Data Risk in the Third-Party Ecosystem

Sponsored by BuckleySandler LLP & Treliant Risk Advisors LLC

Independently conducted by Ponemon Institute LLC

Publication Date: April 2016

Ponemon Institute© Research Report

Data Risk in the Third-Party Ecosystem

Ponemon Institute, March 2016

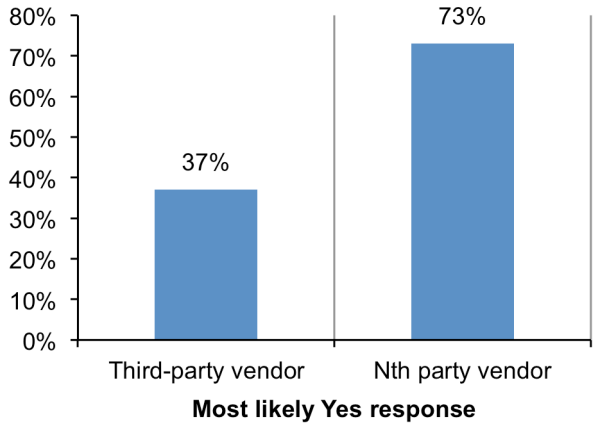
Part 1. Introduction

BuckleySandler LLP and Treliant Risk Advisors LLC sponsored *Data Risk in the Third-Party Ecosystem* study to understand the challenges companies face in protecting sensitive and confidential information shared with third parties. Many companies have both direct and indirect relationships from third parties, fourth parties to N[th1] parties that are important to fulfilling business functions or operations. The study reveals the difficulty companies have in mitigating, detecting and minimizing risks associated with third parties that have access to their sensitive or confidential information.

We surveyed 598 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 vendor 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.

As shown in Figure 1, 37 percent of respondents do not believe their primary third party vendor would notify them if it experienced a data breach involving sensitive and confidential information. Worse, 73 percent of respondents do not believe an N[th] party vendor would notify them if they had a data breach.

Figure 1. Would a vendor fail to notify you if it had a data breach involving your company's sensitive or confidential information?



The following research findings reveal the risk to data in the third-party ecosystem.

- Companies are not able to confirm if third parties have had a data breach or cyber attack involving their sensitive and confidential information.
- Companies are not able to determine the number of third parties with access to their confidential information and how many of these third parties are sharing this data with one or more vendors.
- There is a lack of confidence in third parties' data safeguards, security policies and procedures and if their security posture is sufficient to respond to a data breach or cyber attack.
- Companies rarely conduct reviews of vendor management policies and programs to ensure they address third-party data risk. In addition, a lack of resources makes it difficult for organizations to have a robust vendor management program to manage N[th] party relationships.

[1] N[th] is used to refer to an unknown number in a series of numbers.

- Accountability for the correct handling of an organization's third-party risk management program is decentralized. Similarly, no one department or function is responsible for ensuring that appropriate privacy and security language is included in all vendor contracts.

- Senior leadership and boards of directors are rarely involved in third-party risk management and often do not require assurances that third-party risk is being assessed, managed and monitored.

- Companies rely upon contractual agreements instead of audits and assessments to evaluate the security and privacy practices of third parties.

Part 2. Key findings

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:

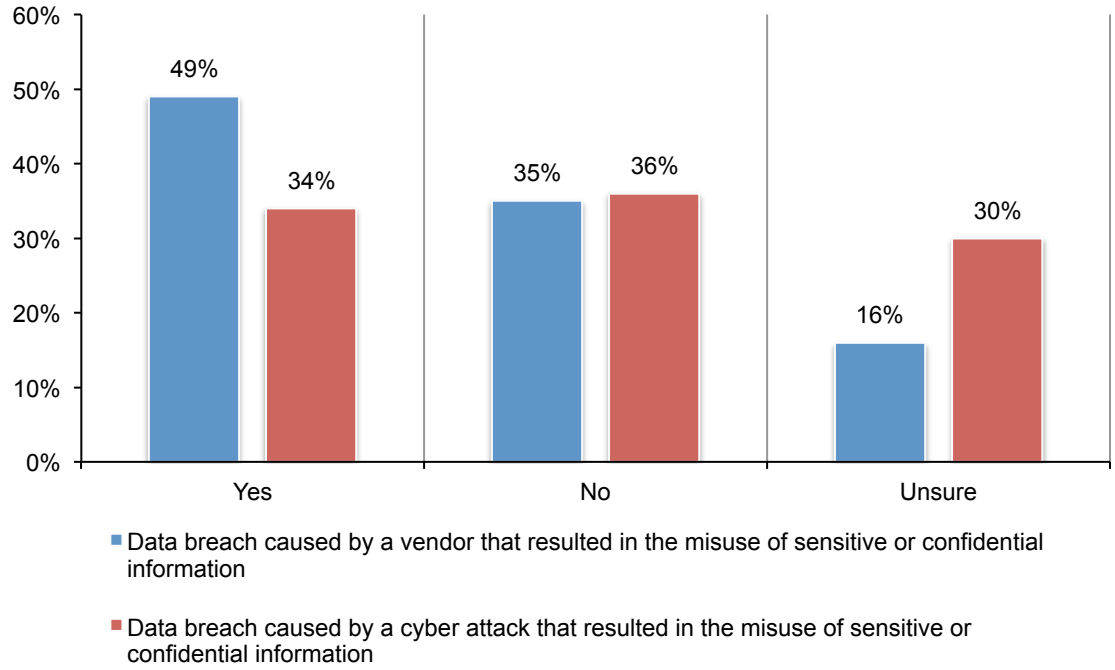
- Data breaches and the associated third-party data risk
- Strategic shortfalls in third-party risk management governance
- Companies do not know how many third parties have access to their confidential data
- The reality of third-party risk management in today's organizations

Data breaches and the associated third-party data risk

Companies are often uncertain if their third parties had a data breach. As discussed previously, respondents are not certain vendors would notify their companies if it had a data breach. Approximately half of respondents (49 percent) confirm their organization experienced a data breach caused by one of their vendors but 16 percent are unsure, as shown in Figure 2.

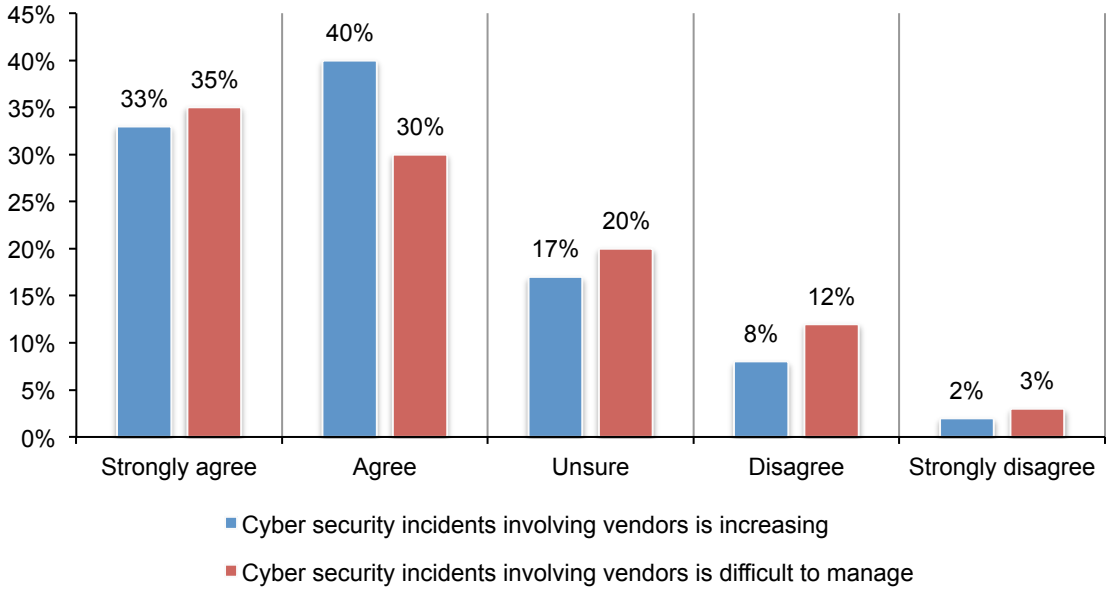
The uncertainty is even higher with regard to a data breach caused by a cyber attack. While 34 percent of respondents say their organization had a data breach caused by a cyber attack against one of their third parties that resulted in the misuse of their company's sensitive or confidential information, an almost equal percentage of respondents (30 percent) are unsure.

Figure 2. Has your organization experienced a data breach or cyber attack?



The number of cybersecurity incidents involving third parties is increasing. As shown in Figure 3, 73 percent of respondents see the number of cybersecurity incidents involving vendors increasing (33 + 40 percent of respondents). Sixty-five percent of respondents also say it is difficult to manage cybersecurity incidents involving vendors (35 + 30 percent of respondents).

