Ponemon INSTITUTE

Data Risk in the Third-Party Ecosystem

Second Annual Study

September 2017
Independently conducted by Ponemon Institute LLC

Sponsored by opus

Ponemon Institute LLC Research Report

PART 1. INTRODUCTION

We are pleased to present the findings of *Data Risk in the Third-Party Ecosystem: Second Annual Study*, sponsored by Opus, to understand trends in the challenges companies face in protecting sensitive and confidential information shared with third parties and their third parties (N^{th} party risk). While the findings of this study reveal that the risk of sharing sensitive and confidential information with third parties is increasing, there are governance and IT security practices that can be implemented to significantly reduce the likelihood of a third-party data breach.

Since the study was first conducted last year, companies have made little progress in improving the overall effectiveness of their third-party risk management programs. This includes understanding how many of their third and N^{th} parties have access to sensitive and confidential data, confirming the existence of adequate safeguards and security policies in third parties and reviewing third-party management policies and programs to ensure risks are addressed. A serious barrier to achieving these objectives is the lack of adequate resources to manage third-party risk, according to 60 percent of participants in this research.

We define the third-party ecosystem as the many direct and indirect relationships companies have with third parties and N^{th} parties. These relationships are important to fulfilling business functions or operations. However, the research underscores the difficulty companies have in detecting, mitigating and minimizing risks associated with third parties that have access to their sensitive or confidential information.

KEY REPORT FINDINGS

Data breaches caused by third parties are on the rise

- Fif y-six percent of respondents confirm that their organizations experienced a data breach caused by one of their vendors, an increase of 7 percent over the last year.
- Cyber attacks against third parties that resulted in the misuse of their company's sensitive or confidential information also increased significantly from 34 percent to 42 percent of respondents.

The effectiveness of third party governance programs remains low

- Less than half of all respondents say managing outsourced relationship risks is a priority in their organization.
- Only 17 percent of respondents rate their companies' effectiveness in mitigating third party risk as highly effective.
- Sixty percent of respondents feel unprepared to check or verify their third parties, down from 66 percent in 2016.

Accountability and board level involvement increased slightly

- Accountability for the third-party risk management program is dispersed throughout the organization. However, 5 percent more respondents now have an owner of the third-party program compared to last year.
- Forty-two percent of respondents strongly agree or agree that their companies' board of directors requires assurances that third-party risk is being assessed, managed and monitored.
- However, only one-third of all respondents say their companies regularly report to the boards of directors on the effectiveness of the third-party management program and potential risks to the organization.

Companies lack visibility into third-party and Nth party relationships

- The average number of third parties with access to confidential or sensitive information has increased by 25 percent over last year from 378 to 471 third parties.
- More than half of all respondents do not keep a comprehensive inventory of all third parties with whom they share sensitive information.
- Visibility gets worse with Nth-party relationships, only 18 percent of respondents say their companies know how their information is being accessed or processed by Nth parties with whom they have no direct relationship.
- Thirteen percent of all respondents could not determine if they had experienced a third-party data breach.

Today's programs are insufficient to manage third-party risks

- Fif y-seven percent of respondents say they are not able to determine if vendors' safeguards and security policies are sufficient to prevent a data breach.
- Less than half of all respondents say that their company evaluates the security and privacy practices of all vendors before starting a business relationship that requires the sharing of sensitive or confidential information.
- If they do conduct an evaluation, it is mostly to acquire signatures on contracts that legally obligate the third party to adhere to security and privacy practices.

BEST PRACTICES IN THIRD-PARTY RISK MANAGEMENT GOVERNANCE

The study found strong correlations between certain best practices and a reduction in the likelihood of third-party data breaches. As shown in Figure 1, the two most effective practices that when deployed reduce the likelihood of a breach are the evaluation of the security and privacy practices of third parties (46 percent likelihood of a data breach vs. 66 percent likelihood) and an inventory of all third parties with whom the organization shares information (46 percent likelihood of a data breach vs. 65 percent likelihood).

Based on this analysis, companies should consider the following actions to reduce the likelihood of a third-party data breach.

1. **Evaluation of the security and privacy practices of all third parties.** In addition to contractual agreements, conduct audits and assessments to evaluate the security and privacy practices of third parties.

2. **Inventory of all third parties with whom you share information.** Create an inventory of third parties who have access to confidential information and how many of these third parties are sharing this data with one or more of their contractors.

3. **Frequent review of third-party management policies and programs.** The third-party risk management committee should create a formal process for and regularly review the security and privacy practices of their third and Nth parties to ensure they address new and emerging threats, such as unsecured Internet of Things devices.

4. **Formation of a third-party risk management committee.** Create a cross-functional team to regularly review and update third-party management policies and programs.

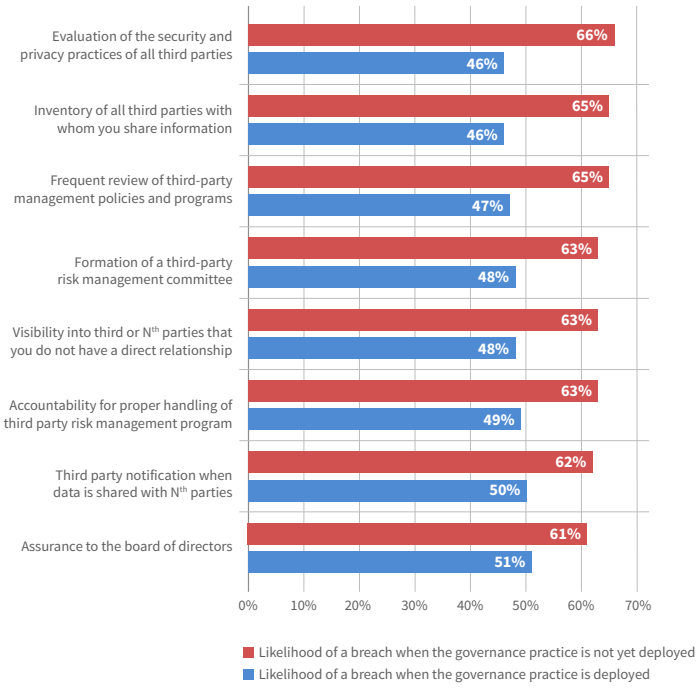
5. **Visibility into third or Nth parties with whom you do not have a direct relationship.** Increase visibility into the security practices of all parties with access to company sensitive information – even subcontractors

6. **Accountability for proper handling of third-party risk management program.** Centralize and assign accountability for the correct handling of your company's third-party risk management program and ensure that appropriate privacy and security language is included in all vendor contracts.

7. **Third party notification when data is shared with Nth parties.** Companies should include in their vendor contract requirements that third parties provide information about possible third-party relationships with whom they will be sharing sensitive information.

8. **Oversight by the board of directors.** Involve senior leadership and boards of directors in third-party risk management programs. This includes regular reports on the effectiveness of these programs based on the assessment, management and monitoring of third-party security practices and policies. Such high-level attention to third-party risk may increase the budget available to address these threats to sensitive and confidential information.

FIGURE 1
Impact of eight third-party risk management practices on the likelihood of a data breach
Mean likelihood of data breach = 56 percent



PART 2. KEY FINDINGS

In this study, we surveyed 625 individuals across multiple industries who are familiar with their organization's approach to managing data risks created through outsourcing. All organizations represented in this study have a third-party data risk management program. In the survey, we asked respondents to consider only those outsourcing relationships that require the sharing of sensitive or confidential information or involve processes or activities that require providing access to sensitive or confidential information.

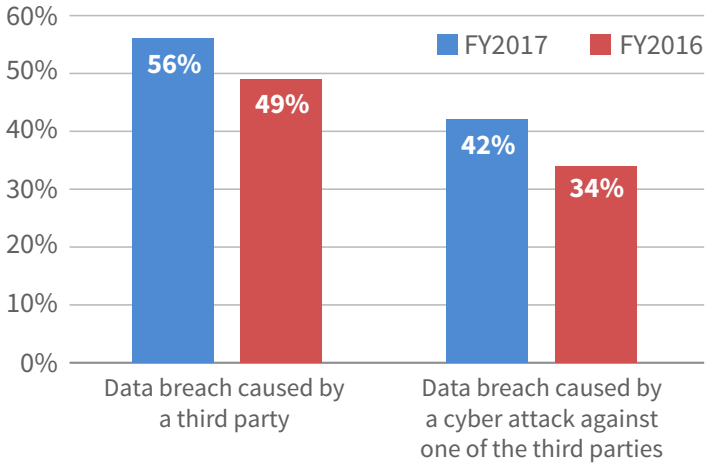
In this section, we present an analysis of the research. The complete audited findings are in the Appendix of this report. We have organized the research according to the following topics:

- Data breaches and the associated third-party data risk
- Strategic shortfalls in third-party risk management governance
- Lack of visibility into third and Nth party relationships
- The realities of today's third-party risk management programs
- Key factors impacting the likelihood of a data breach

Data breaches and the associated third-party data risk

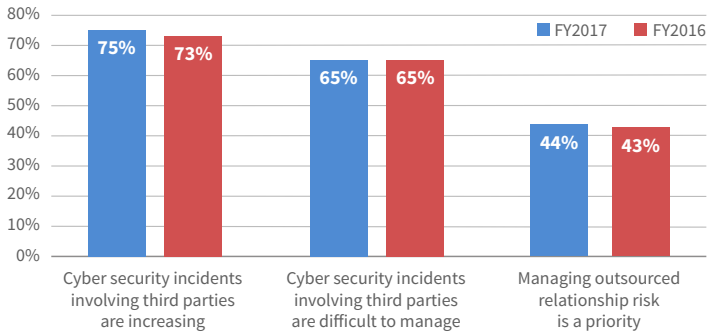
More companies are having data breaches involving third parties. This year, 56 percent of respondents confirm that their organizations experienced a data breach caused by one of their vendors, a significant increase from less than half in last year's research, as shown in Figure 2. Cyber attacks against third parties that resulted in the misuse of their company's sensitive or confidential information also increased from 34 percent of respondents to 42 percent of respondents.

