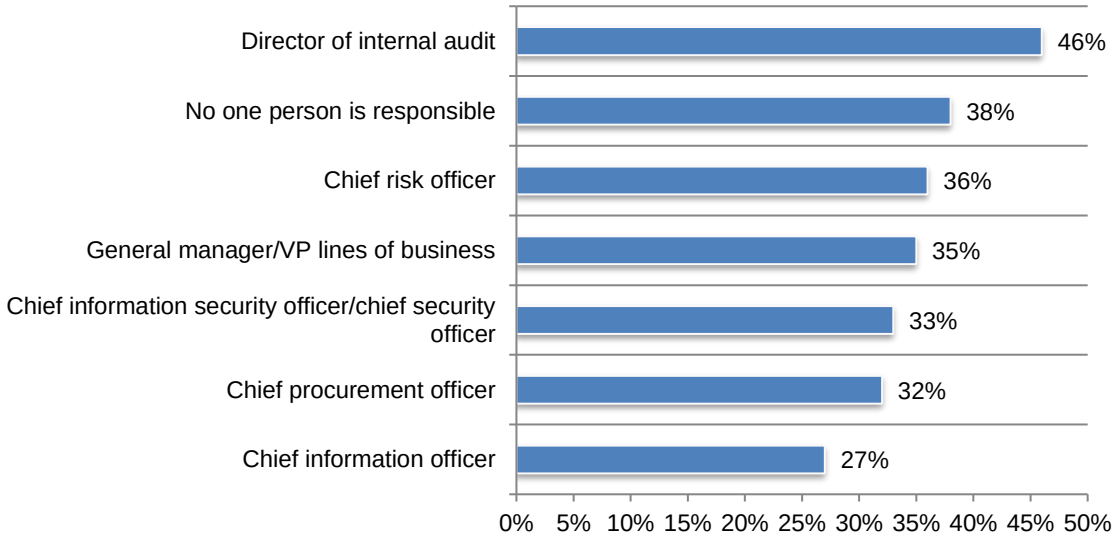
Figure 9. Who is most responsible for managing the risk of IoT devices and approving the uses of IoT devices in the organization?
More than one response allowed



Are third-party risk management policies and programs reviewed? Fifty-six percent of respondents say their companies regularly conduct a regular review of third-party risk management policies and programs to ensure they address the ever-changing landscape or third-party risk and regulations.

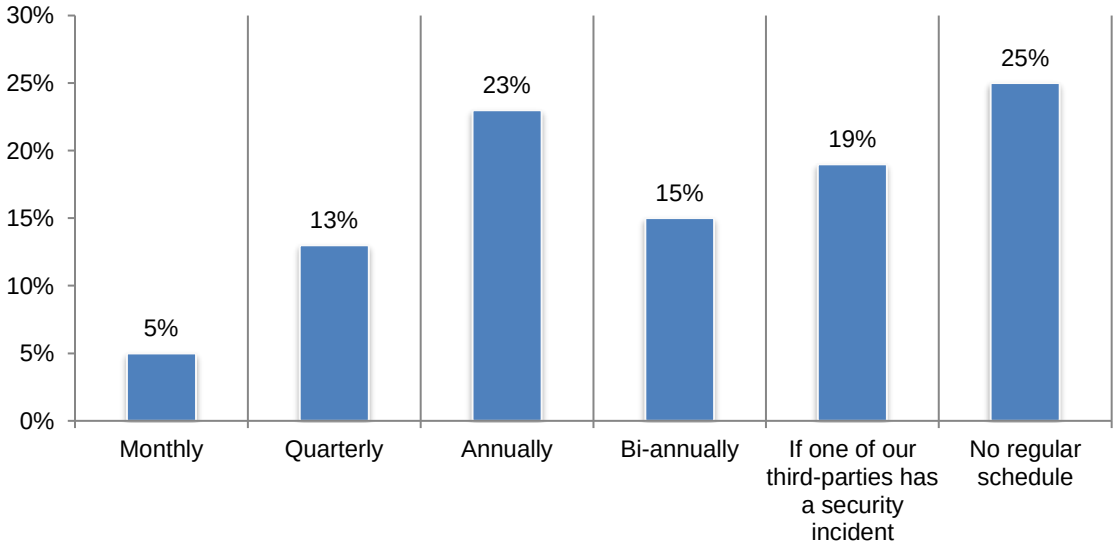
As shown in Figure 10, the director of internal audit, chief risk officer and general manager/VP lines of business are most likely to initiate the review. However, 38 percent of respondents say no one person is responsible.

Figure 10. Who initiates a regular review of third-party risk management policies and programs?
More than one response allowed



As shown in Figure 11, 41 percent of respondents have a regular schedule for this review on a monthly basis (5 percent), quarterly (13 percent) or annually (23 percent).

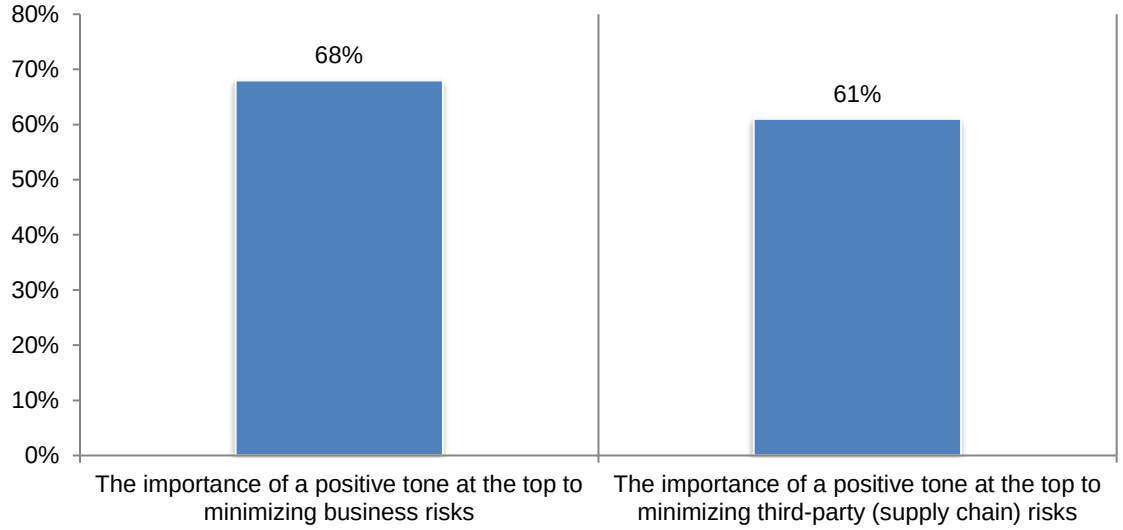
Figure 11. How regularly does this review occur?



Trends in third-party IoT governance

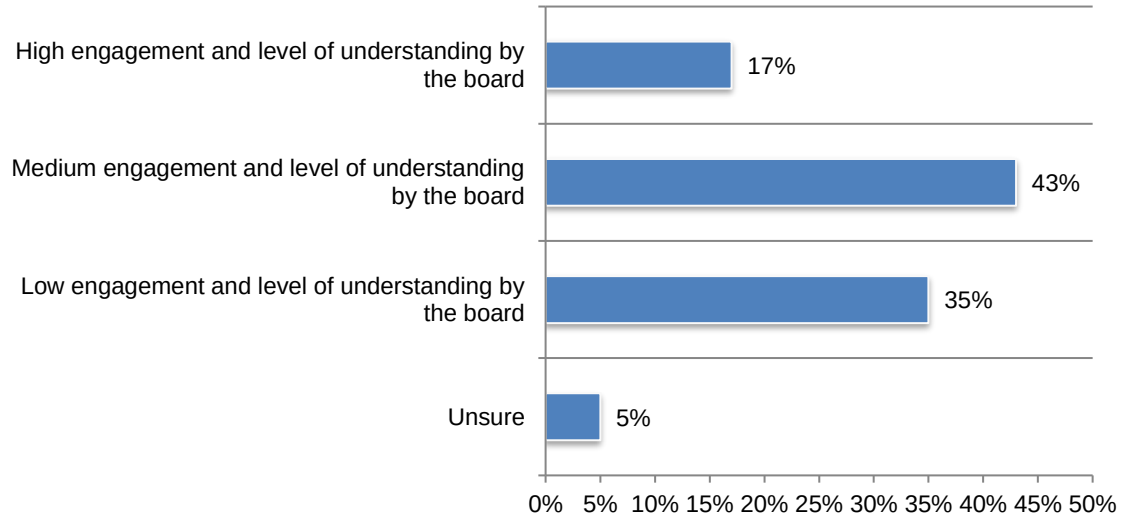
A positive tone at the top is important to minimizing risk. Respondents were asked to rank the importance of a positive tone at the top to minimizing business and third-party risks. Figure 12 presents the very important responses (7+ responses on a scale of 1 = not important to 10 = very important). Not only is a positive tone at the top important to minimizing business risks, it is also important to minimizing third-party risks (68 percent of respondents and 61 percent of respondents, respectively).

Figure 12. The Importance of a positive tone at the top to minimizing business risks and third-party risks
Scale of 1 = not important to 10 = very important, 7+ responses reported



Many boards of directors are not engaged and do not understand the cybersecurity risks relating to vendors and third parties. According to Figure 13, only 17 percent of respondents say their organizations' board of directors have a high engagement and understanding of cybersecurity risks relating to vendors or third parties.

