The Internet of Things (IoT): A New Era of Third- Party Risk

Sponsored by Shared Assessments

Independently conducted by Ponemon Institute LLC

Publication Date: May 2017

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

The Internet of Things: A New Era of Third-Party Risk

Ponemon Institute: May 2017

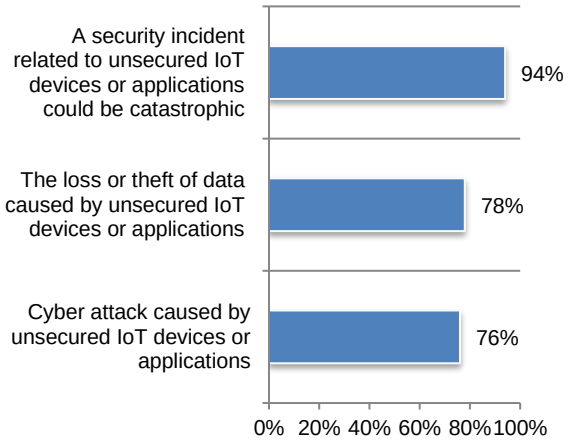
Part 1. Introduction

The Internet of Things: A New Era of Third-Party Risk was sponsored by Shared Assessments and conducted by Ponemon Institute to understand organizations' level of awareness and preparedness for the upcoming enterprise IoT wave. We hope the research findings will help organizations address the risks associated with the proliferation of IoT devices. We surveyed 553 individuals who have a role in the risk management process and are familiar with the use of IoT devices in their organizations.

Participants in the study are aware that IoT introduces new security risks and vulnerabilities into their organizations. However, efforts to mitigate third-party risks in the IoT ecosystem are lagging. According to the research, companies are relying on technologies and governance practices that have not evolved to address emergent IoT threat vectors. Such potential risks include the ability of criminals to harness IoT devices, such as botnets, to attack infrastructure and launch points for malware propagation, SPAM, DDoS attacks and anonymizing malicious activities.

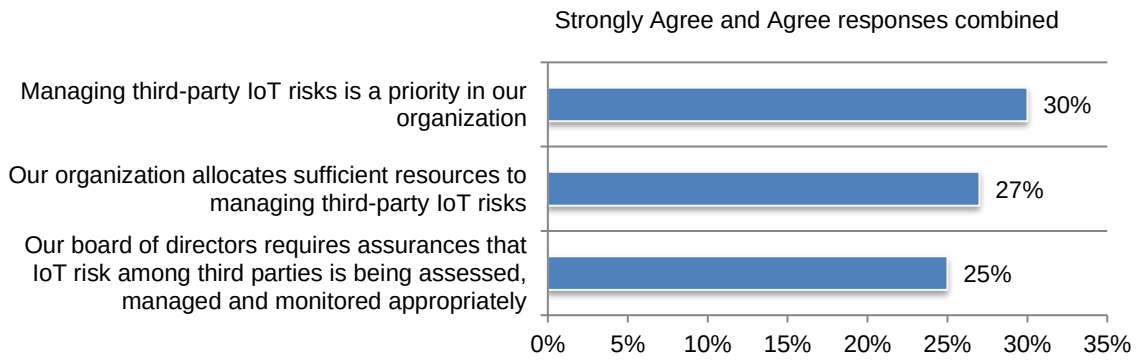
In fact, as shown in Figure 1, 78 percent of respondents say a data breach and 76 percent say a DDoS attack involving an unsecured IoT device is likely to occur within the next two years. Ninety-four percent of respondents say it is likely that either incident would be catastrophic.

Figure 1. IoT risks in the next two years
Very likely, somewhat likely & likely responses combined



Why are respondents so pessimistic about their companies' ability to minimize IoT risks and avoid an attack? According to Figure 2, the major barriers to addressing the risk are: a lack of priority, insufficient resources and boards of directors that are not fulfilling their oversight responsibilities and making management accountable. Specifically, only 30 percent of respondents say managing third-party IoT risks is a priority in their organizations and only 25 percent of respondents say the board of directors wants assurances that IoT risks among third parties is being assessed, managed and monitored appropriately. Because it is not a priority and leadership is not engaged, it is understandable that necessary resources are not being allocated.

Figure 2. Tone at the top and the IoT risk



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:

- Ready or not, IoT third-party risks have arrived
- Problems with third-party IoT governance
- A multi-layered approach to IoT security is needed

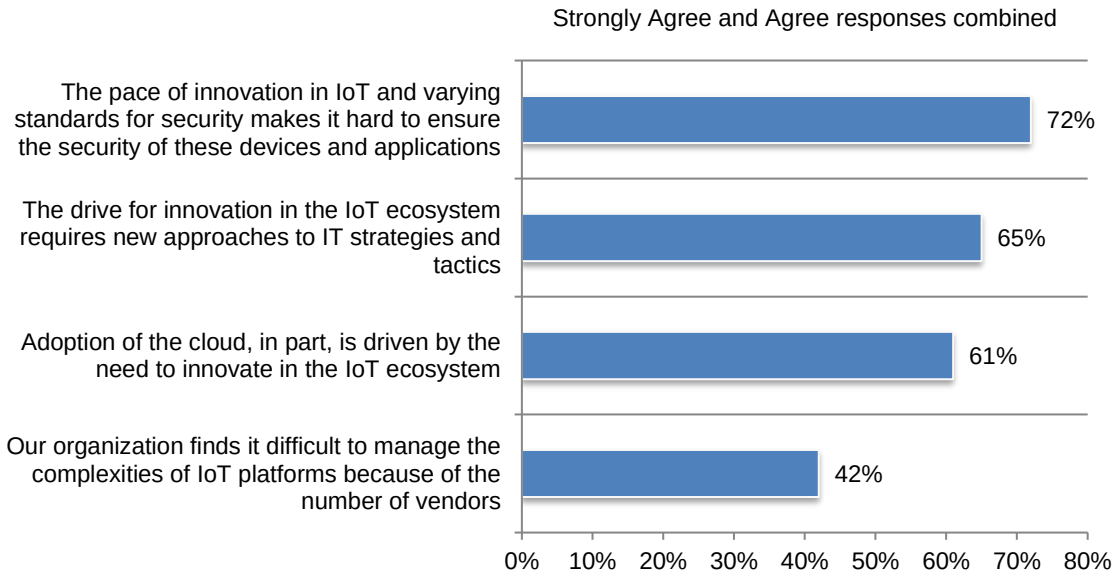
In the context of this research, IoT is defined as the network of physical objects or "things" embedded with electronics, software, sensors and network connectivity, which enables these objects to collect, monitor and exchange data. Examples of IoT devices in the workplace include network-connected printers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

Ready or not IoT third-party risks have arrived

Innovation and complexities in enterprise IoT require new approaches to third-party risk management. According to respondents, the number of IoT devices in their organizations is expected to double in the next two years, from an average of 9,259 to an average 18,631. IoT growth is being driven by the potential to increase efficiencies and improve business outcomes by collecting better data about things in the workplace.[1] However, to ensure the security risks do not outweigh the benefits, new strategies that holistically consider risks in the organization's entire IoT ecosystem are needed.