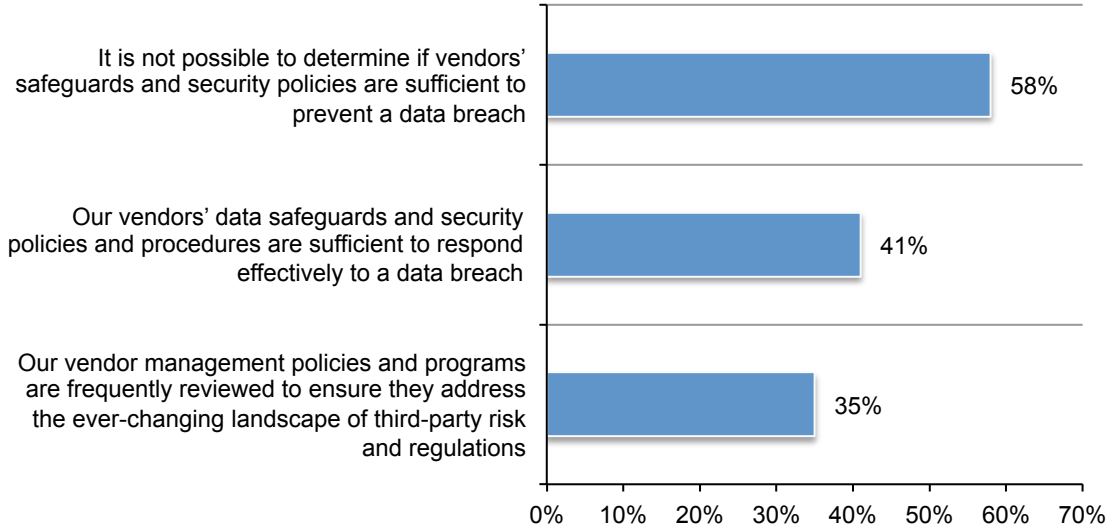
Figure 3. Cybersecurity incidents are increasing and difficult to manage



Respondents admit they are sharing sensitive data with third parties that might have poor security policies. Fifty-eight percent of respondents say they are not able to determine if vendors' safeguards and security policies are sufficient to prevent a data breach. Only 41 percent of respondents say their vendors' data safeguards and security policies and procedures are sufficient to respond effectively to a data breach.

However, respondents admit they are not addressing the problem of third parties inability to respond to data breaches or cyber attacks. Only 35 percent of respondents say a frequent review of vendor management policies is conducted to make sure they address the ever-changing landscape of third-party risk.

Figure 4. Perceptions about vendors' security policies and procedures
Strongly agree and agree responses combined



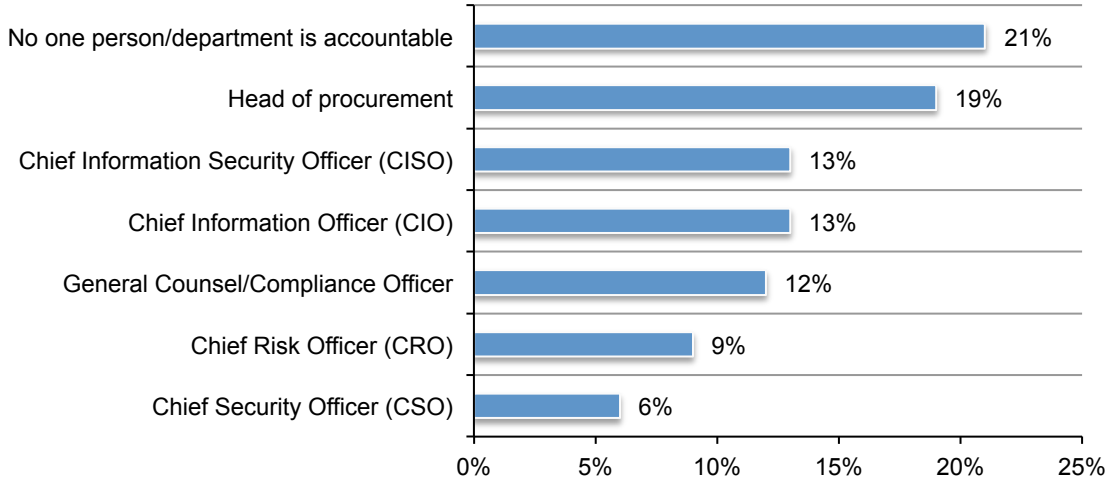
Strategic shortfalls in third-party risk management governance

Companies need to strengthen the governance practices of their vendor management programs. Only 31 percent of respondents rate the effectiveness of their vendor risk management program as highly effective. Possible reasons are shown in Figure 5. Only 38 percent of respondents say their organizations establish and track metrics regarding the effectiveness of the vendor risk management program and less than half (48 percent of respondents) have a vendor risk management committee.

Figure 5. Is the effectiveness of the vendor risk management program measured and is there a vendor risk management committee?

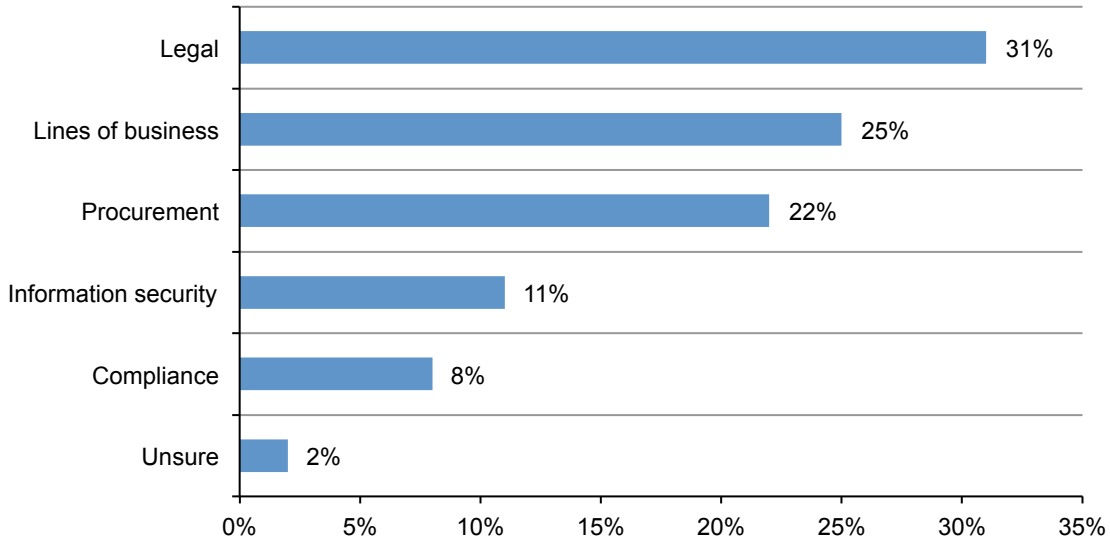
There is no clear accountability for the correct handling of the third-party risk management program. According to Figure 6, 21 percent say there is no one person/department who is accountable. Some respondents say the following are accountable: head of procurement (19 percent), chief information officer (13 percent), chief information security officer (13 percent) and general counsel or compliance (12 percent).

Figure 6. Who is most accountable for the correct handling of the organization's vendor risk management program?
More than one response permitted



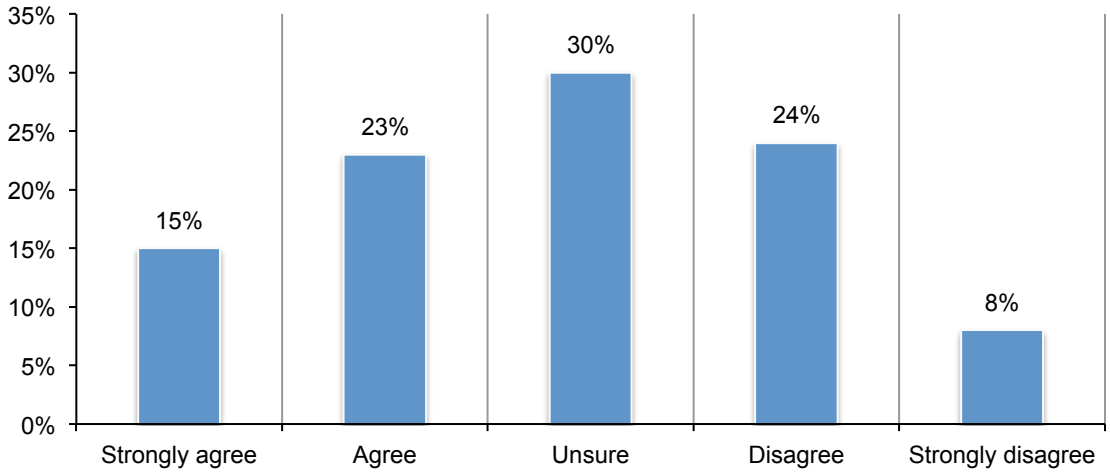
The departments most responsible for ensuring that privacy and security language is included in all contracts with third parties are: legal (31 percent of respondents), lines of business (25 percent of respondents), procurement (22 percent of respondents) and information security (11 percent of respondents), according to Figure 7.

Figure 7. Which department or function is responsible for ensuring that appropriate privacy and security language is included in all vendor contracts?