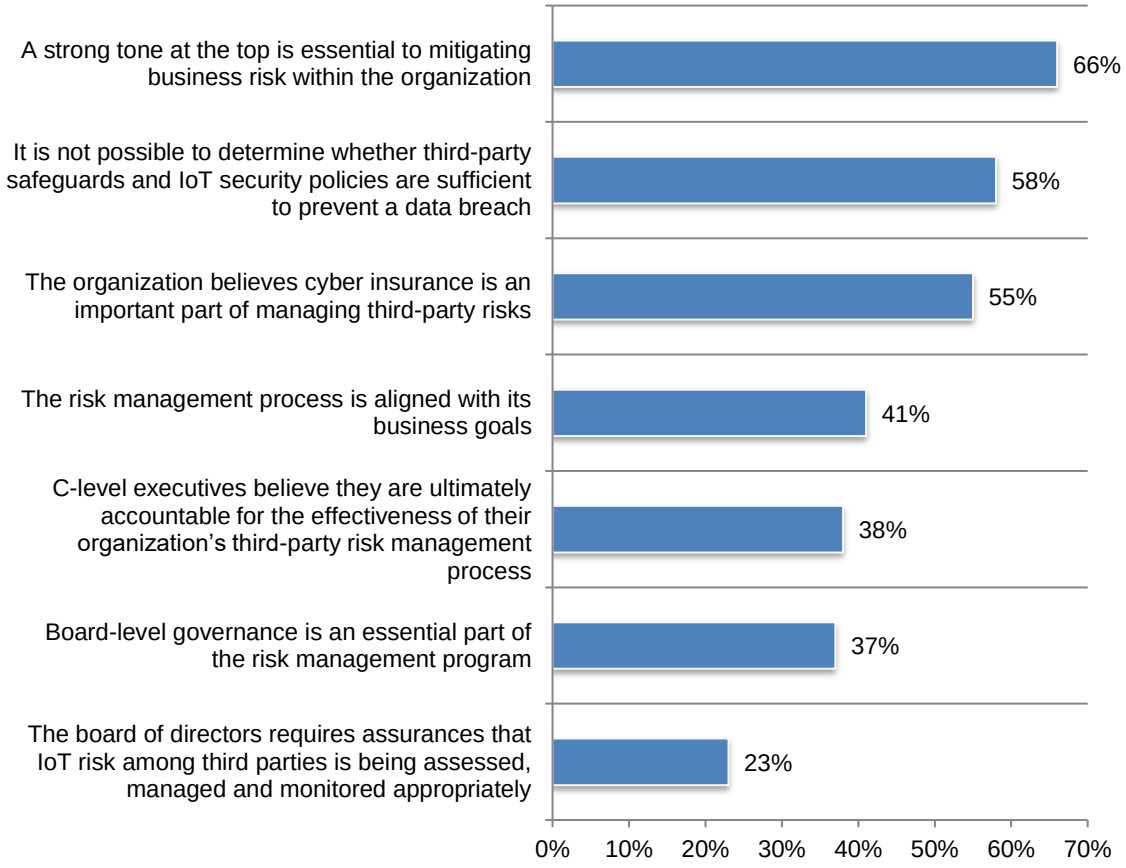
Figure 13. How engaged is your board of directors with cybersecurity risks relating to their vendors?



Findings underscore the importance of a strong tone at the top. As shown in Figure 14, the most important governance practice, according to 66 percent of respondents, is a strong tone at the top, and 55 percent of respondents say cyber insurance is an important part of managing third-party risks.

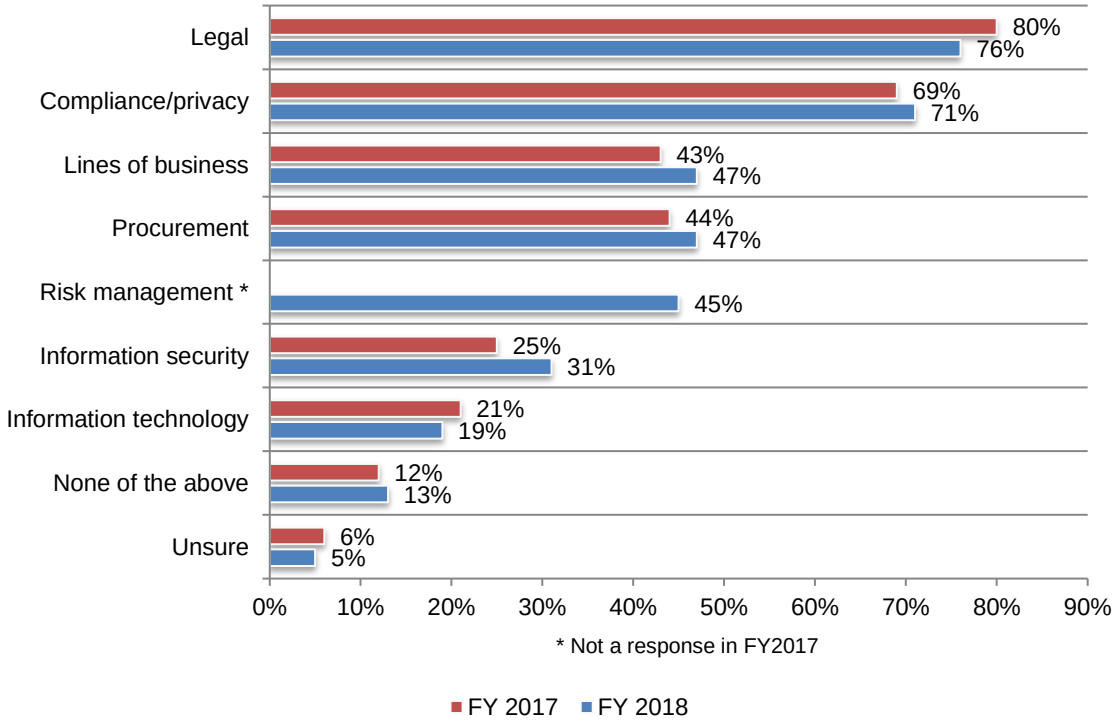
The majority of respondents (58 percent) say with current practices in place it is not possible to determine whether third-party safeguards and IoT security policies are sufficient to prevent a data breach. Only 41 percent of respondents say the risk management process is aligned with its business goals and only 38 percent of respondents say C-level executives believe they are ultimately accountable for the effectiveness of their organizations' third-party risk management process.

Figure 14. Perceptions about IoT governance practices
Strongly agree and Agree responses combined



Legal and compliance/privacy are considered most knowledgeable about privacy and security language to include in third-party contracts. According to Figure 15, legal and compliance are considered most knowledgeable about ensuring contracts have language that protects organizations in their relationships with third parties.

Figure 15. Which department is most knowledgeable to ensure privacy and security language is included in third-party contracts?
More than one response allowed

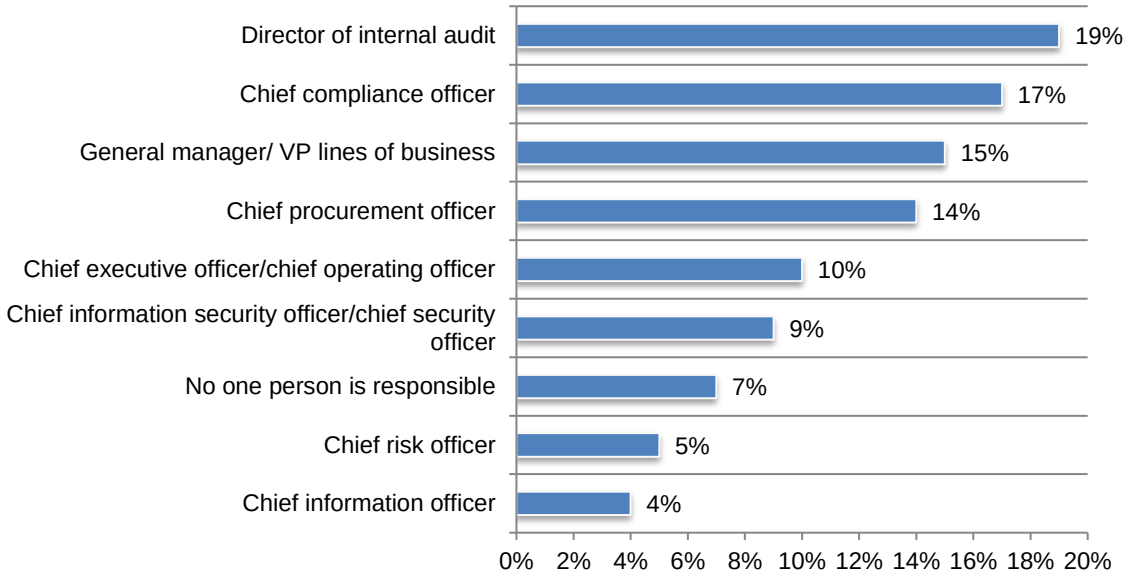


Steps taken to strengthen IoT security in the workplace

Are third parties required to prove compliance with organizations' security and privacy practices? Only 45 percent of respondents are requiring third parties that have access to their sensitive and confidential information to ensure compliance with security and privacy practices. Of those organizations, 51 percent require remediation of third-party weaknesses.

