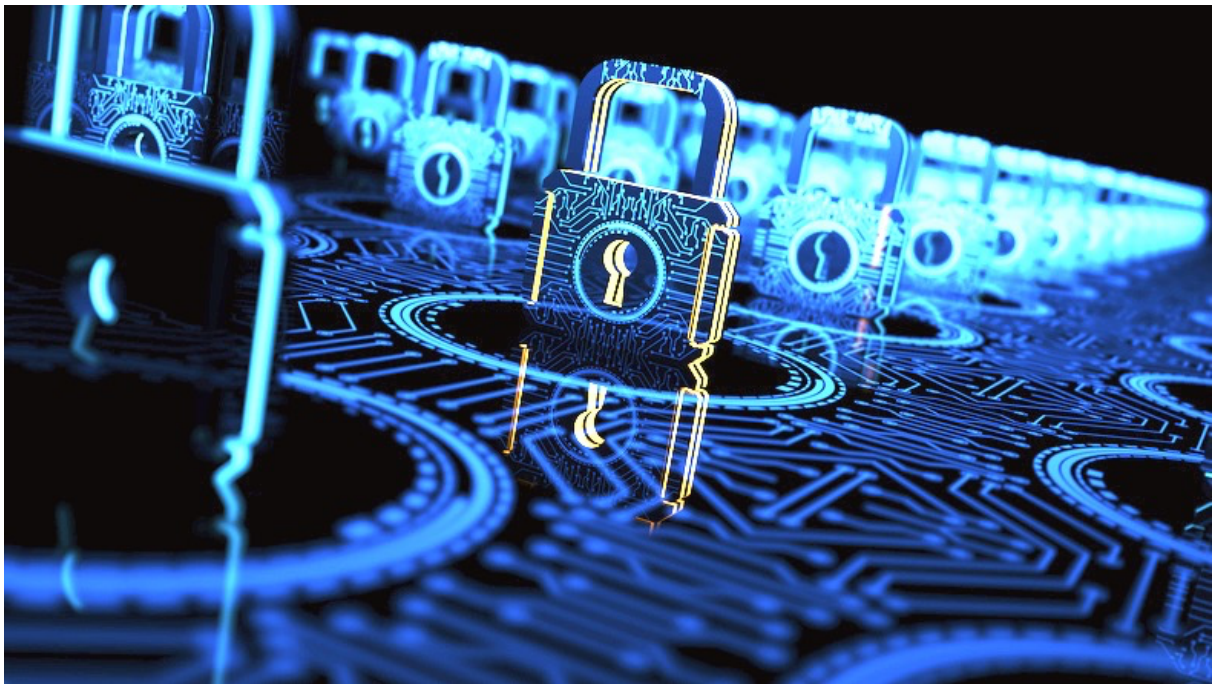
Ponemon INSTITUTE



The 2022 Data Risk in the Third-Party Ecosystem Study

Sponsored by RiskRecon, a Mastercard Company

Independently conducted by Ponemon Institute LLC

Publication Date: September 2022

The 2022 Data Risk in the Third-Party Ecosystem Study

Ponemon Institute, September 2022

Part 1. Introduction

Organizations are dependent upon their third-party vendors to provide such important services as payroll, software development or data processing. However, without having strong security controls in place vendors, suppliers, contractors or business partners can put organizations at risk for a third-party data breach. A third-party data breach is an incident where sensitive data from an organization is not stolen directly from it, but through the vendor's systems that are misused to steal sensitive, proprietary or confidential information.

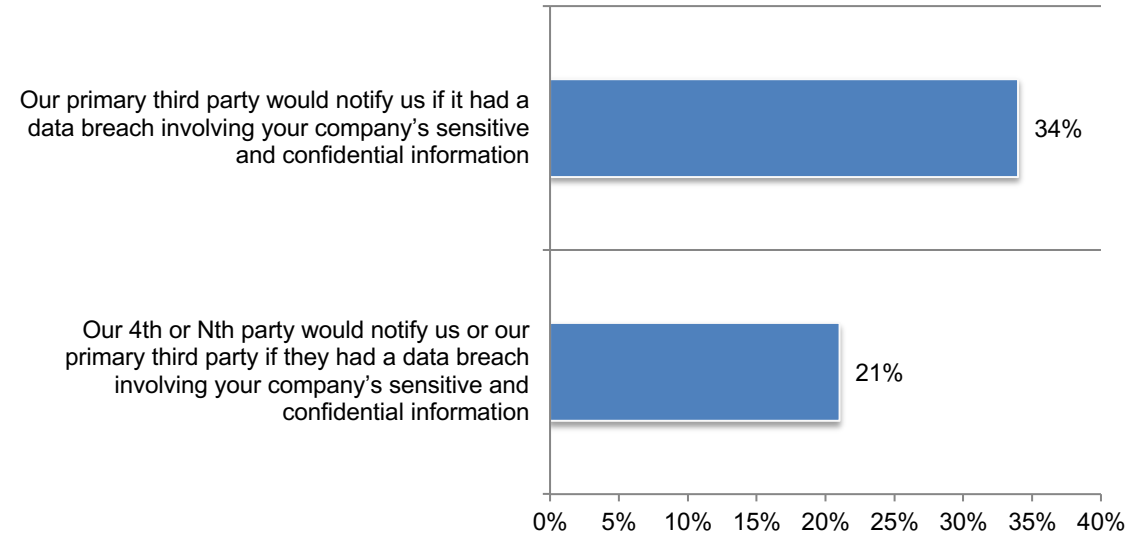
Sponsored by RiskRecon, a Mastercard Company and conducted by Ponemon Institute,1,162 IT and IT security professionals in North America and Western Europe were surveyed. All participants in the research are familiar with their organizations' approach to managing data risks created through outsourcing. Sixty percent of these respondents say the number of cybersecurity incidents involving third parties is increasing.