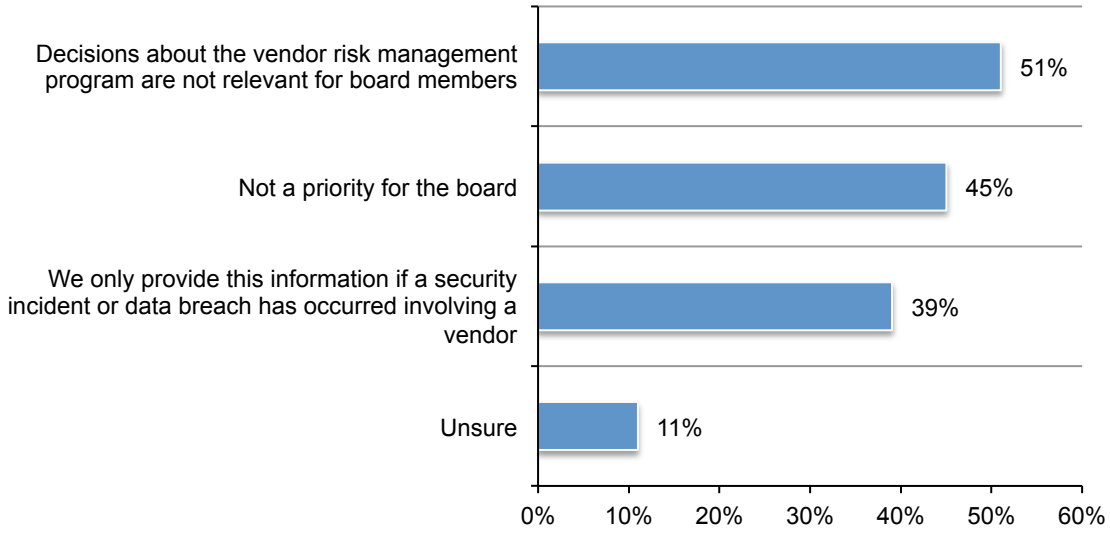
Boards of directors are not involved in third party risk management programs. As shown in Figure 8, 62 percent of respondents (30 + 24 + 8 percent) say their boards of directors do not require assurances that vendor risk is being assessed, managed or monitored appropriately, or they are unsure.

Figure 8. Our board of directors requires assurances that third party risk is being assessed, managed and monitored



As a consequence, only 31 percent of respondents say their company regularly reports to the board of directors on the effectiveness of the vendor management program and potential risks to the organization. The majority of respondents (51 percent) say decisions about third-party risk management is not relevant for the board of directors, as shown in Figure 9. Forty-five percent of respondents believe it is not a priority or it is only relevant if a security breach has occurred involving a vendor (39 percent of respondents).

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



Companies do not know how many third parties have access to their confidential data

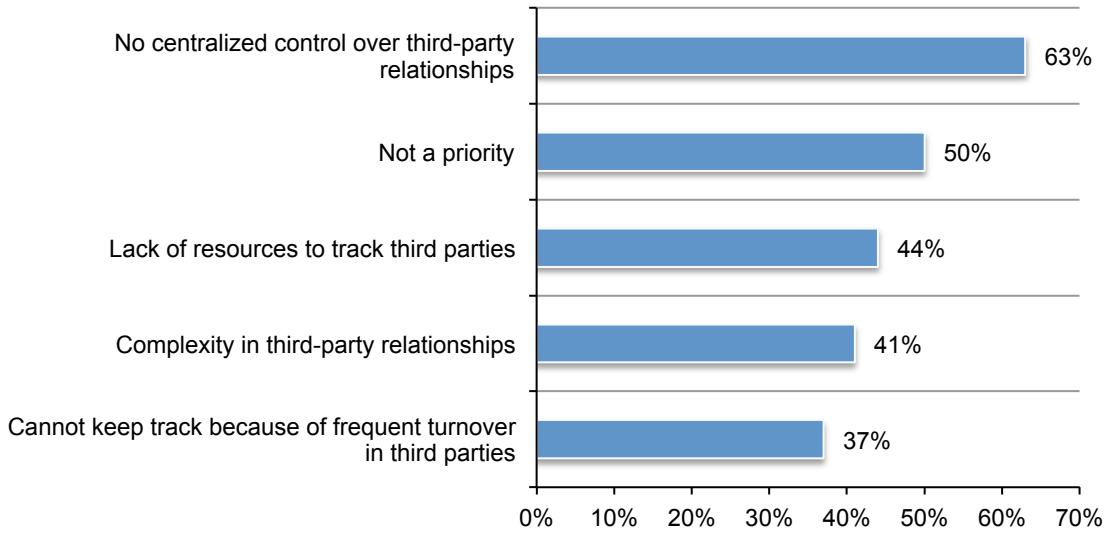
To address the risk, companies should have an inventory of all third-party vendors. Few companies represented in this research are trying to address this risk by creating a comprehensive inventory of all third parties. Sixty-seven percent of respondents say they do not have (60 percent) or are unsure (7 percent) if their company has such an inventory.

Companies with a third-party inventory admit it is not comprehensive**.** Thirty-three percent of respondents say their company does have an inventory of all third parties that have access to their sensitive or confidential information. However, only 18 percent of these companies say the inventory includes all possible vendors with access to their sensitive or confidential information. The average number of third parties in these inventories is 378.

According to Figure 10, 63 percent of respondents blame a lack of centralized control over third-party relationships as a reason for not having a comprehensive inventory and 50 percent say it is not a priority. Other reasons are a lack of resources to track third parties (44 percent of respondents), complexity of these relationships (41 percent of respondents) and inability to keep track because of frequent turnover in third parties (37 percent of respondents).

Respondents believe about 37 percent of their primary vendors are sharing sensitive and confidential information with other vendors (N^{th} party risk), but very few (33 percent of respondents) say they are notified if such sharing is taking place

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

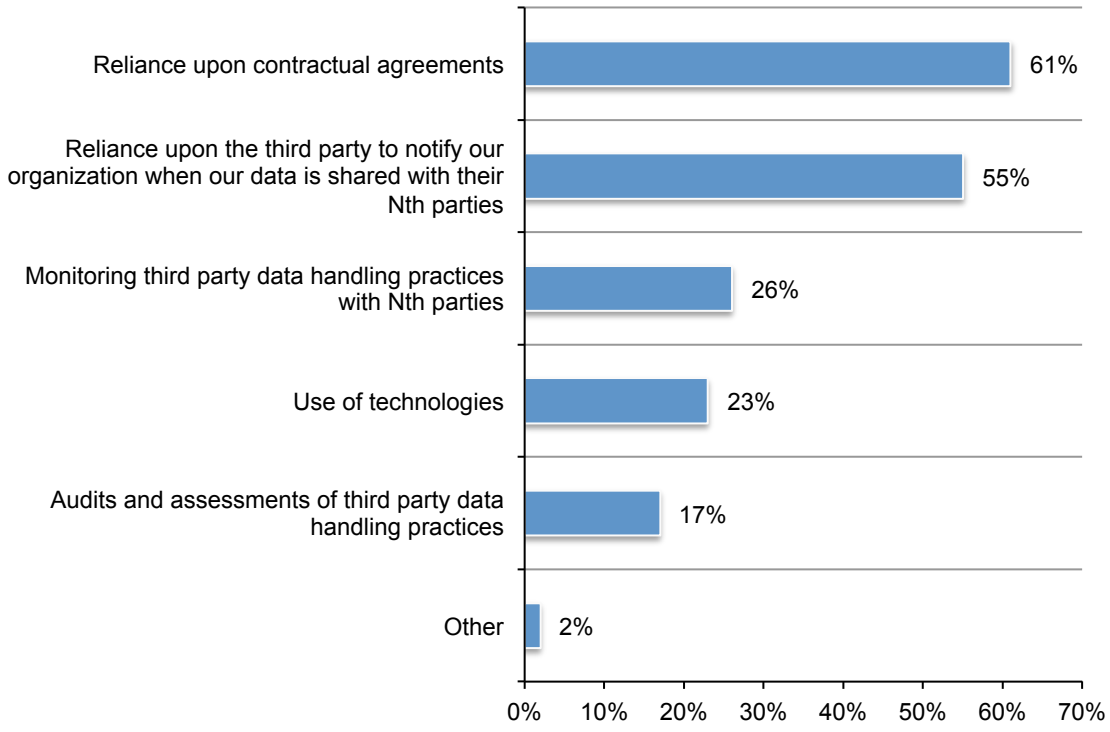


.

Companies lack visibility into Nth party vendors that have their sensitive or confidential data. Only 20 percent of respondents say their companies know how their information is being accessed or processed by vendors with whom they have no direct relationship.

According to Figure 11, 61 percent of these respondents say they have visibility into vendors' practices due to reliance upon contractual agreements and 55 percent rely upon the third party to notify their organization when their data is shared with their Nth parties.