FIGURE 2
Has your organization experienced a data breach or cyber attack caused by a third party?
Yes responses reported



Additionally, the number of cybersecurity incidents involving third parties continues to increase. As shown in Figure 3, 75 percent of respondents say the number of cybersecurity incidents involving vendors is increasing. Similarly, there has been no improvement in managing and preventing cybersecurity risks involving third parties (unchanged at 65 percent of respondents). A key barrier to reducing incidents is that only 44 percent of respondents say managing outsourced relationship risks is a priority.

FIGURE 3
Cybersecurity incidents are increasing and difficult to manage
Strongly Agree and Agree responses combined

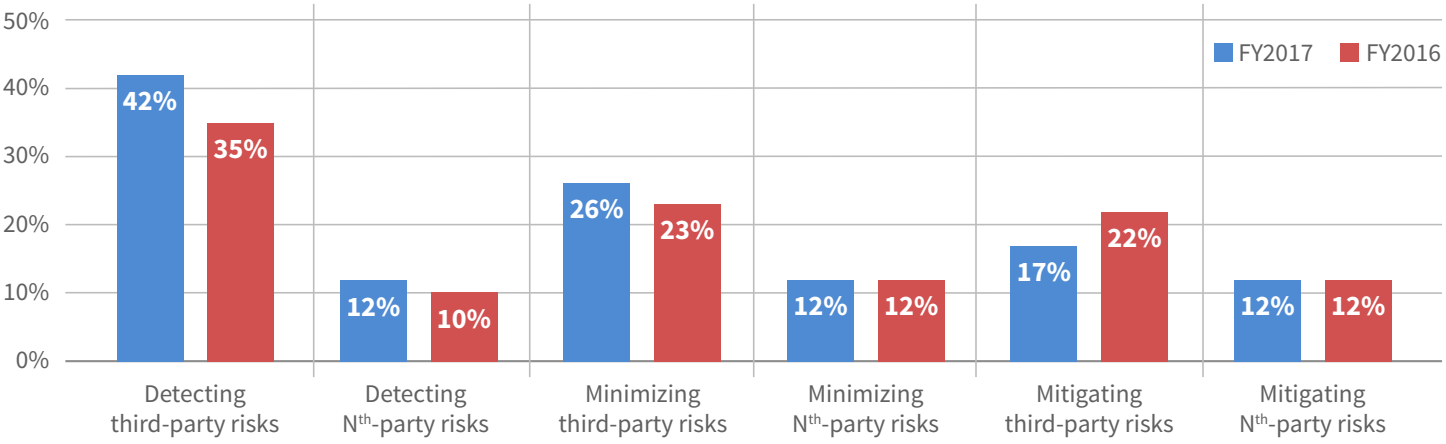


Strategic shortfalls in third-party risk management governance

The effectiveness of managing third-party risks is not improving. We asked participants to rate the effectiveness in dealing with third party and Nth party risks from a scale of 1=not effective to 10=highly effective. Figure 4 presents the highly effective responses (7 + on a scale of 1=not effective to 10=highly effective). Only 17 percent of respondents rate their companies' effectiveness in mitigating third-party risk as highly effective. When it comes to Nth party risk, only 12 percent rate their effectiveness as high.

Respondents seem to be more effective in detecting third-party risks (an increase from 35 percent to 42 percent of respondents), but only 12 percent of respondents rate the detection of Nth party risks as highly effective. Effectiveness in mitigating third-party risks decreased significantly.

FIGURE 4
How effective are organizations in dealing with third party and Nth party risks?
1=not effective to 10=highly effective, 7+ responses reported



Accountability for the third-party risk management program is dispersed throughout the organization. As shown in Figure 5, there are significant trends in accountability for the correct handling of the third-party risk management programs since last year's report.

The response "no one person or department is accountable" has decreased from 21 percent to 16 percent and fewer companies are assigning accountability to the head of procurement (19 percent vs. 16 percent last year). Most accountability (35 percent of respondents) seems to rest with the IT and IT security function: CIO (15 percent of respondents) + CISO (13 percent) + CSO (5 percent) + CTO (2 percent).

Board of directors' involvement in third-party risk management programs improves slightly. As shown in Figure 6, last year only 38 percent of respondents strongly agreed (15 percent + 23 percent) that their companies' board of directors requires assurances that third-party risk is being assessed, managed and monitored. This year, 42 percent agree their boards are engaged in third-party risks affecting the organization.

FIGURE 5
Who is most accountable for the correct handling of the organization's third-party risk management program?

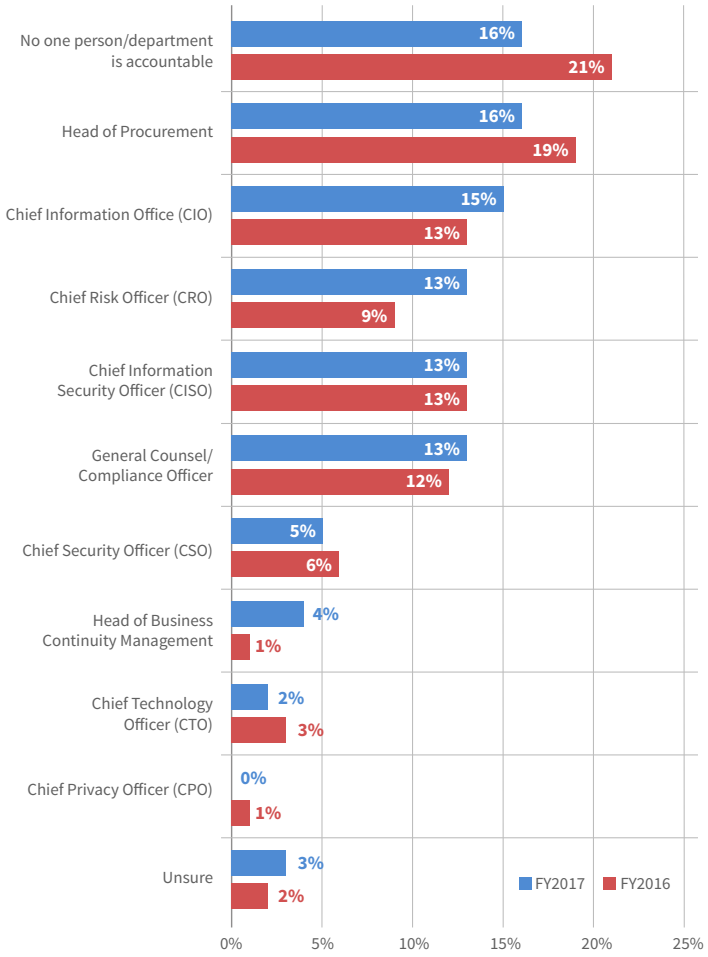
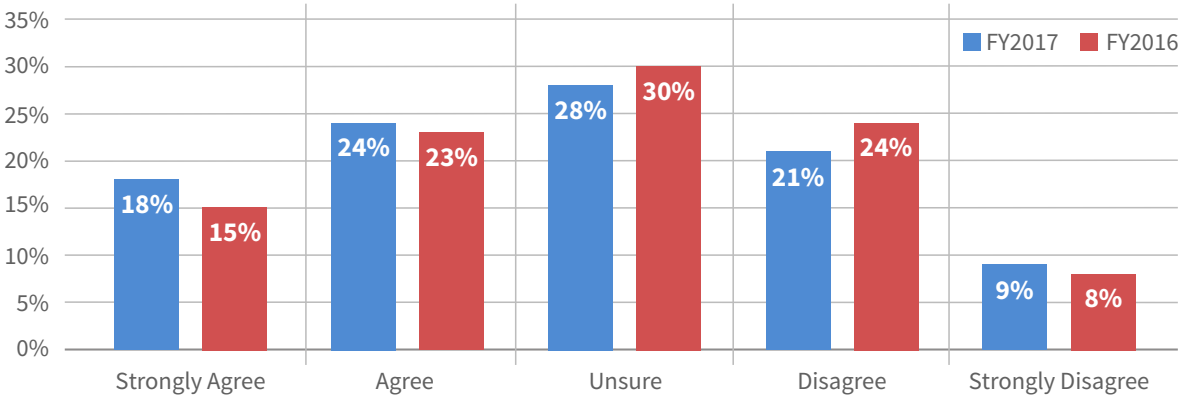


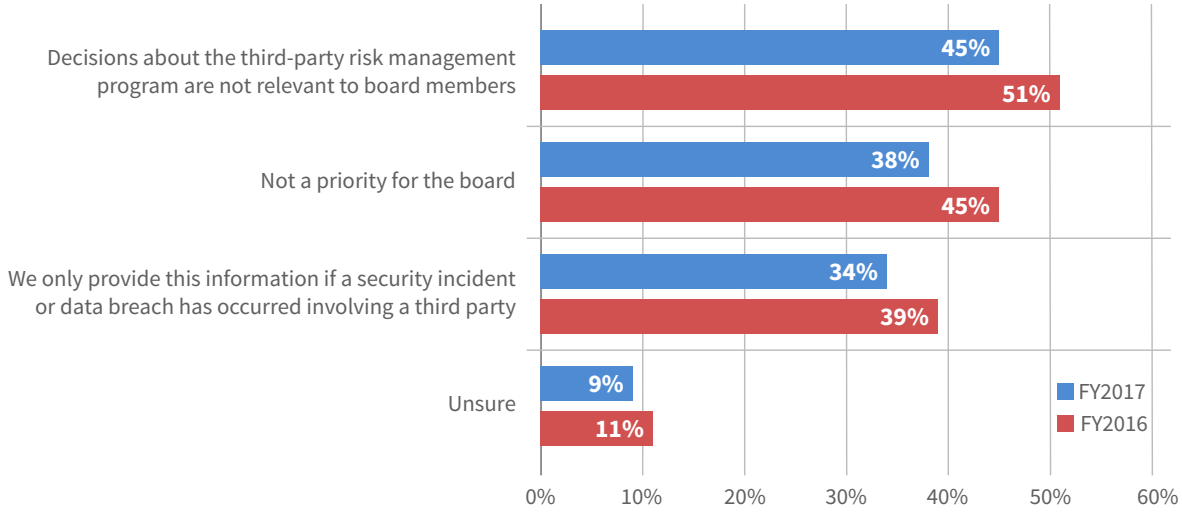
FIGURE 6
Our board of directors requires assurances that third-party risk is being assessed, managed, and monitored.