We define the third-party ecosystem as the many direct and indirect relationships companies have with third parties and Nth 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 and Nth parties that have access to their sensitive or confidential information.

Third-and-Nth party data breaches may be underreported. Respondents were asked to rate how confident their organizations are that a third or Nth party would disclose a data breach involving its sensitive and confidential information on a scale from 1 = not confident to 10 = highly confident.

Figure 1 shows the very and highly confident responses (7+ on the 10-point scale).
Only about one-third of respondents say that they have confidence that a primary third party would notify their organizations (34 percent) and even fewer respondents (21 percent) say the Nth party would disclose the breach.

Figure 1. How confident is your organization that a third party or Nth party would disclose a data breach involving sensitive and confidential information?
On a scale from 1 = not confident to 10 = highly confident, 7+ responses presented



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

1. **Create an inventory of all third parties with whom you share information and evaluate their security and privacy practices.** Before onboarding new third parties, conduct audits and assessments to evaluate the effectiveness of their security and privacy practices. However, only 36 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.

   Organizations should have a comprehensive list 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. Identify vendors who no longer meet your organization's security and privacy standards. Facilitate the offboarding of these third parties without causing business continuity issues.

2. **Conduct frequent reviews of third-party management policies and programs**. Only 43 percent of respondents say their organizations' third-party management policies and programs are frequently reviewed to ensure they address the ever-changing landscape of third-party risk and regulations. Organizations should consider automating third-party risk evaluation and management.

3. **Study the causes and consequences of recent third-party breaches and incorporate the takeaways in your assessment processes.** Only 40 percent of respondents say their third parties' data safeguards, security policies and procedures are sufficient to prevent a data breach and only 39 percent of respondents say these data safeguards, security policies and procedures enable organizations to minimize the consequences of a data breach. In the past year, breaches were caused by such vulnerabilities as unsecured data on the Internet, not configuring cloud storage buckets properly and not assessing and monitoring password managers.

4. **Improve visibility into third or Nth parties with whom you do not have a direct relationship**. More than half (53 percent) of respondents say they are relying upon the third party to notify their organization when data is shared with Nth parties.

   A barrier to visibility is that only 35 percent of respondents say their organizations are monitoring third-party data handling practices with Nth parties. To increase visibility into the security practices of all parties with access to company sensitive information – even subcontractors, notification when data is shared with Nth parties is critical. In addition, organizations should include in their vendor contracts requirements that third parties provide information about possible third-party relationships with whom they will be sharing sensitive information.

5. **Form a third-party risk management committee and establish accountability for the proper handling of third-party risk management program**. Many organizations have strategic shortfalls in third-party risk management governance. Specifically, only 42 percent of respondents say managing outsourced relationship risk is a priority in our organization and only 40 percent of respondents say there are enough resources to manage these relationships.

   To improve third-party governance practices, organizations should centralize and assign accountability for the correct handling of their company's third-party risk management program and ensure that appropriate privacy and security language is included in all vendor contracts. Create a cross-functional team to regularly review and update third-party management policies and programs.

6. **Require 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.

Part 2. Key Findings

In this study, 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 combined global findings. The complete audited findings are in the Appendix of this report. We have organized the research according to the following topics:

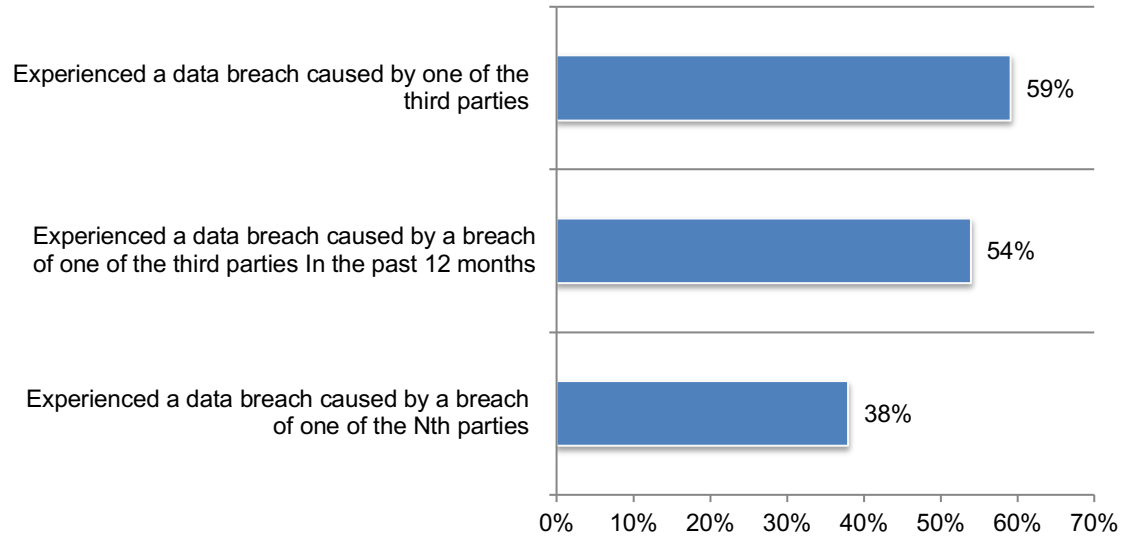
- Strategic shortfalls in third-party risk management governance
- Lack of visibility into third-and- Nth party relationships
- The realities of today's third-party risk management programs
- Key factors impacting the likelihood of a data breach
- North America and Western Europe differences