As shown in Figure 2, the pace of innovation in IoT and the varying standards for security among third parties make it hard to ensure the security of these devices and applications, according to 72 percent of respondents. In addition, the drive for innovation requires new approaches to IT strategies and tactics, and 61 percent say adoption of the cloud is driven, in part, by the need to innovate in the IoT ecosystem. Forty-two percent of respondents say the number of vendors they use makes it difficult to manage the complexities of IoT platforms.

Figure 2. Perceptions about innovation and IoT risks

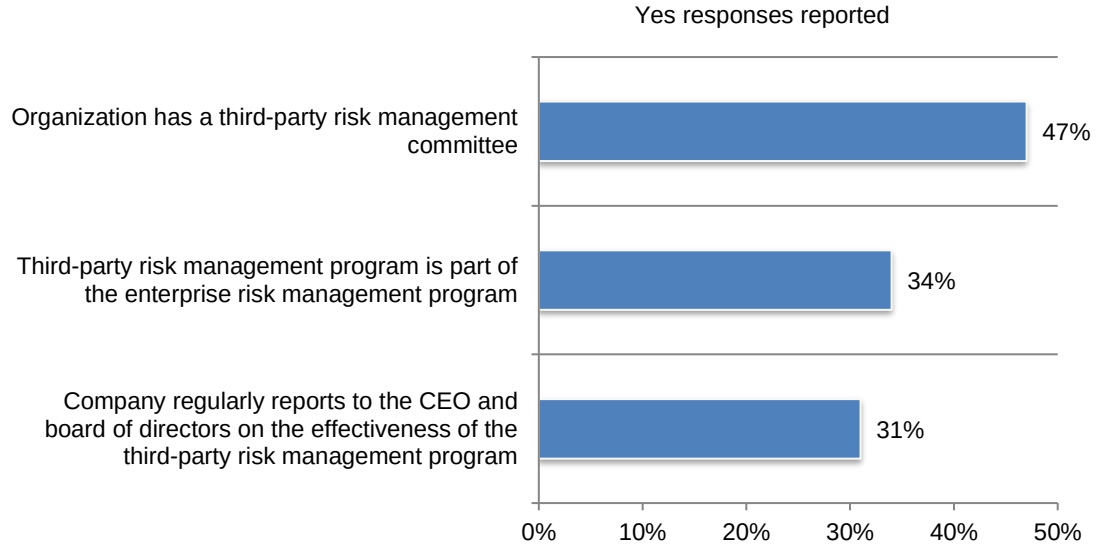


[1] "The Two Faces of IoT Security: How the Internet of Things Introduces Some Risks & Mitigates Others," CyberTrend.com, May 2017.

Current third-party risk management programs are not ready for IoT. The findings demonstrate that fifty-six percent of organizations represented in this study have a third-party risk management program. Of these, only 24 percent of respondents rate their third-party risk management program as highly effective.

Reasons for not achieving a high level of effectiveness are shown in Figure 3. Specifically, only 47 percent have a third-party risk management committee, only 31 percent regularly report to the CEO and board of directors on the effectiveness of the third-party risk management program and only 34 percent say their third-party risk management program is part of their organization's enterprise risk management program.

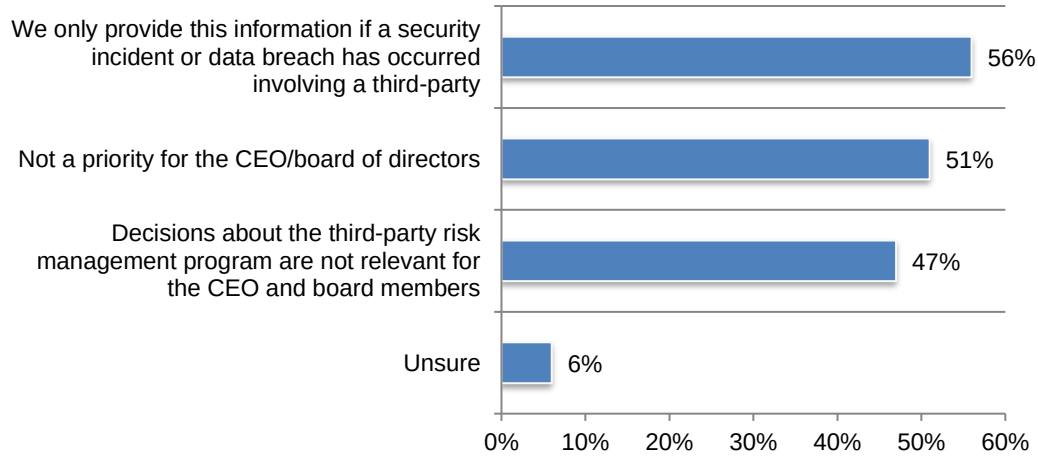
Figure 3. Why current third-party risk management programs are not ready for IoT



As shown above, a total of 69 percent of respondents (100 percent – 31 percent) do not keep their CEO and board informed about the effectiveness of the third-party risk management program.

Reasons for this lack of communication are shown in Figure 4. Fifty-six percent of respondents say they only provide this information if a security or data breach has occurred involving a third-party and more than half (51 percent) say it is not a priority for the CEO and board.