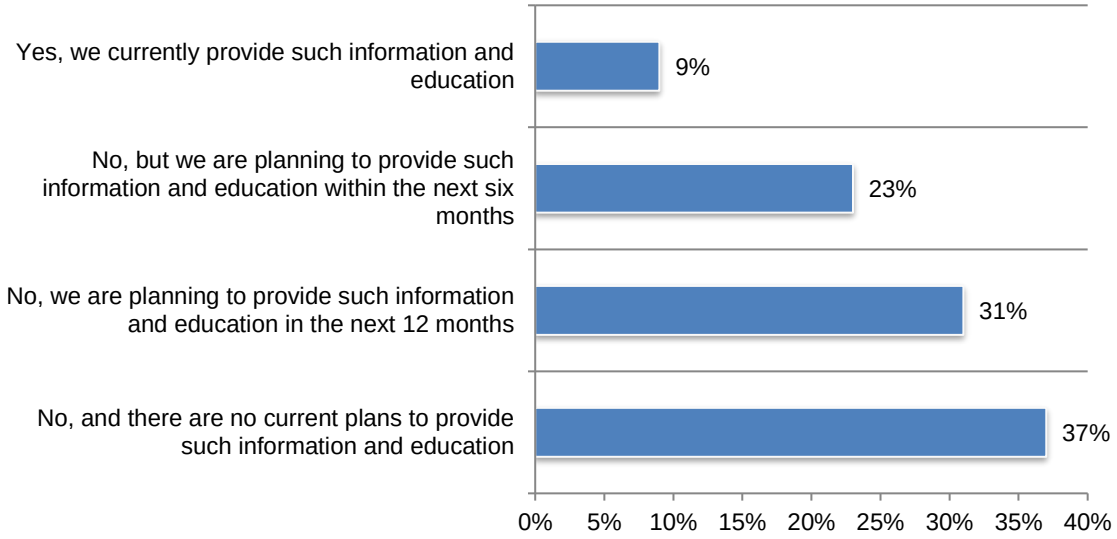
As shown in Figure 16, the person most accountable for remediating these weaknesses, is the director of internal audit, followed by the chief compliance officer.

Figure 16. Who is most accountable to ensure weaknesses are remediated?
Only one choice permitted



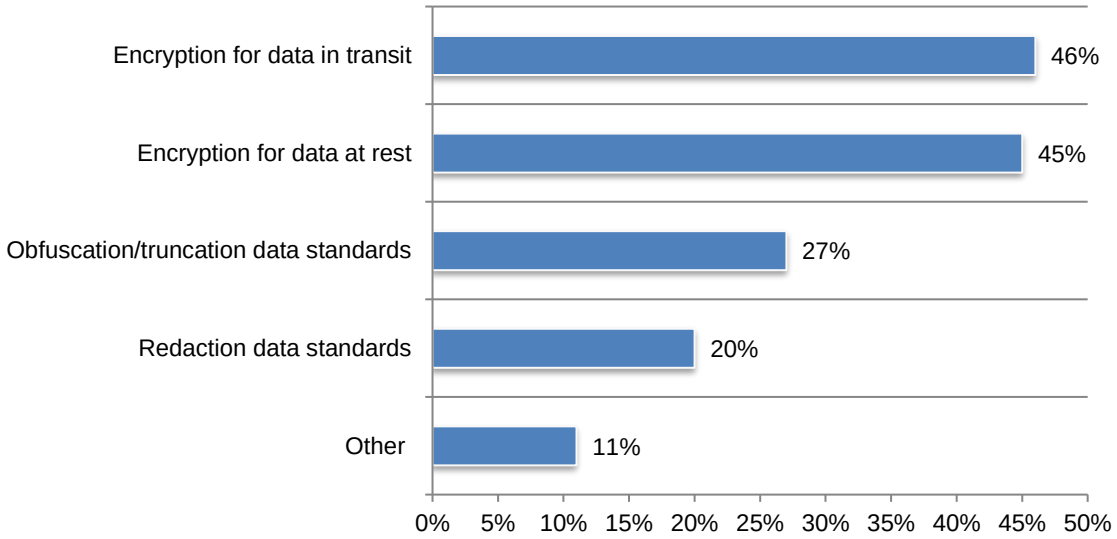
Most companies are planning to conduct training programs about risks created by IoT devices. According to Figure 17, only 9 percent of respondents say their organizations currently inform and educate employees and third parties about the risks created by IoT devices in the workplace and what steps are needed to minimize the risk. However, 23 percent of respondents say their organizations plan to do so in the next six months, and 31 percent say they will in the next 12 months.

Figure 17. Does your organization inform and educate employees and third parties about the risks created by IoT devices?



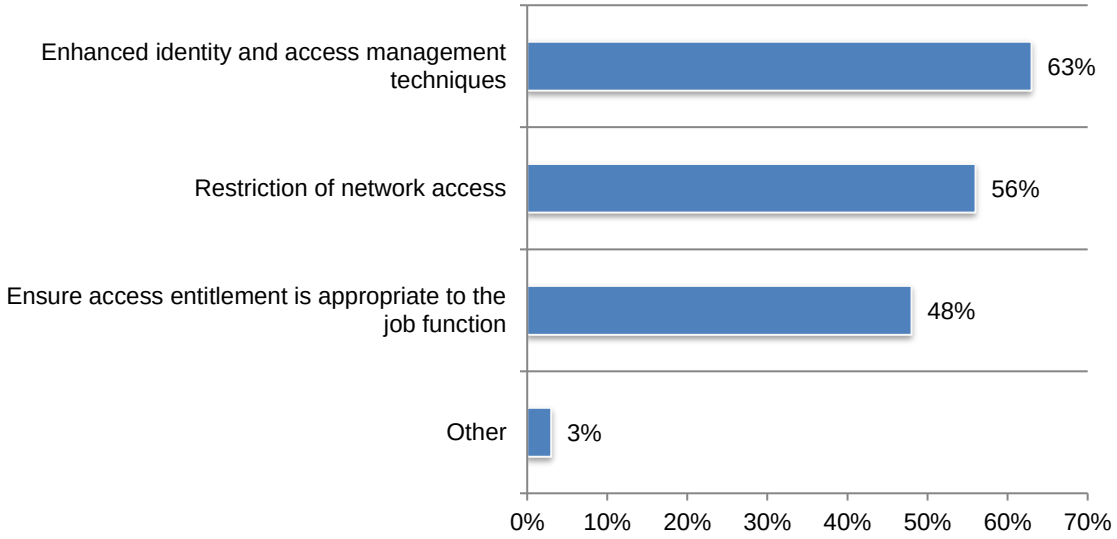
High-value assets are vulnerable in the IoT ecosystem. Only 44 percent of respondents say their organizations take comprehensive steps to protect their organizations' high-value data. As shown in Figure 18, of those organizations that take steps to protect high-value assets, most use encryption for data in transit and data at rest.

Figure 18. Steps taken to protect high-value data assets
More than one response allowed



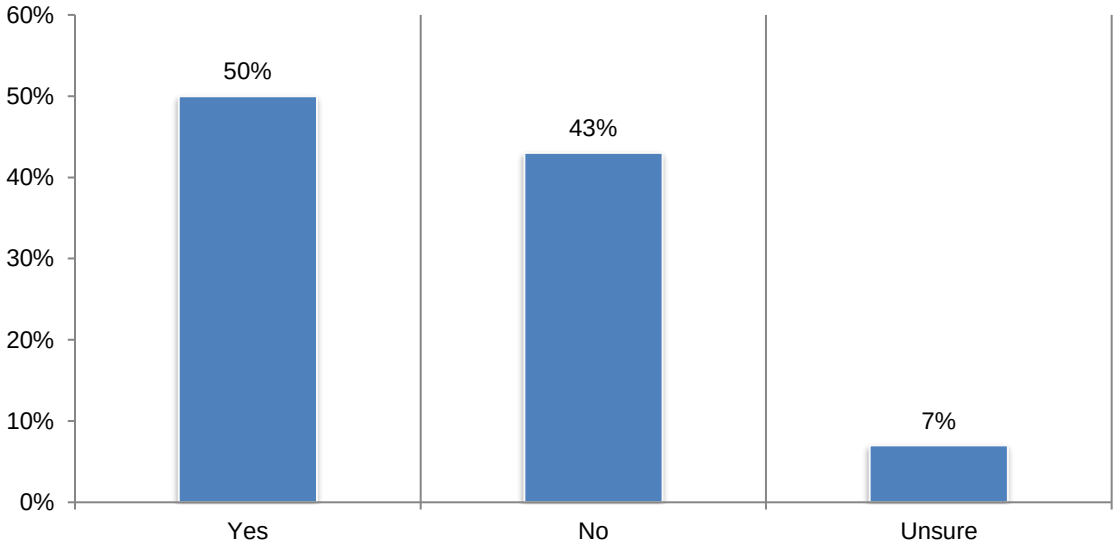
To ensure appropriate access to high-value assets, 44 percent of the organizations that focus on protecting high-value assets use enhanced identity and access management techniques to ensure appropriate access to high-value data assets, as shown in Figure 19.

Figure 19. Steps taken to ensure appropriate access to high-value data assets
More than one response allowed



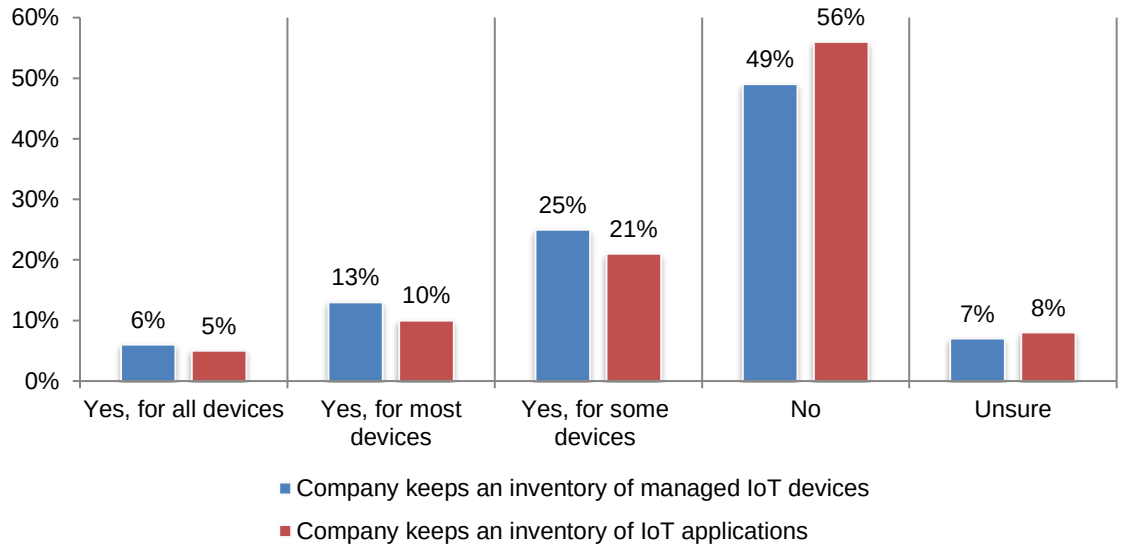
More organizations are monitoring the risk of IoT devices used in the workplace. Fifty percent of respondents say their organizations monitor IoT devices in the workplace, as shown in Figure 20.