Communication with the board of directors about third-party risks rarely occurs. Only 33 percent of respondents say their companies regularly report to the boards of directors on the effectiveness of the third-party management program and potential risks to the organization.

Of the 67 percent of respondents who say their companies *do not* regularly report to the board, the primary reason is that third-party risk management is not relevant for the board of directors, as shown in Figure 7. However, this is a significant decrease from last year. Thirty-eight percent of respondents believe it is not a priority or it is only relevant if a security breach has occurred involving a vendor (34 percent of respondents).

FIGURE 7
Reasons for not regularly reporting third-party risks to the board of directors
More than one response permitted



Lack of visibility into third and Nth party relationships

Few companies are able to maintain a comprehensive inventory of all third parties with whom they share information. As shown in Figure 8, most respondents (65 percent) say they do not have (57 percent) or are unsure (8 percent) if their company has such an inventory. Of the 35 percent of respondents in companies with a third-party inventory, 84 percent admit that the inventory does not include all third parties their company has a relationship with that might have access to their sensitive and confidential information. And within the third-party inventory, it is estimated that 30 percent of all third parties have access to sensitive and confidential information.

Reliance on third-party relationships continues to rise. As shown in Figure 9, of the 35 percent of respondents who say their organizations have a comprehensive inventory of all third parties with whom it shares sensitive and confidential information, 57 percent say the inventory contains more than 100 third parties, up 10 percent from last year. On average, respondents report this inventory has 471 third parties, up significantly from 378 in 2016.

FIGURE 8
Does your company have a comprehensive inventory of all third parties with whom it shares sensitive and confidential information?

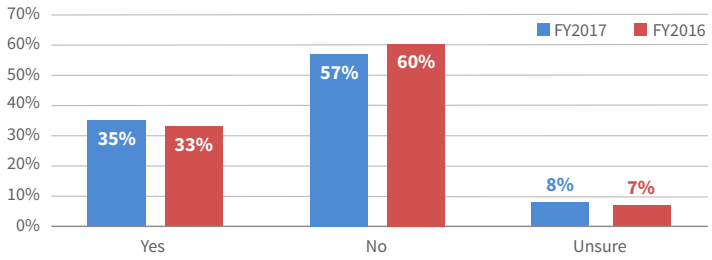
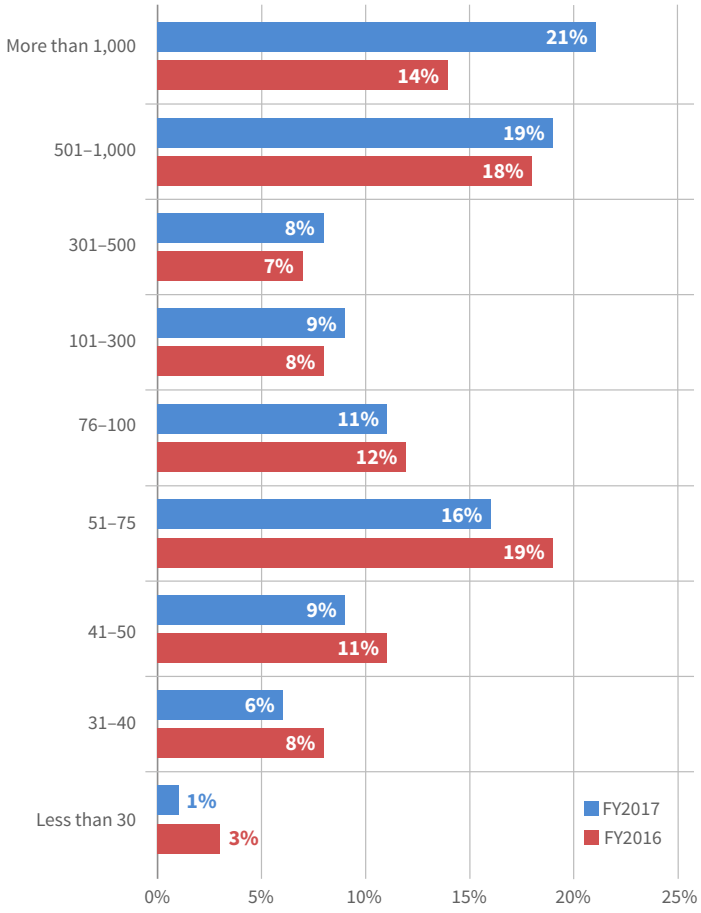
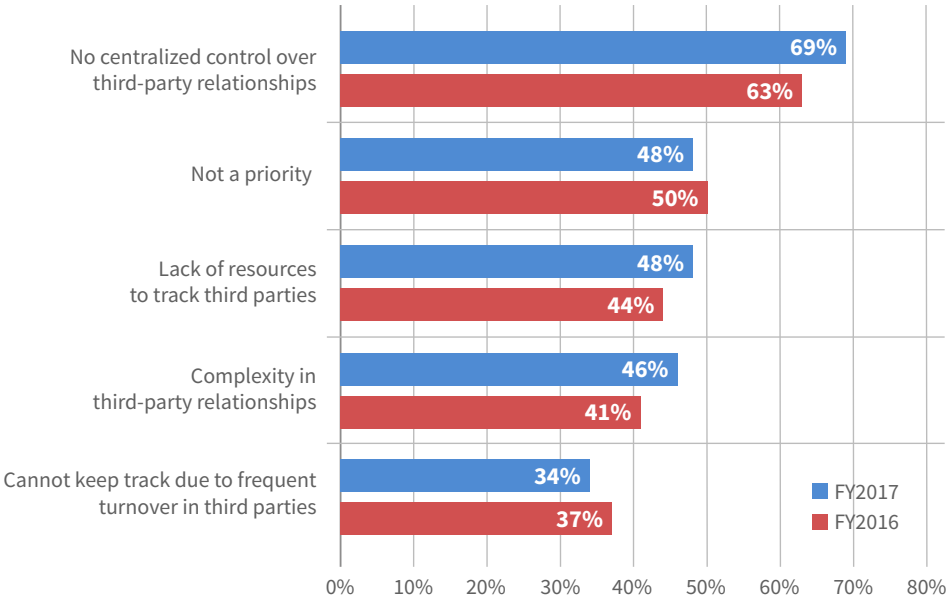


FIGURE 9
How many third parties are in this inventory?



Reasons for not having a comprehensive inventory are shown in Figure 10. Most respondents cite a lack of centralized control over third-party relationships, a lack of resources to track third parties, complexity of these relationships and the inability to keep track because of frequent turnover in third parties.

FIGURE 10
Reasons companies do not have a comprehensive inventory of all third parties
More than one response permitted



Companies lack visibility into Nth parties that have their sensitive or confidential data. Only 18 percent of respondents say their companies know how their information is being accessed or processed by Nth parties with whom they have no direct relationship.

According to Figure 11, of the 18 percent of respondents who say they have such visibility, 67 percent say visibility is due to reliance upon contractual agreements and 59 percent of respondents say they trust the third party to notify their organization when their data is shared with their Nth parties.

Third parties rarely inform companies about their sharing with Nth parties. We asked *all* respondents to estimate the percentage of all third parties they believe are outsourcing their sensitive and confidential data to Nth parties. According to these respondents, an average of 40 percent of their primary vendors are sharing sensitive and confidential information with other vendors (Nth party risk). However, according to Figure 12, only 31 percent of respondents say they are notified if such sharing is taking place, a decrease from 33 percent of respondents in last year's study.

FIGURE 11
How does your organization achieve visibility into vendors your company does not have a direct relationship with?
More than one response permitted

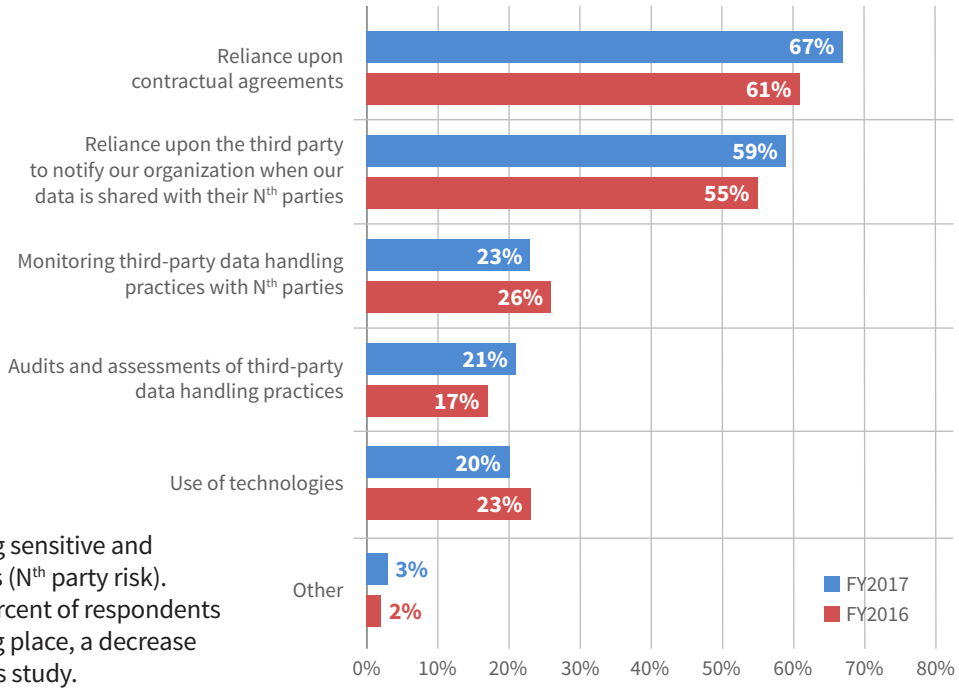
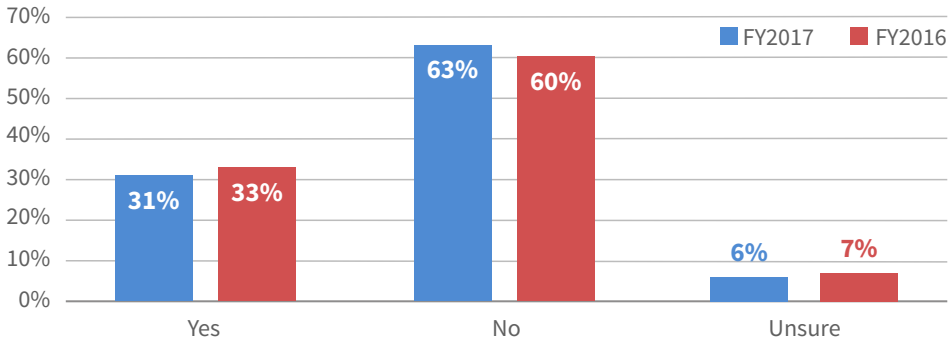