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

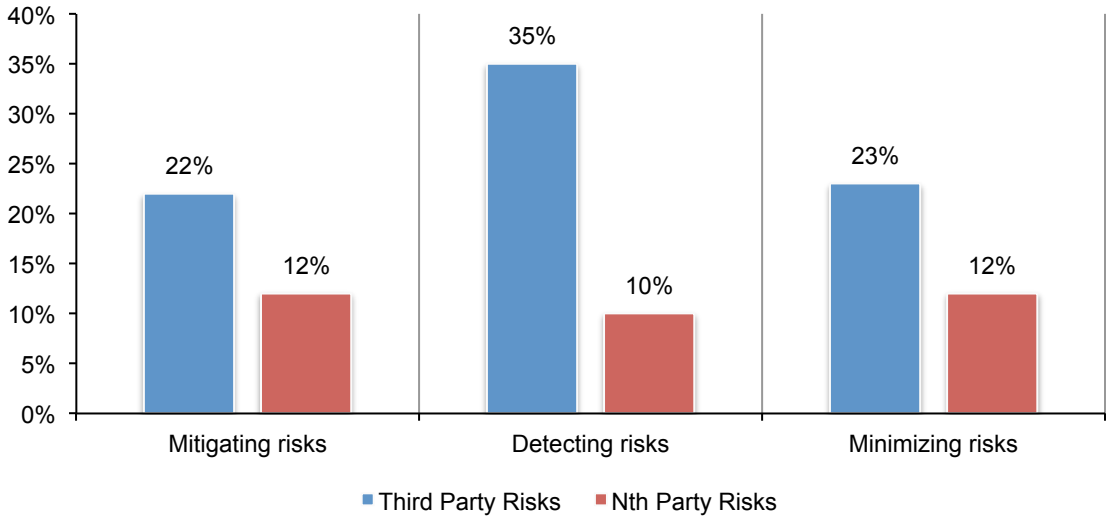


The reality of third-party risk management in today's organizations

Companies are not effective in mitigating, detecting or minimizing both third party and Nth party risks. Figure 12 presents the level of effectiveness in dealing with third party and Nth party risks. Only 22 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.

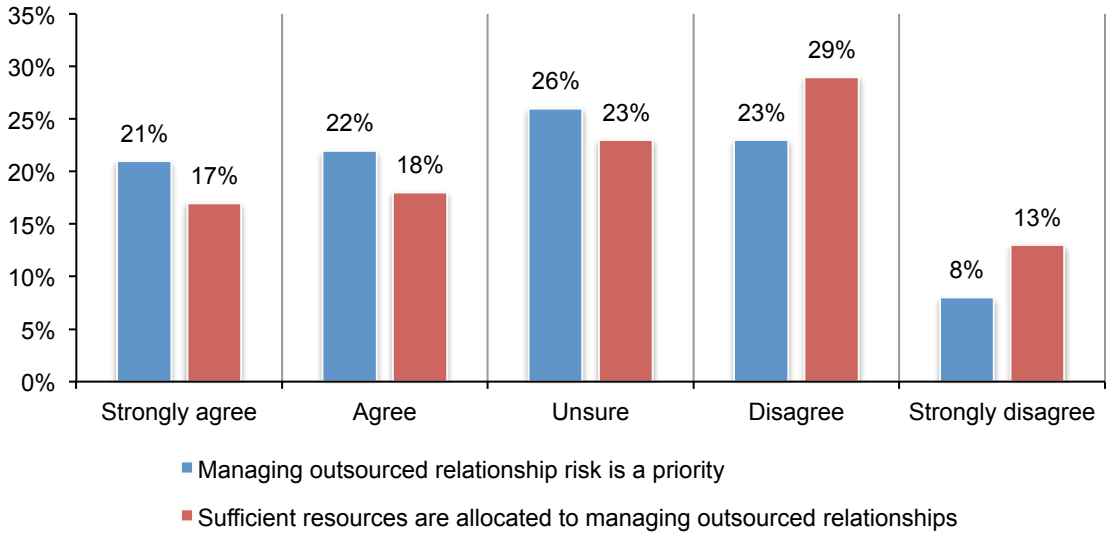
A higher percentage (35 percent) of respondents say their organization is highly effective in detecting third party risks, but only 10 percent of respondents rate the detection of Nth party risks as highly effective. Twenty-three percent of respondents rate their organization's effectiveness in minimizing third party risks as highly effective and only 12 percent rate their effectiveness in minimizing Nth party risks as highly effective.

Figure 12. How effective are organizations in dealing with third party and Nth party risks?
Percentage of respondents who selected 7, 8, 9 or 10 on a 10-point effectiveness scale



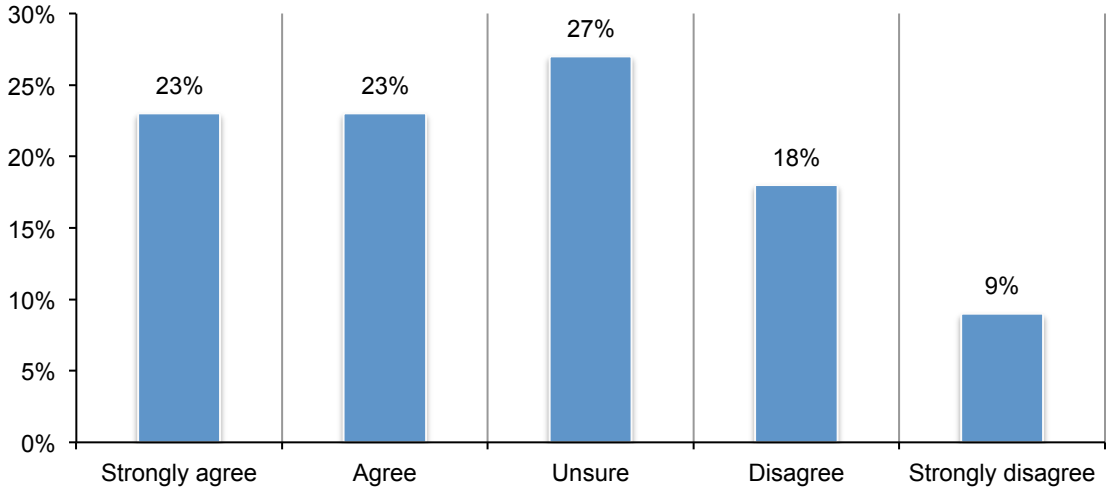
Organizations lack the resources to manage risks from outsourcing sensitive or confidential information According to Figure 13, 57 percent of respondents (26 + 23 + 8 percent) say addressing this risk is not a priority or they are unsure. Because it is not a priority, only 35 percent of respondents say enough resources are made available to manage outsourced relationships.

Figure 13. Perceptions about the management of outsourced relationships



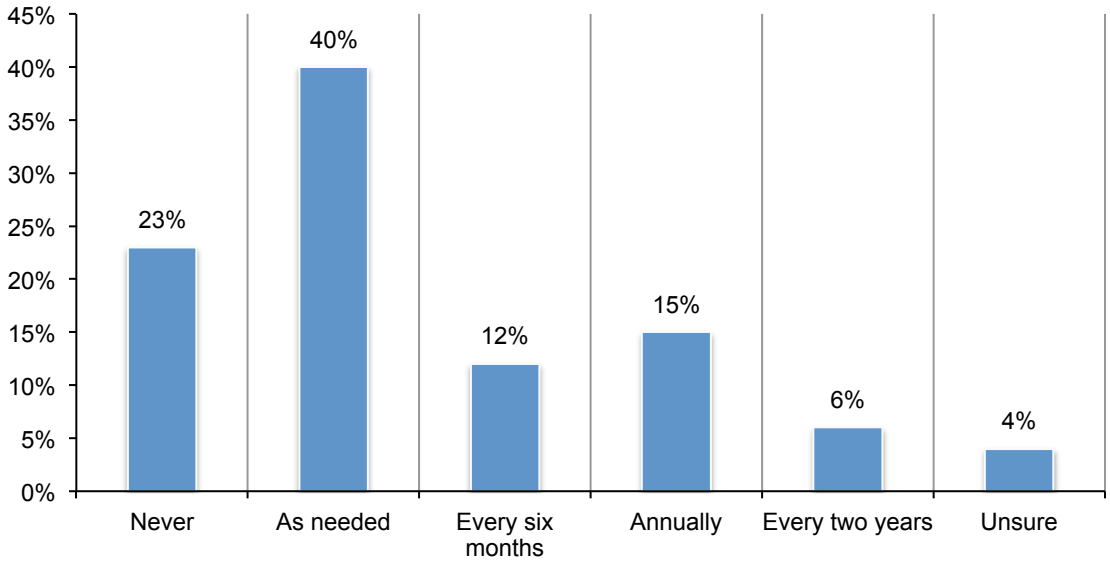
Most companies do not determine an acceptable level of third party risk. According to Figure 14**,** most respondents say their organizations have not determined the acceptable level of security risk from their vendors to meet business objectives (27 percent of respondents) or they are unsure (27 percent of respondents).

Figure 14. Our organization has determined the acceptable level of security risk from vendors



While 52 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. Moreover, 63 percent of respondents say risk levels are only updated as needed (40 percent) or never (23 percent), as shown in Figure 15.