Figure 20. Does your organization monitor the risk of IoT devices in the workplace or used by third parties?



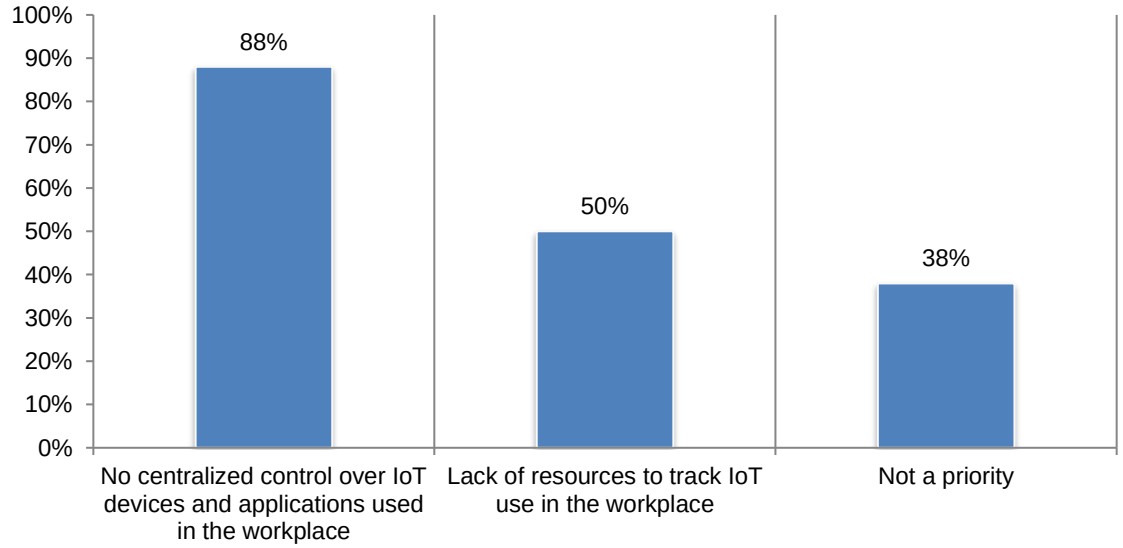
Inventories of managed IoT devices and applications are difficult to keep because of the lack of centralized control over IoT devices and applications in the workplace. Only 45 percent of respondents say it is possible to keep an inventory of managed IoT devices and applications. Of those companies, 44 percent of respondents say they keep an inventory for all, most or some devices, as shown in Figure 21.

Figure 21. Does your company keep an inventory of managed IoT devices and IoT applications?



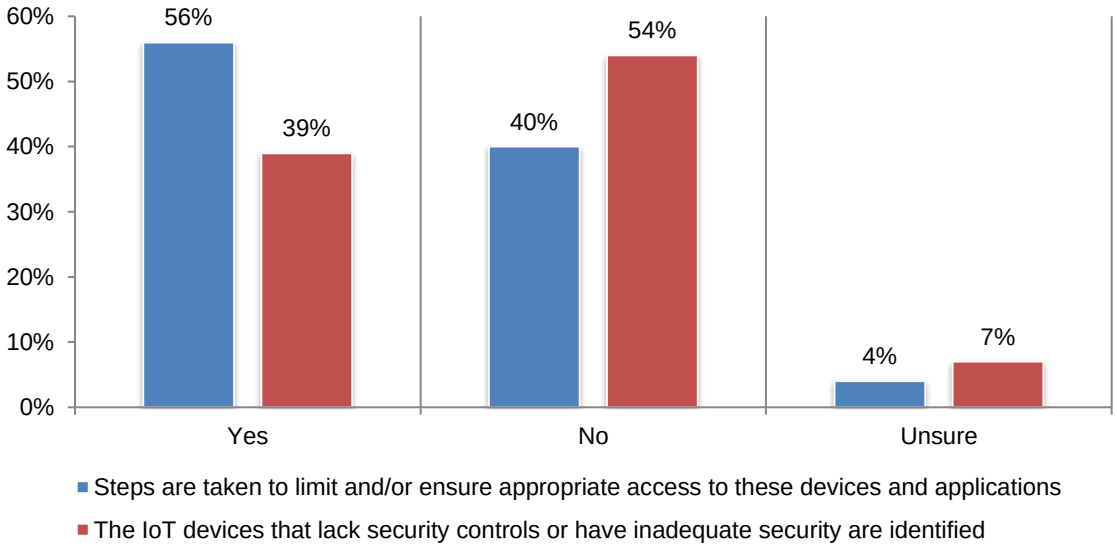
According to Figure 22, 88 percent of respondents say there is no centralized control over IoT devices and applications used in the workplace.

Figure 22. If no or unsure, why?
More than one response allowed



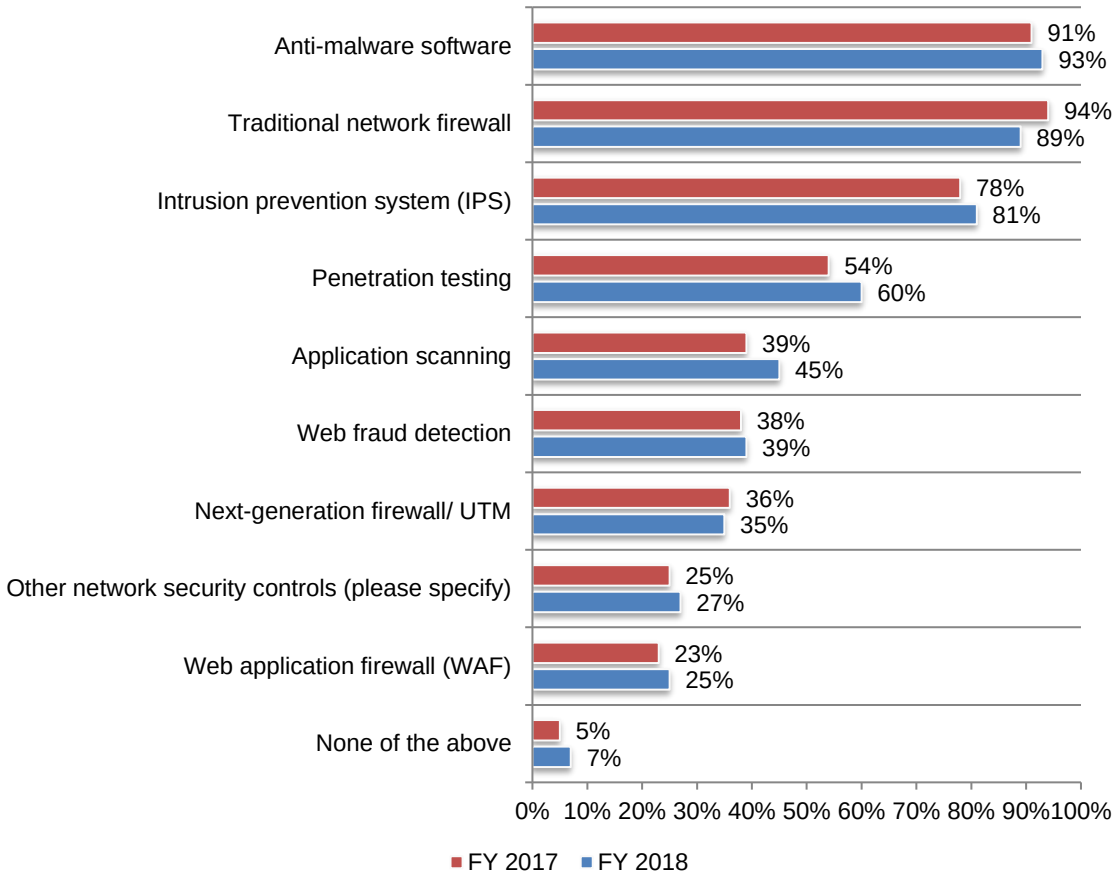
Two important steps organizations can take to minimize third party risk include ensuring appropriate access to IoT devices and applications and identifying the IoT devices that have inadequate security. As shown in Figure 23, 56 percent of respondents say they are taking steps to limit and/or ensure appropriate access to these devices and applications. Only 39 percent of respondents say IoT devices that lack security controls or that have inadequate security are identified.

Figure 23. Does your organization ensure appropriate access to IoT devices and applications and identify the IoT devices that have inadequate security?