FIGURE 12
Do third parties notify your organization when your data is shared with Nth parties?



Many third-party data breaches go undetected. When asked to rate their confidence in a third party or Nth party vendor notifying their organization about a data breach from a scale of 1=not confident to 10=high confidence, only 35 percent of respondents say a third party would contact them about the data breach, as shown in Figure 13. A very small percentage (11 percent) are confident they would learn that their sensitive data was lost or stolen by a Nth vendor.

The realities of today's third-party risk management programs

As shown in Figure 14, 57 percent of respondents say they are not able to determine if vendors' safeguards and security policies are sufficient to prevent a data breach. Only 43 percent of respondents say their vendors' data safeguards and security policies and procedures are sufficient to respond effectively to a data breach, according to Figure 16.

FIGURE 13
We are confident a third party would notify us if they had a data breach?
1=not confident to 10=high confidence, 7+ responses

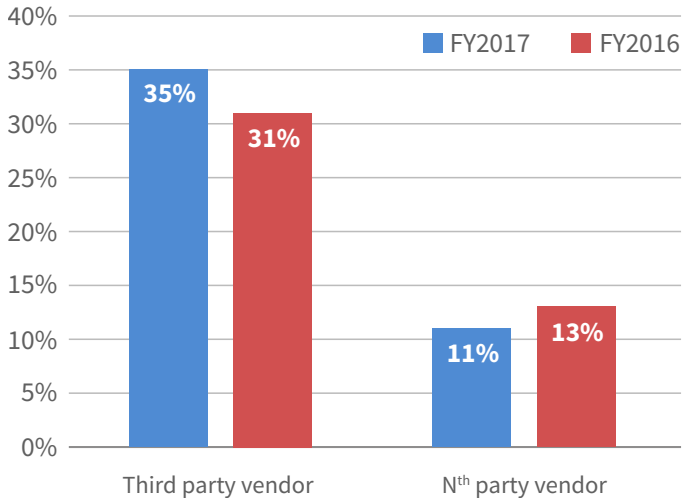
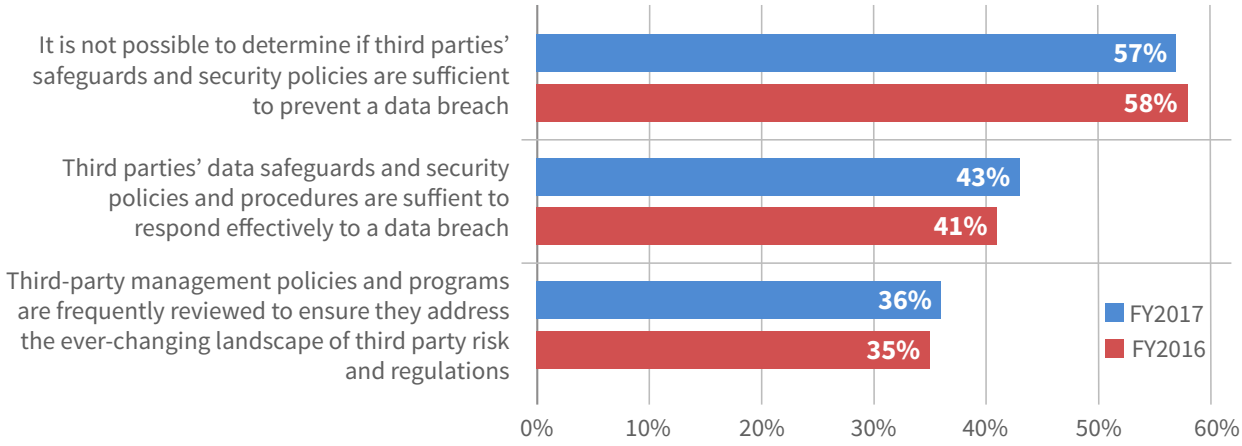


FIGURE 14
Perceptions about vendors' security policies and procedures
Strongly agree and Agree responses combined



Most companies do not determine an acceptable level of third-party risk. According to Figure 15, 54 percent of respondents say their organizations are not determining the acceptable level of security risk from third parties or are unsure. This is unchanged from last year.

While 55 percent of respondents say their vendor management program defines and ranks levels of risk, the indicators of risk applied are mostly operational and do not reveal potential problems related to the third parties' access and use of a company's sensitive or confidential information (as shown in Figure 15). Moreover, 58 percent of these respondents say risk levels are only updated as needed (38 percent) or never (20 percent), as shown in Figure 16. This is a slight decrease from 63 percent of respondents in last year's report (40 percent + 23 percent).

FIGURE 15
Our organization has determined the acceptable level of security risk from third parties

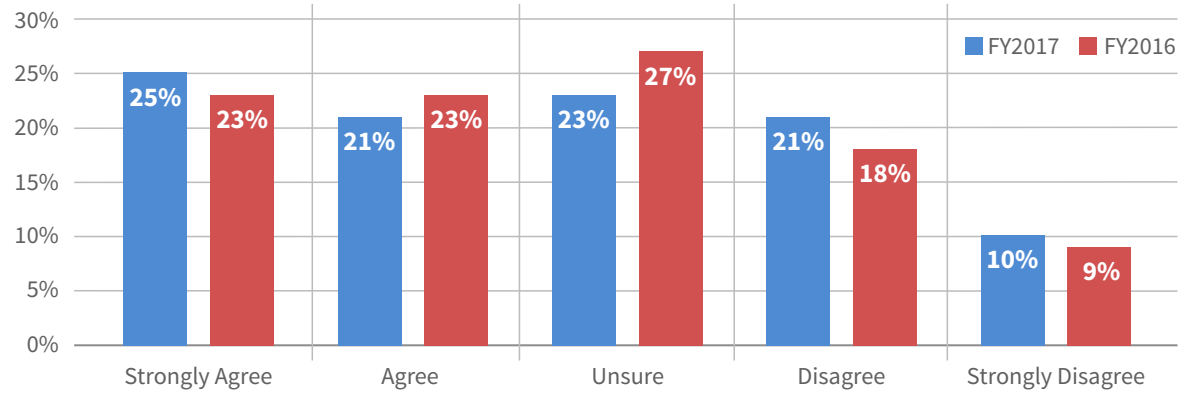
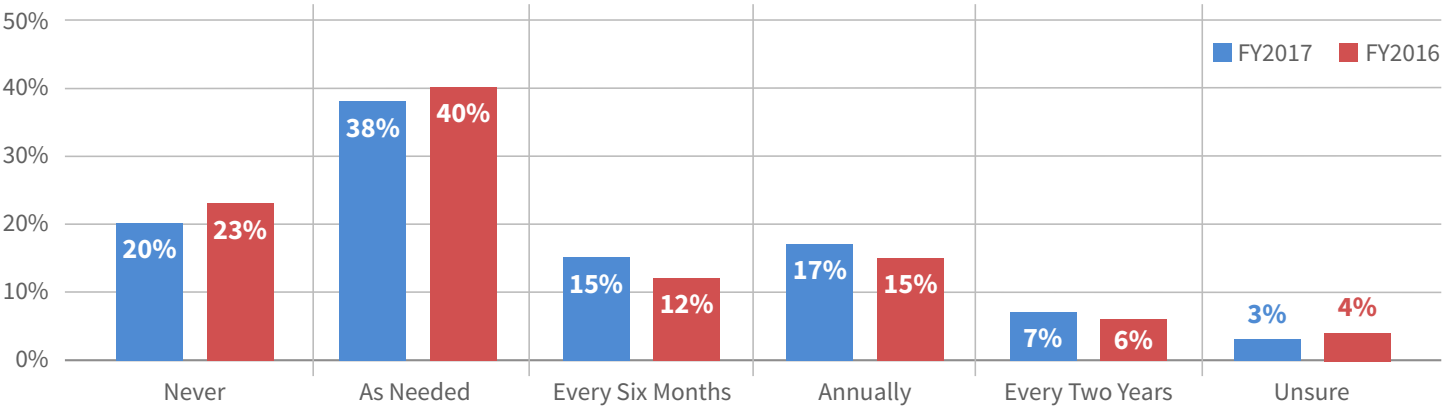


FIGURE 16
Third-party risk levels are rarely updated



If the third-party management program defines and ranks level of risks (55 percent of respondents), the most important indicator of risk continues to be, according to 76 percent of respondents, the overall decline in the quality of the third party's services and 71 percent say it is IT glitches, operational failures and stoppages, as shown in Figure 17. Less than half (48 percent of respondents) say a lack of screening or background checks for key personnel hired by the third party and only 23 percent of respondents say poorly written security and privacy policies and procedures are an indicator of risk.