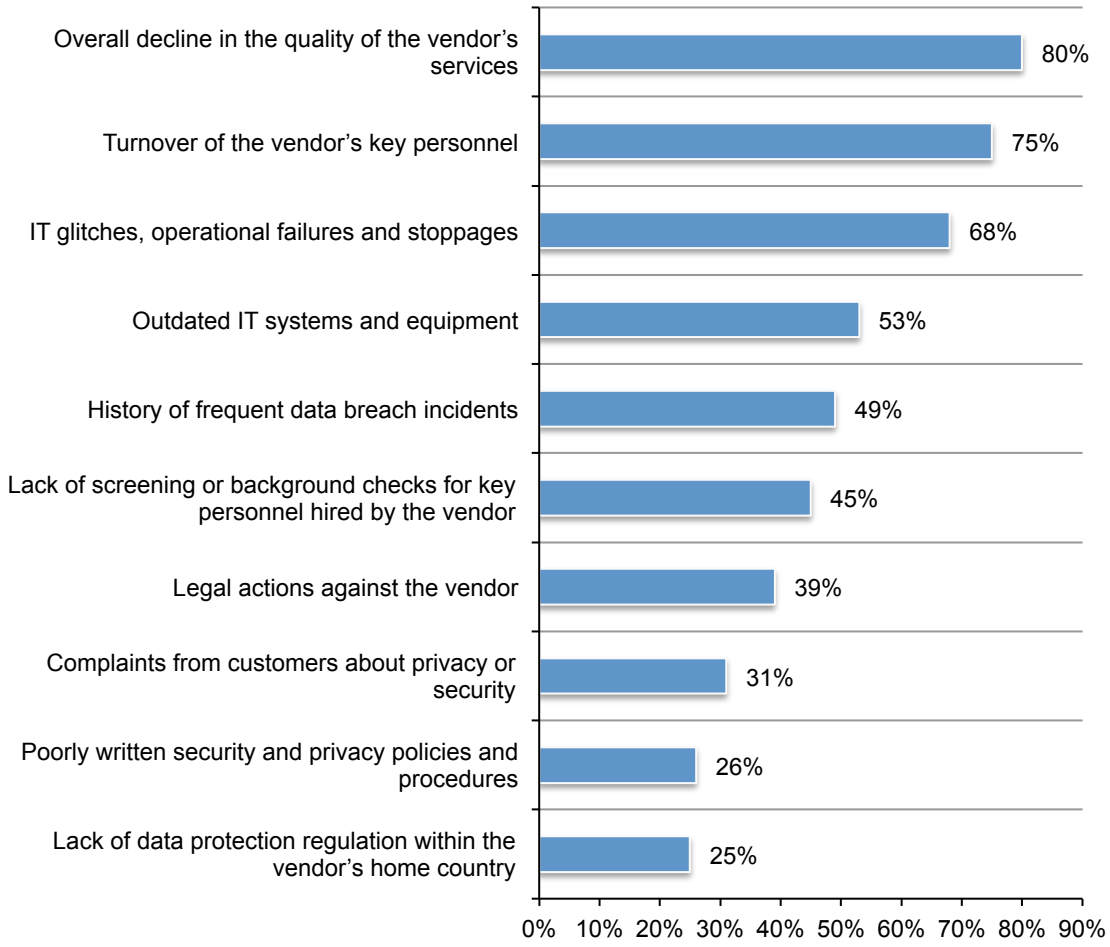
Figure 15. Third party risk levels are rarely updated



The most important indicator of risk, according to 80 percent of respondents, is the overall decline in the quality of the third party's services and 75 percent say it is the turnover of the third party's key personnel, as shown in Figure 16.

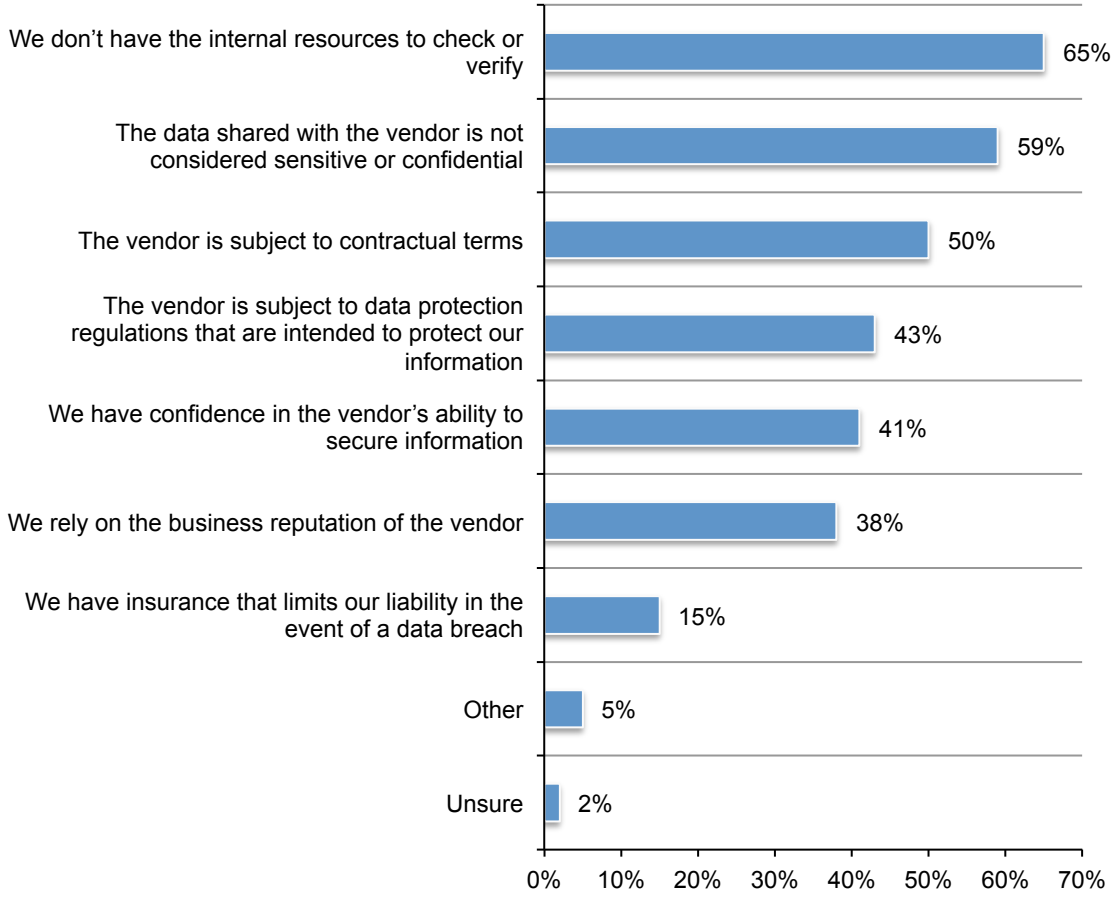
Only 31 percent say complaints from customers about privacy or security are a risk indicator and only 16 percent of respondents say that either discovery that the third party is using a subcontractor that has access to their company's information or a failed IT security audit would be an indicator of risk.

Figure 16. Indicators of third-party risk
More than one response permitted



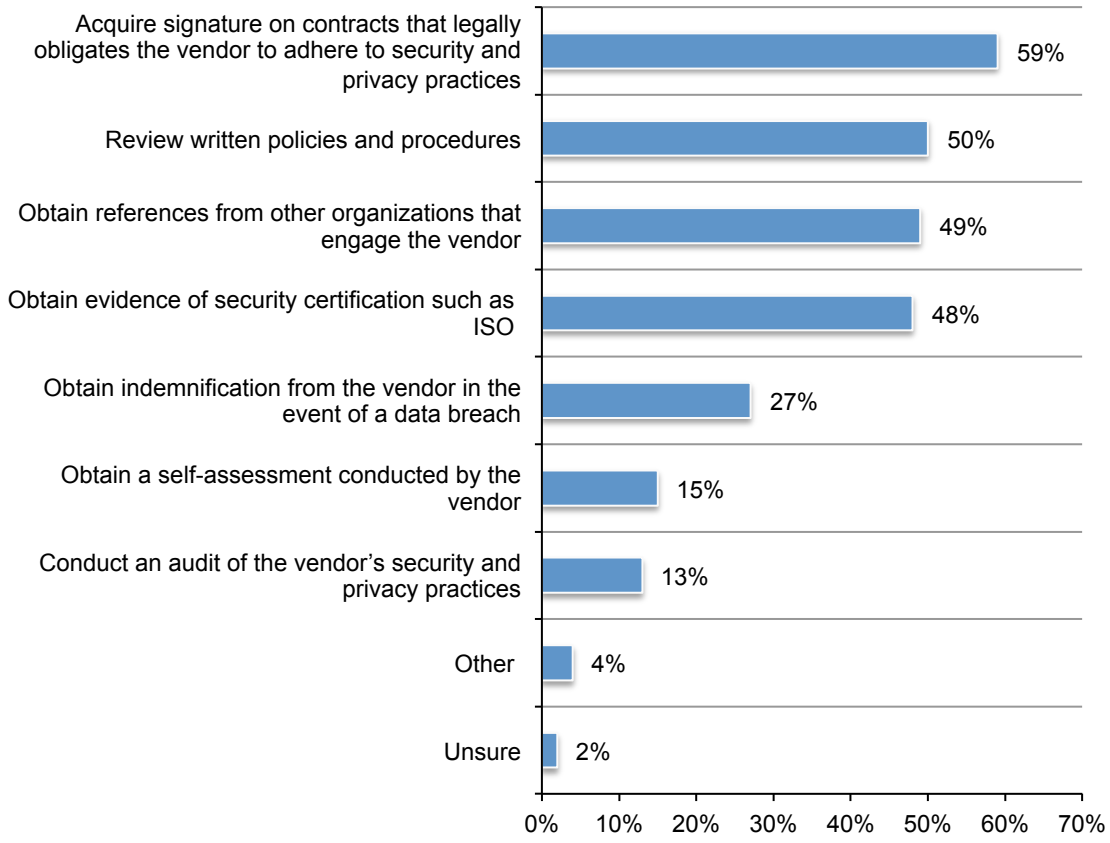
Companies are relying upon contractual arrangements to evaluate third parties. Only 38 percent of respondents say that before starting a business relationship that requires the sharing of sensitive or confidential information their company evaluates the security and privacy practices of all vendors. Figure 17 shows why organizations are not performing evaluations.