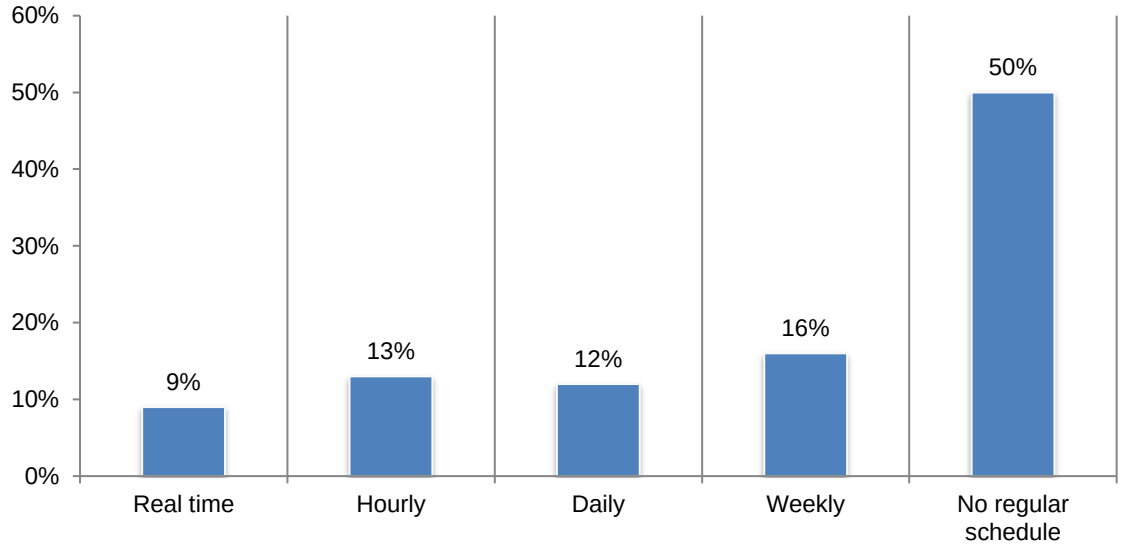
More organizations are using penetration testing and application scanning. While anti-malware software and traditional network firewalls continue to be the primary solutions used to protect the network from insecure IoT devices or applications, 60 percent of respondents say they are using penetration testing (an increase from 54 percent of respondents), and 45 percent of respondents say they use application scanning (an increase from 39 percent of respondents).

Figure 24. What are the solutions used to protect your network from insecure IoT devices or applications?
More than one response allowed



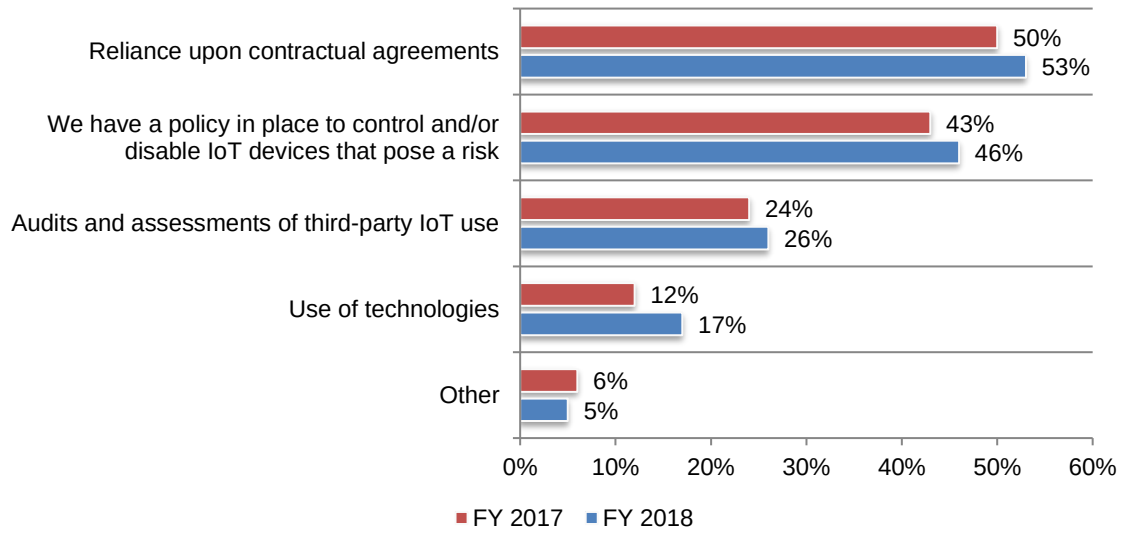
Scanning of IoT devices is ad hoc. Almost half of respondents (49 percent) say they use technologies to scan and identify IoT devices in the workplace. However, of these organizations, 50 percent of respondents say there is no regular schedule to scan.

Figure 25. How often do you scan and identify IoT devices in the workplace?



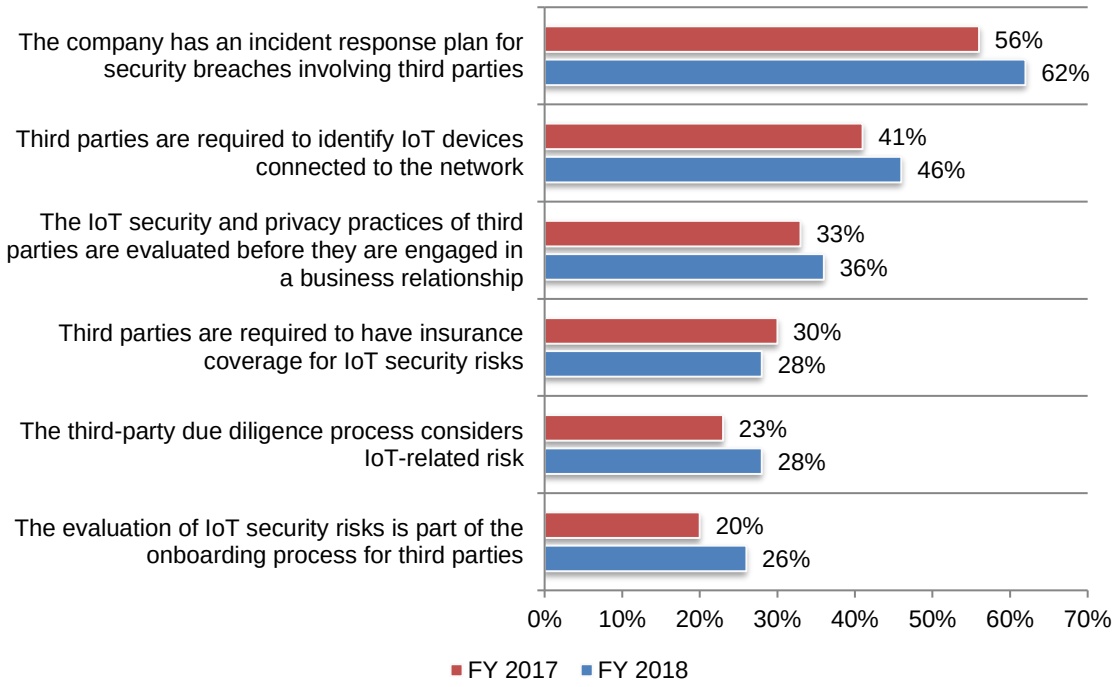
Only 42 percent of respondents say they have the ability to control and/or disable IoT devices that pose a risk to their organization. Of those respondents, most rely on contractual agreements to control and/or disable risky IoT devices, as shown in Figure 26.

Figure 26. How do you control and/or disable IoT devices that pose a risk?
More than one response allowed



Since last year, more organizations have an incident response plan. As shown in Figure 27, 62 percent of respondents say they have an incident response plan for security breaches involving third parties (an increase from 56 percent of respondents in last year's research). There is also an increase in requiring third parties to identify IoT devices connected to the network (an increase from 41 percent of respondents to 46 percent of respondents) and in making IoT-related risks part of the third-party due diligence process.

Figure 27. What steps do you take to manage third-party IoT risk?
Yes responses reported



Conclusion and recommendations

Third party IoT risks appear now to be clearly on the radar, yet much work needs to be done to ensure controls minimize the risks they pose. Only a small perecentage of organizations in this study said they can even inventory all of their IoT devices, and most could not identify a majority of their IoT assets.

Organizations continue to struggle with the security risks posed by IoT, which occurs both internal to their own organization and across the complexities of the ever-expanding network of third parties and the supply chain.

There is a clear imperative for organizations to assign accountability and ownership of IoT-related oversight across their organization in ways that more effectively cover “things” within the information technology, operational technology and consumer technology risk management areas. Organizations need to ensure that IoT security is taken seriously and educate management at all levels (up to and including governing boards).

Recommendations

Recommendations to improve third-party risk management programs to more effectively address IoT risks include:

1. Update asset management processes and inventory systems to include IoT devices and applications, and understand the security characteristics of all inventoried devices. When devices are found to have inadequate IoT security controls, replace them.

2. Identify and assign accountability for approval, monitoring, use and deployment of IoT devices and applications within your organization.

3. Ensure that IoT devices, applications, and metrics are included, monitored and reported as part of your third-party risk management program.

4. Verify that specific third-party IoT related controls included in contract clauses, policies and procedures can be operationalized and monitored for adherence and compliance.

5. Collaborate with industry peers, colleagues, and experts to identify successful approaches, techniques, solutions and standards to monitor and mitigate third-party IoT device and application risks.

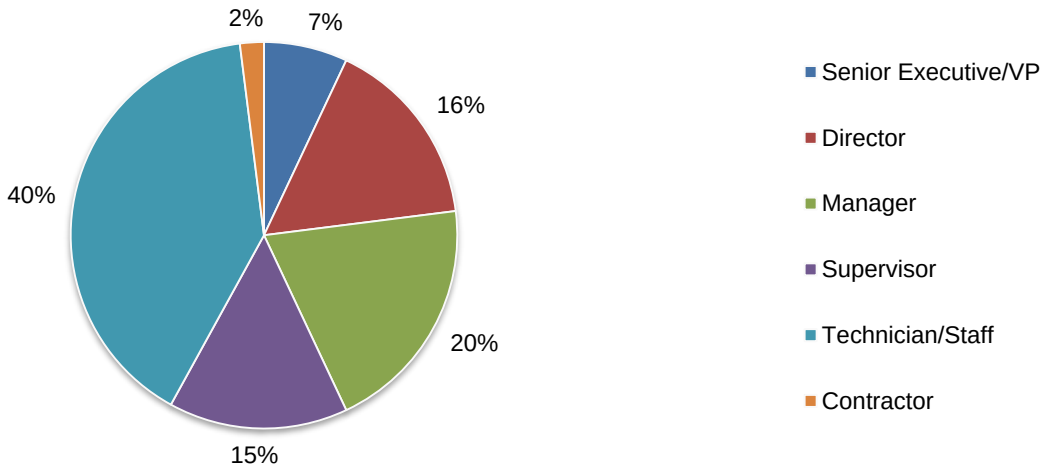
Part 3. Methods

A sampling frame of 17,053 individuals who have a role in the risk management process in their organizations and are familiar with the use of IoT devices in their organizations were selected as participants in the research. Table 1 shows a total of 689 returns. Screening and reliability checks required the removal of 84 surveys. Our final sample consisted of 605 surveys, or a 3.5 percent response rate.