Strategic shortfalls in third-party risk management governance

Cybersecurity incidents involving third parties are increasing and third-party data breaches are prevalent. Third-party data breaches can be caused by vendors, suppliers, contractors or business partners that may have weaker security controls than the organizations they provide services to. Stolen data may include sensitive, proprietary or confidential information such as credit card numbers, trade secrets, customer and patient data.

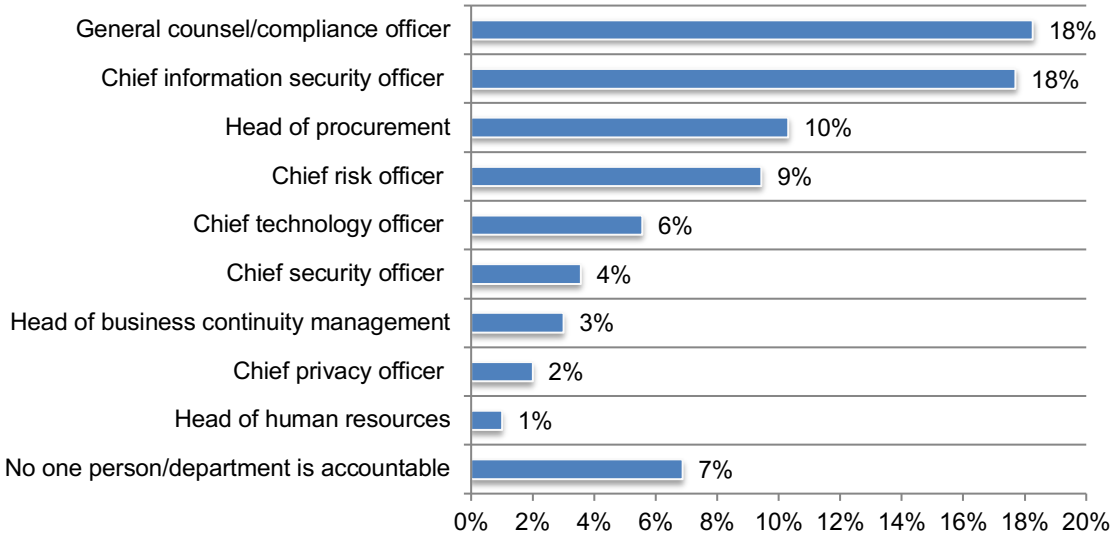
According to the research, 59 percent of respondents confirm that their organizations have experienced a data breach caused by one of their third parties and 54 percent of these respondents say it was as recent as the past 12 months, as shown in Figure 2. Of these respondents, 38 percent say the breach was caused by one of the Nth parties, indicating the flaws in third parties' security controls in place for their Nth parties.

Figure 2. Has your organization ever and in the past 12 months experienced a data breach or cyber attack caused by a third party?
Yes responses reported



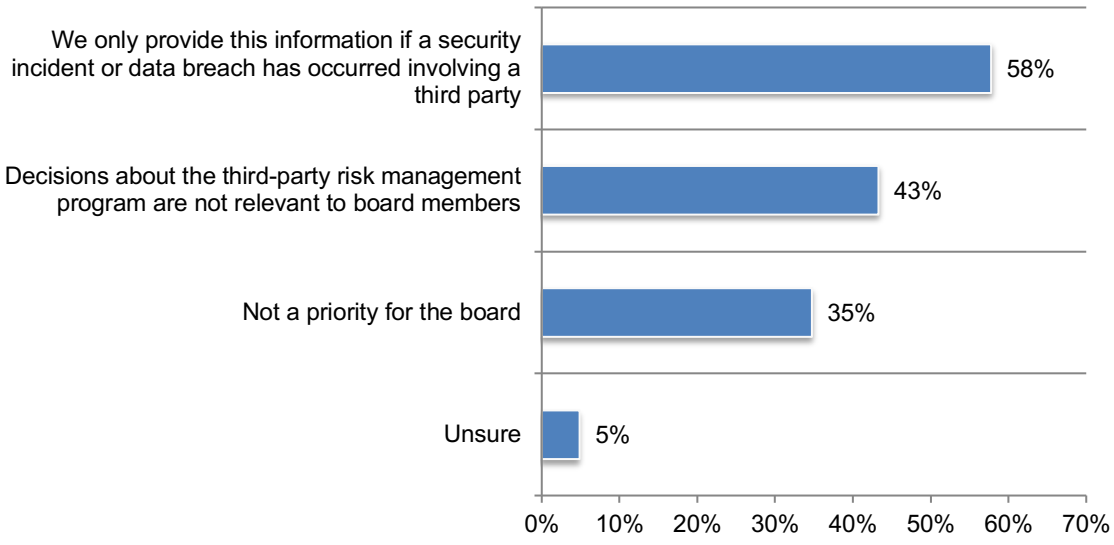
The lack of accountability and involvement by the boards of directors are barriers to achieving a robust third-party security posture. As shown in Figure 3, no single function emerges as having full accountability for the third-party risk management program. Most accountability (36 percent of respondents) seems to rest with the general counsel/compliance officer (18 percent of respondents) and CISO (18 percent of respondents).

