Data Risk in the Third-Party Ecosystem: Third Annual Study

Sponsored by Opus

Independently conducted by Ponemon Institute LLC

Publication Date: November 2018

Ponemon INSTITUTE

Data Risk in the Third-Party Ecosystem: Third Annual Study

Ponemon INSTITUTE

Data Risk in the Third-Party Ecosystem: Third Annual Study

Ponemon Institute, November 2018

Part 1. Introduction

We are pleased to present the findings of *Data Risk in the Third-Party Ecosystem: Third Annual Study*, sponsored by Opus, to understand the challenges companies face in protecting sensitive and confidential information shared with third parties and their third parties (Nth party risk). The mitigation of third-party risk has become even more important because of the EU's General Data Protection Regulation that went into effect May 25, 2018 and the California Privacy Act.

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.

The results of the study are based on a survey of more than 1,000 IT and IT security practitioners in the US and UK who are directly familiar with their organizations' approach to managing data risks created through outsourcing and who are involved in managing these risks. Unless otherwise noted, the report presents the combined the US and UK findings.

Following are key takeaways from the research.

Most companies are having data breaches involving third parties, but many go undetected.

- Fifty-nine percent of respondents confirm that their organizations experienced a data breach caused by one of their third parties and 42 percent of respondents say they had such a data breach in the past 12 months. Additionally, 22 percent of respondents don't know if they had a third-party data breach in the past 12 months.

- The occurrence of a third-party data breach is even higher in the US organizations represented in this research. Sixty-one percent of US respondents confirm that their organizations experienced a data breach caused by one of their third parties, an increase from 56 percent of respondents in 2017 and 49 percent of respondents in 2016.

- Only 29 percent of respondents say a third party would contact them about the data breach. A very small percentage (12 percent) are confident they would learn that their sensitive data was lost or stolen by an Nth vendor.

Despite the risk, the management of outsourced relationships is not a priority.

- Seventy-six percent of respondents say the number of cybersecurity incidents involving vendors is increasing, but only 46 percent of respondents say managing outsourced relationship risks is a priority.

- Only 37 percent of respondents say they have sufficient resources to manage third-party relationships.

- Only 39 percent of respondents say their companies regularly report to the boards of directors on the effectiveness of their organizations third-party management program and potential risks.

- Only 35 percent of respondents rate their third-party risk management program as highly effective, and 57 percent of respondents do not know if their organizations' vendor safeguards are sufficient to prevent a breach.

A lack of visibility causes organizations to lose control over the ability to protect their information assets once they are shared with third parties.

- Only 34 percent of respondents say they have a comprehensive inventory of all their third parties.
- Sixty-nine percent of respondents cite a lack of centralized control over the management of third-party relationships as to why they do not have such an inventory.
- Almost half of respondents (48 percent) say complexity in third-party relationships is a barrier to creating a comprehensive inventory of all third parties.
- Only 15 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.

Third-party security practices and policies are rarely assessed to ensure they are effective.

- Only 42 percent of respondents say their organizations are frequently reviewing the policies and programs of their third parties to ensure they address the ever-changing landscape of third-party risk and regulations.
- Moreover, 54 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.

Part 2. Best Practices in Third-Party Risk Management Governance

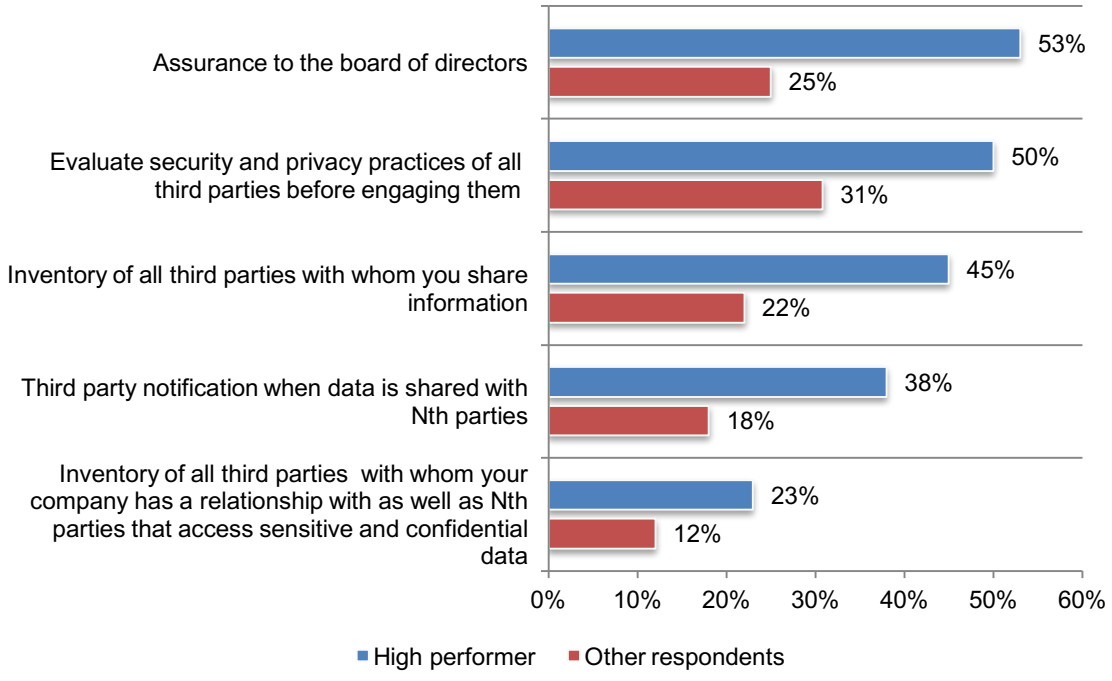
As part of this study, we conducted a special analysis of those organizations that have been able to avoid a third-party data breach in the past 12 months (36 percent) or ever (32 percent). We refer to these as high-performing organizations and compare them to those respondents who report their organization had a data breach caused by a third party in the past 12 months (42 percent) or ever (59 percent).

Figure 1 presents the differences in "Yes" responses between high performing and other respondents in their organizations' adoption of specific governance practices that can reduce the risk of a third party. As shown in the figure, 53 percent of high-performing organizations say their organizations establish good communication practices with the board of directors by regularly reporting on steps taken to protect sensitive and confidential information assets from a third-party data breach. Only 25 percent of respondents in other organizations say they are providing such assurance to the board.

Following are the other governance practices more likely to be implemented by high-performing organizations that illustrate why they have been successful in avoiding a third-party data breach.

- Evaluation of security and privacy practices of all third parties before engaging them
- Establishment of an inventory of third parties with whom the organization shares information
- Ensure third parties provide notification when data is shared with Nth parties
- Inventory all third parties and Nth parties with whom there is a relationship

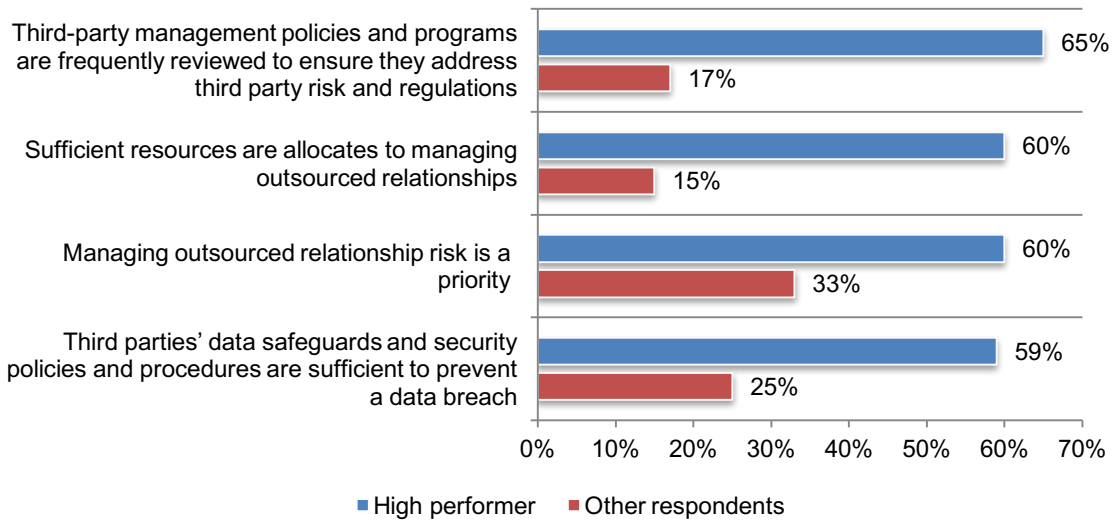
Figure 1. Differences in governance practices in high-performing organizations and the overall sample of organizations
Yes responses



In high performing organizations, third-party governance is a priority with sufficient resources allocated. Figure 2 presents other governance practices that respondents in high performing organizations **strongly agree or agree** are being implemented. In every case, high performing organizations are more mature in the management of outsourced relationships.

These include the frequent review of third-party management policies and programs to ensure they address third-party risk and regulations and are sufficient to prevent a data breach. To accomplish these governance practices, high performing organizations have sufficient resources to manage outsourced relationships.

Figure 2. Differences in other governance practices
Strongly agree and Agree responses combined



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 (50 percent of high-performing organizations vs. 31 percent of other organizations).

2. **An 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 (45 percent of high-performing organizations vs 22 percent of other organizations).

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 (65 percent of high-performing organizations vs. 17 percent of other organizations.

4. **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 (38 percent of high-performing organizations vs. 18 percent of other organizations).

5. **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 (53 percent of high-performing organizations vs. 25 percent of other organizations).

Other recommendations include the following.

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

7. **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

8. **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.

Part 3. Key Findings

In this study, we surveyed 1,038 individuals across multiple industries in the United States and, for the first time, the United Kingdom who are familiar with their organizations' approach to managing data risks created through outsourcing. All organizations represented in this study have a third-party data risk management program.

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:

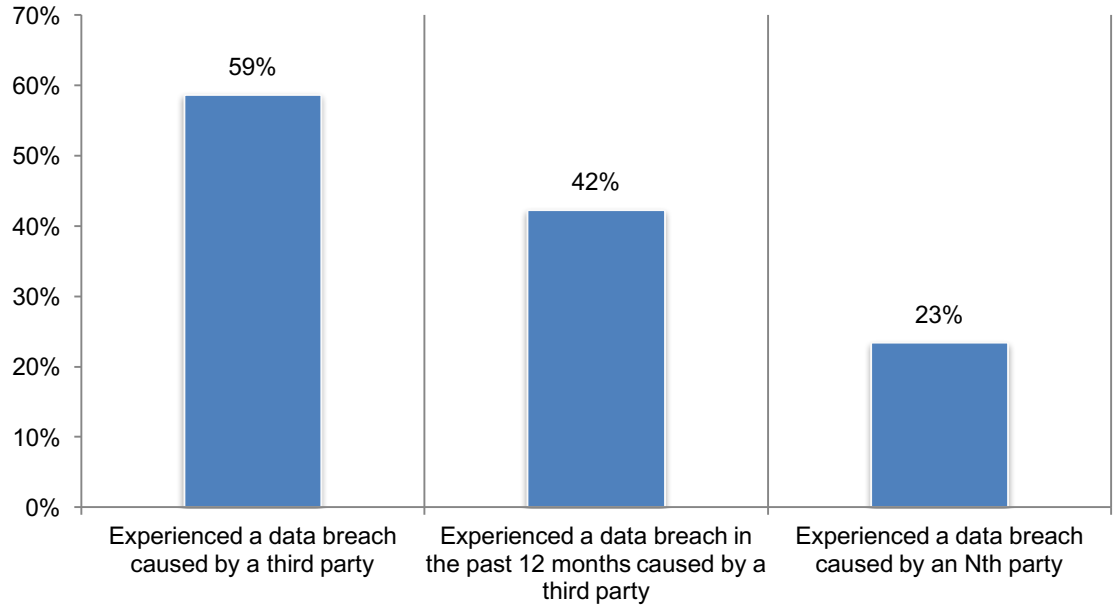
- Data breaches and the associated third-party data risk
- Strategic shortfalls in third-party risk management governance
- Lack of visibility into third and Nth party relationships
- The realities of today's third-party risk management programs

Data breaches and the associated third-party data risk

Most companies are having data breaches involving third parties. This year, 59 percent of respondents confirm that their organizations experienced a data breach caused by one of their vendors and 23 percent of respondent say their organizations experienced a breach caused by one of their Nth parties, as shown in Figure 3.

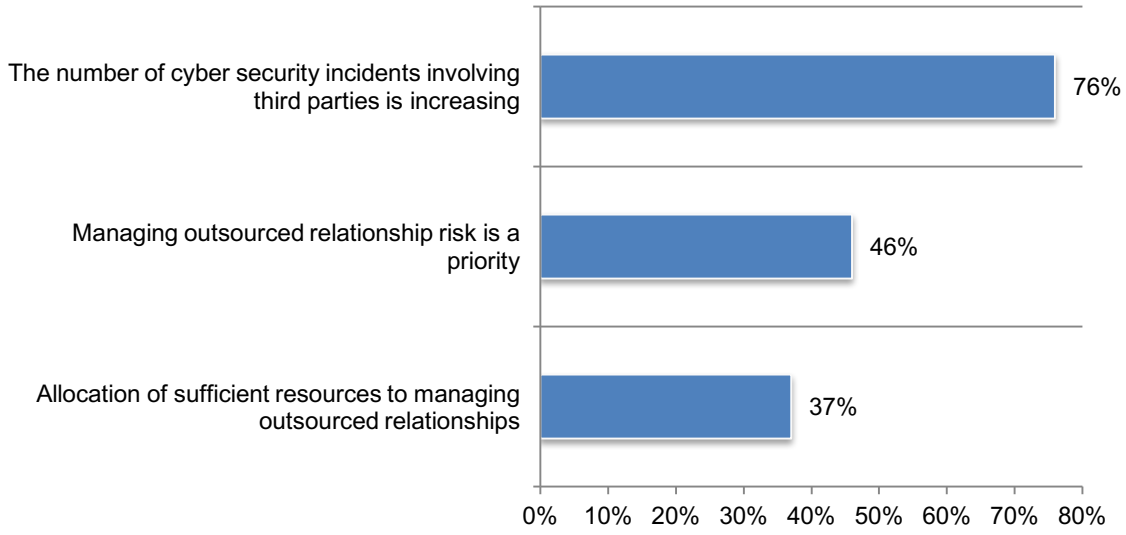
In the past 12 months, 42 percent of respondents say their organizations had such a data breach. Fifty-three percent of respondents say the occurrence of the breach encouraged them to make changes to their third-party risk management program.