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



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 (59 percent of respondents) or they review written policies and procedures (50 percent of respondents), as shown in Figure 18. Rarely does the evaluation consist of conducting an audit of the vendor's security and privacy practices (13 percent of respondents) or obtaining indemnification from the third party in the event of a data breach (27 percent of respondents).

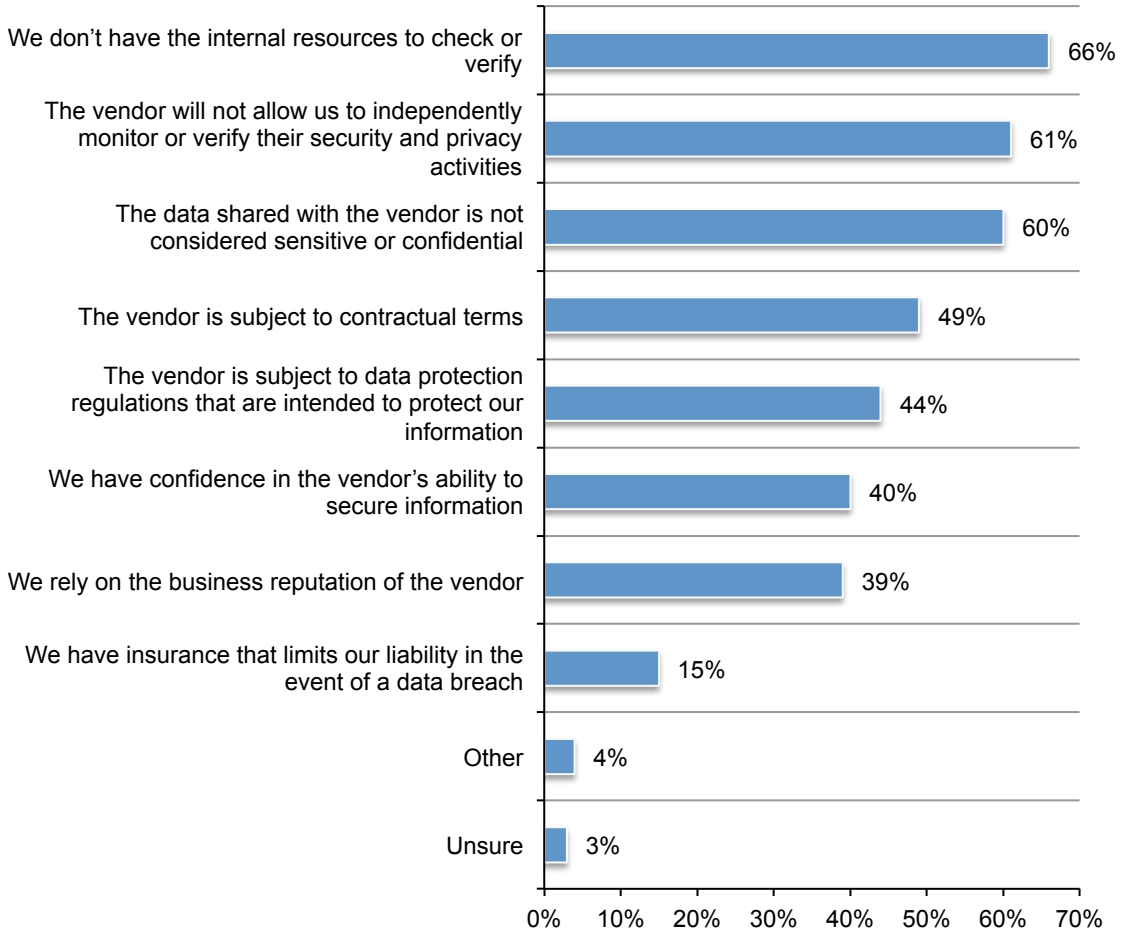
Figure 18. Steps taken to evaluate third parties
More than one response permitted



Companies are not evaluating or monitoring the privacy and security practices of third parties. Sixty percent of respondents say their companies do not monitor the security and privacy practices of vendors with whom they share sensitive or confidential information.

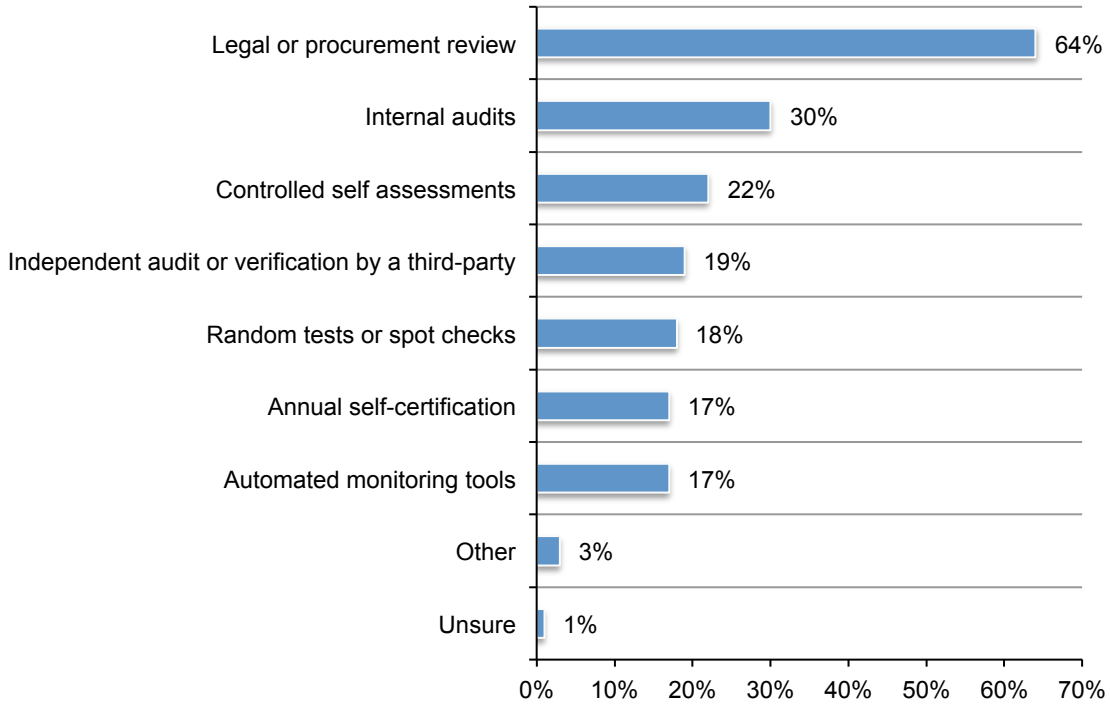
As shown in Figure 19, the primary reasons for not monitoring are: not having the internal resources to check or verify (66 percent of respondents), the third party will not allow us to independently monitor or verify their security and privacy activities (61 percent of respondents) and the data shared with the vendor is not considered sensitive or confidential (60 percent of respondents).

Figure 19. Reasons for not monitoring security and privacy practices
More than one response permitted



According to Figure 20, companies that monitor to ensure the adequacy of security and privacy practices rely upon legal or procurement review (64 percent of respondents), internal audits (30 percent of respondents) or controlled self-assessments (22 percent of respondents).

Figure 20. Third party monitoring procedures used to ensure the adequacy of security and privacy practices
More than one response permitted



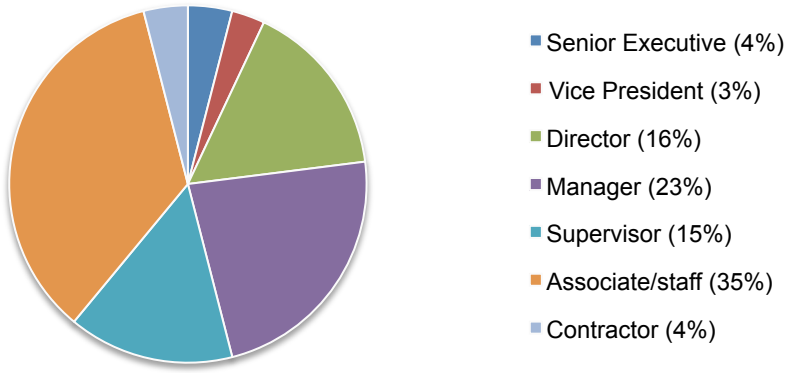
Part 3. Methods

A sampling frame of 15,480 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 679 total returns. Screening and reliability checks required the removal of 81 surveys. Our final sample consisted of 598 surveys or a 3.9 percent response.