Figure 3. Who is most accountable for the correct handling of the organization's third-party risk management program?



Boards of directors are not kept informed about third-party risks. Only 40 percent of respondents say their organizations regularly report to the board about the state of their third-party risk management programs and the risks facing them. According to Figure 4, it is only when a security incident or data breach has occurred involving a third party (58 percent of respondents) and 35 percent of respondents say it is not a priority for the board. Forty-three percent say decisions about the third-party risk management program are not relevant to board members.

Figure 4. Reasons for not regularly reporting third-party risks to the board of directors
More than one response permitted



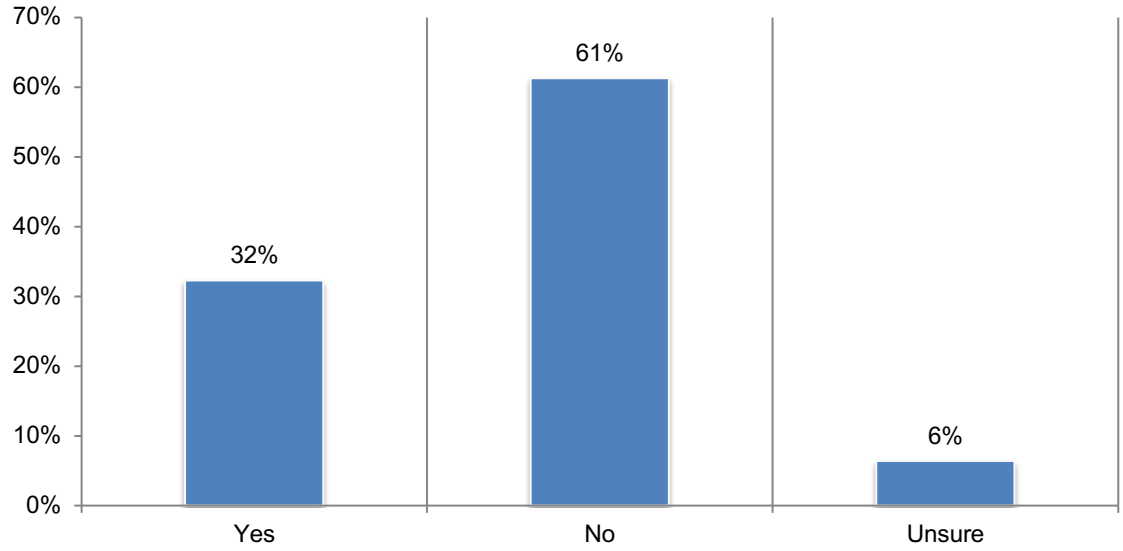
There is a lack of visibility into third-and-Nth party relationships

Few companies maintain a comprehensive inventory of all third parties with whom they share information. As shown in Figure 5, 67 percent of respondents say they do not have (61 percent) or are unsure (6 percent) if their company has such an inventory.

Of the 32 percent of respondents who say their organizations have a comprehensive inventory, it is estimated that an average of 2,103 third parties are in this inventory. Within the third-party inventory, it is estimated that an average of 48 percent of all third parties are sharing sensitive and confidential information with Nth parties.

Of the 32 percent of respondents in companies with a third-party inventory, 68 percent admit that the inventory does not include all third-and Nth-parties their organizations have a relationship with that might have access to their sensitive and confidential information.

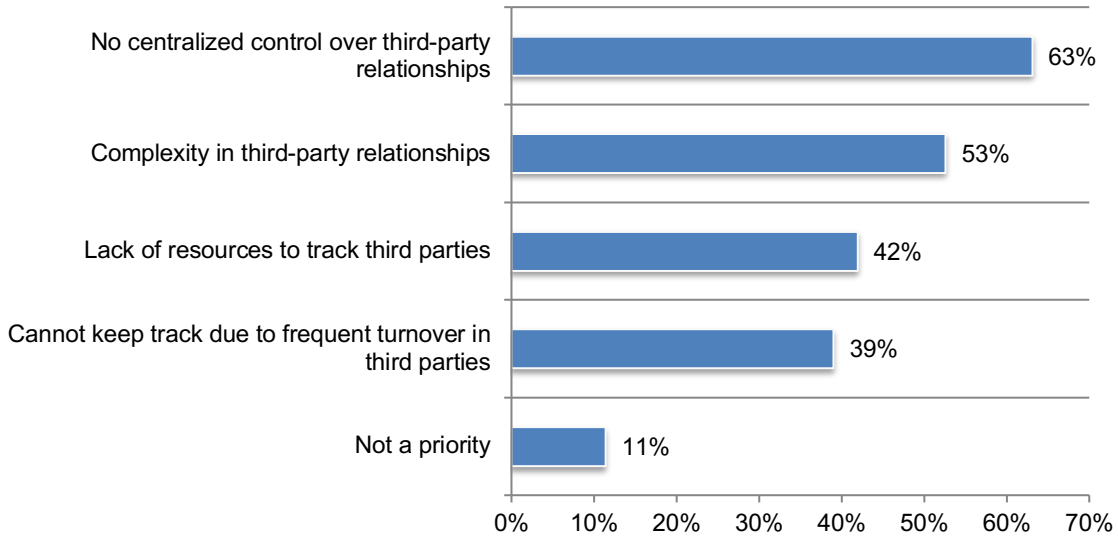
Figure 5. Does your company have a comprehensive inventory of all third parties with whom it shares sensitive and confidential information?