Figure 3. Has your organization experienced a data breach or cyber attack caused by a third party?
Yes responses reported



In many organizations, managing outsourced relationship risk is not a priority. As shown in Figure 4, 76 percent of respondents say the number of cybersecurity incidents involving vendors is increasing. However, only 46 percent of respondents say managing outsourced relationship risks is a priority. Further, only 37 percent of respondents say they have sufficient resources to managing these relationships.

Figure 4. Cybersecurity incidents are increasing and difficult to manage
Strongly agree and Agree responses combined



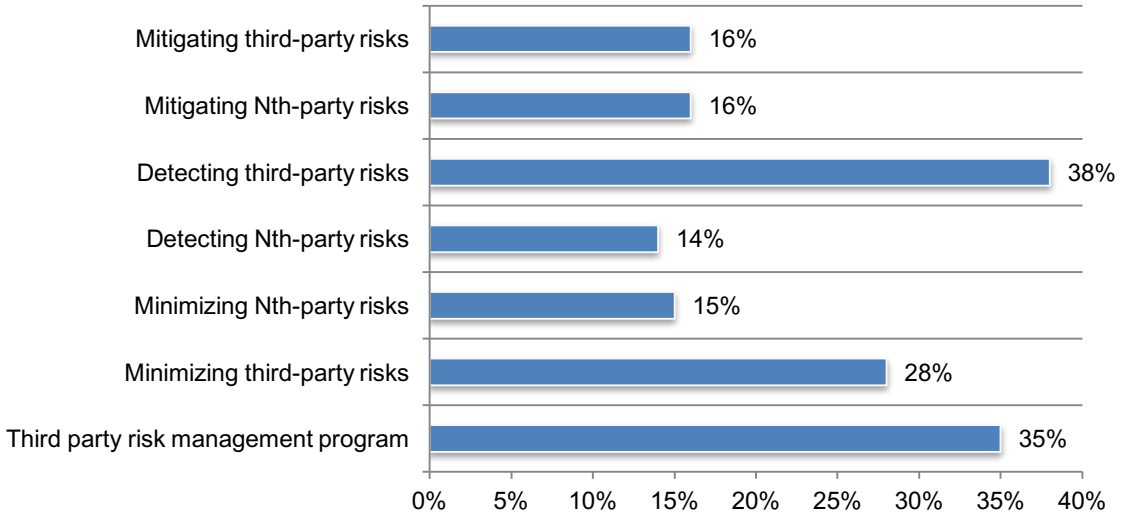
Strategic shortfalls in third-party risk management governance

Third-party risk management programs are failing to effectively mitigate, detect and minimize third-party risks. We asked respondents to rate their organization's effectiveness in dealing with third party and Nth party risks from a scale of 1 = not effective to 10 = highly effective. Figure 5 presents the highly effective responses (7 + on a scale of 1 = not effective to 10 = highly effective).

Both third-party and Nth-party risks are equally difficult to mitigate. Only 16 percent of respondents say their organizations are highly effective in mitigating third-party risks or in mitigating Nth-party risks. More respondents believe their organizations are highly effective in detecting third-party risks (38 percent) but not in detecting Nth-party risks (only 14 percent).

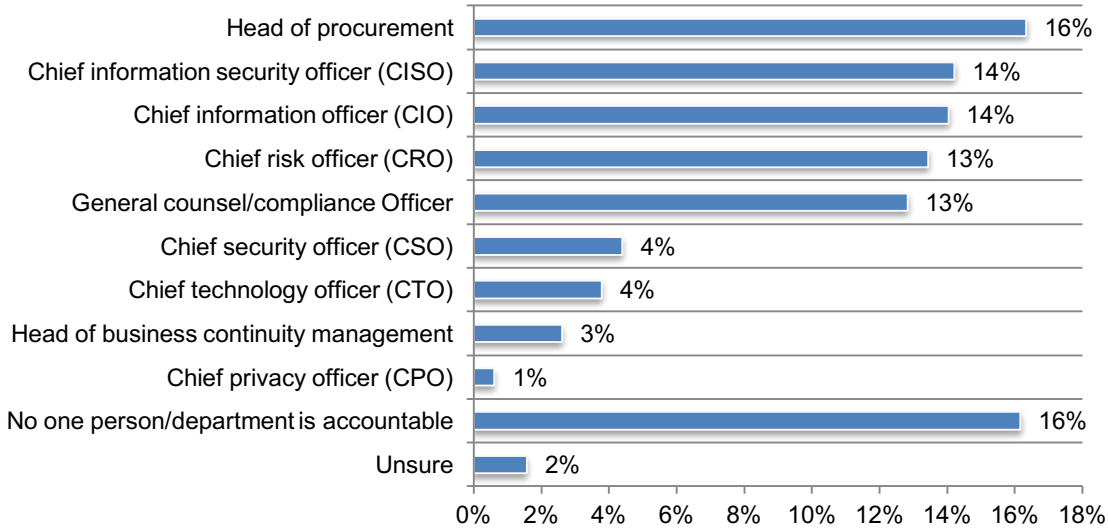
Most organizations are not effective in minimizing third party or Nth party risks, 28 percent and 15 percent of respondents. It is not surprising, therefore, that only 35 percent of respondents rate their organization's third-party risk management program as highly effective.

Figure 5. How effective are organizations in dealing with third party and Nth party risks?
1 = not effective to 10 = highly effective, 7 + responses reported



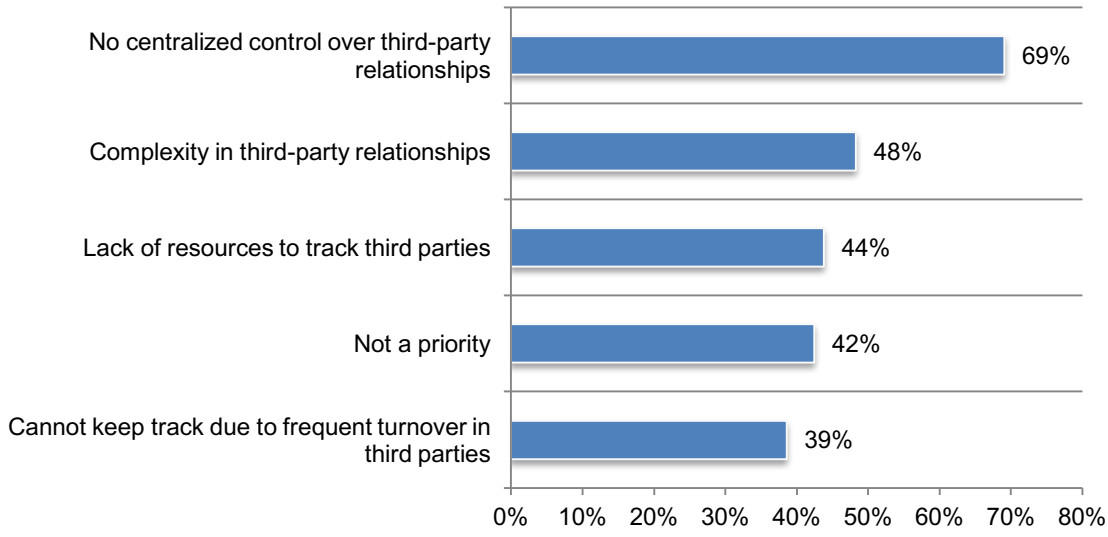
Accountability for the third-party risk management program is dispersed throughout the organization. As shown in Figure 6, most accountability (37 percent of respondents) seems to rest with the IT and IT security function: CIO (14 percent of respondents) + CISO (14 percent) + CSO (5 percent) + CTO (4 percent).

Figure 6. Who is most accountable for the correct handling of the organization's third-party risk management program?



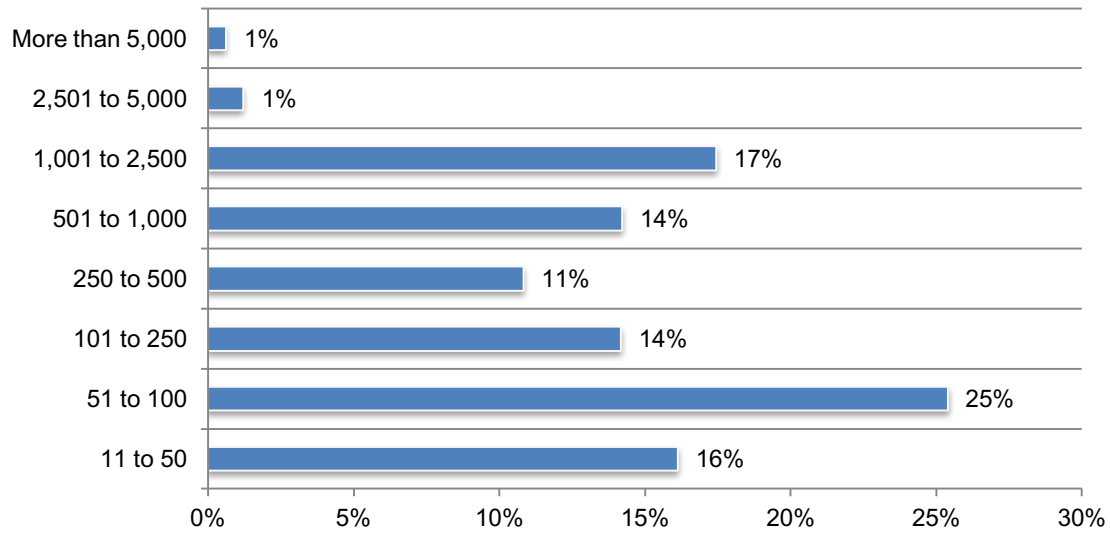
Because accountability for the third-party risk management program is not centralized within one function, it can create a barrier to having a comprehensive inventory of all third parties. Only 34 percent of respondents say they have a comprehensive inventory of all their third parties. Of these respondents, 69 percent of respondents cite a lack of centralized control over third-party relationships as to why they do not have such an inventory. Almost half of respondents (48 percent) say complexity in third-party relationships is a barrier, as shown in Figure 7.

Figure 7. Reasons companies do not have a comprehensive inventory of all third parties
More than one response permitted



Few companies are able to maintain a comprehensive inventory of all third parties with whom they share information. in Figure 8, of the 34 percent of respondents who say their organizations have a comprehensive inventory of all third parties with whom it shares sensitive and confidential information, 58 percent say the inventory contains more than 100 third parties. On average, respondents report this inventory has 583 third parties.

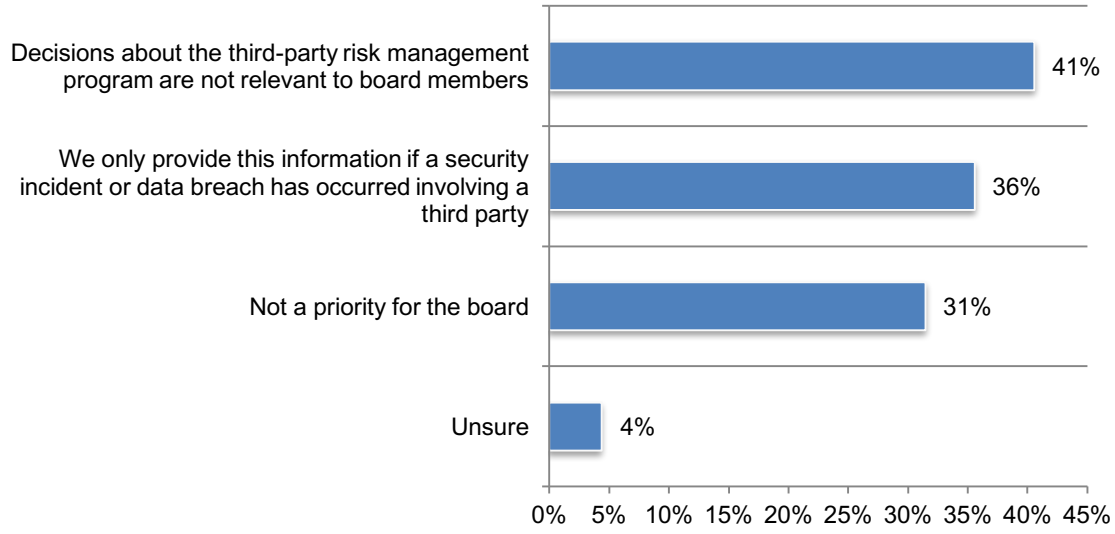
Figure 8. How many third parties are in this inventory?
Extrapolated value = 583



Communication with the board of directors about third-party risks rarely occurs. Only 39 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 61 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 (41 percent), as shown in Figure 9. Thirty-one percent of respondents believe it is not a priority or it is only relevant if a security breach has occurred involving a vendor (36 percent of respondents).