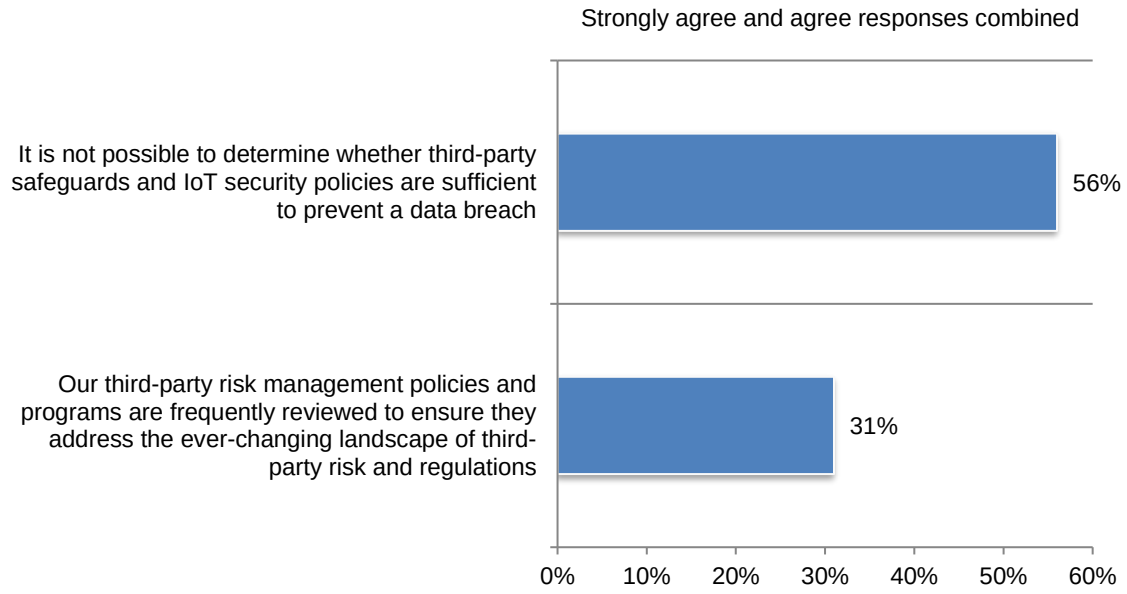
Figure 4. Why organizations do not regularly report to the CEO and board of directors



Problems with third-party IoT governance

Governance programs are ignoring the IoT risk. Only 31 percent of organizations represented in this study are reviewing third-party risk management policies and programs to ensure they address the ever-changing landscape of third-party risk and regulations. The majority (56 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.

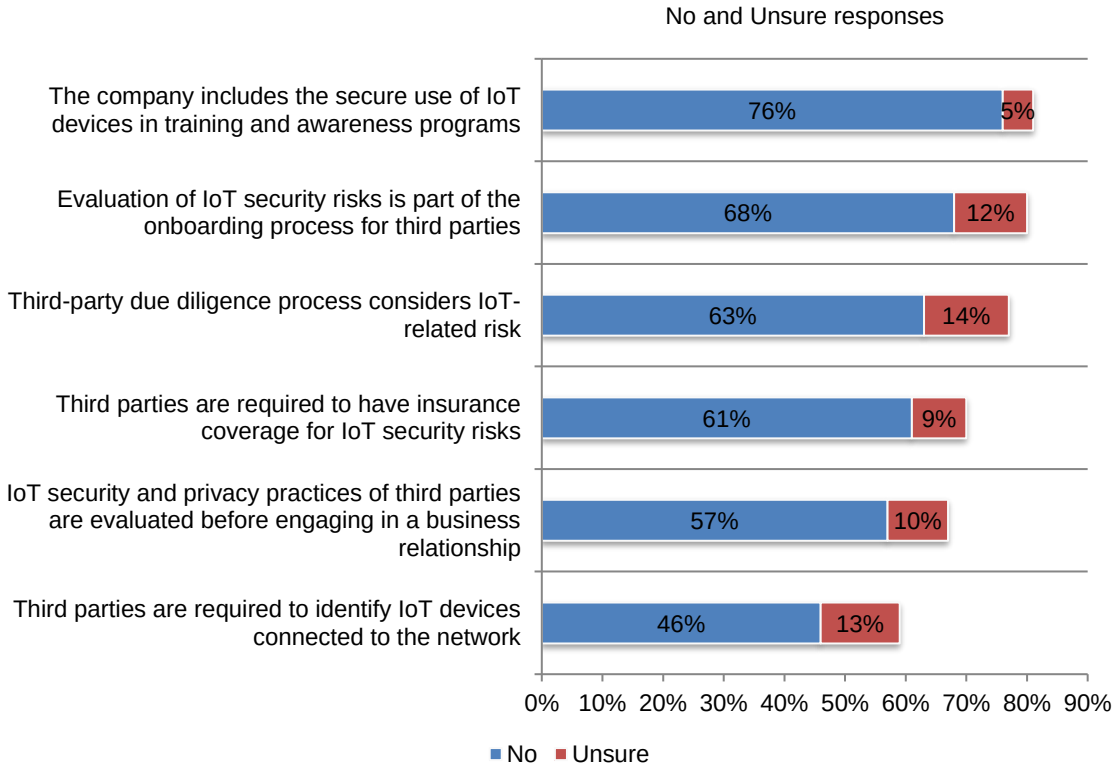
Figure 5. Perceptions about IoT governance practices



Governance programs fail to address IoT third-party risk. Figure 6 presents the "no" and "unsure" responses to questions concerning important IoT risk planning activities. As shown, most organizations do not have the programs and policies in place to mitigate third-party IoT risks. Specifically, companies are not doing the following:

- Including the secure use of IoT devices in training and awareness programs (81 percent)
- Evaluating IoT security risks as part of the onboarding process (80 percent)
- Considering IoT-related risks in the third-party due diligence process (77 percent)
- Requiring third parties to have insurance coverage for IoT security risks (70 percent)
- Evaluating IoT security and privacy practices before engaging in a business relationship (67 percent)
- Requiring third parties to identify IoT devices connect to their network (59 percent)