To have a comprehensive inventory, centralized control over third parties is critical. As discussed previously, accountability for third-party risk management programs is dispersed throughout organizations. This lack of centralized control over third-party relationships (63 percent of respondents) is the primary barrier to determining how many third parties have access to their sensitive and confidential information, as shown in Figure 6.

This is followed by the complexity of these relationships (53 percent of respondents) and the lack of resources (42 percent of respondents). The inability to keep track because of frequent turnover in third parties (39 percent of respondents) may be improved by centralizing control.

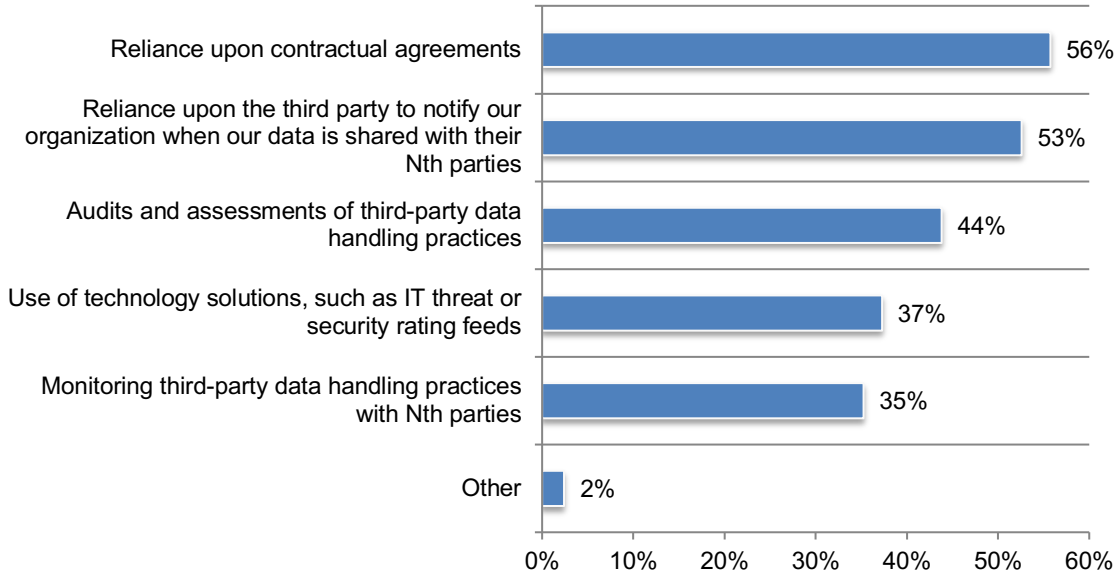
Figure 6. Reasons companies do not have a comprehensive inventory of all third parties
More than one response permitted



Companies lack visibility into Nth parties that have their sensitive or confidential data. Only 36 percent of respondents say their organizations are notified when third parties share their information with Nth parties with whom they have no direct relationship. Only 29 percent of respondents say their organizations have visibility into Nth parties that have access to sensitive and confidential information.

According to Figure 7, of the 29 percent of respondents who say they have such visibility, 56 percent say visibility is due to reliance upon contractual agreements and 53 percent of respondents say they trust the third party to notify their organizations when their data is shared with their Nth parties. Only 44 percent of respondents say their organizations conduct audits and assessments of third-party data handling practices and only 35 percent monitor third-party data handling practices with Nth parties.

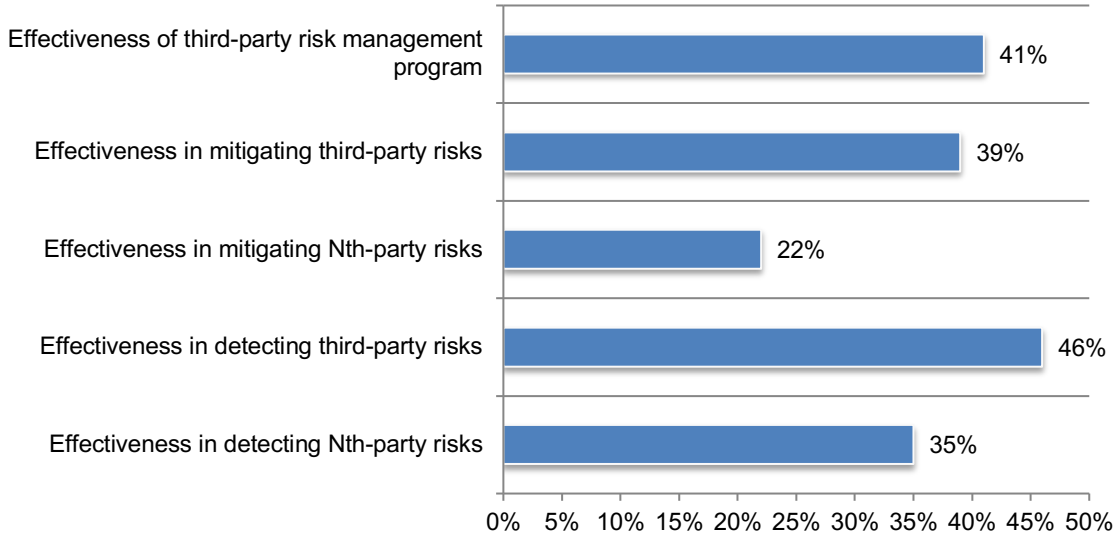
Figure 7. How does your organization achieve visibility into vendors your company does not have a direct relationship with?
More than one response permitted