Table 1. Sample response	Freq	Pct%
Sampling frame	17,073	100.0%
Total returns	689	4.0%
Rejected or screened surveys	84	0.5%
Final sample	605	3.5%

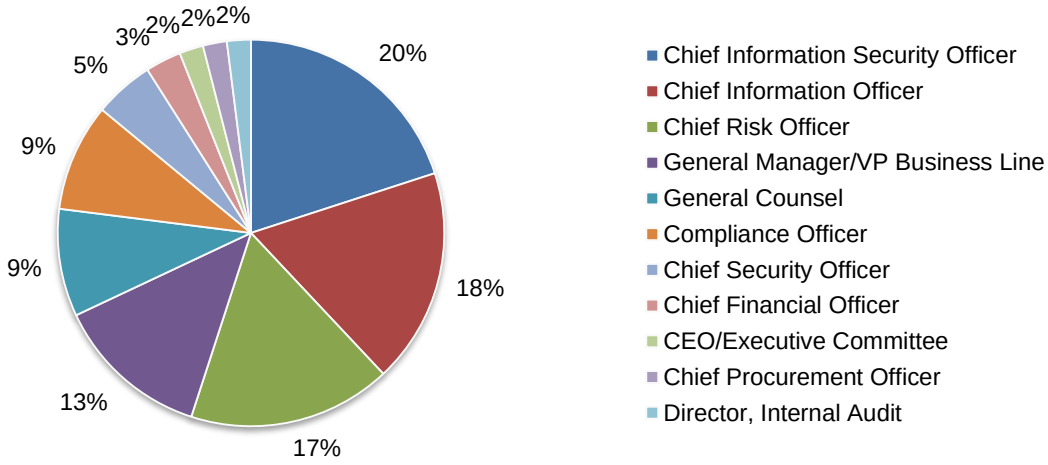
Pie Chart 1 reports the respondents' organizational level within participating organizations. By design, more than half of the respondents (58 percent) are at or above the supervisory levels.

Pie Chart 1. Position level within the organization



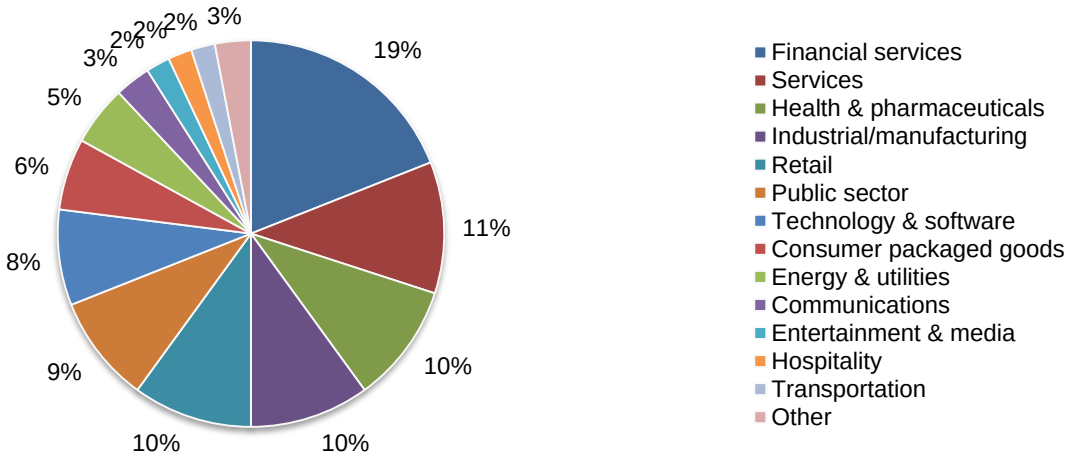
Pie Chart 2 reveals that 20 percent of respondents report directly to the chief information security officer, 18 percent report to the chief information officer and 17 percent report to the chief risk officer.

Pie Chart 2. The primary person reported to within the organization



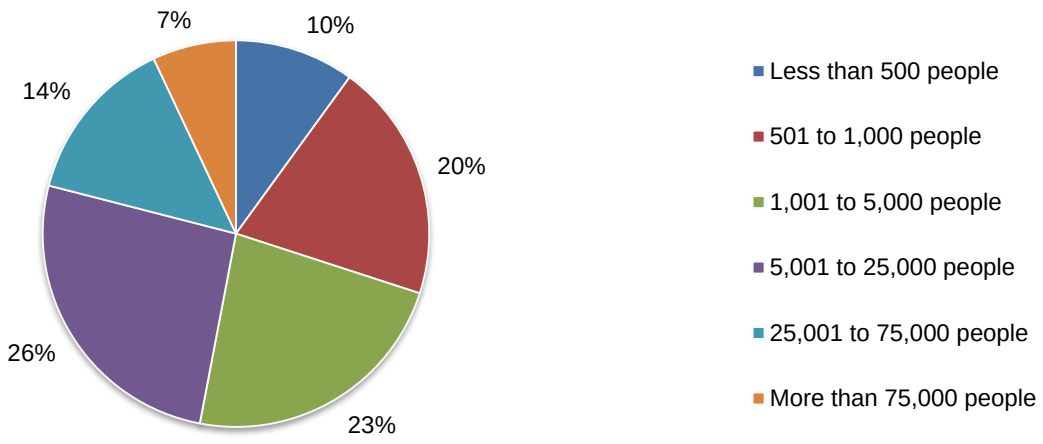
Pie Chart 3 reports the industry classification of respondents' organizations. This chart identifies financial services (19 percent of respondents), which includes asset management and insurance, as the largest segment, followed by services (11 percent of respondents), health and pharmaceuticals, industrial/manufacturing and retail (each at 10 percent of respondents).

Pie Chart 3. Primary industry classification



Seventy percent of the respondents are from organizations with a global headcount of more than 1,000 employees, as shown in Pie Chart 4.

Pie Chart 4. Worldwide headcount of the organization



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 involved in the protection of confidential information. 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 made 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 all survey questions contained in this study. All survey responses were fielded and collected in March 2017 and April 2017.

Survey response	Freq	Pct%
Total sampling frame	17,073	100.0%
Total returns	689	4.0%
Rejected surveys	84	0.5%
Final sample	605	3.5%

Part 1. Screening questions

S1. Does your organization have a third-party risk management program?	FY 2018
Yes	100%
No (Stop)	0%
Total	100%

S2. How familiar are you with your organization's approach to managing third-party risks?	FY 2018	FY 2017
Very familiar	33%	31%
Familiar	42%	45%
Somewhat familiar	25%	24%
No knowledge (Stop)	0%	0%
Total	100%	100%

S3. Do you have any involvement in managing third-party risks?	FY 2018	FY 2017
Yes, full involvement	31%	29%
Yes, partial involvement	50%	49%
Yes, minimal involvement	19%	22%
No involvement (Stop)	0%	0%
Total	100%	100%

S4. How familiar are you with the use of IoT devices in your organization?	FY 2018	FY 2017
Very familiar	19%	17%
Familiar	30%	29%
Somewhat familiar	51%	54%
No knowledge (Stop)	0%	0%
Total	100%	100%

S5. Does your position in the organization require you to participate in corporate governance and or risk oversight activities?	FY 2018
Yes	100%
No (Stop)	0%
Total	100%

Part 2. Attributions about tone at the top and IoT risk

Strongly agree and Agree responses combined	FY 2018	FY 2017
Q1a. Our organization considers third-party risk a serious threat to our high value assets.	71%	
Q1b. C-level executives believe they are ultimately accountable for the effectiveness of their organization's third-party risk management process.	38%	
Q1c. Our organization believes cyber insurance is an important part of managing third-party risks.	55%	
Q1d. Migration to the cloud significantly increases third-party risk for my organization.	46%	
Q1e. My organization's risk management process is aligned with its business goals.	41%	
Q1f. A strong tone at the top is essential to mitigating business risk within my organization.	66%	
Q1g. Board-level governance is an essential part of my organization's risk management program.	37%	
Q1h. Our organization allocates sufficient resources to managing third-party IoT risks.	30%	27%
Q1i. Our organization has an approved coherent risk appetite framework incorporating clearly expressed risk tolerance levels across all levels of the organization.	31%	
Q1j. The rise of the Internet of Things (IoT) significantly increases third-party risk for my organization.	66%	
Q1k. Our board of directors requires assurances that IoT risk among third parties is being assessed, managed and monitored appropriately.	23%	25%
Q1l. It is not possible to determine whether third-party safeguards and IoT security policies are sufficient to prevent a data breach.	58%	56%
Q1m. Adoption of the cloud, in part, is driven by the need to innovate in the IoT ecosystem.	60%	61%
Q1n. The drive for innovation in the IoT ecosystem requires new approaches to IT strategies and tactics.	71%	65%
Q1o. Our organization finds it difficult to manage the complexities of IoT platforms because of the number of vendors.	44%	42%
Q1p. The pace of innovation in IoT and varying standards for security makes it hard to ensure the security of these devices and applications.	76%	72%
Q1q. The IoT ecosystem is vulnerable to a ransomware attack.	60%	55%