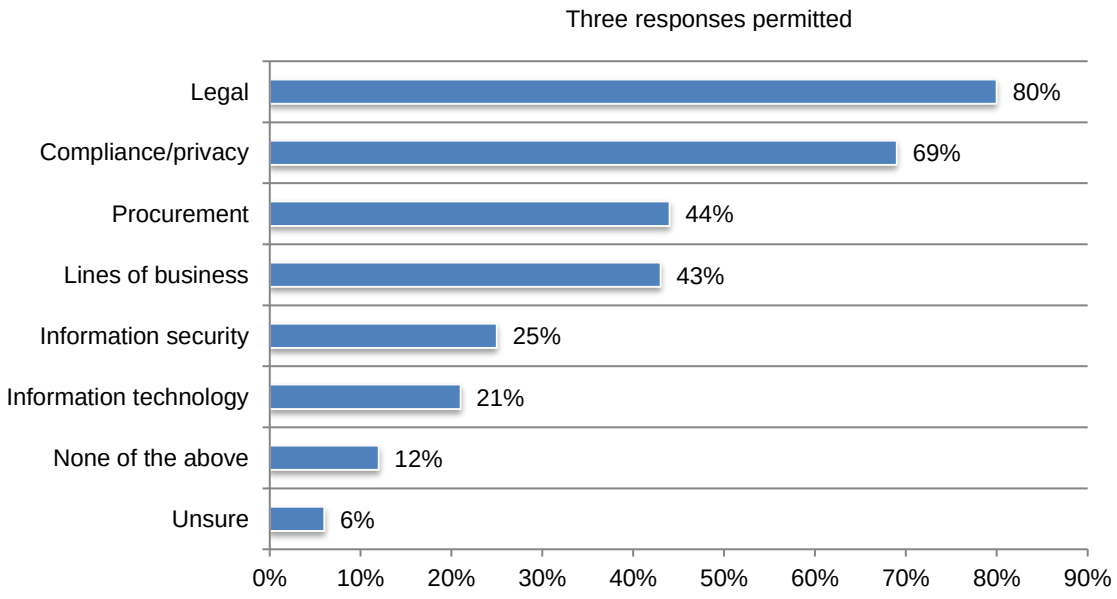
Figure 6. Governance practices most organizations do not follow



Legal is most often responsible for ensuring appropriate privacy and security language is included in third-party contracts. Sixty-two percent of respondents say their organizations require third parties to ensure compliance with their security and privacy practices.

As shown in Figure 7, 80 percent of respondents say making sure contracts protect the organization from a security or privacy incident caused by a third party is the responsibility of the legal department.

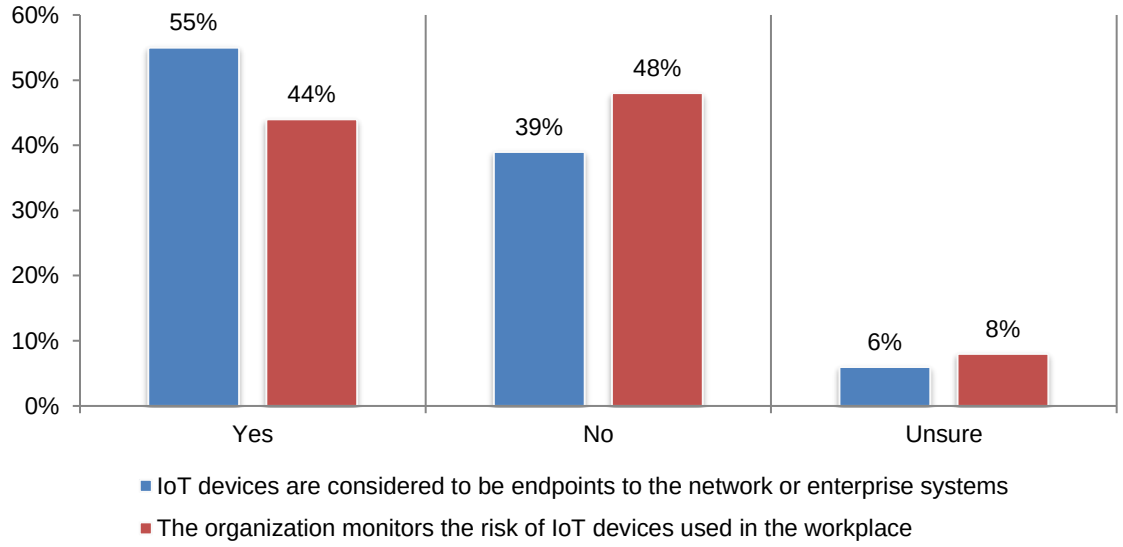
Figure 7. Which department is responsible for ensuring privacy and security language is included in third-party contracts?



A multi-layered approach to IoT security is needed

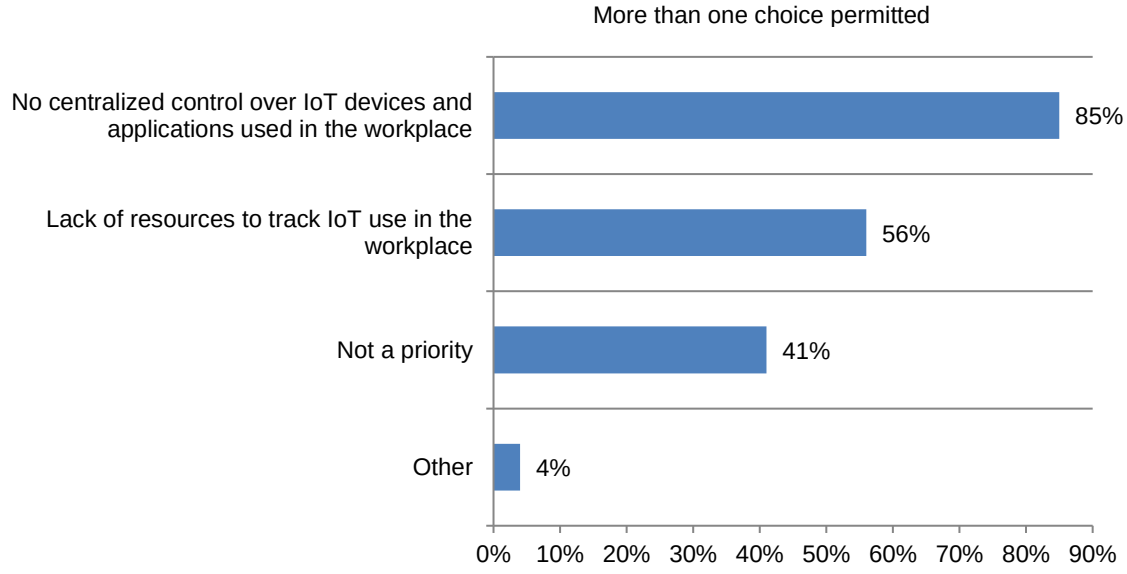
Keeping track of the network of physical objects connected to the Internet is very difficult. Seventy-two percent of respondents say they only know some of the physical objects connected to the Internet (37 percent) or none of them (35 percent). As shown in Figure 8, 55 percent of respondents consider IoT devices to be endpoints to their network or enterprise systems. However, only 44 percent of respondents say their organizations monitor the risk of IoT devices used in the workplace.

Figure 8. Are IoT devices considered endpoints and are they monitored?