Most organizations are unable to mitigate third-party and Nth-party risks. We asked participants to rate the effectiveness of their third-party risk management program and in dealing with third-party and Nth party risks on a scale from 1 = not effective to 10 = highly effective.

Figure 8 presents the highly effective responses (7 + on a scale of 1 = not effective to 10 = highly effective). Only 39 percent of respondents rate their companies' effectiveness in mitigating third-party risk as highly effective. When it comes to Nth party risk, only 22 percent rate their effectiveness as high. Forty-six percent of respondents say their organizations are effective in detecting third-party risks. Only 35 percent of respondents say their organizations are effective in detecting Nth-party risks.

Figure 8. How effective is your organization in mitigating and detecting third-party and Nth party risks in your organization's third-party risk management program?
On a scale from 1 = not effective to 10 = highly effective, 7+ responses presented

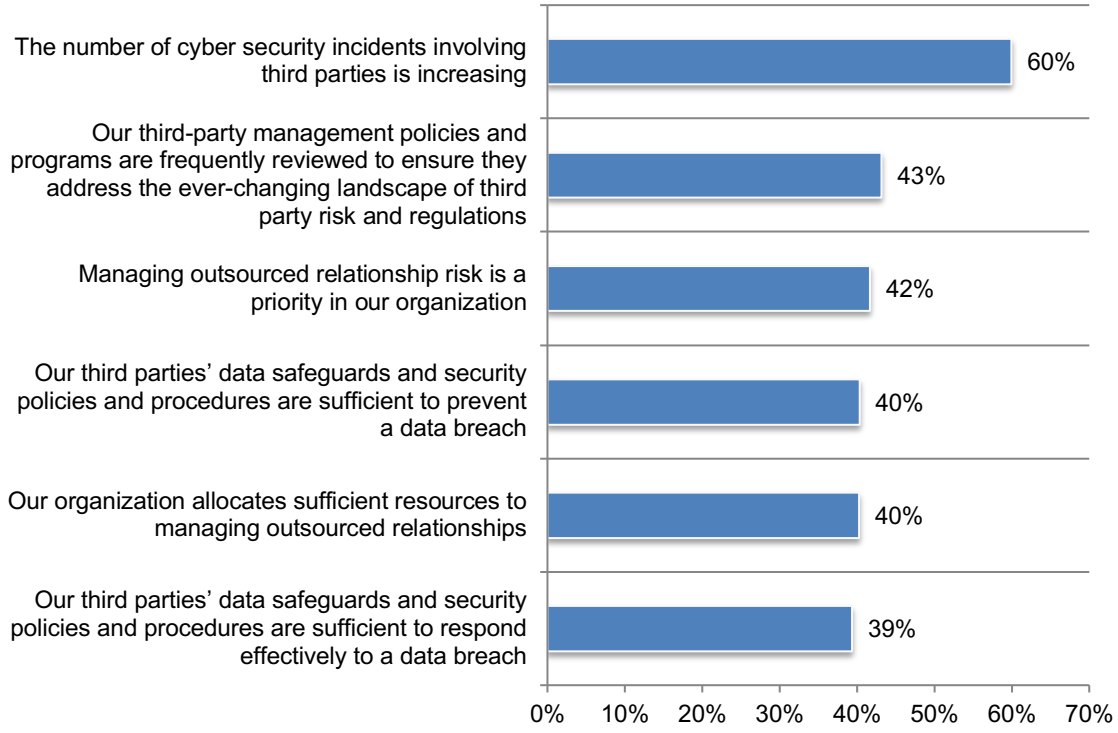


The realities of today's third-party risk management programs

Organizations believe they are at risk because of the failure to take appropriate steps to safeguard sensitive and confidential information shared with third parties. Figure 9 presents a list of reasons respondents believe are the causes of ineffectiveness in detecting, minimizing and mitigating third-and-Nth party risks. Only 39 percent of respondents say their third parties' data safeguards and security policies and procedures are sufficient to respond effectively to a data breach and only 40 percent say they are sufficient to prevent a data breach.