Q2. Using the following 10-point scale, please rate the importance of a positive tone at the top to minimizing business risks within your organization. 1 = not important to 10 = very important.	FY 2018
1 or 2	6%
3 or 4	9%
5 or 6	17%
7 or 8	25%
9 or 10	43%
Total	100%
Extrapolated value	7.30

Q3. Using the following 10-point scale, please rate the importance of a positive tone at the top to minimizing third-party (supply chain) risks within your organization. 1 = not important to 10 = very important.	FY 2018
1 or 2	5%
3 or 4	12%
5 or 6	22%
7 or 8	24%
9 or 10	37%
Total	100%
Extrapolated value	7.02

Q4a. Does your organization have a third-party risk management program?	FY 2018	FY 2017
Yes	60%	56%
No [please proceed to Q7]	40%	44%
Total	100%	100%

Q4b. If yes, please rate the effectiveness of your third-party risk management program using the scale below. 1=not effective to 10=very effective.	FY 2018	FY 2017
1 or 2	15%	19%
3 or 4	19%	21%
5 or 6	38%	36%
7 or 8	18%	15%
9 or 10	10%	9%
Total	100%	100%
Extrapolated value	5.28	4.98

Q5. Does your organization have a third-party risk management committee?	FY 2018	FY 2017
Yes	49%	47%
No	49%	50%
Unsure	2%	3%
Total	100%	100%

Q6. Is your third-party risk management program part of your organization's enterprise risk management program?	FY 2018	FY 2017
Yes	42%	34%
No	55%	61%
Unsure	3%	5%
Total	100%	95%

Q7. How engaged is your board of directors with cybersecurity risks relating to your vendors?	FY 2018
High engagement and level of understanding by the board	17%
Medium engagement and level of understanding by the board	43%
Low engagement and level of understanding by the board	35%
Unsure	5%
Total	100%

Q8a. Does your company conduct a regular review of third-party risk management policies and programs to ensure they address the ever-changing landscape of third-party risk and regulations?	FY 2018
Yes	56%
No	44%
Total	100%

Q8b. If yes, who initiates the review? Please select all that apply.	FY 2018
Chief executive officer/chief operating officer	12%
Chief compliance officer	17%
Director of internal audit	46%
General manager / VP lines of business	35%
Chief risk officer	36%
Chief information officer	27%
Chief information security officer/chief security officer	33%
Chief technology officer	9%
Chief procurement officer	32%
No one person is responsible	38%
Other (please specify)	3%
Total	288%

Q8c. If yes, how regularly does this review occur?	FY 2018
Monthly	5%
Quarterly	13%
Annually	23%
Bi-annually	15%
If one of our third-parties has a security incident	19%
No regular schedule	25%
Total	100%

Q8d. If no, why? Please select all that apply.	FY 2018
Not a priority for the CEO/board of directors	37%
Decisions about the third-party risk management program are not relevant for the CEO and board members	41%
We only provide this information if a security incident or data breach has occurred involving a third-party	54%
Unsure	8%
Total	140%

Q9a. Does your company require third parties that have access to sensitive and confidential information to ensure compliance with your security and privacy practices?	FY 2018
Yes	45%
No	49%
Unsure	6%
Total	100%

Q9b. If yes, does your company require remediation of identified third-party control weaknesses?	FY 2018
Yes	51%
No	44%
Unsure	5%
Total	100%

Q9c. If yes, who is most accountable to ensure weaknesses are remediated?	FY 2018
Chief executive officer/chief operating officer	10%
Chief compliance officer	17%
Director of internal audit	19%
General manager/ VP lines of business	15%
Chief risk officer	5%
Chief information officer	4%
Chief information security officer/chief security officer	9%
Chief technology officer	0%
Chief procurement officer	14%
No one person is responsible	7%
Other (please specify)	0%
Total	100%

Q10. Which department/function is most knowledgeable to ensure appropriate privacy and security requirements are included in all contracts with third parties? Please check all that apply.	FY 2018	FY 2017
Legal	76%	80%
Risk management	45%	
Information technology	19%	21%
Procurement	47%	44%
Compliance/privacy	71%	69%
Information security	31%	25%
Lines of business	47%	43%
None of the above	13%	12%
Unsure	5%	6%
Total	354%	300%

Q11. Does your organization inform and educate employees and third parties about the risks created by IoT devices in the workplace and what steps they need to take to minimize the risk?	FY 2018
Yes, we currently provide such information and education	9%
No, but we are planning to provide such information and education within the next six months	23%
No, we are planning to provide such information and education in the next 12 months	31%
No, and there are no current plans to provide such information and education	37%
Total	100%

Part 3: IoT risk management

Q12. Does the IoT risk increase because lines of business demand innovation, speed to market and functionality?	FY 2018
Yes	63%
No	30%
Unsure	7%
Total	100%

Q13. Does your organization take comprehensive steps to protect its high value assets.	FY 2018
Yes	44%
No	50%
Unsure	6%
Total	100%

Q14a. Please check all steps taken to protect your organization's high-value data assets.	FY 2018
Encryption for data at rest	45%
Encryption for data in transit	46%
Redaction data standards	20%
Obfuscation/truncation data standards	27%
Other (Please specify)	11%
Total	149%

Q14b. Please check all steps taken to ensure appropriate access to high-value data assets.	FY 2018
Restriction of network access	56%
Enhanced identity and access management techniques	63%
Ensure access entitlement is appropriate to the job function	48%
Other (Please specify)	3%
Total	170%

Q15. Are you aware of the network of physical objects in your company that are connected to the Internet (i.e. printers or building automation solutions)?	FY 2018	FY 2017
Yes, all of them	8%	9%
Yes, most of them	18%	19%
Yes, some of them	40%	37%
No	34%	35%
Total	100%	100%

Q16a. Has **your organization** experienced the loss or theft of data caused by unsecured IoT devices or applications in the past 12 months?	FY 2018	FY 2017
Yes	21%	15%
No	53%	54%
Unsure	26%	31%
Total	100%	100%

Q16b. Has your organization experienced the loss or theft of data caused by **third parties'** unsecured IoT devices or applications in the past 12 months?	FY 2018
Yes	14%
No	51%
Unsure	35%
Total	100%

Q17a. How likely is your **organization** to experience the loss or theft of data caused by unsecured IoT devices or applications in the next 24 months?	FY 2018	FY 2017
Very likely	26%	23%
Somewhat likely	28%	25%
Likely	27%	30%
Not likely	18%	20%
Not possible	1%	2%
Total	100%	100%

17b. How likely is your organization to experience the loss or theft of data caused by **third parties'** unsecured IoT devices or applications in the next 24 months?	FY 2018
Very likely	22%
Somewhat likely	23%
Likely	30%
Not likely	23%
Not possible	2%
Total	100%

Q18a. Has your **organization** experienced a cyber attack, such as a distributed denial of service (DDoS), caused by unsecured IoT devices or applications in the past 12 months?	FY 2018	FY 2017
Yes	21%	16%
No	53%	59%
Unsure	26%	25%
Total	100%	100%

Q18b. Has **your** organization experienced a cyber attack, such as a distributed denial of service (DDoS), caused by **third parties'** unsecured IoT devices or applications in the past 12 months?	FY 2018
Yes	18%
No	56%
Unsure	26%
Total	100%

Q19a. How likely is **your organization** to experience a cyber attack, such as a distributed denial of service (DDoS), caused by unsecured IoT devices or applications in the next 24 months?	FY 2018	FY 2017
Very likely	28%	21%
Somewhat likely	25%	23%
Likely	29%	32%
Not likely	16%	21%
Not possible	2%	3%
Total	100%	100%

Q19b. How likely is your organization to experience a cyber attack, such as a distributed denial of service (DDoS), caused by **third parties'** unsecured IoT devices or applications in the next 24 months?	FY 2018
Very likely	26%
Somewhat likely	23%
Likely	28%
Not likely	23%
Not possible	0%
Total	100%

Q20. What is the likelihood a security incident related to unsecured IoT devices or applications could be catastrophic to your organization?	FY 2018	FY 2017
Very likely	44%	40%
Somewhat likely	41%	39%
Likely	12%	15%
Not likely	3%	4%
Not possible	0%	2%
Total	100%	100%

Q21a. Who is most responsible for **managing** the risk of IoT devices in the organization? Please check the top two responses.	FY 2018
Chief executive officer/chief operating officer	6%
Chief compliance officer	12%
Director of internal audit	15%
General manager/ VP lines of business	35%
Chief risk officer	16%
Chief information officer	27%
Chief information security officer/chief security officer	34%
Chief technology officer	10%
Chief procurement officer	6%
No one person is responsible	36%
Other (please specify)	3%
Total	200%

Q21b. Who is most responsible for **approving** the specific use of IoT devices in the organization and providing security scanning updates? Please check the top two choices.	FY 2018
Chief executive officer/chief operating officer	16%
Chief compliance officer	18%
Director of internal audit	6%
General manager/ VP lines of business	43%
Chief risk officer	21%
Chief information officer	17%
Chief information security officer/chief security officer	40%
Chief technology officer	6%
Chief procurement officer	3%
No one person is responsible	30%
Other (please specify)	0%
Total	200%

Q22. Does your organization consider IoT devices to be endpoints to your network or enterprise systems?	FY 2018	FY 2017
Yes	60%	55%
No	35%	39%
Unsure	5%	6%
Total	100%	100%

Q23. Does your organization monitor the risk of IoT devices used in the workplace?	FY 2018	FY 2017
Yes	50%	44%
No	43%	48%
Unsure	7%	8%
Total	100%	100%

Q24. Does your organization monitor the risk of IoT devices used by third parties?	FY 2018
Yes	29%
No	61%
Unsure	10%
Total	100%

Part 4. IoT security risk

Q25a. Do you believe it is possible to keep an inventory of managed IoT devices and applications?	FY 2018
Yes	45%
No	49%
Unsure	6%
Total	100%