Figure 9. Reasons for not regularly reporting third-party risks to the board of directors
More than one response permitted

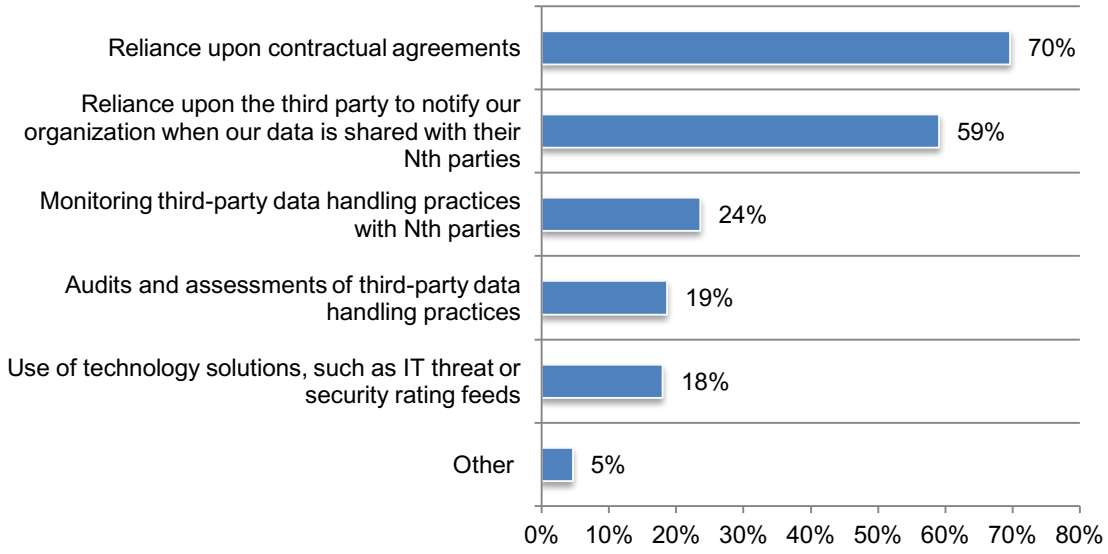


Lack of visibility into third and Nth party relationships

Companies lack visibility into Nth parties that have their sensitive or confidential data. Only 15 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.

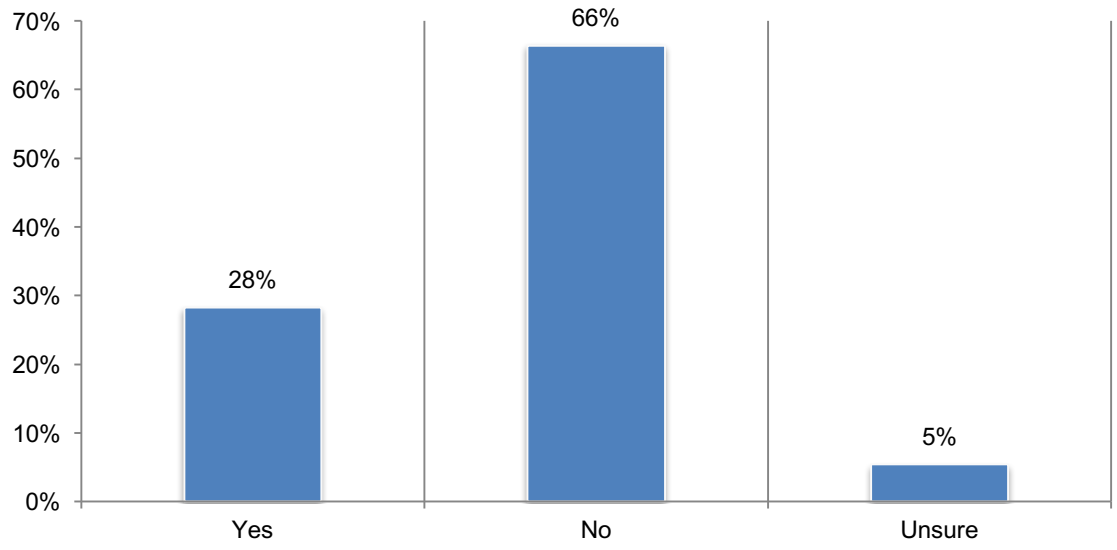
According to Figure 10, of the 15 percent of respondents who say they have such visibility, 70 percent say visibility is due to reliance upon contractual agreements, and 59 percent of respondents say they trust the third party to notify their organization when their data is shared with their Nth parties.

Figure 10. How does your organization achieve visibility into vendors your company does not have a direct relationship with?
More than one response permitted



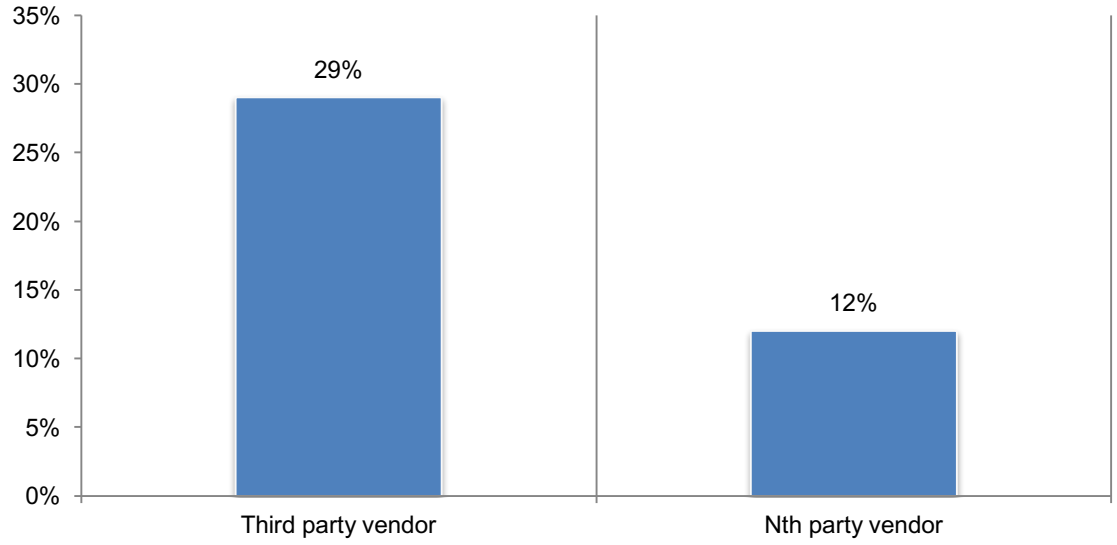
Third parties rarely inform companies about their sharing with Nth parties. We asked **all** respondents to estimate the percentage of all third parties they believe are outsourcing their sensitive and confidential data to Nth parties. According to these respondents, an average of 41 percent of their primary vendors are sharing sensitive and confidential information with other vendors (N^{th} party risk). However, according to Figure 11, only 28 percent of respondents say they are notified if such sharing is taking place.

Figure 11. 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 29 percent of respondents say a third party would contact them about the data breach, as shown in Figure 12. A very small percentage (12 percent) are confident they would learn that their sensitive data was lost or stolen by a Nth vendor.

Figure 12. We are confident a third party would notify us if they had a data breach
1 = not confident to 10 = high confidence, 7+ responses

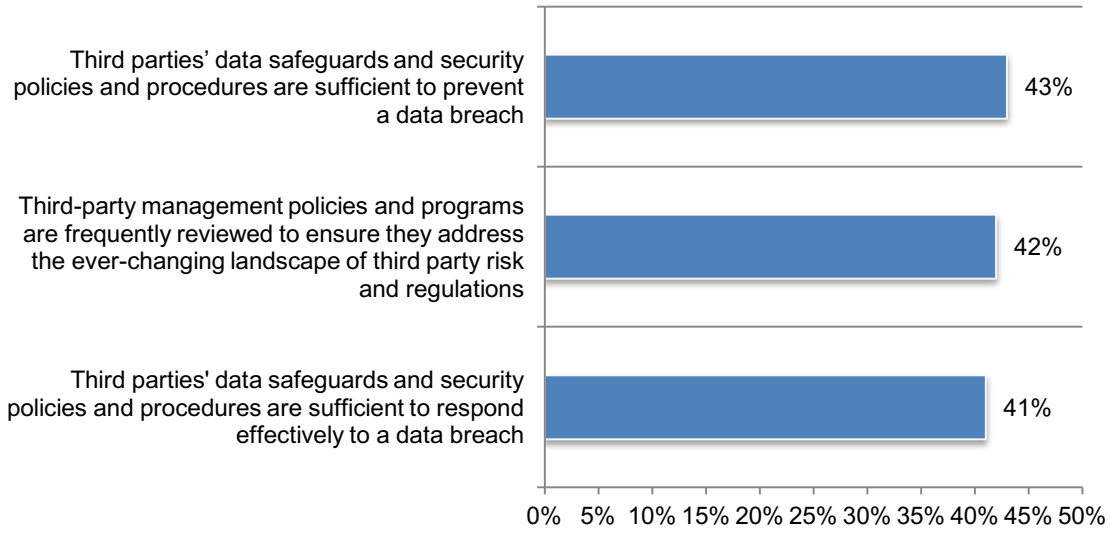


The realities of today's third-party risk management programs

Most companies lack confidence in their third parties' security policies and procedures. As shown in Figure 13, only 43 percent of respondents say their third parties' data safeguards and security policies and procedures are sufficient to prevent a data breach and only 41 percent of respondents say these safeguards and security policies are sufficient to respond to a data breach.

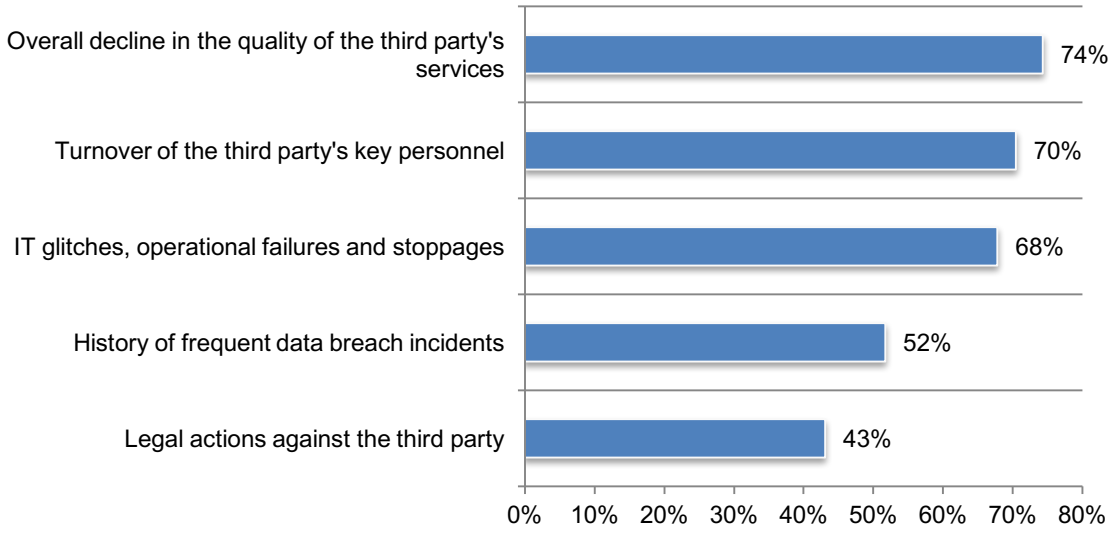
However, many organizations are not proactive in managing third-party risk. Specifically, only 42 percent of respondents say their organizations are frequently reviewing the policies and programs of their third parties to ensure they address the ever-changing landscape of third-party risk and regulations.

Figure 13. Perceptions about vendors' security policies and procedures
Strongly agree and Agree responses combined



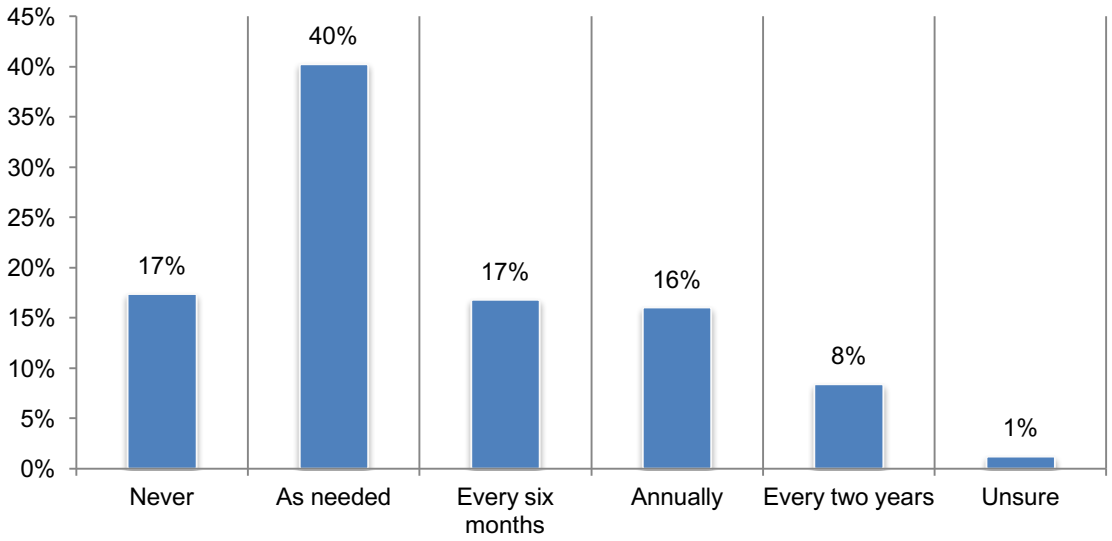
Indicators of risk fail to reveal third-party security vulnerabilities. Fifty-seven percent of respondents say their third-party management programs define and rank levels of risk. According to Figure 14, 74 percent of respondents say an overall decline in the quality of the third party's services is the number one indicator of risk followed by 70 percent of respondents who say it is turnover of key personnel. These indicators of risk 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.