Companies rely on contractual arrangements to evaluate third parties. Only 40 percent of respondents say that before starting a business relationship that requires the sharing of sensitive or confidential information their company evaluates the security and privacy practices of all vendors. Figure 18 shows why organizations *are not* performing evaluations.

As shown, the top two reasons are a lack of resources and the belief that the data shared with third parties is not considered sensitive or confidential (63 and 55 percent of respondents, respectively). Since last year's report, respondents say their companies are increasingly relying upon third parties need to comply with data protection regulations and the business reputation of the company (50 percent and 47 percent of respondents, respectively).

FIGURE 17
Indicators of third-party risk
More than one response permitted

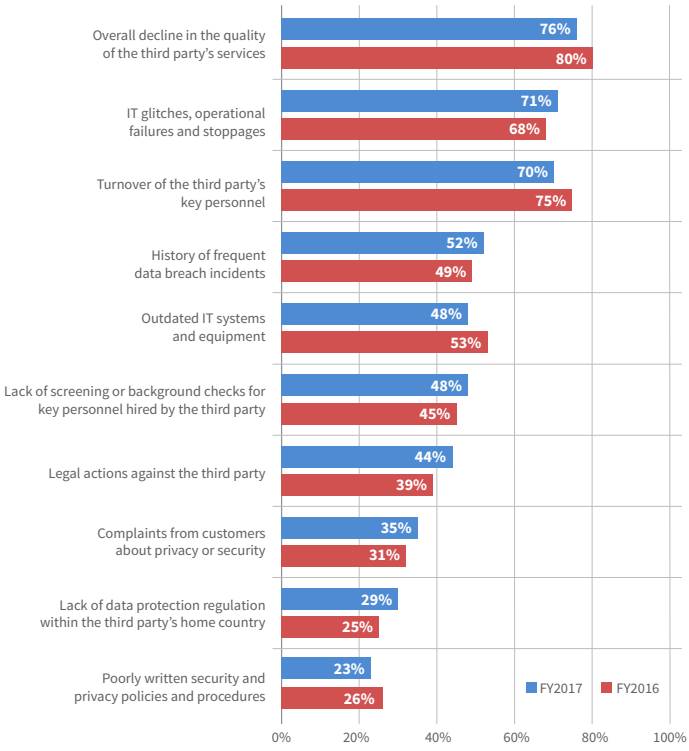
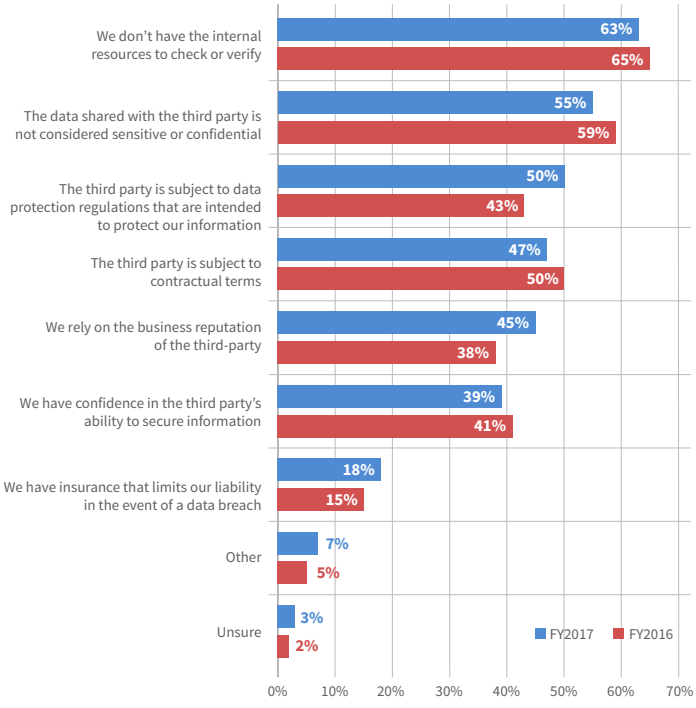


FIGURE 18
Reasons for not performing and evaluation
More than one response permitted



If they *do conduct* an evaluation (40 percent of respondents), it is mostly to acquire signatures on contracts that legally obligate the third party to adhere to security and privacy practices (62 percent of respondents) or they obtain references from other organizations that engage the third party (55 percent of respondents), as shown in Figure 19. Only 16 percent of respondents say they conduct an audit of the third party's security and privacy practices and only 14 percent of respondents say they obtain a self-assessment conducted by the third party.

Companies are not monitoring the privacy and security practices of third parties. Fif y-six percent of respondents say their companies *do not* monitor the security and privacy practices of vendors with whom they share sensitive or confidential information or they are unsure.

As shown in Figure 20, the primary reasons for not monitoring are: the third party does not allow the company to independently monitor or verify their security and privacy practices (62 percent of respondents) or they don't have the internal resources to check or verify (60 percent of respondents). More companies are relying upon insurance that limits their liability in the event of a data breach (an increase from 15 percent to 27 percent of respondents).

FIGURE 19
Steps taken to evaluate third parties
More than one response permitted

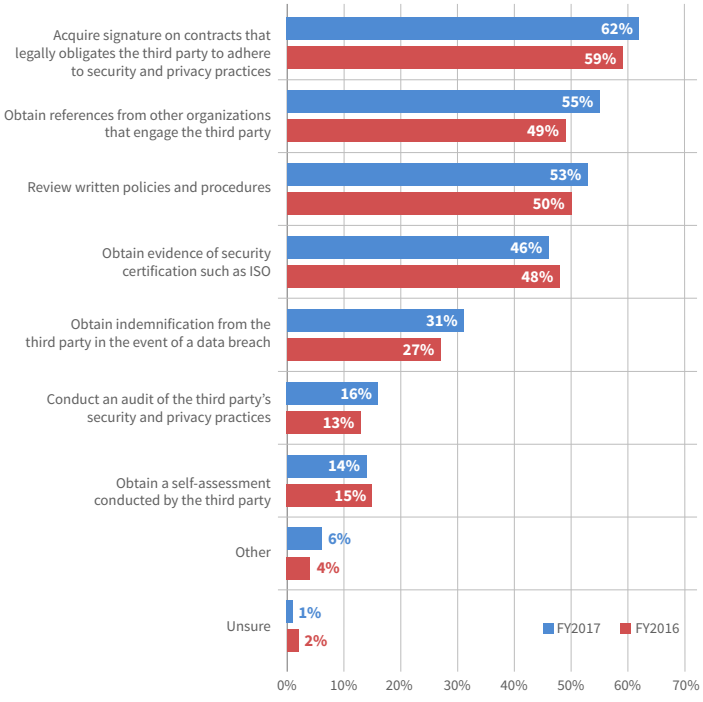
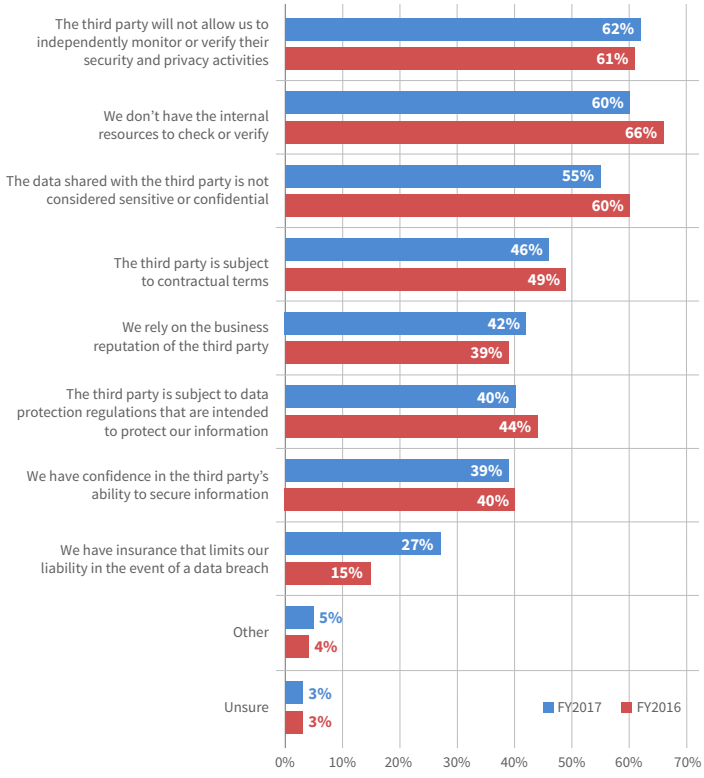


FIGURE 20
Reasons for not monitoring security and privacy practices
More than one response permitted



Forty-four percent of respondents say their companies monitor the security and privacy practices of third parties to ensure the adequacy of these practices. Figure 21 reveals that 67 percent of respondents say their companies rely upon legal or procurement review. Only 34 percent of respondents say they are conducting internal audits (or controlled self-assessments (25 percent of respondents).

The legal department continues to ensure appropriate privacy and security language is included in contracts. The departments most responsible for ensuring that privacy and security language is included in all contracts with third parties are: legal (36 percent of respondents), lines of business (21 percent of respondents), procurement (18 percent of respondents) and information security (14 percent of respondents), according to Figure 22.