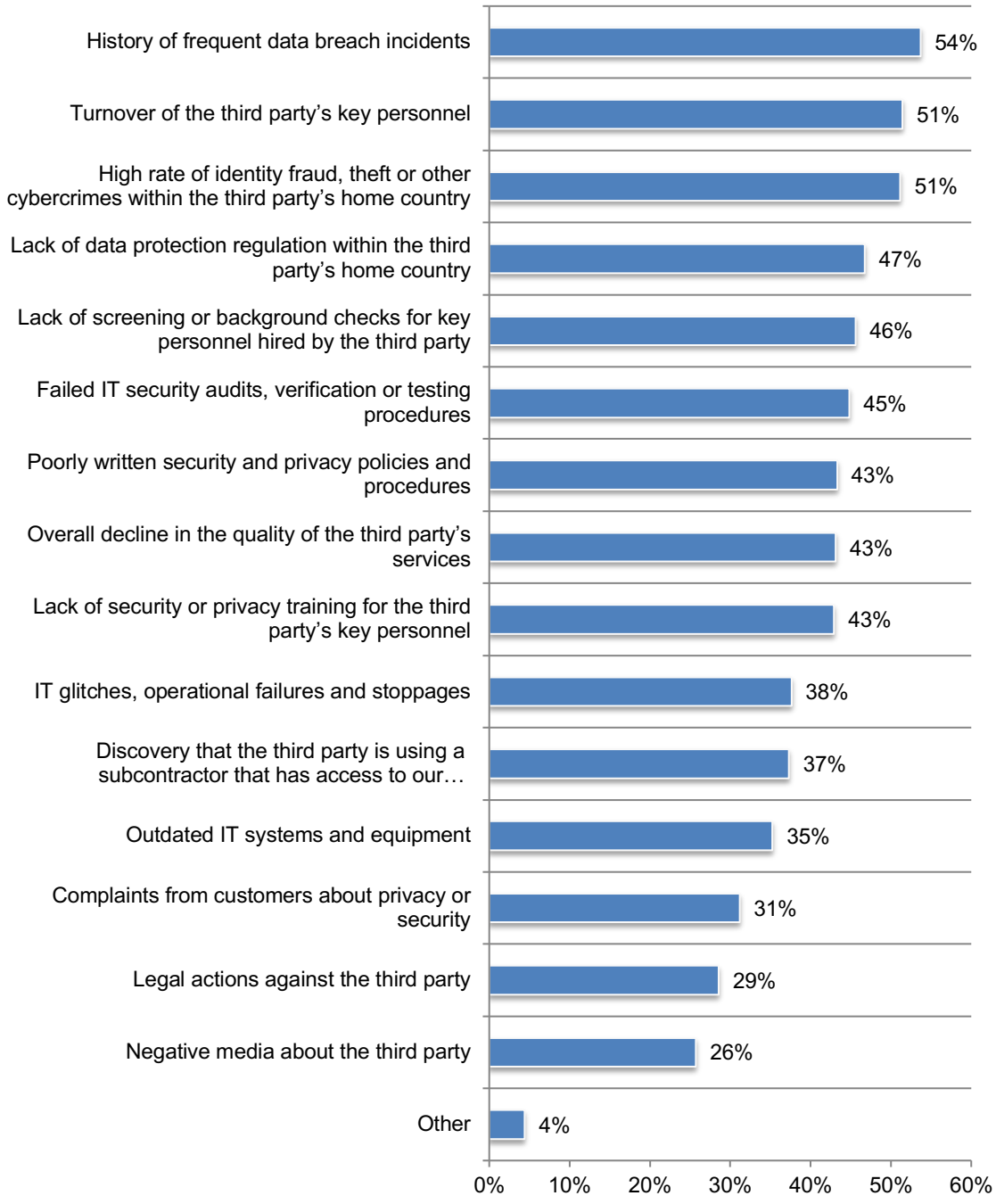
According to the research, organizations also need to improve their third-party risk management practices. Specifically, only 42 percent of respondents say managing outsourced relationship risk is a priority, only 40 percent of respondents say there are sufficient resources allocated to the management of risks and only 43 percent of respondents say there is a frequent review of third-party risk management policies and programs to ensure they address the ever-changing third-party risks and regulations.

Figure 9. Perceptions about vendors' security policies and procedures
Strongly agree and Agree responses combined



A history of frequent data breach incidents is the top indicator of third-party risk. Fifty-eight percent of respondents say their organizations' third-party management program defines and ranks levels of risk. Sixty-two percent of respondents say risk levels are updated every six months (33 percent of respondents) or annually (29 percent of respondents). Figure 11 presents an extensive list of indicators of third-party risk. Turnover of key personnel and a high rate of cybercrimes in the third party's home country are risk indicators according to 51 percent of respondents.