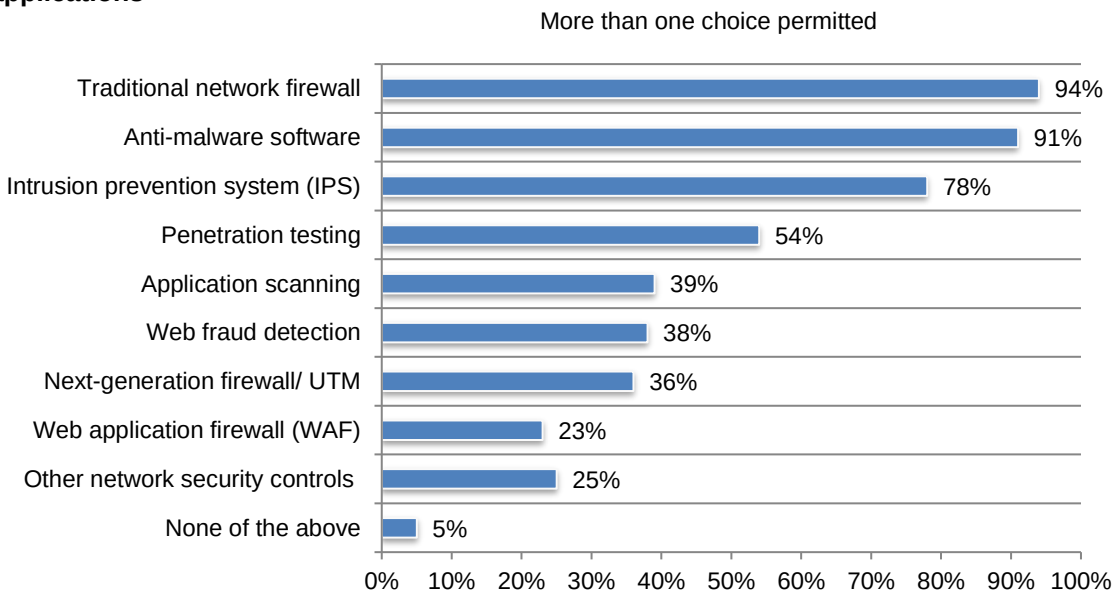
Most companies are not keeping an inventory of managed IoT devices and applications. Only 16 percent of respondents say their organizations keep an inventory. As shown in Figure 9, the barrier to having such an inventory is that there is no centralized control over IoT devices and applications used in the workplace (85 percent) or the lack of resources to track IoT use in the workplace (56 percent).

Figure 9. Why companies do not keep an inventory of managed IoT devices and applications in the workplace



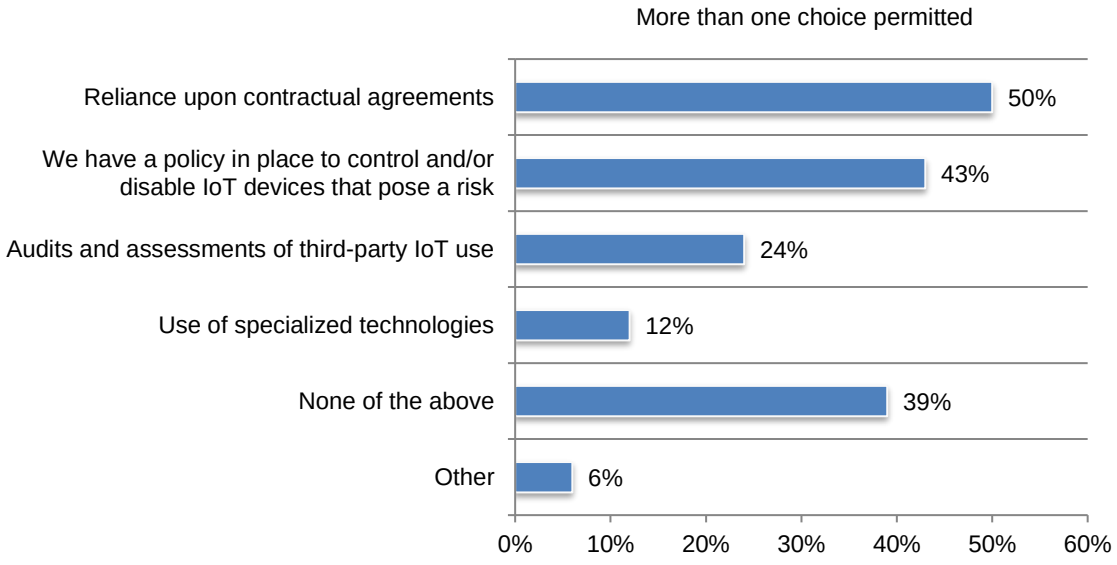
New technology strategies and tactics are needed in the IoT ecosystem. To understand how to mitigate IoT third-party risks, organizations need to recognize the many players in the value chain where potential threat vectors may reside. These are the manufacturer of the device, service providers, application developers and cellular operators.[2] However, as shown in Figure 10, current strategies mainly rely upon traditional network firewalls and anti-malware software.

Figure 10. Steps organizations take to protect their network from insecure IoT devices or applications



Most organizations are unable to control and/or disable risky IoT devices. Only 44 percent of respondents say their organization has the ability to protect their network or enterprise systems from risky IoT devices. Those who have control say it is through contractual agreements (50 percent) or policies that enable the control and/or disablement of the device, as shown in Figure 11.

Figure 11. How does your organization control IoT devices that pose a risk?



[2] Ibid.

Conclusion: Clearly IoT risks have arrived!

This research demonstrates the extent to which organizations are currently struggling to deal with the security risks posed by IoT. Clearly IoT risks have arrived and need to be addressed!

IoT risk exposure occurs both directly within enterprise infrastructure and indirectly through outsourcing to third parties, including cloud service providers. The study definitively demonstrates that IoT security is not being effectively addressed by risk management programs, is not regularly reported and is not currently considered a high priority with most governing boards charged with overseeing enterprise risk.

There is a clear imperative for organizations to better understand the inherent risks posed by IoT devices in their supply chain, ensure IoT security is taken seriously, and educate management at all levels (up to and including governing boards). IoT security concerns should be integrated effectively during the device design/build phases of product development.