FIGURE 21
Third-party monitoring procedures used to ensure the adequacy of security and privacy practices
More than one response permitted

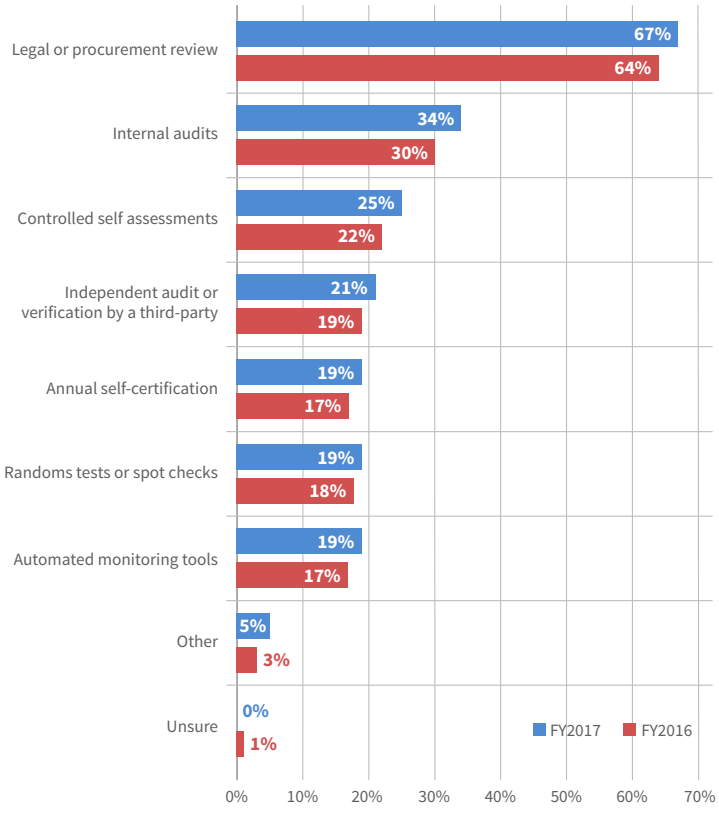
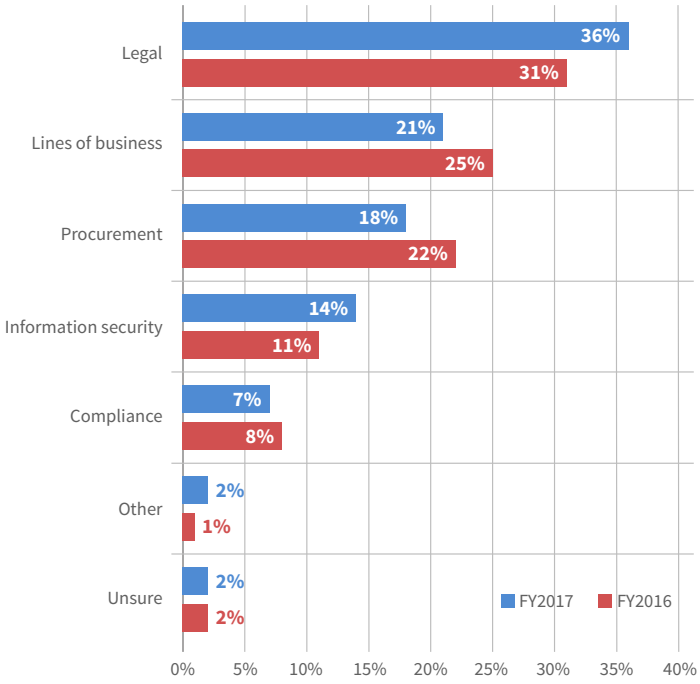


FIGURE 22
Which department or function is responsible for ensuring that appropriate privacy and security language is included in all third-party contracts?
More than one response permitted



Additionally, as shown in Figure 23, only 36 percent of respondents say their companies require third parties to indemnify and/or ensure compliance with their security and privacy practices.

Key factors impacting the likelihood of a data breach

To understand why certain companies represented in this study reduced the likelihood of a data breach, we did a cross tab analysis on eight third-party risk management practices and their influence on reducing the risk of a third-party data breach.

Figure 24 summarizes the relationship between these practices and the likelihood of data breach. As shown, the two most effective practices that when deployed reduce the likelihood of a breach are the evaluation of the security and privacy practices of third parties (46 percent likelihood of a data breach vs. 66 percent likelihood) and an inventory of all third parties with whom the organization shares information (46 percent likelihood of a data breach vs. 65 percent likelihood).

FIGURE 23
Does your company require third parties to indemnify and/or ensure compliance with your security and privacy practices?

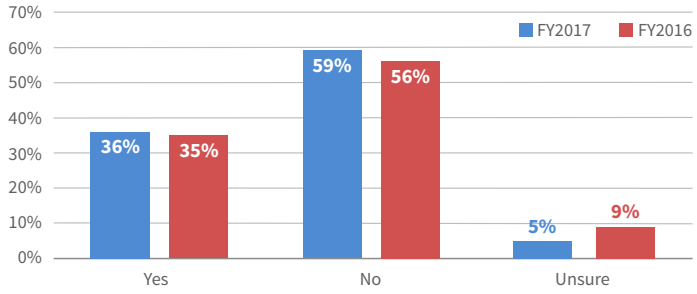
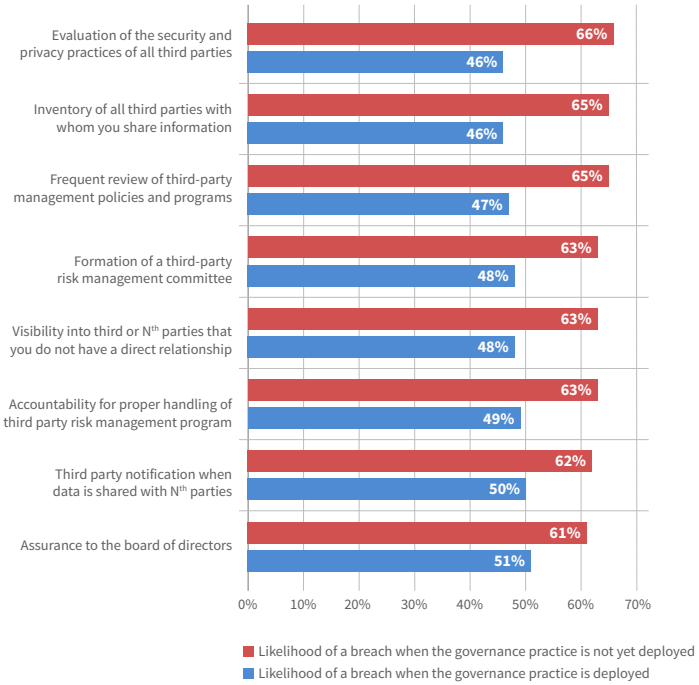


FIGURE 24
Impact of eight third-party risk management attributes on the likelihood of a data breach
Mean likelihood of data breach = 56 percent



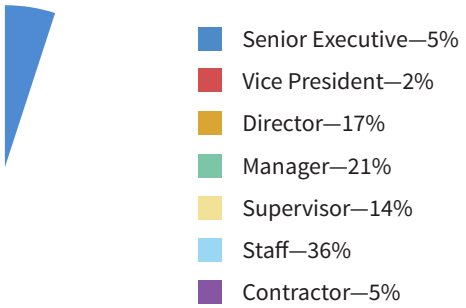
PART 4. METHODS

A sampling frame of 15,300 individuals located in the United States was selected as participants in this survey. To ensure knowledgeable responses, all respondents are familiar with their organization's approach to managing data risks created through outsourcing and are involved in managing the data risks created by outsourcing. Table 1 shows 701 total returns. Screening and reliability checks required the removal of 76 surveys. Our final sample consisted of 625 surveys or a 4.1 percent response.

Pie Chart 1 reports the respondents' organizational levels within the participating organizations. By design, more than half of the respondents (59 percent) are at or above the supervisory levels.

Table 1. Sample response	FY2017	FY2016
Sampling frame	15,300	15,480
Total returns	701	679
Rejected of screen surveys	76	81
Final sample	625	598
Response rate	4.1%	3.9%

PIE CHART 1
Current position within the organization

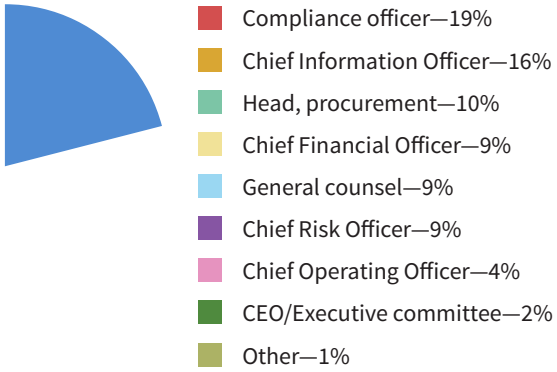


As shown in Pie Chart 2, 21 percent of respondents report to the CISO/CSO, 19 percent report to the compliance officer and 10 percent indicated they report to the head of procurement.

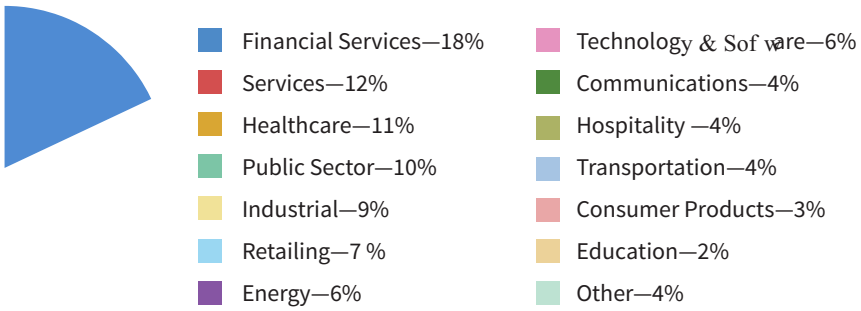
Pie Chart 3 reports the industry segments of respondents' organizations. This chart identifies financial services (18 percent) as the largest segment, followed by services (12 percent), healthcare (11 percent), and public sector (10 percent).

As shown in Pie Chart 4, 69 percent of respondents are from organizations with a global headcount of more than 1,000 employees.