Figure 14. The top five indicators of third-party risk
More than one response permitted



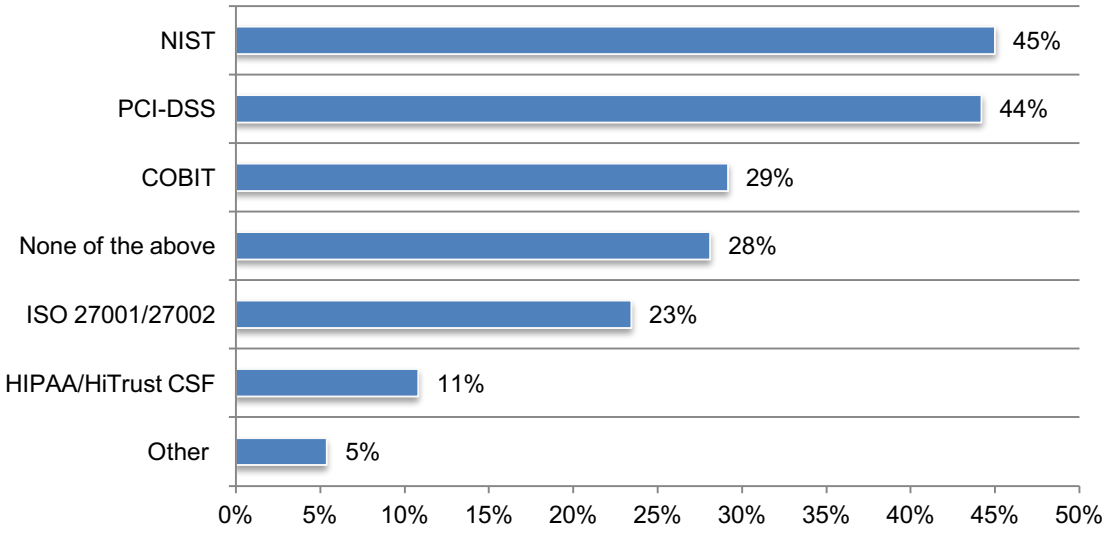
Moreover, 57 percent of these respondents say risk levels are only updated as needed (40 percent) or never (17 percent), as shown in Figure 15.

Figure 15. Third-party risk levels are rarely updated



According to Figure 16, NIST and PCI-DSS are the security controls most often used by organizations represented in this research.

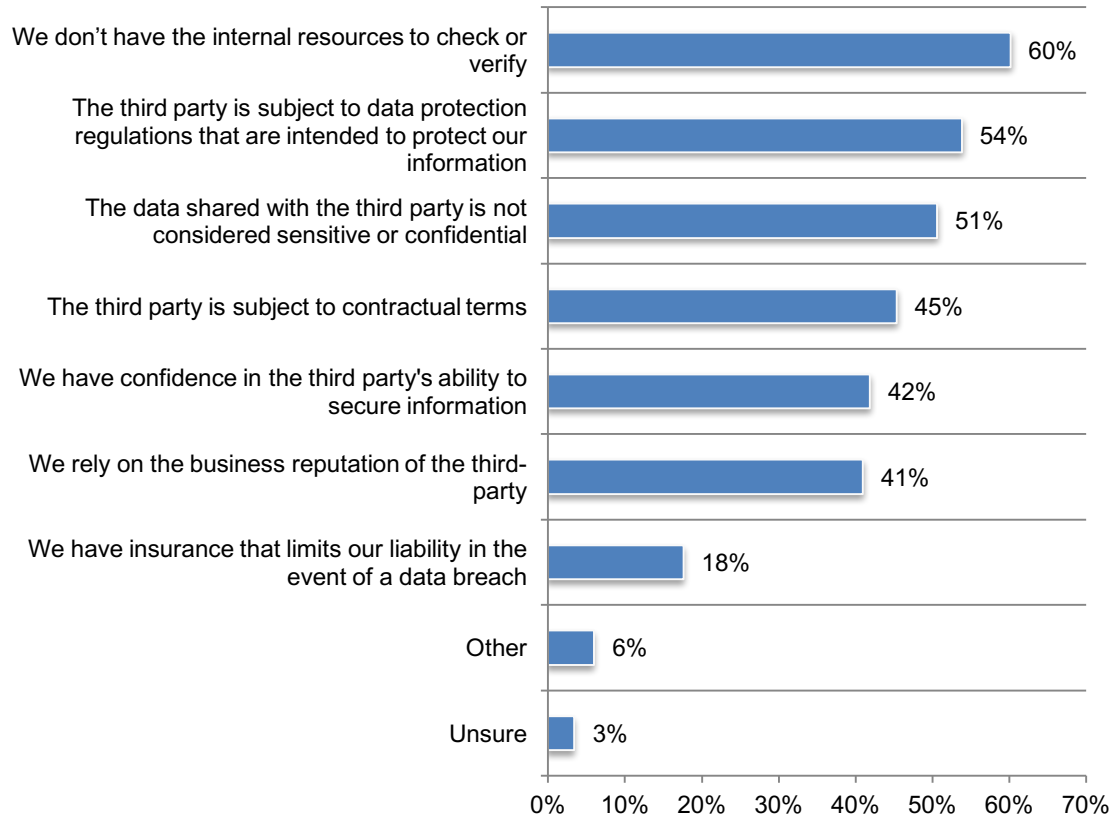
Figure 16. What information security control standard(s) does your organization use or plan to use?
More than one response permitted



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 17 shows why organizations **are not** performing evaluations.

As shown, the top two reasons are a lack of resources, and the belief that the third party is subject to data protection regulations that are intended to protect the organization's information (60 and 54 percent of respondents, respectively).

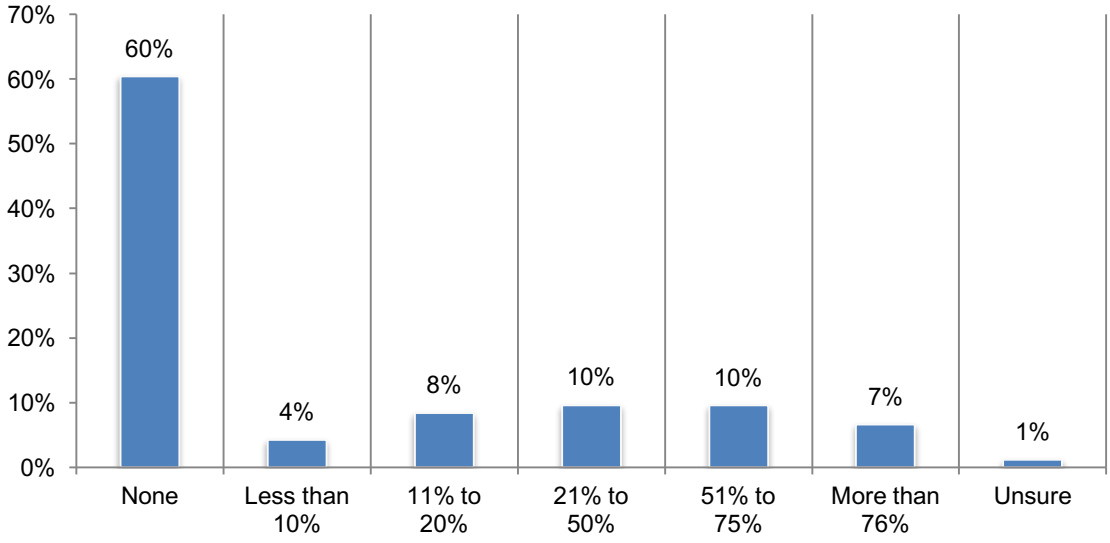
Figure 17. Reasons for not performing an evaluation
More than one response permitted



Companies rely upon contracts, and not direct observations to ensure that their third parties have appropriate security practices and controls in place. As discussed above, only 40 percent of companies are evaluating the third parties with whom they share information.

Instead, they are relying on contracts or trusting the third party will take appropriate steps to secure their information assets. Further, as shown in Figure 18, 60 percent of companies are not requiring their third parties to respond to questionnaires about their security practices or conduct remote or onsite assessments.

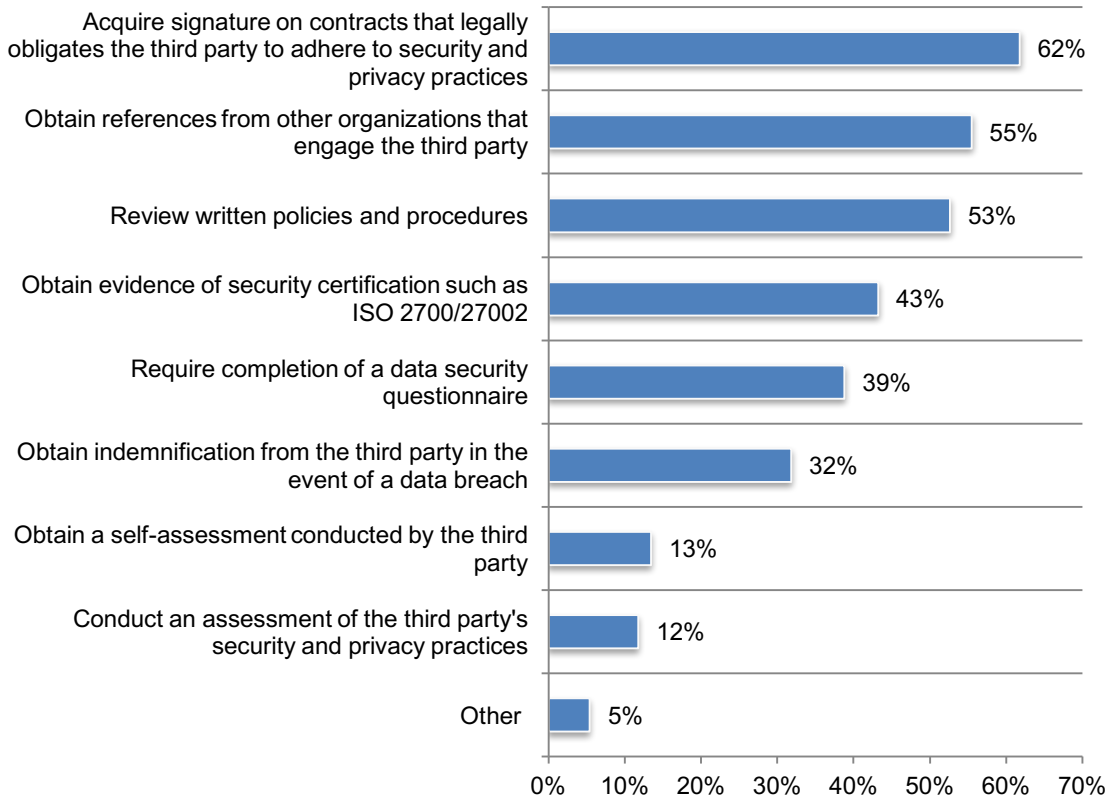
Figure 18. Percentage of third parties required to fill out security questionnaires and/or conduct remote or onsite assessments



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 12 percent of respondents say they conduct an assessment of the third party's security and privacy practices, and only 13 percent of respondents say they obtain a self-assessment conducted by the third party.

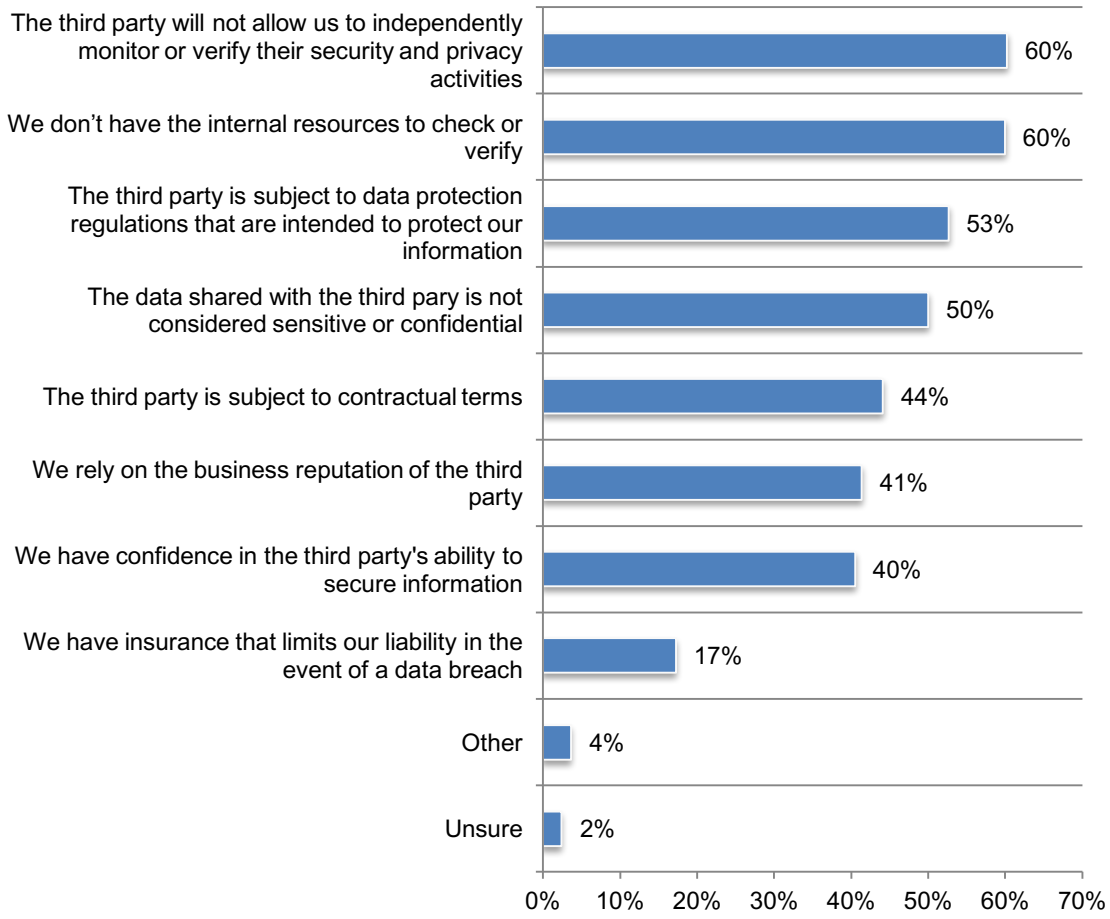
Figure 19. Steps taken to evaluate third parties
More than one response permitted



Companies are not monitoring the privacy and security practices of third parties. Fifty-four 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.