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

1. Ensure inclusion of third-party and IoT risks occurs at all governance levels including the Board.
2. Update asset management processes and inventory systems to include IoT devices, and understand the security characteristics of all inventoried devices. When devices are found to have inadequate security controls, replace them.
3. Continue to leverage and enhance contracts and policies and expand scope to include IoT specific requirements.
4. Expand third-party assessment techniques and processes to ensure presence and effectiveness of controls specific to IoT devices.
5. Develop specific sourcing and procurement requirements to ensure only IoT devices that are designed with security functions included and enabled are considered for product selection or acquisition.
6. Devise new strategies, technologies and tactics directed specifically at reducing threats posed by IoT devices.
7. Collaborate with industry experts, peers, associations and regulators to ensure IoT risk management best practices are devised, communicated and implemented.
8. Include IoT in communication, awareness and training at all levels: board, executive, corporate, business unit and third-party.
9. Recognize the increasing dependence on technology to support the business and the risk posed by this dependence.
10. Embrace new technologies and innovations, but not at the expense of security, and ensure security controls are included as fundamental and core requirements.

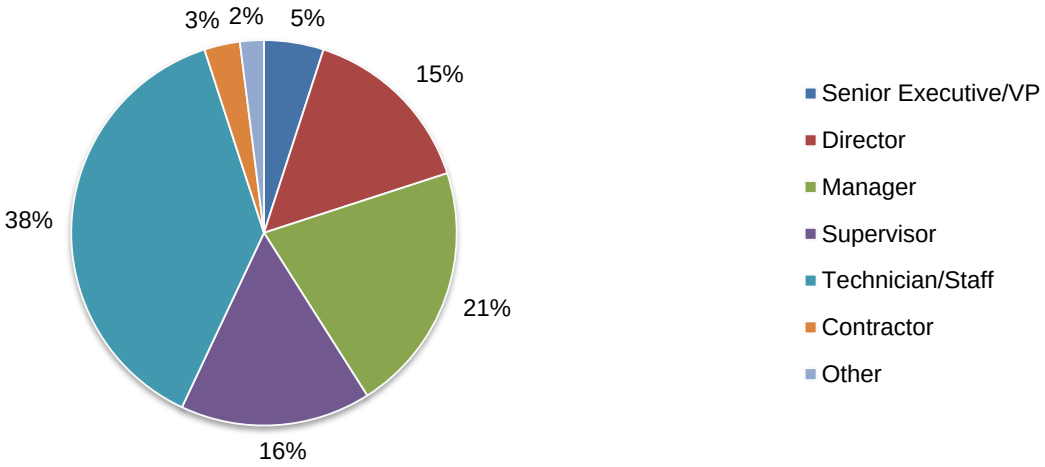
Part 3. Methods

A sampling frame of 15,780 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 608 total returns. Screening and reliability checks required the removal of 55 surveys. Our final sample consisted of 553 surveys, or a 3.5 percent response.

Table 1. Sample response	Freq	Pct%
Sampling frame	15,780	100.00%
Total returns	608	3.85%
Rejected or screened surveys	55	0.35%
Final sample	553	3.50%

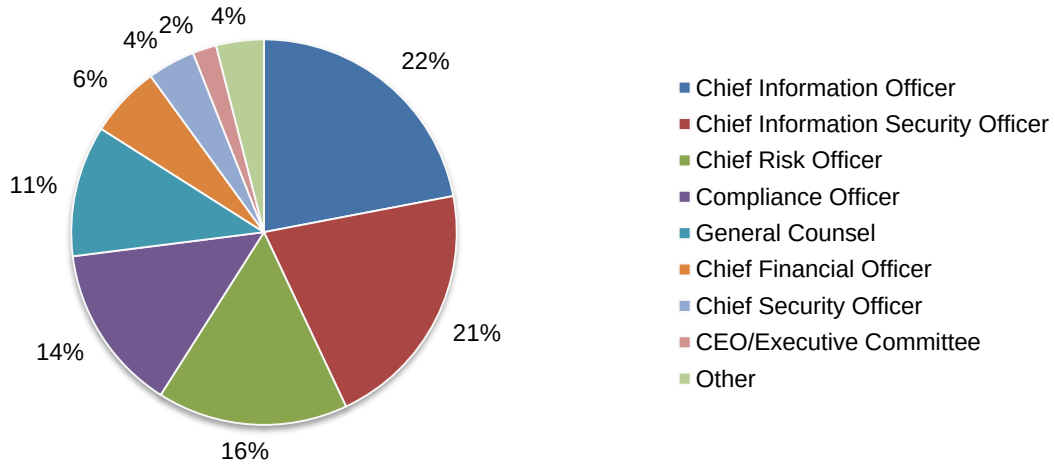
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, more than half of the respondents (57 percent) are at or above the supervisory levels.

Pie Chart 1. Position level within the organization



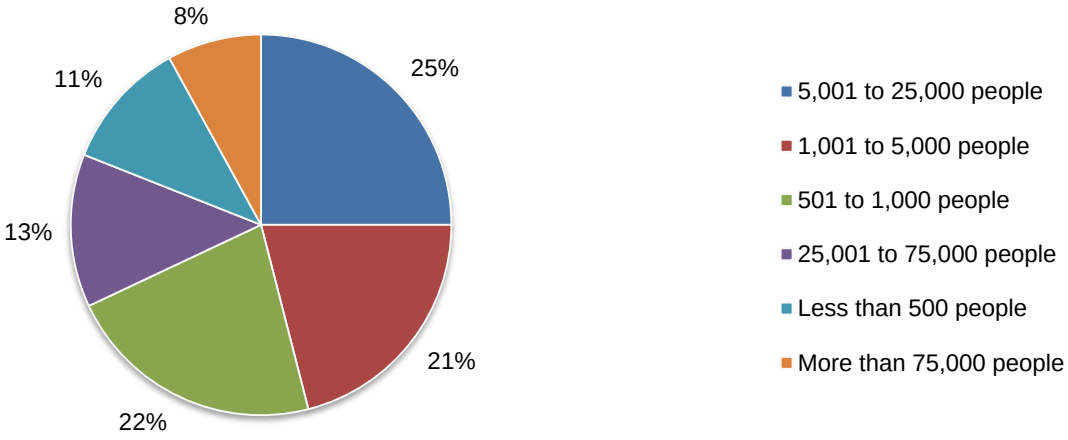
As shown in Pie Chart 2, 22 percent of respondents report directly to the chief information officer, 21 percent report to the chief information security officer and 16 percent report to the chief risk officer.