Table 1. Sample response	Freq	Pct%
Sampling frame	15,480	100.0%
Total returns	679	4.4%
Rejected or screened surveys	81	0.5%
Final sample	598	3.9%

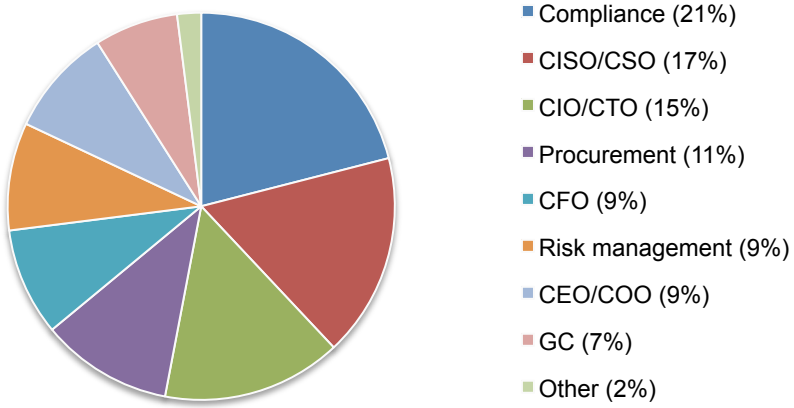
Pie Chart 1 reports the respondents' organizational levels within the participating organizations. By design, more than half of the respondents (61 percent) are at or above the supervisory levels.

Pie Chart 1. Current position within the organization



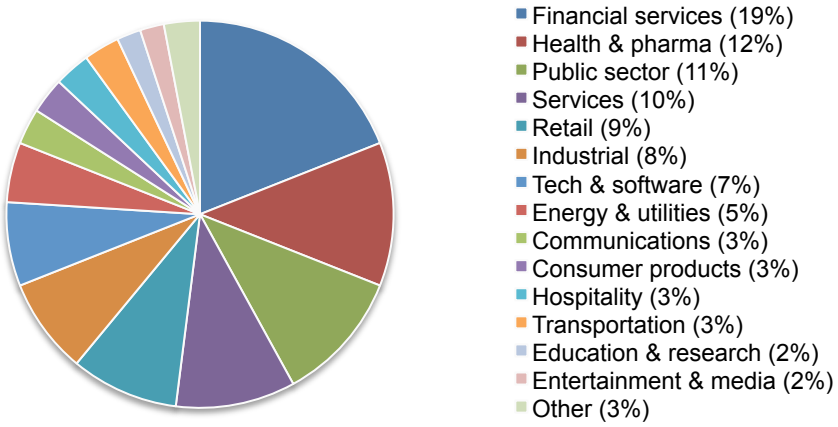
As shown in Pie Chart 2, 21 percent of respondents report to the compliance officer, 15 percent report to the CIO and 14 percent indicated they report to the CISO.

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



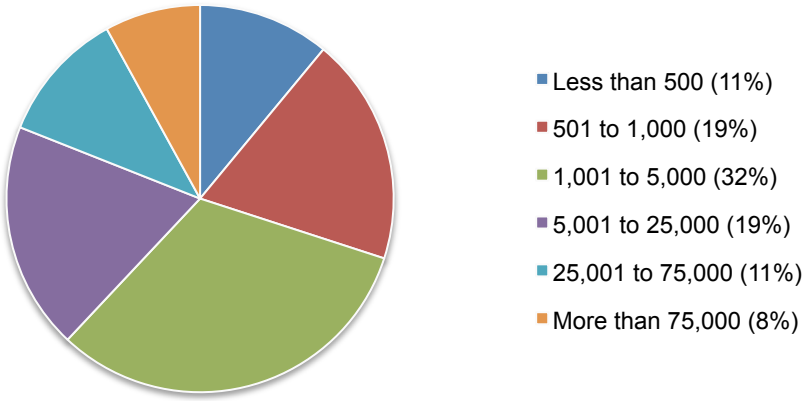
Pie Chart 3 reports the industry segments of respondents' organizations. This chart identifies financial services (19 percent) as the largest segment, followed by health and pharmaceutical (12 percent), public sector (11 percent), and services (10 percent).

Pie Chart 3. Industry distribution of respondents' organizations



As shown in Pie Chart 4, 70 percent of respondents are from organizations with a global headcount of more than1,000 employees.

Pie Chart 4. Worldwide headcount of the organization



Part 4. Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals 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 December 2015.

Survey response	Freq	Pct%
Sampling frame	15,480	100.0%
Total returns	679	4.4%
Rejected or screened surveys	81	0.5%
Final sample	598	3.9%

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

S2. Does your company have a vendor data risk management program?	Pct%
Yes	100%
No (Stop)	0%
Total	100%

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

Part 1: Background

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

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

Q1c. If yes to one or both of the questions above, did you make any changes to your company's vendor risk management program?	Pct%
Yes	45%
No	50%
Unsure	5%
Total	100%

Q2a. How confident are you that your primary vendor would notify you if they had a data breach involving your company's sensitive and confidential information? 1 = not confident to 10 = highly confident	Pct%
1 or 2	12%
3 or 4	25%
5 or 6	32%
7 or 8	21%
9 or 10	10%
Total	100%
Extrapolated value	5.34

Q2b. How confident are you that an N^{th} party vendor would notify you or your primary vendor if they had a data breach involving your company's sensitive and confidential information? 1 = not confident to 10 = highly confident	Pct%
1 or 2	33%
3 or 4	40%
5 or 6	14%
7 or 8	8%
9 or 10	5%
Total	100%
Extrapolated value	3.74

Q3. Who is most accountable for the correct handling of your organization's vendor risk management program?	Pct%
No one person/department is accountable	21%
Head of procurement	19%
Chief Information Officer (CIO)	13%
Chief Information Security Officer (CISO)	13%
General Counsel/Compliance Officer	12%
Chief Risk Officer (CRO)	9%
Chief Security Officer (CSO)	6%
Chief Technology Officer (CTO)	3%
Chief Privacy Officer (CPO)	1%
Head of business continuity management	1%
Head of human resources	0%
Unsure	2%
Total	100%

Q4. Do vendors notify your organization when your data is shared with the N^{th} parties?	Pct%
Yes	33%
No	60%
Unsure	7%
Total	100%

Q5. Does your organization establish and track metrics regarding the effectiveness of the vendor risk management program?	Pct%
Yes	38%
No	57%
Unsure	5%
Total	100%

Q6. Does your organization have a vendor risk management committee?	Pct%
Yes	48%
No	50%
Unsure	2%
Total	100%

Q7. Which department/function is responsible for ensuring appropriate privacy and security language is included in all contracts with vendors?	Pct%
Legal	31%
Lines of business	25%
Procurement	22%
Information security	11%
Compliance	8%
Unsure	2%
Other (please specify)	1%
None of the above	0%
Total	100%

Q8a. Does your company have a comprehensive inventory of all third parties with whom it shares sensitive and confidential information?	Pct%
Yes (Proceed to Q9.)	33%
No	60%
Unsure	7%
Total	100%

Q8b. If no or unsure, why? Please check all that apply	Pct%
No centralized control over third-party relationships	63%
Not a priority	50%
Lack of resources to track third parties	44%
Complexity in third-party relationships	41%
Cannot keep track because of frequent turnover in third parties	37%
Total	235%

Q9. If yes, how many third parties are in this inventory?	Pct%
Less than 10	0%
11 to 20	1%
21 to 30	2%
31 to 40	8%
41 to 50	11%
51 to 75	19%
76 to 100	12%
101 to 300	8%
301 to 500	7%
501 to 1,000	18%
1,000+	14%
Total	100%
Extrapolated value	378

Q10a. Does the inventory of third parties include all the vendors (i.e. N^{th} party risk) your company has a relationship with that might have access to your company's sensitive and confidential data?	Pct%
Yes	18%
No	77%
Unsure	5%
Total	100%

Q10b. If yes, what percentage of these vendors (i.e., N^{th} party risk) do you believe have access to your sensitive and confidential information?	Pct%
None	1%
Less than 10%	2%
11% to 20%	16%
21% to 50%	21%
51% to 75%	29%
76% to 100%	31%
Total	100%
Extrapolated value	55%

Q11. What percentage of all vendors do you believe are outsourcing your sensitive and confident data to N^{th} parties?	Pct%
None	0%
Less than 10%	5%
11% to 20%	26%
21% to 50%	45%
51% to 75%	18%
76% to 100%	6%
Total	100%
Extrapolated value	37%

Q12a. Do you have visibility into vendors your company does not have a direct relationship with but that access your company's sensitive and confidential information (N^{th} parties)?	Pct%
Yes	20%
No	71%
Unsure	9%
Total	100%

Q12b. If yes, how do you achieve visibility? Please check all that apply.	Pct%
Monitoring third party data handling practices with N^{th} parties	26%
Audits and assessments of third party data handling practices	17%
Reliance upon the third party to notify our organization when our data is shared with their N^{th} parties	55%
Reliance upon contractual agreements	61%
Use of technologies	23%
Other (please specify)	2%
Total	184%

Q13a. Using the following 10-point scale, please rate how effective your organization is in mitigating third party risks.	Pct%
1 or 2	12%
3 or 4	21%
5 or 6	45%
7 or 8	17%
9 or 10	5%
Total	100%
Extrapolated value	5.14

Q13b. Using the following 10-point scale, please rate how effective your organization is in mitigating Nth party risks.	Pct%
1 or 2	27%
3 or 4	42%
5 or 6	19%
7 or 8	8%
9 or 10	4%
Total	100%
Extrapolated value	3.90