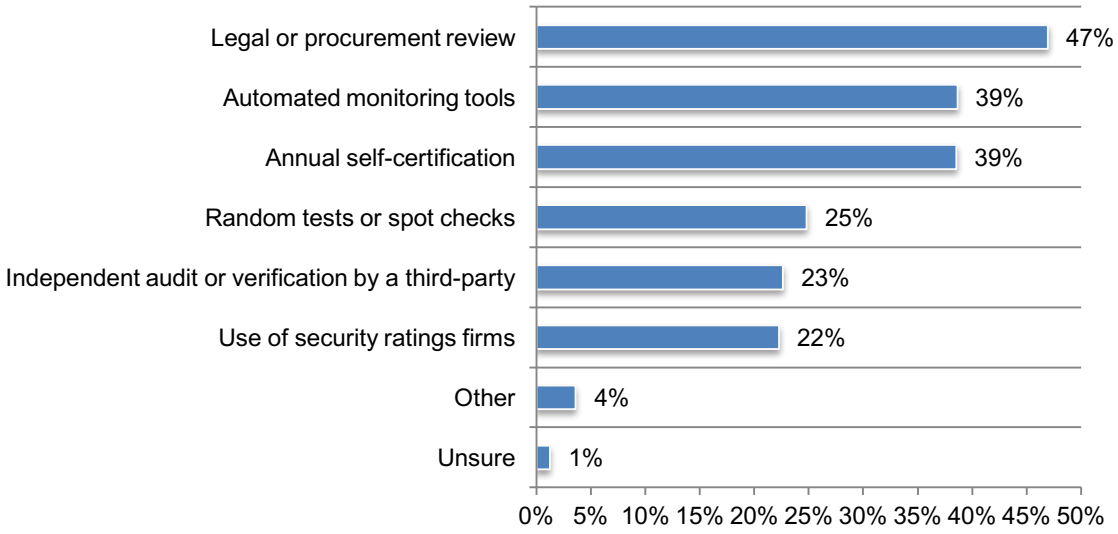
As shown in Figure 20, the primary reasons for not monitoring are: the third party does not allow the company to independently monitor or verify their security and privacy practices (60 percent of respondents) or they don't have the internal resources to check or verify (60 percent of respondents).

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



Third party monitoring mostly involves legal or procurement review. Forty 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 47 percent of respondents say their companies rely upon legal or procurement review. Only 23 percent of respondents say they are conducting independent audits or verification by a third-party.

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



Part 4. Key Trends in Third-Party Risk Management

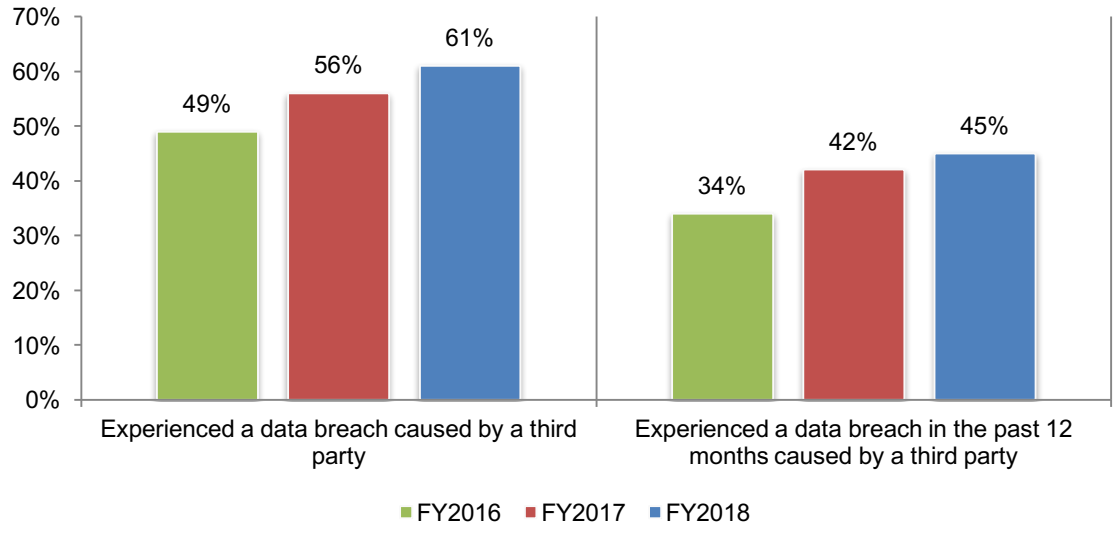
In this section, we present the key trends in US third-party risk management since the study was first conducted in 2016. The 2018 study is the first year UK organizations participated.

Data breaches involving third parties are on the rise. Figure 22 illustrates the growing problem of third-party breaches. Since the study was first conducted in 2016, companies that ever had a data breach caused by a third party has increased from 49 percent to 61 percent. Third party data breaches over a 12-month period has increased from 34 percent to 45 percent.

Companies continue to lack visibility into the number of third parties they are sharing sensitive information with. Since 2016, more respondents are reporting that their organizations have a comprehensive inventory of all third parties with whom they share sensitive or confidential information from 33 percent of respondents in 2016 to 36 percent of respondents in this year's study.

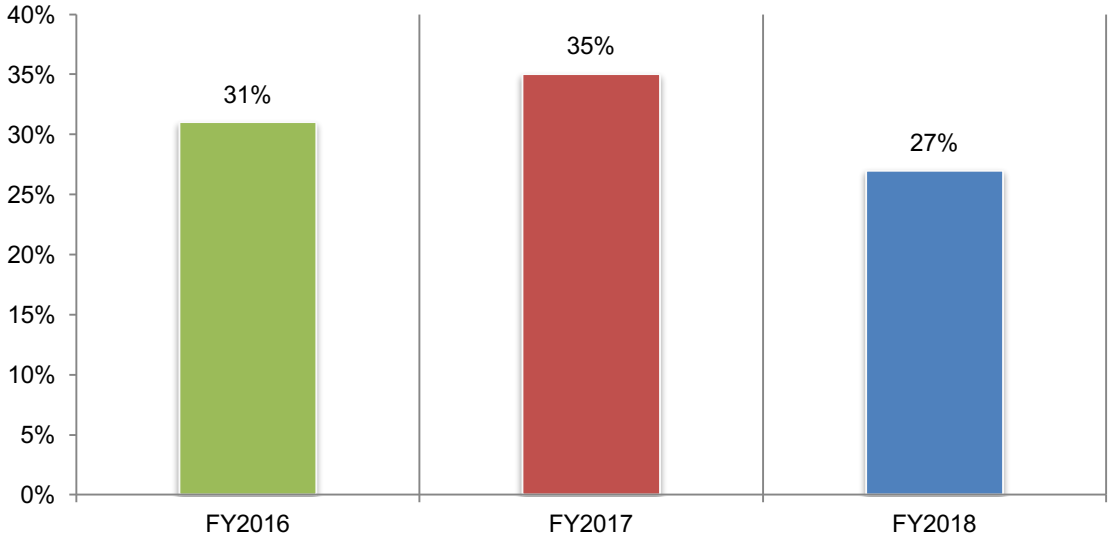
The number of third parties that companies are doing business with is increasing. Of those that have an inventory, the average number of third parties has increased from 378 in 2016 to 471 in 2017 and to 588 in 2018, when normalized for historical ranges. Moreover, the average percentage of third parties sharing organizations' sensitive and confidential data with Nth parties has increased from 37 percent in 2016 to 43 percent in 2018.

Figure 22. Has your organization ever or in the past 12 months experienced a data breach caused by a third party?
Yes responses presented



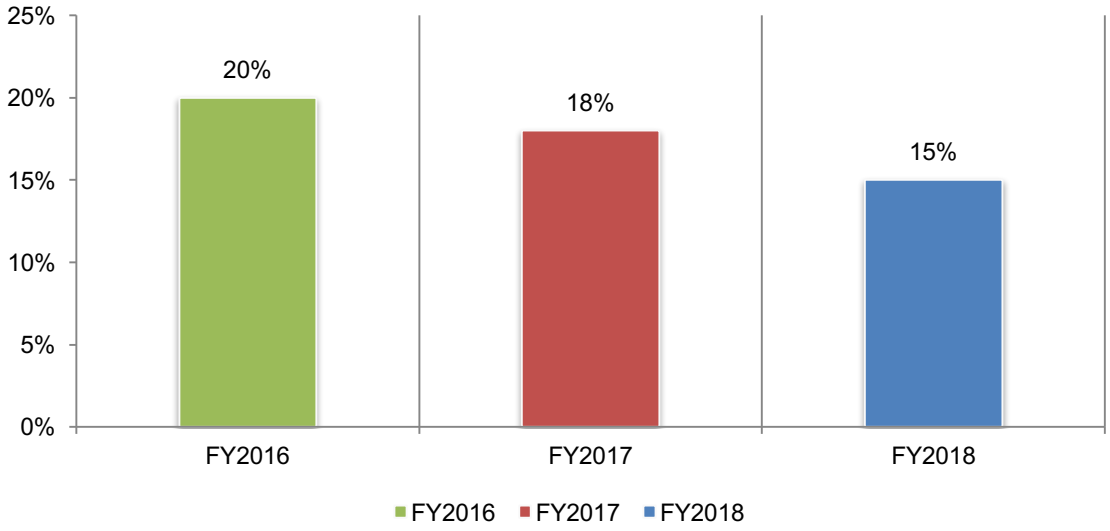
Organizations lack confidence in data breach notification by third parties. According to Figure 23, respondents' confidence that if a third party had a data breach involving their sensitive or confidential information would notify their organizations has dropped significantly since last year.

Figure 23. 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, 7+ responses presented



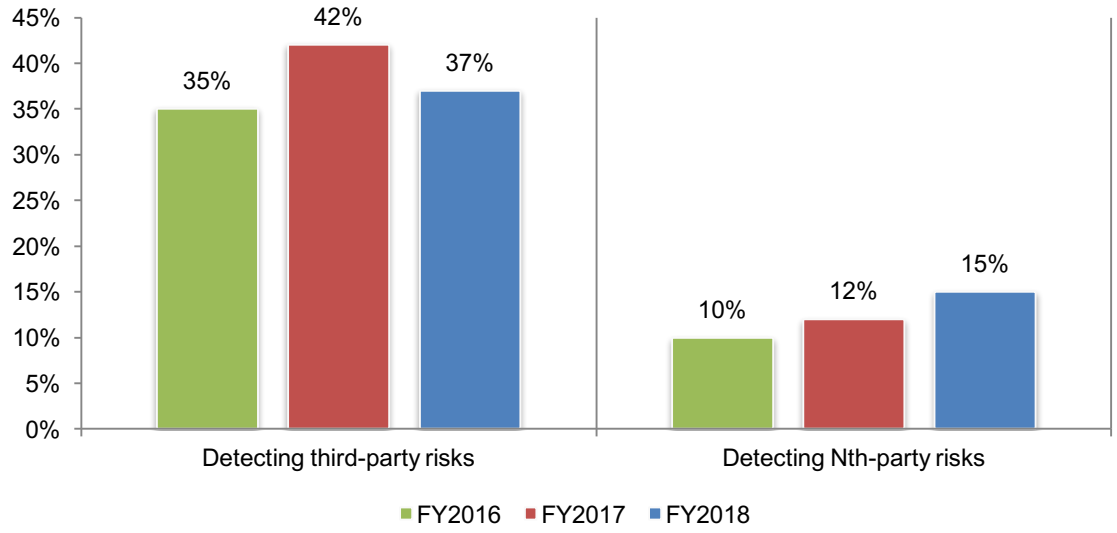
Visibility into Nth parties continues to decline. According to Figure 24, the percentage of organizations with visibility into Nth parties they have do not have a direct relationship with but that access their sensitive and confidential information has steadily declined since 2016.

Figure 24. Do you have visibility into Nth parties?
Yes responses presented



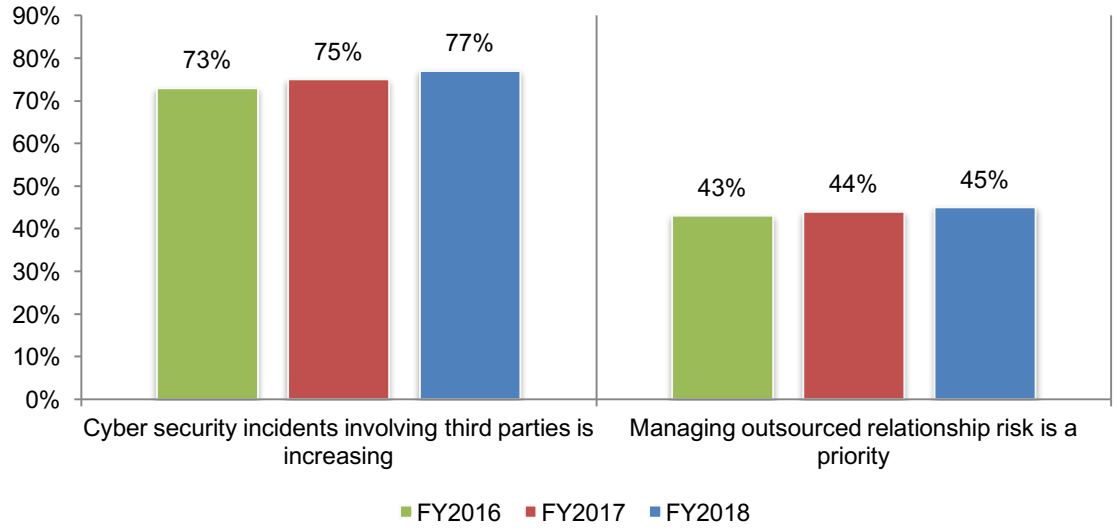
The ability to detect third party risks declines. Respondents were asked to rate the effectiveness of detecting third-party and Nth-party risks on a scale of 1 = not effective to 10 = highly effective. As shown in Figure 25, effectiveness in detecting third-party risks has declined since 2017 and effectiveness in detecting Nth-party risks remains very low.