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



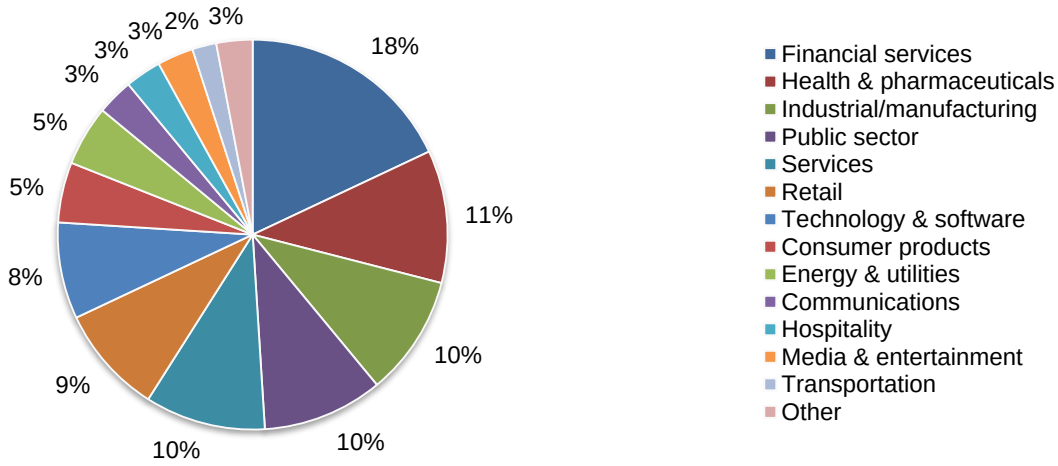
Sixty-eight percent of the respondents are from organizations with a global headcount of more than 500 employees, as shown in Pie Chart 4.

Pie Chart 4. Worldwide headcount of the organization



Pie Chart 5 reports the industry classification of respondents' organizations. This chart identifies financial services (18 percent of respondents) as the largest segment, followed by health and pharmaceuticals (11 percent of respondents).

Pie Chart 5. Primary industry classification



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	15,780	100.00%
Total returns	608	3.85%
Rejected surveys	55	0.35%
Final sample	553	3.50%

Part 1. Screening questions

S1. How familiar are you with your organization's approach to managing third-party risks?	Pct%
Very familiar	31%
Familiar	45%
Somewhat familiar	24%
No knowledge (Stop)	0%
Total	100%

S2. How familiar are you with the use of IoT devices in your organization?	Pct%
Very familiar	17%
Familiar	29%
Somewhat familiar	54%
No knowledge (Stop)	0%
Total	100%

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

Part 2. The state of third-party risk management

Q1a. Does your organization have a third-party risk management program?	Pct%
Yes	56%
No [please proceed to Q5]	44%
Total	100%

Q1b. If yes, please rate the effectiveness of your third-party risk management program using the scale below. 1=not effective to 10=very effective.	Pct%
1 or 2	19%
3 or 4	21%
5 or 6	36%
7 or 8	15%
9 or 10	9%
Total	100%
Extrapolated value	4.98

Q2. Does your organization have a third-party risk management committee?	Pct%
Yes	47%
No	50%
Unsure	3%
Total	100%

Q3a. Does your company regularly report to the CEO and board of directors on the effectiveness of the third-party risk management program?	Pct%
Yes	31%
No	65%
Unsure	4%
Total	100%

Q3b. If no, why? Please select all that apply.	Pct%
Not a priority for the CEO/board of directors	51%
Decisions about the third-party risk management program are not relevant for the CEO and board members	47%
We only provide this information if a security incident or data breach has occurred involving a third-party	56%
Unsure	6%
Total	160%

Q4. Is your third-party risk management program part of your organization's enterprise risk management program?	Pct%
Yes	34%
No	61%
Unsure	5%
Total	100%

Q5. Does your company require third parties to ensure compliance with your security and privacy practices?	Pct%
Yes	62%
No	33%
Unsure	5%
Total	100%

Q6. Which department/function is responsible for ensuring appropriate privacy and security language is included in all contracts with third parties? Please check the top 3 responses.	Pct%
Legal	80%
Information technology	21%
Procurement	44%
Compliance/privacy	69%
Information security	25%
Lines of business	43%
None of the above	12%
Unsure	6%
Total	300%

Part 3: IoT risk management

Q7. 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)?	Pct%
Yes, all of them	9%
Yes, most of them	19%
Yes, some of them	37%
No	35%
Total	100%

Q8a. Has your organization experienced the loss or theft of data caused by unsecured IoT devices or applications in the past 12 months?	Pct%
Yes	15%
No	54%
Unsure	31%
Total	100%

Q8b. 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?	Pct%
Very likely	23%
Somewhat likely	25%
Likely	30%
Not likely	20%
Not possible	2%
Total	100%

Q9a. Has your organization experienced a cyber attack, such as a denial of service (DoS), caused by unsecured IoT devices or applications in the past 12 months?	Pct%
Yes	16%
No	59%
Unsure	25%
Total	100%

Q9b. How likely is your organization to experience a cyber attack, such as a denial of service (DoS), caused by unsecured IoT devices or applications in the next 24 months?	Pct%
Very likely	21%
Somewhat likely	23%
Likely	32%
Not likely	21%
Not possible	3%
Total	100%

Q10. What is the likelihood a security incident related to unsecured IoT devices or applications could be catastrophic to your organization?	Pct%
Very likely	40%
Somewhat likely	39%
Likely	15%
Not likely	4%
Not possible	2%
Total	100%

Q11a. Who is most responsible for managing the risk of IoT devices in the organization? Please check the top 3 responses.	Pct%
General Counsel	37%
Chief Information Officer	51%
Chief Technology Officer	33%
Chief Information Security Officer	60%
Chief Risk Officer	38%
Head of Procurement	12%
Head of Product Engineering	11%
No one person/department is responsible	55%
Unsure	3%
Total	300%

Q11b. Who is most responsible for approving the specific use of IoT devices in the organization and providing security scanning updates? Please check the top 3 choices.	Pct%
General Counsel	31%
Chief Information Officer	63%
Chief Technology Officer	26%
Chief Information Security Officer	69%
Chief Risk Officer	20%
Head of Procurement	11%
Head of Product Engineering	19%
No one person/department is responsible	54%
Unsure	7%
Total	300%

Q12. Does your organization consider IoT devices to be endpoints to your network or enterprise systems?	Pct%
Yes	55%
No	39%
Unsure	6%
Total	100%

Q13. Does your organization monitor the risk of IoT devices used in the workplace?	Pct%
Yes	44%
No	48%
Unsure	8%
Total	100%

Part 4. IoT security risk

Q14a. Does your company keep an inventory of managed IoT devices and applications in the workplace?	Pct%
Yes, for all devices	5%
Yes, for most devices	11%
Yes, for some devices	26%
No	50%
Unsure	8%
Total	100%