Q14a. Using the following 10-point scale, please rate how effective your organization is in detecting third party risks.	Pct%
1 or 2	15%
3 or 4	23%
5 or 6	27%
7 or 8	23%
9 or 10	12%
Total	100%
Extrapolated value	5.38

Q14b. Using the following 10-point scale, please rate how effective your organization is in detecting Nth party risks.	Pct%
1 or 2	40%
3 or 4	43%
5 or 6	7%
7 or 8	7%
9 or 10	3%
Total	100%
Extrapolated value	3.30

Q15a. Using the following 10-point scale, please rate your organization's effectiveness in **minimizing** third party risks.	Pct%
1 or 2	11%
3 or 4	20%
5 or 6	46%
7 or 8	18%
9 or 10	5%
Total	100%
Extrapolated value	5.22

Q15b. Using the following 10-point scale, please rate your organization's effectiveness in **minimizing** Nth party risks.	Pct%
1 or 2	29%
3 or 4	41%
5 or 6	18%
7 or 8	9%
9 or 10	3%
Total	100%
Extrapolated value	3.82

Q16. Using the following 10-point scale, please rate the effectiveness of your organization's vendor risk management program.	Pct%
1 or 2	19%
3 or 4	12%
5 or 6	38%
7 or 8	23%
9 or 10	8%
Total	100%
Extrapolated value	5.28

Part 2. Attributions

Q17. Managing outsourced relationship risk is a priority in our organization.	Pct%
Strongly agree	21%
Agree	22%
Unsure	26%
Disagree	23%
Strongly disagree	8%
Total	100%

Q18. Our organization allocates sufficient resources to managing outsourced relationships.	Pct%
Strongly agree	17%
Agree	18%
Unsure	23%
Disagree	29%
Strongly disagree	13%
Total	100%

Q19. Our organization has determined the acceptable level of security risk from our vendors in order to meet our business objectives.	Pct%
Strongly agree	23%
Agree	23%
Unsure	27%
Disagree	18%
Strongly disagree	9%
Total	100%

Q20. Our board of directors requires assurances that vendor risk is being assessed, managed and monitored appropriately.	Pct%
Strongly agree	15%
Agree	23%
Unsure	30%
Disagree	24%
Strongly disagree	8%
Total	100%

Q21. The number of cybersecurity incidents involving vendors is increasing.	Pct%
Strongly agree	33%
Agree	40%
Unsure	17%
Disagree	8%
Strongly disagree	2%
Total	100%

Q22. The number of cybersecurity incidents involving vendors is difficult to manage.	Pct%
Strongly agree	35%
Agree	30%
Unsure	20%
Disagree	12%
Strongly disagree	3%
Total	100%

Q23. Our vendors' data safeguards and security policies and procedures are sufficient to respond effectively to a data breach.	Pct%
Strongly agree	21%
Agree	20%
Unsure	33%
Disagree	19%
Strongly agree	7%
Total	100%

Q24. It is not possible to determine if vendors' safeguards and security policies are sufficient to prevent a data breach.	Pct%
Strongly agree	25%
Agree	33%
Unsure	19%
Disagree	18%
Strongly agree	5%
Total	100%

Q25. Our vendor management policies and programs are frequently reviewed to ensure they address the ever-changing landscape of third-party risk and regulations.	Pct%
Strongly agree	17%
Agree	18%
Unsure	25%
Disagree	26%
Strongly agree	14%
Total	100%

Part 3. Secure outsourcing management

Q26a. Do you evaluate the security and privacy practices of all vendors (i.e. from third to Nth vendors) before you engage them in a business relationship that requires the sharing of sensitive or confidential information?	Pct%
Yes	38%
No	54%
Unsure	8%
Total	100%

Q26b. If yes, how do you perform this evaluation? Please check all that apply.	Pct%
Review written policies and procedures	50%
Acquire signature on contracts that legally obligates the vendor to adhere to security and privacy practices	59%
Obtain indemnification from the vendor in the event of a data breach	27%
Conduct an audit of the vendor's security and privacy practices	13%
Obtain a self-assessment conducted by the vendor	15%
Obtain references from other organizations that engage the vendor	49%
Obtain evidence of security certification such as ISO	48%
Other (please specify)	4%
Unsure	2%
Total	267%

Q26c. If no, why don't you perform an evaluation? Please check all that apply.	Pct%
We don't have the internal resources to check or verify	65%
We have confidence in the vendor's ability to secure information	41%
We rely on the business reputation of the vendor	38%
We have insurance that limits our liability in the event of a data breach	15%
The vendor is subject to data protection regulations that are intended to protect our information	43%
The vendor is subject to contractual terms	50%
The data shared with the vendor is not considered sensitive or confidential	59%
Other	5%
Unsure	2%
Total	318%

Q27a. Do you monitor the security and privacy practices of vendors that you share sensitive or confidential consumer information on an ongoing basis?	Pct%
Yes	40%
No	52%
Unsure	8%
Total	100%

Q27b. If yes, what monitoring procedures does your organization employ to ensure the adequacy of security and privacy practices? Please check all that apply.	Pct%
Legal or procurement review	64%
Internal audits	30%
Independent audit or verification by a third-party	19%
Automated monitoring tools	17%
Controlled self assessments	22%
Random tests or spot checks	18%
Annual self-certification	17%
Other	3%
Unsure	1%
Total	191%

Q27c. If no, why doesn't your organization monitor the vendor's security and privacy practices? Please check all that apply.	Pct%
We don't have the internal resources to check or verify	66%
We have confidence in the vendor's ability to secure information	40%
We rely on the business reputation of the vendor	39%
We have insurance that limits our liability in the event of a data breach	15%
The vendor is subject to data protection regulations that are intended to protect our information	44%
The vendor is subject to contractual terms	49%
The data shared with the vendor is not considered sensitive or confidential	60%
The vendor will not allow us to independently monitor or verify their security and privacy activities	61%
Other	4%
Unsure	3%
Total	381%

Q28a. Does your vendor management program define and rank levels of risk?	Pct%
Yes	52%
No	43%
Unsure	5%
Total	100%

Q28b. If yes, what are indicators of risk? Please check all that apply.	Pct%
Failed IT security audits, verification or testing procedures	16%
Overall decline in the quality of the vendor's services	80%
Discovery that the vendor is using a subcontractor that has access to our company's information	16%
Complaints from customers about privacy or security	31%
History of frequent data breach incidents	49%
Legal actions against the vendor	39%
Negative media about the vendor	20%
IT glitches, operational failures and stoppages	68%
Poorly written security and privacy policies and procedures	26%
Lack of security or privacy training for the vendor's key personnel	15%
Lack of screening or background checks for key personnel hired by the vendor	45%
High rate of identity fraud, theft or other cyber crimes within the vendor's home country	14%
Lack of data protection regulation within the vendor's home country	25%
Turnover of the vendor's key personnel	75%
Outdated IT systems and equipment	53%
Other	5%
Total	577%

Q28c. If yes, how often are the risk levels updated?	Pct%
Never	23%
As needed	40%
Every six months	12%
Annually	15%
Every two years	6%
Unsure	4%
Total	100%

Q29a. Does your company regularly report to the board of directors on the effectiveness of the vendor management program and potential risks to the organization?	Pct%
Yes	31%
No	57%
Unsure	12%
Total	100%

Q29b. If no, why?	Pct%
Not a priority for the board	45%
Decisions about the vendor risk management program are not relevant for board members	51%
We only provide this information if a security incident or data breach has occurred involving a vendor	39%
Unsure	11%
Total	146%

Q30. Does your company require vendors to indemnify and/or ensure compliance with your security and privacy practices?	Pct%
Yes	35%
No	56%
Unsure	9%
Total	100%

Part 4. Demographics and organizational characteristics

D1. What organizational level best describes your current position?	Pct%
Senior Executive	4%
Vice President	3%
Director	16%
Manager	23%
Supervisor	15%
Associate/staff	35%
Contractor	4%
Other	0%
Total	100%

D2. Check the Primary Person you or your supervisor reports to within the organization.	Pct%
CEO/executive committee	3%
Chief operating officer	6%
Chief financial officer	9%
General counsel	7%
Head, procurement	11%
Chief information officer	15%
Compliance officer	21%
Chief information security officer	14%
Chief security officer	3%
Chief risk officer	9%
Other	2%
Total	100%

D3. What industry best describes your organization's industry focus?	Pct%
Agriculture & food services	1%
Communications	3%
Consumer products	3%
Defense & aerospace	1%
Education & research	2%
Energy & utilities	5%
Entertainment & media	2%
Financial services	19%
Health & pharmaceuticals	12%
Hospitality	3%
Industrial	8%
Public sector	11%
Retail	9%
Services	10%
Technology & software	7%
Transportation	3%
Other	1%
Total	100%

D4. What is the worldwide headcount of your organization?	Pct%
Less than 500	11%
501 to 1,000	19%
1,001 to 5,000	32%
5,001 to 25,000	19%
25,001 to 75,000	11%
More than 75,000	8%
Total	100%

Please contact research@ponemon.org if you have any questions about Ponemon Institute's services or survey methodology. For additional information about this survey, please visit: BuckleySandler LLP at www.buckleysandler.com and Treliant Risk Advisors LLC at www.treliant.com

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 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.