Figure 25. Effectiveness in detecting third-party and Nth-party risks
1 = not effective to 10 = highly effective, 7+ responses presented



Cyber security incidents involving third parties is increasing, but the priority of safeguarding sensitive and confidential information is not. Figure 26 shows the third-party risk gap over the past three years. While respondents have not wavered in their belief that cyber security incidents involving third parties are increasing, the priority of managing outsourced relationship risk remains stagnant at 45 percent in 2018.

Figure 26. The gap in third-party risk
Strongly agree and agree responses combined



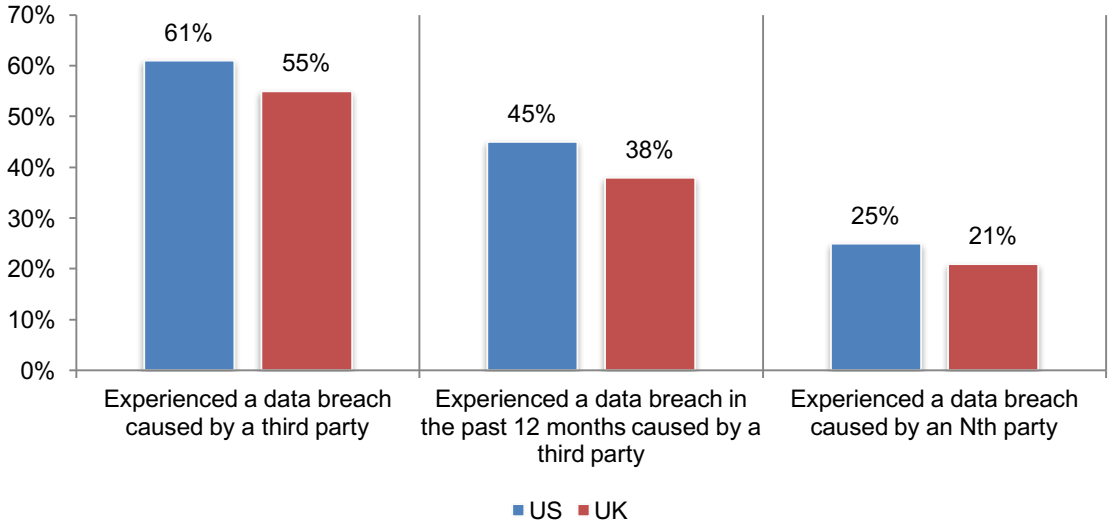
Part 5. Key Differences between US and UK Respondents

In this section of the report, we present the most salient differences between the 632 respondents in the US and 406 respondents in the UK.

UK respondents report fewer data breaches caused by third parties and Nth parties. As shown in Figure 27, 61 percent of respondents in the US vs. 55 percent of respondents in the UK have at least once experienced a data breach experienced by a third party.

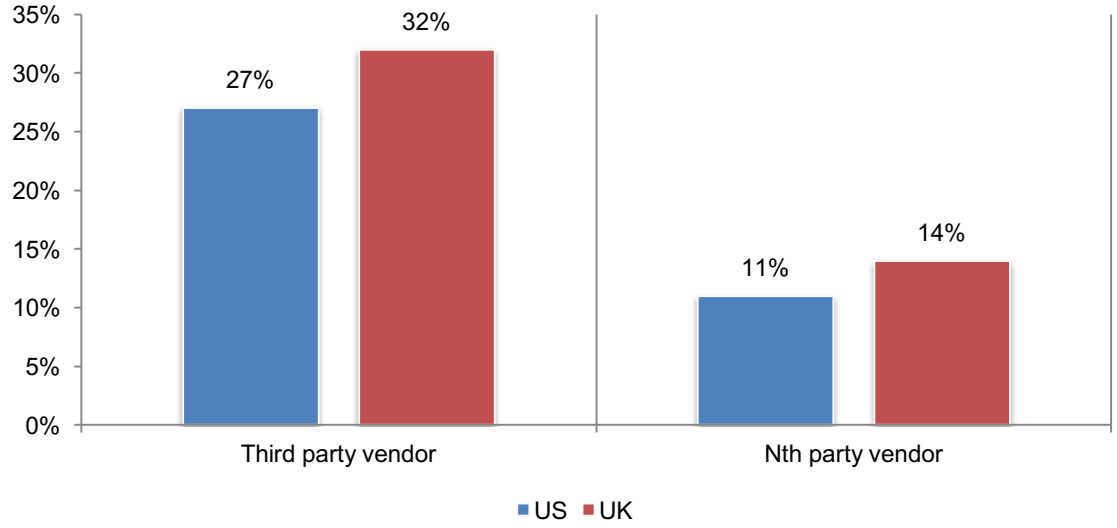
In the past 12 months, 45 percent of US vs. 38 percent of UK respondents were breached in the past 12 months. While it is difficult to determine with certainty that an Nth party caused a data breach, 25 percent of respondents in the US had such a breach vs. 21 percent in the UK.

Figure 27. Has your organization ever experienced a data breach and did you have a data breach in the past 12 months
Yes responses



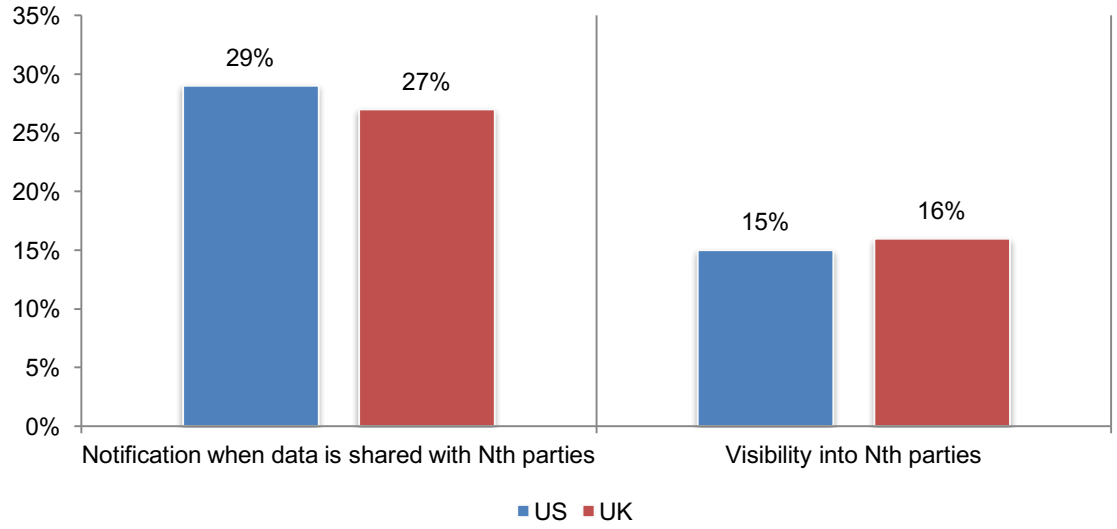
UK companies also have more confidence the third or Nth party would notify them should a data breach occur. Figure 28 shows the percentage of respondents who are highly confident the third-party vendor or Nth party vendor would notify them if they had a data breach involving their sensitive and confidential information. The UK companies are slightly more confident than US companies.

Figure 28. Confidence in notification by a third or Nth party if they had a data breach
1 = not confident to 10 = highly confident, 7+ responses reported



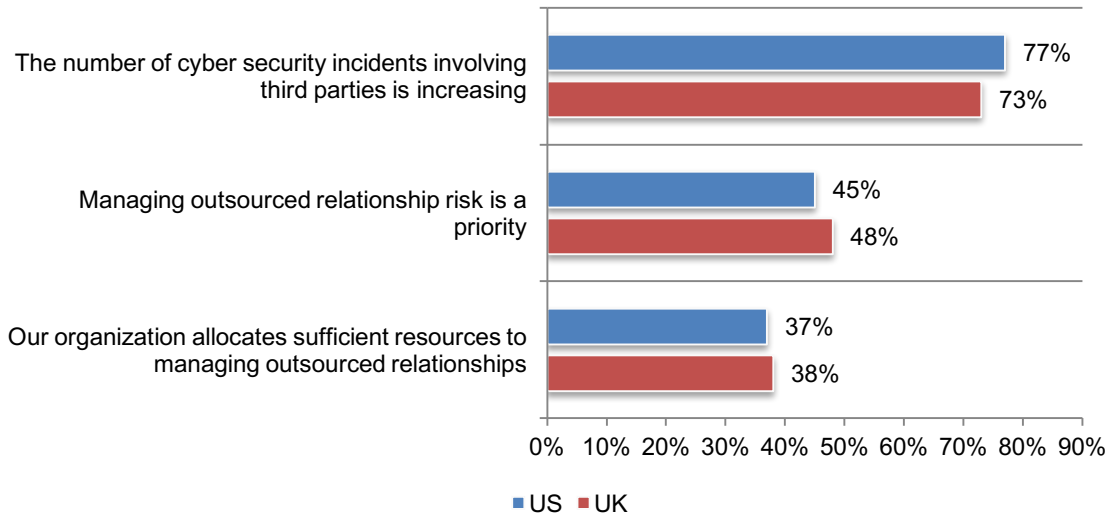
Both US and UK companies are at risk for a third-party breach because of a lack of visibility with Nth parties that have their confidential information assets. According to Figure 29, few respondents believe their third parties would notify them if they were sharing with Nth parties and many lack visibility into Nth parties.

Figure 29. Visibility into the practices of Nth parties
Yes responses



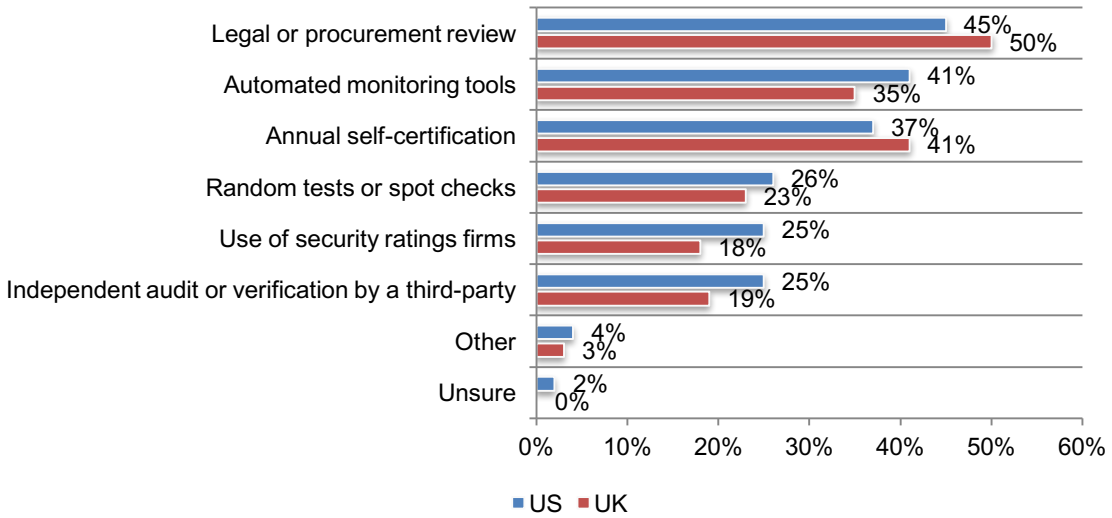
UK and US organizations have similar perceptions about third-party risk. As shown in Figure 30, respondents in both countries believe the number of cybersecurity incidents involving third parties is increasing. They also agree that very often managing outsourced relationships is not a priority of their organizations as evidenced by not having sufficient resources.

Figure 30. Perceptions about managing third party risk
Strongly agree and Agree responses combined



US and UK companies favor different monitoring procedures. According to Figure 31, both respondents in the UK and US mostly rely upon legal or procurement reviews of security and privacy practices. However, US companies are mostly using automated monitoring tools, use of security rating firms and independent audit or verification by the third party. UK companies are more likely to use annual self-certifications.

Figure 31. What monitoring procedures does your organization use to ensure adequacy of security and privacy practices?
More than one response permitted



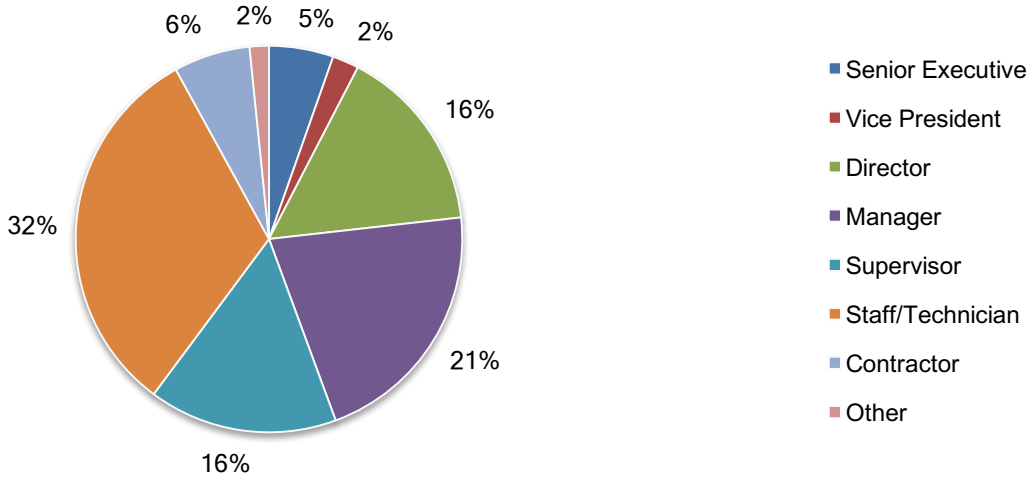
Part 6. Methods

A sampling frame of 15,800 individuals located in the United States and 10,995 individuals located in the United Kingdom were 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 1,140 total returns. Screening and reliability checks required the removal of 102 surveys. Our final sample consisted of 1,038 surveys or a 3.9 percent response.