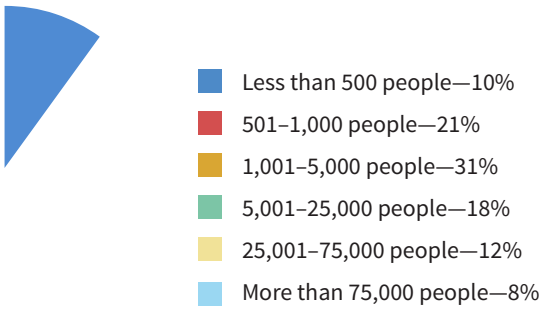
PIE CHART 2
Primary person you or your leader reports to



PIE CHART 3
Industry distribution of respondents' organizations



PIE CHART 4
Worldwide headcount of the organization



PART 5. 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 familiar with their organization's approach to managing data risks created through outsourcing and have involvement in managing the data risks created by outsourcing. 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 all survey questions contained in this study. All survey responses were captured in June 2017.

Survey response	FY2017	FY2016
Sampling frame	15,300	15,480
Total returns	701	679
Rejected or screened surveys	76	81
Final sample	625	598
Response rate	4.1%	3.9%

S1. How familiar are you with your organization's approach to managing data risks created through outsourcing?	FY2017	FY2016
Very familiar	35%	31%
Familiar	40%	41%
Somewhat familiar	25%	28%
No knowledge (Stop)	0%	0%
Total	100%	100%

S2. Does your company have a third-party data risk management program?	FY2017	FY2016
Yes	100%	100%
No (Stop)	0%	0%
Total	100%	100%

S3. Do you have any involvement in managing the data risks created by outsourcing?	FY2017	FY2016
Yes, full involvement	33%	29%
Yes, partial involvement	53%	56%
Yes, minimal involvement	14%	15%
No involvement (Stop)	0%	0%
Total	100%	100%

Part 1: Background

Q1a. Has your organization ever experienced a data breach caused by one of your third parties that resulted in the misuse of your company's sensitive or confidential information?	FY2017	FY2016
Yes	56%	49%
No	31%	35%
Unsure	13%	16%
Total	100%	100%

Q1b. Has your organization ever experienced a data breach caused by a cyber attack against one of your third parties that resulted in the misuse of your company's sensitive or confidential information?	FY2017	FY2016
Yes	42%	34%
No	36%	36%
Unsure	22%	30%
Total	100%	100%

Q1c. If yes to one or both of the questions above, did you make any changes to your company's third-party risk management program?	FY2017	FY2016
Yes	51%	45%
No	46%	50%
Unsure	3%	5%
Total	100%	100%

Q2a. How confident are you that your primary third party would notify you if it had a data breach involving your company's sensitive and confidential information? (1 = not confident to 10 = highly confident)	FY2017	FY2016
1 or 2	11%	12%
3 or 4	19%	25%
5 or 6	35%	32%
7 or 8	26%	21%
9 or 10	9%	10%
Total	100%	100%
Extrapolated value	5.56	5.34

Q2b. How confident are you that an Nth party would notify you or your primary third party if they had a data breach involving your company's sensitive and confidential information? (1 = not confident to 10 = highly confident)	FY2017	FY2016
1 or 2	35%	33%
3 or 4	39%	40%
5 or 6	15%	14%
7 or 8	7%	8%
9 or 10	4%	5%
Total	100%	100%
Extrapolated value	3.62	3.74

Q3. Who is **most accountable** for the correct handling of your organization's third-party risk management program?	FY2017	FY2016
General counsel/compliance Officer	13%	12%
Chief technology officer (CTO)	2%	3%
Chief information officer (CIO)	15%	13%
Chief information security officer (CISO)	13%	13%
Chief security officer (CSO)	5%	6%
Head of business continuity management	4%	1%
Chief privacy officer (CPO)	0%	1%
Head of human resources	0%	0%
Head of procurement	16%	19%
Chief risk officer (CRO)	13%	9%
No one person/department is accountable	16%	21%
Unsure	3%	2%
Total	100%	100%

Q4. Do third parties notify your organization when your data is shared with the Nth parties?	FY2017	FY2016
Yes	31%	33%
No	63%	60%
Unsure	6%	7%
Total	100%	100%

Q5. Does your organization have a third-party risk management committee?	FY2017	FY2016
Yes	46%	48%
No	51%	50%
Unsure	3%	2%
Total	100%	100%

Q6. Which department/function is responsible for ensuring appropriate privacy and security language is included in all contracts with third parties?	FY2017	FY2016
Legal	36%	31%
Procurement	18%	22%
Compliance	7%	8%
Information security	14%	11%
Lines of business	21%	25%
None of the above	0%	0%
Other (please specify)	2%	1%
Unsure	2%	2%
Total	100%	100%

Q7a. Does your company have a comprehensive inventory of all third parties with whom it shares sensitive and confidential information?	FY2017	FY2016
Yes (Proceed to Q8.)	35%	33%
No (Proceed to Q10.)	57%	60%
Unsure (Proceed to Q10.)	8%	7%
Total	100%	100%

Q7b. If no or unsure, why? Please check all that apply	FY2017	FY2016
Lack of resources to track third parties	48%	44%
No centralized control over third-party relationships	69%	63%
Complexity in third-party relationships	46%	41%
Cannot keep track due to frequent turnover in third parties	34%	37%
Not a priority	48%	50%
Total	245%	235%

Q8. How many third parties are in this inventory?	FY2017	FY2016
Less than 10	0%	0%
11 to 20	0%	1%
21 to 30	1%	2%
31 to 40	6%	8%
41 to 50	9%	11%
51 to 75	16%	19%
76 to 100	11%	12%
101 to 300	9%	8%
301 to 500	8%	7%
501 to 1,000	19%	18%
More than 1,000	21%	14%
Unsure	0%	0%
Total	100%	100%
Extrapolated value	471	378

Q9a. Does the inventory include all third parties (i.e. Nth party risk) your company has a relationship with that might have access to your company's sensitive and confidential data?	FY2017	FY2016
Yes	16%	18%
No	80%	77%
Unsure	4%	5%
Total	100%	100%

Q9b. What percentage of these third parties (i.e., Nth party risk) do you believe have access to your sensitive and confidential information?	FY2017
None	5%
Less than 10%	17%
11% to 20%	31%
21% to 50%	25%
51% to 75%	16%
More than 76%	6%
Unsure	0%
Total	100%
Extrapolated value	30%

Q10. What percentage of all third parties do you believe are outsourcing your sensitive and confidential data to Nth parties?	FY2017	FY2016
None	2%	0%
Less than 10%	3%	5%
11% to 20%	20%	26%
21% to 50%	41%	45%
51% to 75%	29%	18%
More than 76%	5%	6%
Unsure	0%	0%
Total	100%	100%
Extrapolated value	40%	37%

Q11a. Do you have visibility into third parties your company does not have a direct relationship with but that access your company's sensitive and confidential information (Nth parties)?	FY2017	FY2016
Yes	18%	20%
No	70%	71%
Unsure	12%	9%
Total	100%	100%

Q11b. If yes, how do you achieve visibility? Please check all that apply.	FY2017	FY2016
Monitoring third-party data handling practices with Nth parties	23%	26%
Audits and assessments of third-party data handling practices	21%	17%
Reliance upon the third party to notify our organization when our data is shared with their Nth parties	59%	55%
Reliance upon contractual agreements	67%	61%
Use of technologies	20%	23%
Other (please specify)	3%	2%
Total	193%	184%

Q12a. Using the following 10-point scale, please rate how effective your organization is in **mitigating** third-party risks. (1 = not effective to 10 = highly effective)	FY2017	FY2016
1 or 2	13%	12%
3 or 4	17%	21%
5 or 6	53%	45%
7 or 8	13%	17%
9 or 10	4%	5%
Total	100%	100%
Extrapolated value	5.06	5.14

Q12b. Using the following 10-point scale, please rate how effective your organization is in **mitigating** Nth-party risks. (1 = not effective to 10 = highly effective)	FY2017	FY2016
1 or 2	27%	27%
3 or 4	46%	42%
5 or 6	15%	19%
7 or 8	9%	8%
9 or 10	3%	4%
Total	100%	100%
Extrapolated value	3.80	3.90
Q13a. Using the following 10-point scale, please rate how effective your organization is in **detecting** third-party risks. (1 = not effective to 10 = highly effective)	FY2017	FY2016
1 or 2	13%	15%
3 or 4	19%	23%
5 or 6	26%	27%
7 or 8	28%	23%
9 or 10	14%	12%
Total	100%	100%
Extrapolated value	5.72	5.38

Q13b. Using the following 10-point scale, please rate how effective your organization is in **detecting** Nth-party risks. (1 = not effective to 10 = highly effective)	FY2017	FY2016
1 or 2	38%	40%
3 or 4	41%	43%
5 or 6	9%	7%
7 or 8	8%	7%
9 or 10	4%	3%
Total	100%	100%
Extrapolated value	3.48	3.30

Q14a. Using the following 10-point scale, please rate your organization's effectiveness in **minimizing** third-party risks. (1 = not effective to 10 = highly effective)	FY2017	FY2016
1 or 2	9%	11%
3 or 4	23%	20%
5 or 6	42%	46%
7 or 8	19%	18%
9 or 10	7%	5%
Total	100%	100%
Extrapolated value	5.34	5.22

Q14b. Using the following 10-point scale, please rate your organization's effectiveness in **minimizing** Nth-party risks. (1 = not effective to 10 = highly effective)	FY2017	FY2016
1 or 2	33%	29%
3 or 4	38%	41%
5 or 6	17%	18%
7 or 8	8%	9%
9 or 10	4%	3%
Total	100%	100%
Extrapolated value	3.74	3.82

Q15. Using the following 10-point scale, please rate the effectiveness of your organization's third party risk management program. (1 = not effective to 10 = highly effective)	FY2017	FY2016
1 or 2	16%	19%
3 or 4	11%	12%
5 or 6	40%	38%
7 or 8	26%	23%
9 or 10	7%	8%
Total	100%	100%
Extrapolated value	5.44	5.28