Q25b. If yes, does your company keep an inventory of managed IoT devices?	FY 2018	FY 2017
Yes, for all devices	6%	5%
Yes, for most devices	13%	11%
Yes, for some devices	25%	26%
No	49%	50%
Unsure	7%	8%
Total	100%	100%

Q25c. If no or unsure, why? Please check all that apply.	FY 2018	FY 2017
Lack of resources to track IoT use in the workplace	50%	56%
No centralized control over IoT devices and applications used in the workplace	88%	85%
Not a priority	38%	41%
Total	176%	182%

Q26a. Does your company keep an inventory of IoT applications?	FY 2018
Yes, for all applications	5%
Yes, for most applications	10%
Yes, for some applications	21%
No	56%
Unsure	8%
Total	100%

Q26b. If no or unsure, why? Please check all that apply.	FY 2018
Lack of resources to track IoT use in the workplace	49%
No centralized control over IoT devices and applications used in the workplace	85%
Not a priority	36%
Total	170%

Q27a. If your organization keeps an inventory of IoT devices, how many are in this inventory?	FY 2018	FY 2017
Less than 100	10%	13%
100 to 1,000	38%	45%
1,001 to 10,000	22%	20%
10,001 to 50,000	21%	18%
50,001 to 100,000	5%	3%
More than 100,000	4%	1%
Total	100%	100%
Extrapolated value	15,874	10,104

Q27b. If yes, how many IoT devices will your organization have in the workplace in the next 24 months?	FY 2018	FY 2017
Less than 100	5%	11%
100 to 1,000	28%	33%
1,001 to 10,000	21%	19%
10,001 to 50,000	30%	26%
50,001 to 100,000	9%	5%
More than 100,000	7%	6%
Total	100%	100%
Extrapolated value	24,762	19,382

Q27c. If no, do you take steps to limit and/or ensure appropriate access to these devices and applications in the workplace?	FY 2018
Yes	56%
No	40%
Unsure	4%
Total	100%

Q28a. Does your organization identify the IoT devices that lack security controls or have inadequate security?	FY 2018
Yes	39%
No	54%
Unsure	7%
Total	100%

Q28b. If yes, do you replace these devices with secure devices?	FY 2018
Yes, immediately	12%
Yes, but not immediately	21%
No	61%
Unsure	6%
Total	100%

Q29. What steps are you taking to protect your network from insecure IoT devices or applications? Please check all that apply.	FY 2018	FY 2017
Web application firewall (WAF)	25%	23%
Application scanning	45%	39%
Penetration testing	60%	54%
Anti-malware software	93%	91%
Intrusion prevention system (IPS)	81%	78%
Traditional network firewall	89%	94%
Next-generation firewall/ UTM	35%	36%
Web fraud detection	39%	38%
Other network security controls (please specify)	27%	25%
None of the above	7%	5%
Total	501%	483%

Q30. Do you use technologies to scan and identify IoT devices in the workplace?	FY 2018
Yes	49%
No	45%
Unsure	6%
Total	100%

Q31. If yes, how often do you scan?	FY 2018
Real time	9%
Hourly	13%
Daily	12%
Weekly	16%
No regular schedule	50%
Total	100%

Q32a. Do you have the ability to control and/or disable IoT devices that pose a risk to your organization?	FY 2018	FY 2017
Yes	42%	44%
No	51%	50%
Unsure	7%	6%
Total	100%	100%

Q32b. If yes, how do you achieve control? Please check all that apply.	FY 2018	FY 2017
We have a policy in place to control and/or disable IoT devices that pose a risk	46%	43%
Audits and assessments of third-party IoT use	26%	24%
Reliance upon contractual agreements	53%	50%
Use of technologies	17%	12%
Other	5%	6%
Total	147%	135%

Part 5. Third-party IoT risk management planning

Q33a. Do you evaluate the IoT security and privacy practices of third parties **before** you engage them in a business relationship?	FY 2018	FY 2017
Yes	36%	33%
No	55%	57%
Unsure	9%	10%
Total	100%	100%

Q33b. If yes, how do you perform this evaluation? Please check all that apply.	FY 2018	FY 2017
Review written policies and procedures	52%	51%
Acquire signature on contracts that legally obligates the third-party to adhere to security and privacy practices	57%	54%
Obtain indemnification from the third-party in the event of a data breach	31%	35%
Conduct an audit of the vendor's IoT security and privacy practices	16%	12%
Obtain a self-assessment conducted by the third-party	12%	9%
Obtain references from other organizations that engage the third-party	14%	8%
Obtain evidence of security certification such as ISO 27001, SOC 2, NIST and others	26%	29%
Other (please specify)	5%	3%
Unsure	1%	2%
Total	214%	203%

Q34. Do you require third parties to identify IoT devices connected to your network?	FY 2018	FY 2017
Yes	46%	41%
No	45%	46%
Unsure	9%	13%
Total	100%	100%

Q35. Is the evaluation of IoT security risks part of the onboarding process for third parties?	FY 2018	FY 2017
Yes	26%	20%
No	63%	68%
Unsure	11%	12%
Total	100%	100%

Q36. Does the third-party due diligence process consider IoT-related risk?	FY 2018	FY 2017
Yes	28%	23%
No	59%	63%
Unsure	13%	14%
Total	100%	100%

Q37. Does your company require third parties to have insurance coverage for IoT security risks?	FY 2018	FY 2017
Yes	28%	30%
No	63%	61%
Unsure	9%	9%
Total	100%	100%

Q38a. Does your company have an incident response plan for security breaches involving third parties?	FY 2018	FY 2017
Yes	62%	56%
No	33%	38%
Unsure	5%	6%
Total	100%	100%

Q38b. If yes, does it include security breaches that result from unsecured IoT devices?	FY 2018	FY 2017
Yes	30%	22%
No	63%	72%
Unsure	7%	6%
Total	100%	100%

Part 6. Demographics and organizational characteristics

D1. What organizational level best describes your current position?	FY 2018	FY 2017
Senior Executive/VP	7%	5%
Director	16%	15%
Manager	20%	21%
Supervisor	15%	16%
Technician/Staff	40%	38%
Contractor	2%	3%
Other	0%	2%
Total	100%	100%

D2. Check the **Primary Person** you report to within the organization.	FY 2018	FY 2017
CEO/Executive Committee	2%	2%
Chief Financial Officer	3%	6%
General Counsel	9%	11%
Chief Privacy Officer	0%	1%
Chief Information Officer	18%	22%
Chief Technology Officer	0%	0%
Chief Procurement Officer	2%	0%
Compliance Officer	9%	14%
Director, Internal Audit	2%	0%
Head, Human Resources VP	0%	1%
Chief Security Officer	5%	4%
Chief Information Security Officer	20%	21%
Chief Risk Officer	17%	16%
General Manager / VP Business Line	13%	
Other	0%	2%
Total	100%	100%

D3. What industry best describes your organization's industry focus?	FY 2018	FY 2017
Aerospace and defense	1%	1%
Agriculture and food services	1%	1%
Communications	3%	3%
Consumer packaged goods	6%	5%
Education & research	1%	1%
Energy & utilities	5%	5%
Entertainment & media	2%	3%
Financial services*	19%	18%
Health & pharmaceuticals	10%	11%
Hospitality	2%	3%
Industrial/manufacturing	10%	10%
Public sector	9%	10%
Retail	10%	9%
Services	11%	10%
Technology & software	8%	8%
Transportation	2%	2%
Other	0%	1%
Total	100%	100%

*Financial services includes asset management and insurance

D4. What is the worldwide headcount of your organization?	FY 2018	FY 2017
Less than 500 people	10%	11%
501 to 1,000 people	20%	22%
1,001 to 5,000 people	23%	21%
5,001 to 25,000 people	26%	25%
25,001 to 75,000 people	14%	13%
More than 75,000 people	7%	8%
Total	100%	100%

Acknowledgments

This is one in a periodic series of third-party risk management (TPRM) research papers that examine – longitudinally – the emergence of issues, the evaluation of practice capabilities and the ways in which TPRM practice effectiveness is evolving.

We'd like to thank the Shared Assessments volunteer subcommittee members who conducted and contributed to this effort:

- **John Bree**, Senior Vice President and Partner, Neo Group
- **Niall Browne**, CISO, Senior Vice President Trust & Security, Domo, Inc.
- **Jonathan Dambrot**, CEO & Founder, Prevalent, Inc.
- **Rocco Grillo**, Executive Managing Director, Stroz Friedberg, LLC
- **Susan Jayson**, Executive Director & Co-Founder, Ponemon Institute
- **Paul Kooney**, Managing Director, Protiviti
- **Shawn Malone**, Founder & CEO, Security Diligence, LLC
- **Larry Ponemon, Ph.D.,** Chairman and Founder, CIPP

We would also like to acknowledge The Santa Fe Group, Shared Assessments Program subject matter experts and other staff who supported this effort:

- **Jenny Burke**, Senior Vice President of Communications & Marketing
- **Bob Jones**, Strategic Advisor
- **Charlie Miller**, Senior Vice President
- **Gary Roboff**, Senior Advisor
- **Marya Roddis**, Vice President of Communications

The Shared Assessments Program has been setting the standard in third-party risk management since 2005. Member-driven development of program resources helps organizations to effectively manage the critical components of the third-party risk management lifecycle by creating efficiencies and lowering costs for conducting rigorous assessments of controls for cybersecurity, IT, privacy, data security and business resiliency. The Shared Assessments Program is managed by The Santa Fe Group (www.santa-fe-group.com), a strategic advisory company based in Santa Fe, New Mexico. For more information on Shared Assessments, please visit http://www.sharedassessments.org.

Join the dialog with peer companies and learn how you can optimize your compliance programs while building a better understanding of what it takes to create a more risk sensitive environment in your organization.

Please contact research@ponemon.org or call us at 800.877.3118 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.