Table 1. Sample response	US	UK	FY2018
Sampling frame	15,800	10,995	26,795
Total returns	688	452	1,140
Rejected or screened surveys	56	46	102
Final sample	632	406	1,038
Response rate	4.0%	3.7%	3.9%

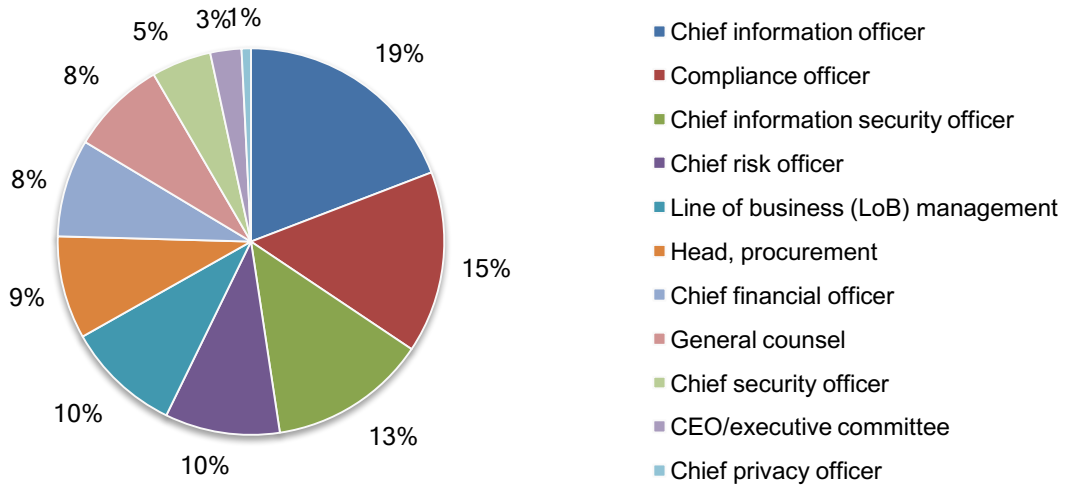
Pie Chart 1 reports the respondents' organizational levels within the participating organizations. By design, more than half of the respondents (60 percent) are at or above the supervisory levels.

Pie Chart 1. Current position within the organization



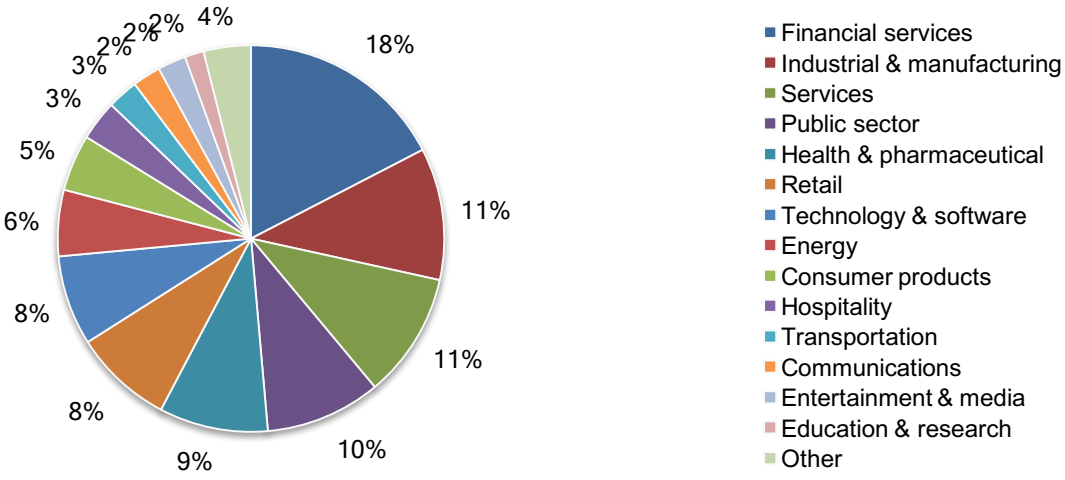
As shown in Pie Chart 2, 19 percent of respondents report to the chief information officer, 15 percent of respondents report to the compliance officer, 13 percent of respondents report to the chief information security officer, 10 percent of respondents report to the chief risk officer and 10 percent of respondents report to the lines of business management.

Pie Chart 2. Primary person you or your leader reports to



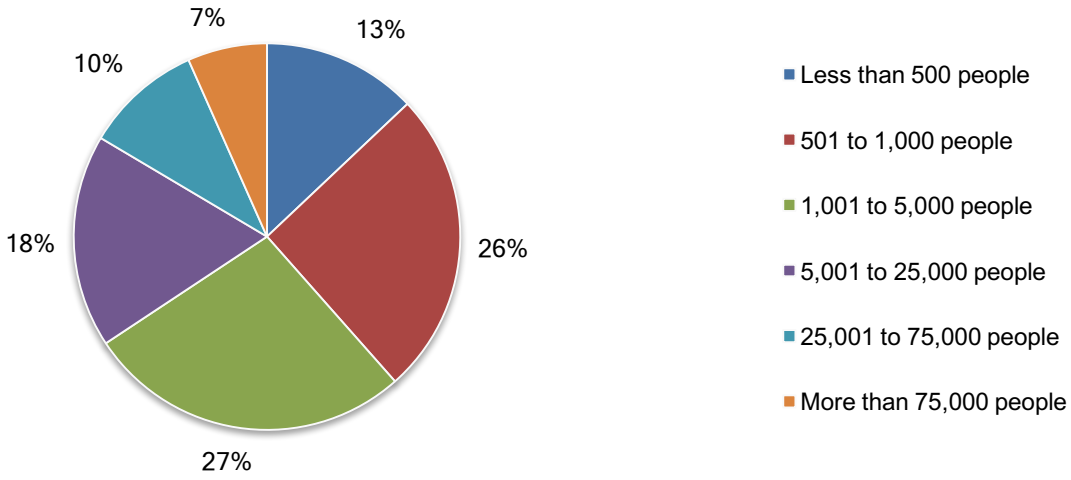
Pie Chart 3 reports the industry segments of respondents' organizations. This chart identifies financial services (18 percent of respondents) as the largest segment, followed by industrial and manufacturing (11 percent), services sector (11 percent), and public sector (10 percent).

Pie Chart 3. Industry distribution of respondents' organizations



As shown in Pie Chart 4, 62 percent of respondents are from organizations with a global headcount of more than 1,000 employees.

Pie Chart 4. Worldwide headcount of the organization



Part 7. 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 between July 19 and August 1, 2018.

Survey response	**US**	**UK**	**FY2018**
Sampling frame	15,800	10,995	26,795
Total returns	688	452	1,140
Rejected or screened surveys	56	46	102
Final sample	632	406	1,038
Response rate	4.0%	3.7%	3.9%
Sampling weights	0.61	0.39	1.00

S1. How familiar are you with your organization's approach to managing data risks created through outsourcing?	US	UK	FY2018
Very familiar	34%	27%	31%
Familiar	42%	45%	43%
Somewhat familiar	24%	28%	26%
No knowledge (Stop)	0%	0%	0%
Total	100%	100%	100%

S2. Does your company have a third-party data risk management program?	US	UK	FY2018
Yes	100%	100%	100%
No (Stop)	0%	0%	0%
Total	100%	100%	100%

S3. Do you have any involvement in managing the data risks created by outsourcing?	US	UK	FY2018
Yes, full involvement	37%	30%	34%
Yes, partial involvement	45%	49%	47%
Yes, minimal involvement	18%	21%	19%
No involvement (Stop)	0%	0%	0%
Total	100%	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?	US	UK	FY2018
Yes	61%	55%	59%
No	29%	36%	32%
Unsure	10%	9%	10%
Total	100%	100%	100%

Q1b. **In the past 12 months**, has your organization experienced a data breach caused by a breach of one of your third parties that resulted in the misuse of your company's sensitive or confidential information?	US	UK	FY2018
Yes	45%	38%	42%
No	35%	38%	36%
Unsure	20%	24%	22%
Total	100%	100%	100%

Q1c. Has your organization **ever** experienced a data breach caused by a breach of one of your Nth parties that resulted in the misuse of your company's sensitive or confidential information?	US	UK	FY2018
Yes	25%	21%	23%
No	35%	33%	34%
Unsure	40%	46%	42%
Total	100%	100%	100%

Q1d. If you answered yes to any of the questions above, did your organization make any changes to its third-party risk management program?	US	UK	FY2018
Yes	55%	49%	53%
No	39%	48%	43%
Unsure	6%	3%	5%
Total	100%	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)	US	UK	FY2018
1 or 2	12%	10%	11%
3 or 4	23%	21%	22%
5 or 6	38%	37%	38%
7 or 8	19%	21%	20%
9 or 10	8%	11%	9%
Total	100%	100%	100%
Extrapolated value	5.26	5.54	5.37

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)	US	UK	FY2018
1 or 2	38%	40%	39%
3 or 4	34%	31%	33%
5 or 6	17%	15%	16%
7 or 8	8%	10%	9%
9 or 10	3%	4%	3%
Total	100%	100%	100%

Extrapolated value	3.58	3.64	3.60

Q3. Who is **most accountable** for the correct handling of your organization's third party-risk management program?	US	UK	FY2018
General counsel/compliance Officer	14%	11%	13%
Chief technology officer (CTO)	3%	5%	4%
Chief information officer (CIO)	16%	11%	14%
Chief information security officer (CISO)	15%	13%	14%
Chief security officer (CSO)	4%	5%	4%
Head of business continuity management	3%	2%	3%
Chief privacy officer (CPO)	1%	0%	1%
Data protection officer (DPO)	0%	0%	0%
Head of human resources	0%	0%	0%
Head of procurement	14%	20%	16%
Chief risk officer (CRO)	15%	11%	13%
No one person/department is accountable	15%	18%	16%
Unsure	0%	4%	2%
Total	100%	100%	100%

Q4a. Does your company have a comprehensive inventory of all third parties with whom it shares sensitive and confidential information?	US	UK	FY2018
Yes (Proceed to Q5.)	36%	30%	34%
No	60%	65%	62%
Unsure	4%	5%	4%
Total	100%	100%	100%

Q4b. If no or unsure, why? Please check all that apply	US	UK	FY2018
Lack of resources to track third parties	43%	45%	44%
No centralized control over third-party relationships	71%	66%	69%
Complexity in third-party relationships	51%	44%	48%
Cannot keep track due to frequent turnover in third parties	37%	41%	39%
Not a priority	44%	40%	42%
Total	246%	236%	242%

Q5. How many third parties are in this inventory?	US	UK	FY2018
Less than 10	0%	0%	0%
11 to 50	13%	21%	16%
51 to 100	25%	26%	25%
101 to 250	13%	16%	14%
250 to 500	12%	9%	11%
501 to 1,000	15%	13%	14%
1,001 to 2,500	19%	15%	17%
2,501 to 5,000	2%	0%	1%
More than 5,000	1%	0%	1%
Unsure	0%	0%	0%

Total	100%	100%	100%
Extrapolated value	670	448	583

*Scale different in FY2017 & FY2016

Q6. Does the inventory include all third parties your company has a relationship with as well as Nth parties that might have access to sensitive and confidential data?	US	UK	FY2018
Yes	19%	15%	17%
No	78%	80%	79%
Unsure	3%	5%	4%
Total	100%	100%	100%

Q7. What percentage of all third parties do you believe are sharing your sensitive and confidential data with Nth parties?	US	UK	FY2018
None	0%	4%	2%
Less than 10%	4%	5%	4%
11% to 20%	17%	21%	19%
21% to 50%	39%	41%	40%
51% to 75%	33%	26%	30%
More than 76%	7%	3%	5%
Unsure	0%	0%	0%
Total	100%	100%	100%
Extrapolated value	43%	37%	41%

Q8. Do third parties notify your organization when your data is shared with the Nth parties?	US	UK	FY2018
Yes	29%	27%	28%
No	66%	67%	66%
Unsure	5%	6%	5%
Total	100%	100%	100%

Q9a. Do you have visibility into Nth parties your company does not have a direct relationship with but that access your company's sensitive and confidential information (Nth parties)?	US	UK	FY2018
Yes	15%	16%	15%
No	76%	73%	75%
Unsure	9%	11%	10%
Total	100%	100%	100%

Q9b. If yes, how do you achieve visibility? Please check all that apply.	US	UK	FY2018
Monitoring third-party data handling practices with Nth parties	24%	23%	24%
Audits and assessments of third-party data handling practices	19%	18%	19%
Reliance upon the third party to notify our organization when our data is shared with their Nth parties	61%	56%	59%

Reliance upon contractual agreements	70%	69%	70%
Use of technology solutions, such as IT threat or security rating feeds	18%	18%	18%
Other (please specify)	5%	4%	5%
Total	197%	188%	193%

Q10a. 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)	US	UK	FY2018
1 or 2	12%	14%	13%
3 or 4	23%	25%	24%
5 or 6	48%	46%	47%
7 or 8	12%	9%	11%
9 or 10	5%	6%	5%
Total	100%	100%	100%
Extrapolated value	5.00	4.86	4.95

Q10b. 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)	US	UK	FY2018
1 or 2	24%	28%	26%
3 or 4	44%	38%	42%
5 or 6	16%	20%	18%
7 or 8	11%	10%	11%
9 or 10	5%	4%	5%
Total	100%	100%	100%
Extrapolated value	4.08	3.98	4.04
Q11a. 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)	US	UK	FY2018
1 or 2	16%	13%	15%
3 or 4	21%	25%	23%
5 or 6	26%	22%	24%
7 or 8	25%	27%	26%
9 or 10	12%	13%	12%
Total	100%	100%	100%
Extrapolated value	5.42	5.54	5.47