Q14b. If no or unsure, why? Please check all that apply	Pct%
Lack of resources to track IoT use in the workplace	56%
No centralized control over IoT devices and applications used in the workplace	85%
Not a priority	41%
Other	4%
Total	186%

Q15a. How many IoT devices does **your organization** have in the workplace? Your best guess is welcome.	Pct%
Less than 100	13%
100 to 500	19%
501 to 1,000	26%
1,001 to 10,000	20%
10,001 to 25,000	11%
25,001 to 50,000	7%
50,001 to 100,000	3%
More than 100,000	1%
Total	100%
Extrapolated value	9,259

Q15b. How many IoT devices will your organization have in the workplace in the next 24 months? Your best guess is welcome.	Pct%
Less than 100	11%
100 to 500	16%
501 to 1,000	17%
1,001 to 10,000	19%
10,001 to 25,000	16%
25,001 to 50,000	10%
50,001 to 100,000	5%
More than 100,000	6%
Total	100%
Extrapolated value	18,631

Q16. What steps are you taking to protect your network from insecure IoT devices or applications? Please select all that apply.	Pct%
Web application firewall (WAF)	23%
Application scanning	39%
Penetration testing	54%
Anti-malware software	91%
Intrusion prevention system (IPS)	78%
Traditional network firewall	94%
Next-generation firewall/ UTM	36%
Web fraud detection	38%
Other network security controls (please specify)	25%
None of the above	5%
Total	483%

Q17a. Do you have the ability to control and/or disable IoT devices that pose a risk to your organization?	Pct%
Yes	44%
No	50%
Unsure	6%
Total	100%

Q17b. If yes, how do you achieve control? Please check all that apply.	Pct%
We have a policy in place to control and/or disable IoT devices that pose a risk	43%
Audits and assessments of third-party IoT use	24%
Reliance upon contractual agreements	50%
Use of specialized technologies	12%
None of the above	39%
Other	6%
Total	174%

Part 5. Attributions: Please rate the following statements using the five-point scale provided below each item. Strongly Agree and Agree responses combined.	SA% + A%
Q18. Managing third-party IoT risks is a priority in our organization	30%
Q19. Our organization allocates sufficient resources to managing third-party IoT risks	27%
Q20. Our board of directors requires assurances that IoT risk among third parties is being assessed, managed and monitored appropriately	25%
Q21. It is not possible to determine whether third-party safeguards and IoT security policies are sufficient to prevent a data breach	56%
Q22. Our third-party risk management policies and programs are frequently reviewed to ensure they address the ever-changing landscape of third-party risk and regulations	31%
Q23. Adoption of the cloud, in part, is driven by the need to innovate in the IoT ecosystem	61%
Q24. The drive for innovation in the IoT ecosystem requires new approaches to IT strategies and tactics	65%
Q25. Our organization finds it difficult to manage the complexities of IoT platforms because of the number of vendors	42%
Q26. The pace of innovation in IoT and varying standards for security makes it hard to ensure the security of these devices and applications	72%
Q27. The IoT ecosystem is vulnerable to a ransomware attack	55%

Part 6. Third-party IoT risk management planning

Q28a. Do you evaluate the IoT security and privacy practices of third parties before you engage them in a business relationship?	Pct%
Yes	33%
No	57%
Unsure	10%
Total	100%

Q28b. If yes, how do you perform this evaluation? Please check all that apply.	Pct%
Review written policies and procedures	51%
Acquire signature on contracts that legally obligates the third-party to adhere to security and privacy practices	54%
Obtain indemnification from the third-party in the event of a data breach	35%
Conduct an audit of the vendor's IoT security and privacy practices	12%
Obtain a self-assessment conducted by the third-party	9%
Obtain references from other organizations that engage the third-party	8%
Obtain evidence of security certification such as ISO 27001, SOC 2, NIST and others	29%
Other (please specify)	3%
Unsure	2%
Total	203%

Q29. Do you require third parties to identify IoT devices connected to your network?	Pct%
Yes	41%
No	46%
Unsure	13%
Total	100%

Q30. Is the evaluation of IoT security risks part of the onboarding process for third parties?	Pct%
Yes	20%
No	68%
Unsure	12%
Total	100%

Q31. Does the third-party due diligence process consider IoT-related risk?	Pct%
Yes	23%
No	63%
Unsure	14%
Total	100%

Q32. Does your company require third parties to have insurance coverage for IoT security risks?	Pct%
Yes	30%
No	61%
Unsure	9%
Total	100%

Q33a. Does your company have an incident response plan for security breaches involving third parties?	Pct%
Yes	56%
No	38%
Unsure	6%
Total	100%

Q33b. If yes, does it include security breaches that result from unsecured IoT devices?	Pct%
Yes	22%
No	72%
Unsure	6%
Total	100%

Q34. Does your company include the secure use of IoT devices in training and awareness programs?	Pct%
Yes	19%
No	76%
Unsure	5%
Total	100%

Part 7. Demographics and organizational characteristics

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

D2. Check the **Primary Person** you report to within the organization.	Pct%
CEO/Executive Committee	2%
Chief Financial Officer	6%
General Counsel	11%
Chief Privacy Officer	1%
Chief Information Officer	22%
Compliance Officer	14%
Human Resources VP	1%
Chief Information Security Officer	21%
Chief Security Officer	4%
Chief Risk Officer	16%
Other	2%
Total	100%
D3. What is the worldwide headcount of your organization?	Pct%
5,001 to 25,000 people	25%
1,001 to 5,000 people	21%
501 to 1,000 people	22%
25,001 to 75,000 people	13%
Less than 500 people	11%
More than 75,000 people	8%
Total	100%

D4. What industry best describes your organization's industry focus?	Pct%
Agriculture & food services	1%
Communications	3%
Consumer products	5%
Defense & aerospace	1%
Education & research	1%
Energy & utilities	5%
Financial services	18%
Health & pharmaceuticals	11%
Hospitality	3%
Industrial/manufacturing	10%
Media & entertainment	3%
Public sector	10%
Retail	9%
Services	10%
Technology & software	8%
Transportation	2%
Other	0%
Total	100%

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. Program Tools are kept current with regulations, industry standards and guidelines and the current threat environment; and are adopted globally across a broad range of industries both by service providers and their customers. Shared Assessments membership and use of the Shared Assessments Program Tools: Agreed Upon Procedures (AUP); Standardized Information Gathering (SIG) questionnaire and Vendor Risk Management Maturity Model (VRMMM), offers companies and their service providers a standardized, more efficient and less costly means for third-party risk management programs. 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.

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.