Part 2. Attributions

Q16. Managing outsourced relationship risk is a priority in our organization.	FY2017	FY2016
Strongly agree	23%	21%
Agree	21%	22%
Unsure	26%	26%
Disagree	21%	23%
Strongly disagree	9%	8%
Total	100%	100%

Q17. Our organization allocates sufficient resources to managing outsourced relationships.	FY2017	FY2016
Strongly agree	19%	17%
Agree	21%	18%
Unsure	22%	23%
Disagree	26%	29%
Strongly disagree	12%	13%
Total	100%	100%

Q18. Our organization has determined the acceptable level of security risk from our third parties in order to meet our business objectives.	FY2017	FY2016
Strongly agree	25%	23%
Agree	21%	23%
Unsure	23%	27%
Disagree	21%	18%
Strongly disagree	10%	9%
Total	100%	100%

Q19. Our board of directors requires assurances that third-party risk is being assessed, managed and monitored appropriately.	FY2017	FY2016
Strongly agree	18%	15%
Agree	24%	23%
Unsure	28%	30%
Disagree	21%	24%
Strongly disagree	9%	8%
Total	100%	100%

Q20. The number of cyber security incidents involving third parties is increasing.	FY2017	FY2016
Strongly agree	36%	33%
Agree	39%	40%
Unsure	15%	17%
Disagree	9%	8%
Strongly disagree	1%	2%
Total	100%	100%

Q21. The number of cyber security incidents involving third parties is difficult to manage.	FY2017	FY2016
Strongly agree	32%	35%
Agree	33%	30%
Unsure	18%	20%
Disagree	13%	12%
Strongly disagree	4%	3%
Total	100%	100%

Q22. Our third parties' data safeguards and security policies and procedures are sufficient to respond effectively to a data breach.	FY2017	FY2016
Strongly agree	18%	21%
Agree	25%	20%
Unsure	29%	33%
Disagree	22%	19%
Strongly disagree	6%	7%
Total	100%	100%

Q23. It is not possible to determine if third parties' safeguards and security policies are sufficient to prevent a data breach.	FY2017	FY2016
Strongly agree	27%	25%
Agree	30%	33%
Unsure	22%	19%
Disagree	15%	18%
Strongly disagree	6%	5%
Total	100%	100%

Q24. Our third-party management policies and programs are frequently reviewed to ensure they address the ever-changing landscape of third party risk and regulations.	FY2017	FY2016
Strongly agree	15%	17%
Agree	21%	18%
Unsure	26%	25%
Disagree	22%	26%
Strongly disagree	16%	14%
Total	100%	100%

Part 3. Secure outsourcing management

Q25a. Do you evaluate the security and privacy practices of all third parties (i.e. from third to Nth third parties) before you engage them in a business relationship that requires the sharing of sensitive or confidential information?	FY2017	FY2016
Yes	40%	38%
No	56%	54%
Unsure	4%	8%
Total	100%	100%

Q25b. If yes, how do you perform this evaluation? Please check all that apply.	FY2017	FY2016
Review written policies and procedures	53%	50%
Acquire signature on contracts that legally obligates the third party to adhere to security and privacy practices	62%	59%
Obtain indemnification from the third party in the event of a data breach	31%	27%
Conduct an audit of the third party's security and privacy practices	16%	13%
Obtain a self-assessment conducted by the third party	14%	15%
Obtain references from other organizations that engage the third party	55%	49%
Obtain evidence of security certification such as ISO	46%	48%
Other (please specify)	6%	4%
Unsure	1%	2%
Total	284%	267%

Q25c. If no, why don't you perform an evaluation? Please check all that apply.	FY2017	FY2016
We don't have the internal resources to check or verify	63%	65%
We have confidence in the third party's ability to secure information	39%	41%
We rely on the business reputation of the third-party	45%	38%
We have insurance that limits our liability in the event of a data breach	18%	15%
The third party is subject to data protection regulations that are intended to protect our information	50%	43%
The third party is subject to contractual terms	47%	50%
The data shared with the third party is not considered sensitive or confidential	55%	59%
Other	7%	5%
Unsure	3%	2%
Total	327%	318%

Q26a. Do you monitor the security and privacy practices of third parties that you share sensitive or confidential consumer information on an ongoing basis?	FY2017	FY2016
Yes	44%	40%
No	49%	52%
Unsure	7%	8%
Total	100%	100%

Q26b. If yes, what monitoring procedures does your organization employ to ensure the adequacy of security and privacy practices? Please check all that apply.	FY2017	FY2016
Legal or procurement review	67%	64%
Internal audits	34%	30%
Independent audit or verification by a third-party	21%	19%
Automated monitoring tools	19%	17%
Controlled self assessments	25%	22%
Random tests or spot checks	19%	18%
Annual self-certification	19%	17%
Other	5%	3%
Unsure	0%	1%
Total	209%	191%

Q26c. If no, why doesn't your organization monitor the third parties' security and privacy practices? Please check all that apply.	FY2017	FY2016
We don't have the internal resources to check or verify	60%	66%
We have confidence in the third party's ability to secure information	39%	40%
We rely on the business reputation of the third party	42%	39%
We have insurance that limits our liability in the event of a data breach	27%	15%
The third party is subject to data protection regulations that are intended to protect our information	40%	44%
The third party is subject to contractual terms	46%	49%
The data shared with the third party is not considered sensitive or confidential	55%	60%
The third party will not allow us to independently monitor or verify their security and privacy activities	62%	61%
Other	5%	4%
Unsure	3%	3%
Total	379%	381%

Q27a. Does your third-party management program define and rank levels of risk?	FY2017	FY2016
Yes	55%	52%
No	40%	43%
Unsure	5%	5%
Total	100%	100%

Q27b. If yes, what are indicators of risk? Please check all that apply.	FY2017	FY2016
Failed IT security audits, verification or testing procedures	12%	16%
Overall decline in the quality of the third party's services	76%	80%
Discovery that the third party is using a subcontractor that has access to our company's information	13%	16%
Complaints from customers about privacy or security	35%	31%
History of frequent data breach incidents	52%	49%
Legal actions against the third party	44%	39%
Negative media about the third party	16%	20%
IT glitches, operational failures and stoppages	71%	68%
Poorly written security and privacy policies and procedures	23%	26%
Lack of security or privacy training for the third party's key personnel	12%	15%
Lack of screening or background checks for key personnel hired by the third party	48%	45%
High rate of identity fraud, theft or other cyber crimes within the third party's home country	11%	14%
Lack of data protection regulation within the third party's home country	29%	25%
Turnover of the third party's key personnel	70%	75%
Outdated IT systems and equipment	48%	53%
Other	4%	5%
Total	564%	577%

Q27c. If yes, how often are the risk levels updated?	FY2017	FY2016
Never	20%	23%
As needed	38%	40%
Every six months	15%	12%
Annually	17%	15%
Every two years	7%	6%
Unsure	3%	4%
Total	100%	100%

Q28a. Does your company regularly report to the board of directors on the effectiveness of the third-party management program and potential risks to the organization?	FY2017	FY2016
Yes	33%	31%
No	53%	57%
Unsure	14%	12%
Total	100%	100%

Q28b. If no, why?	FY2017	FY2016
Not a priority for the board	38%	45%
Decisions about the third-party risk management program are not relevant to board members	45%	51%
We only provide this information if a security incident or data breach has occurred involving a third party	34%	39%
Unsure	9%	11%
Total	126%	146%

Q29. Does your company require third parties to indemnify and/or ensure compliance with your security and privacy practices?	FY2017	FY2016
Yes	36%	35%
No	59%	56%
Unsure	5%	9%
Total	100%	100%

Part 4. Demographics and organizational characteristics

D1. What organizational level best describes your current position?	FY2017	FY2016
Senior Executive	5%	4%
Vice President	2%	3%
Director	17%	16%
Manager	21%	23%
Supervisor	14%	15%
Staff	36%	35%
Contractor	5%	4%
Other	0%	0%
Total	100%	100%

D2. Check the **Primary Person** you report to within the organization.	FY2017	FY2016
CEO/executive committee	2%	3%
Chief financial officer	9%	9%
General counsel	9%	7%
Chief privacy officer	0%	
Chief information officer	16%	15%
Compliance officer	19%	21%
Human Resources VP	0%	
CISO/CSO	21%	17%
Chief risk officer	9%	9%
Other	1%	2%
Chief operating officer	4%	6%
Head, procurement	10%	11%
Total	100%	100%

D3. What industry best describes your organization's industry focus?	FY2017	FY2016
Financial services	18%	19%
Services	12%	10%
Healthcare	11%	12%
Public sector	10%	11%
Industrial	9%	8%
Retailing	7%	9%
Energy	6%	5%
Technology & software	6%	7%
Communications	4%	3%
Hospitality	4%	3%
Transportation	4%	3%
Consumer products	3%	3%
Education	2%	2%
Other	2%	1%
Aerospace & defense	1%	1%
Entertainment & media	1%	2%
Agriculture & food services	0%	1%
Total	100%	100%

D4. What is the worldwide headcount of your organization?	FY2017	FY2016
Less than 500 people	10%	11%
501 to 1,000 people	21%	19%
1,001 to 5,000 people	31%	32%
5,001 to 25,000 people	18%	19%
25,001 to 75,000 people	12%	11%
More than 75,000 people	8%	8%
Total	100%	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.

As a member of the Council of American Survey Research Organizations (CASRO), we uphold strict data confidentiality, privacy and ethical research standard. 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.

ABOUT OPUS

Free your business

Opus is a leading SaaS provider of Risk and Compliance solutions. We were founded on a simple premise: that faster, better decisions in compliance and risk management give businesses an extraordinary advantage in the marketplace.

Our mission is to free your business from the complexity and uncertainty of managing customer, supplier and third-party risks. We combine the most innovative SaaS platforms with unparalleled data solutions, helping turn information into action so your business can thrive.