Q11b. 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)	US	UK	FY2018
1 or 2	35%	34%	35%
3 or 4	39%	44%	41%
5 or 6	11%	10%	11%
7 or 8	9%	7%	8%
9 or 10	6%	5%	6%

Total	100%	100%	100%
Extrapolated value	3.74	3.60	3.69

Q12a. Using the following 10-point scale, please rate your organization's effectiveness in **minimizing** third-party risks. (1 = not effective to 10 = highly effective)	US	UK	FY2018
1 or 2	8%	10%	9%
3 or 4	21%	24%	22%
5 or 6	43%	40%	42%
7 or 8	22%	21%	22%
9 or 10	6%	5%	6%
Total	100%	100%	100%
Extrapolated value	5.44	5.24	5.36

Q12b. Using the following 10-point scale, please rate your organization's effectiveness in **minimizing** Nth-party risks. (1 = not effective to 10 = highly effective)	US	UK	FY2018
1 or 2	35%	27%	32%
3 or 4	35%	42%	38%
5 or 6	16%	15%	16%
7 or 8	9%	11%	10%
9 or 10	5%	5%	5%
Total	100%	100%	100%
Extrapolated value	3.78	4.00	3.87

Q13. 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)	US	UK	FY2018
1 or 2	13%	11%	12%
3 or 4	17%	14%	16%
5 or 6	35%	38%	36%
7 or 8	26%	27%	26%
9 or 10	9%	10%	9%
Total	100%	100%	100%
Extrapolated value	5.52	5.72	5.60

Part 2. Attributions

Q14. Managing outsourced relationship risk is a priority in our organization.	US	UK	FY2018
Strongly agree	23%	25%	24%
Agree	22%	23%	22%
Unsure	28%	29%	28%
Disagree	19%	16%	18%
Strongly disagree	8%	7%	8%
Total	100%	100%	100%

Q15. Our organization allocates sufficient resources to managing outsourced relationships.	US	UK	FY2018
Strongly agree	18%	18%	18%
Agree	19%	20%	19%
Unsure	23%	21%	22%
Disagree	28%	26%	27%
Strongly disagree	12%	15%	13%
Total	100%	100%	100%

Q16. The number of cyber security incidents involving third parties is increasing.	US	UK	FY2018
Strongly agree	38%	35%	37%
Agree	39%	38%	39%
Unsure	13%	20%	16%
Disagree	8%	7%	8%
Strongly disagree	2%	0%	1%
Total	100%	100%	100%

Q17. Our third parties' data safeguards and security policies and procedures are sufficient to prevent a data breach.	US	UK	FY2018
Strongly agree	15%	19%	17%
Agree	26%	25%	26%
Unsure	15%	11%	13%
Disagree	29%	27%	28%
Strongly disagree	15%	18%	16%
Total	100%	100%	100%

Q18. Our third parties' data safeguards and security policies and procedures are sufficient to respond effectively to a data breach.	US	UK	FY2018
Strongly agree	16%	18%	17%
Agree	25%	23%	24%
Unsure	14%	12%	13%
Disagree	30%	30%	30%
Strongly disagree	15%	17%	16%
Total	100%	100%	100%

Q19. Our third-party management policies and programs are frequently reviewed to ensure they address the ever-changing landscape of third party risk and regulations.	US	UK	FY2018
Strongly agree	17%	16%	17%
Agree	23%	27%	25%
Unsure	18%	16%	17%
Disagree	26%	25%	26%
Strongly disagree	16%	16%	16%
Total	100%	100%	100%

Part 3. Secure outsourcing management

Q20a. Do you evaluate the security and privacy practices of all third parties before you engage them in a business relationship that requires the sharing of sensitive or confidential information?	US	UK	FY2018
Yes	40%	41%	40%
No	55%	53%	54%
Unsure	5%	6%	5%
Total	100%	100%	100%

Q20b. If yes, how do you perform this evaluation? Please check all that apply.	US	UK	FY2018
Review written policies and procedures	55%	49%	53%
Acquire signature on contracts that legally obligates the third party to adhere to security and privacy practices	61%	63%	62%
Obtain indemnification from the third party in the event of a data breach	33%	30%	32%
Conduct an assessment of the third party's security and privacy practices	11%	13%	12%
Obtain a self-assessment conducted by the third party	15%	11%	13%
Obtain references from other organizations that engage the third party	59%	50%	55%
Obtain evidence of security certification such as ISO 2700/27002	44%	42%	43%
Require completion of a data security questionnaire	40%	37%	39%
Other (please specify)	5%	6%	5%
Unsure	0%	1%	0%
Total	323%	302%	315%

Q20c. If no, why don't you perform an evaluation? Please check all that apply.	US	UK	FY2018
We don't have the internal resources to check or verify	59%	62%	60%
We have confidence in the third party's ability to secure information	45%	37%	42%
We rely on the business reputation of the third-party	39%	44%	41%
We have insurance that limits our liability in the event of a data breach	18%	17%	18%
The third party is subject to data protection regulations that are intended to protect our information	55%	52%	54%
The third party is subject to contractual terms	43%	49%	45%
The data shared with the third party is not considered sensitive or confidential	51%	50%	51%
Other	4%	9%	6%
Unsure	3%	4%	3%
Total	317%	324%	320%

Q21a. Do you evaluate the security and privacy practices of all Nth parties before permitting your third parties to share sensitive or confidential with Nth parties?	US	UK	FY2018
Yes	13%	10%	12%
No	81%	83%	82%
Unsure	6%	7%	6%
Total	100%	100%	100%

Q21b. If yes, how do you perform this evaluation? Please check all that apply.	US	UK	FY2018
Require third parties to disclose any subcontractors with whom they will share your sensitive or confidential information	42%	38%	40%
Use technologies that can reveal the identity of your third party's subcontractors	21%	16%	19%
Require third parties to obtain your specific approval before they share sensitive or confidential information with a subcontractor	36%	33%	35%
Require signatures on contracts that legally obligate the third party's subcontractors to adhere to security and privacy practices	40%	42%	41%
Obtain indemnification from the third party's subcontractors in the event of a data breach	27%	31%	29%
Conduct an assessment of the third party's subcontractors' security and privacy practices	19%	25%	21%
Obtain references from other organizations that engage the third party's subcontractors	31%	26%	29%
Obtain evidence that third party's subcontractors have a security certification such as ISO 2700/27002	29%	23%	27%
Require completion of a data security questionnaire	40%	38%	39%
Other (please specify)	3%	5%	4%
Unsure	1%	0%	1%
Total	289%	277%	284%

Q22. What percentage of your third parties do you require to fill out security questionnaires and/or conduct remote or on-site assessments?	US	UK	FY2018
None	60%	61%	60%
Less than 10%	5%	3%	4%
11% to 20%	8%	9%	8%
21% to 50%	10%	9%	10%
51% to 75%	8%	12%	10%
More than 76%	7%	6%	7%
Unsure	2%	0%	1%
Total	100%	100%	100%
Extrapolated value	16%	18%	17%

Q23a. Do you monitor the security and privacy practices of third parties that you share sensitive or confidential consumer information on an ongoing basis?	US	UK	FY2018
Yes	40%	41%	40%
No	54%	55%	54%
Unsure	6%	4%	5%
Total	100%	100%	100%

Q23b. If yes, what monitoring procedures does your organization employ to ensure the adequacy of security and privacy practices? Please check all that apply.	US	UK	FY2018
Legal or procurement review	45%	50%	47%
Independent audit or verification by a third-party	25%	19%	23%
Automated monitoring tools	41%	35%	39%
Random tests or spot checks	26%	23%	25%
Annual self-certification	37%	41%	39%
Use of security ratings firms	25%	18%	22%
Other	4%	3%	4%
Unsure	2%	0%	1%
Total	205%	189%	199%

Q23c. If no, why doesn't your organization monitor the third parties' security and privacy practices? Please check all that apply.	US	UK	FY2018
We don't have the internal resources to check or verify	58%	63%	60%
We have confidence in the third party's ability to secure information	44%	35%	40%
We rely on the business reputation of the third party	39%	45%	41%
We have insurance that limits our liability in the event of a data breach	18%	16%	17%
The third party is subject to data protection regulations that are intended to protect our information	53%	52%	53%
The third party is subject to contractual terms	41%	49%	44%
The data shared with the third party is not considered sensitive or confidential	50%	50%	50%
The third party will not allow us to independently monitor or verify their security and privacy activities	61%	59%	60%
Other	4%	3%	4%
Unsure	2%	3%	2%
Total	370%	375%	372%

Q24. What information security control standard(s) does your organization use or plan to use? Please check all that apply.	US	UK	FY2018
NIST	54%	31%	45%
ISO 27001/27002	25%	21%	23%
PCI-DSS	45%	43%	44%
HIPAA/HiTrust CSF	12%	9%	11%
COBIT	28%	31%	29%
None of the above	25%	33%	28%
Other (please specify)	5%	6%	5%
Total	194%	174%	186%

Q25a. Does your third-party management program define and rank levels of risk?	US	UK	FY2018
Yes	60%	53%	57%
No	38%	42%	40%
Unsure	2%	5%	3%
Total	100%	100%	100%

Q25b. If yes, what are indicators of risk? Please check all that apply.	US	UK	FY2018
Failed IT security audits, verification or testing procedures	15%	11%	13%
Overall decline in the quality of the third party's services	79%	67%	74%
Discovery that the third party is using a subcontractor that has access to our company’s information	14%	12%	13%
Complaints from customers about privacy or security	30%	40%	34%
History of frequent data breach incidents	56%	45%	52%
Legal actions against the third party	47%	37%	43%
Negative media about the third party	21%	18%	20%
IT glitches, operational failures and stoppages	69%	66%	68%
Poorly written security and privacy policies and procedures	26%	21%	24%
Lack of security or privacy training for the third party's key personnel	11%	19%	14%
Lack of screening or background checks for key personnel hired by the third party	40%	45%	42%
High rate of identity fraud, theft or other cyber crimes within the third party's home country	15%	16%	15%
Lack of data protection regulation within the third party's home country	32%	34%	33%
Turnover of the third party's key personnel	72%	68%	70%
Outdated IT systems and equipment	39%	34%	37%
Other	5%	7%	6%
Total	571%	540%	559%

Q25c. If yes, how often are the risk levels updated?	US	UK	FY2018
Never	17%	18%	17%
As needed	41%	39%	40%
Every six months	16%	18%	17%
Annually	16%	16%	16%
Every two years	8%	9%	8%
Unsure	2%	0%	1%
Total	100%	100%	100%

Q26a. 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?	US	UK	FY2018
Yes	41%	36%	39%
No	48%	50%	49%
Unsure	11%	14%	12%
Total	100%	100%	100%

Q26b. If no, why? Please select all that apply.	US	UK	FY2018
Not a priority for the board	33%	29%	31%
Decisions about the third-party risk management program are not relevant to board members	39%	43%	41%
We only provide this information if a security incident or data breach has occurred involving a third party	34%	38%	36%
Unsure	4%	5%	4%
Total	110%	115%	112%

Part 4. Demographics and organizational characteristics

D1. What organizational level best describes your current position?	US	UK	FY2018
Senior Executive	5%	6%	5%
Vice President	3%	1%	2%
Director	16%	15%	16%
Manager	20%	23%	21%
Supervisor	15%	17%	16%
Staff/Technician	33%	30%	32%
Contractor	6%	7%	6%
Other	2%	1%	2%
Total	100%	100%	100%

D2. Check the **Primary Person** you report to within the organization.	US	UK	FY2018
CEO/executive committee	3%	2%	3%
Chief financial officer	7%	10%	8%
Chief information officer	18%	21%	19%
Chief information security officer	14%	12%	13%
Chief privacy officer	0%	2%	1%
Chief risk officer	10%	9%	10%
Chief security officer	5%	5%	5%
Compliance officer	16%	14%	15%
General counsel	8%	8%	8%
Head, procurement	9%	8%	9%
Line of business (LoB) management	10%	9%	10%
Other	0%	0%	0%
Total	100%	100%	100%

D3. What industry best describes your organization's industry focus?	US	UK	FY2018
Agriculture & food services	1%	0%	1%
Communications	2%	3%	2%
Consumer products	4%	6%	5%
Defense & aerospace	1%	0%	1%
Education & research	2%	1%	2%
Energy	6%	5%	6%
Entertainment & media	2%	3%	2%
Financial services	18%	17%	18%
Health & pharmaceutical	10%	8%	9%
Hospitality	3%	4%	3%
Industrial & manufacturing	10%	13%	11%
Public sector	9%	11%	10%
Retail	8%	9%	8%
Services	11%	10%	11%
Technology & software	8%	7%	8%
Transportation	3%	2%	3%
Other	2%	1%	2%
Total	100%	100%	100%

D4. What is the worldwide headcount of your organization?	US	UK	FY2018
Less than 500 people	11%	16%	13%
501 to 1,000 people	22%	31%	26%
1,001 to 5,000 people	28%	26%	27%
5,001 to 25,000 people	19%	16%	18%
25,001 to 75,000 people	11%	8%	10%
More than 75,000 people	9%	3%	7%
Total	100%	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.

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.

About Opus

Free your business

About Opus

Opus is a global risk and compliance SaaS and data solution provider, founded on a simple premise: that faster, better decisions in compliance and risk management give businesses an extraordinary advantage in the marketplace.

Today, the world's most respected global corporations rely on Opus to free their business from the complexity and uncertainty of managing customer, supplier and third-party risks. By combining the most innovative SaaS platforms with unparalleled data solutions, Opus turns information into action so businesses thrive.

For more information about Opus, please visit www.opus.com.