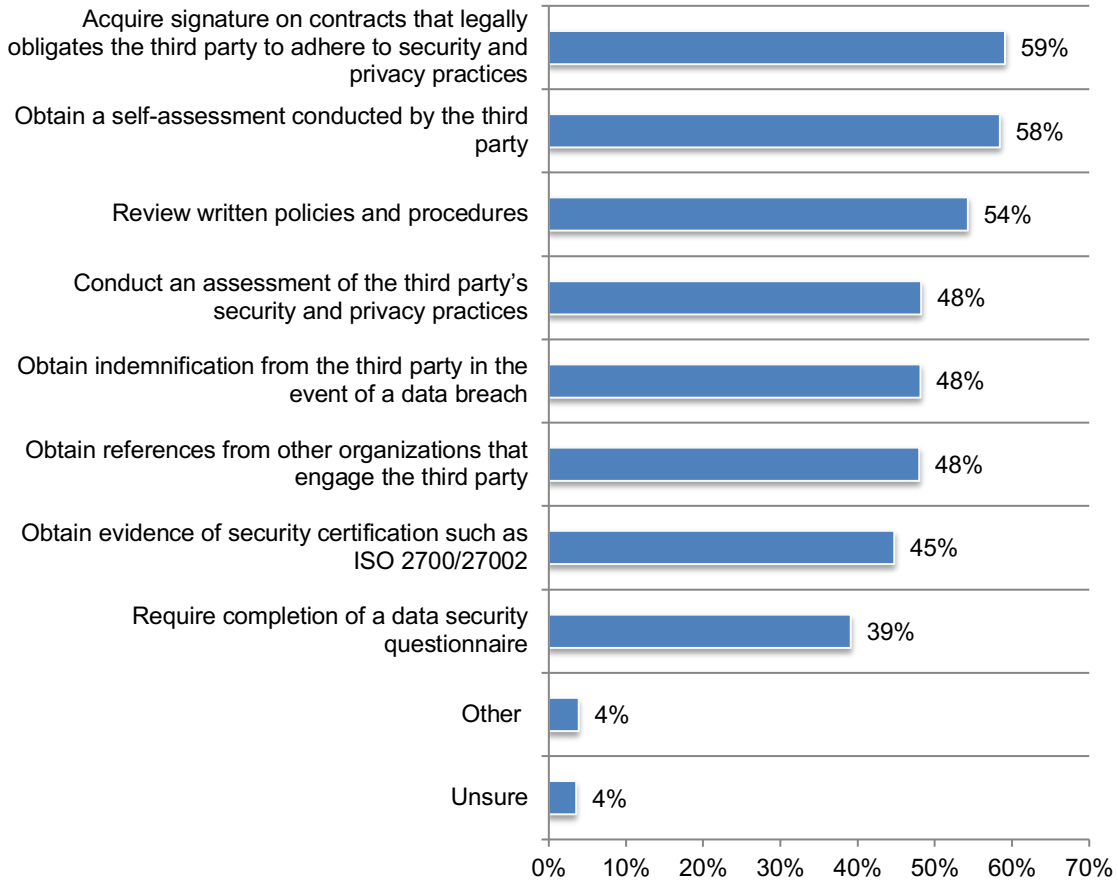
Figure 10. What are indicators of risk?
More than one response permitted



Companies rely on contractual arrangements to evaluate third parties. Only 36 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.

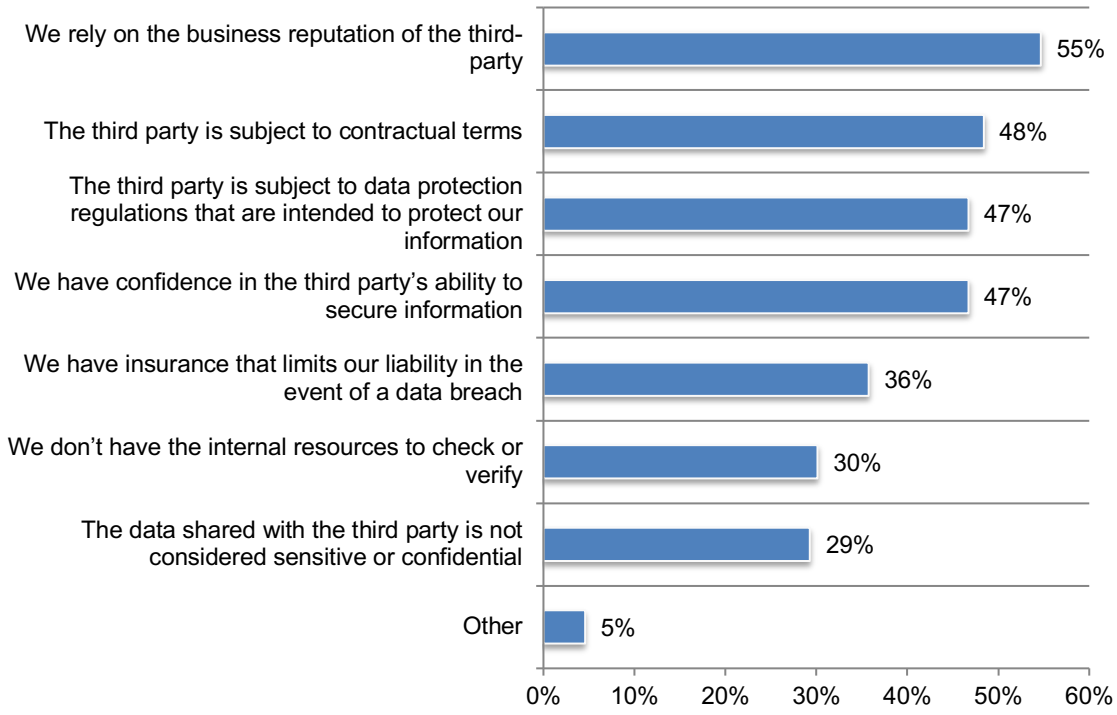
Figure 11 shows the steps taken to perform such an evaluation. Fifty-nine percent of respondents say their organizations acquire signatures on contracts that legally obligate the third party to adhere to security and privacy practices followed by a self-assessment conducted by the third party (58 percent of respondents). Only 39 percent of respondents say the completion of a data security questionnaire is required.

Figure 11. How do you perform this evaluation?
More than one response permitted



Reliance on business reputations and contracts are the primary reasons for not performing an evaluation of potential third parties. As shown in Figure 12, about half (47 percent) of respondents say they do not conduct evaluations because of third parties' requirement to comply with data protection regulations or they have confidence in the third party's ability to secure information.

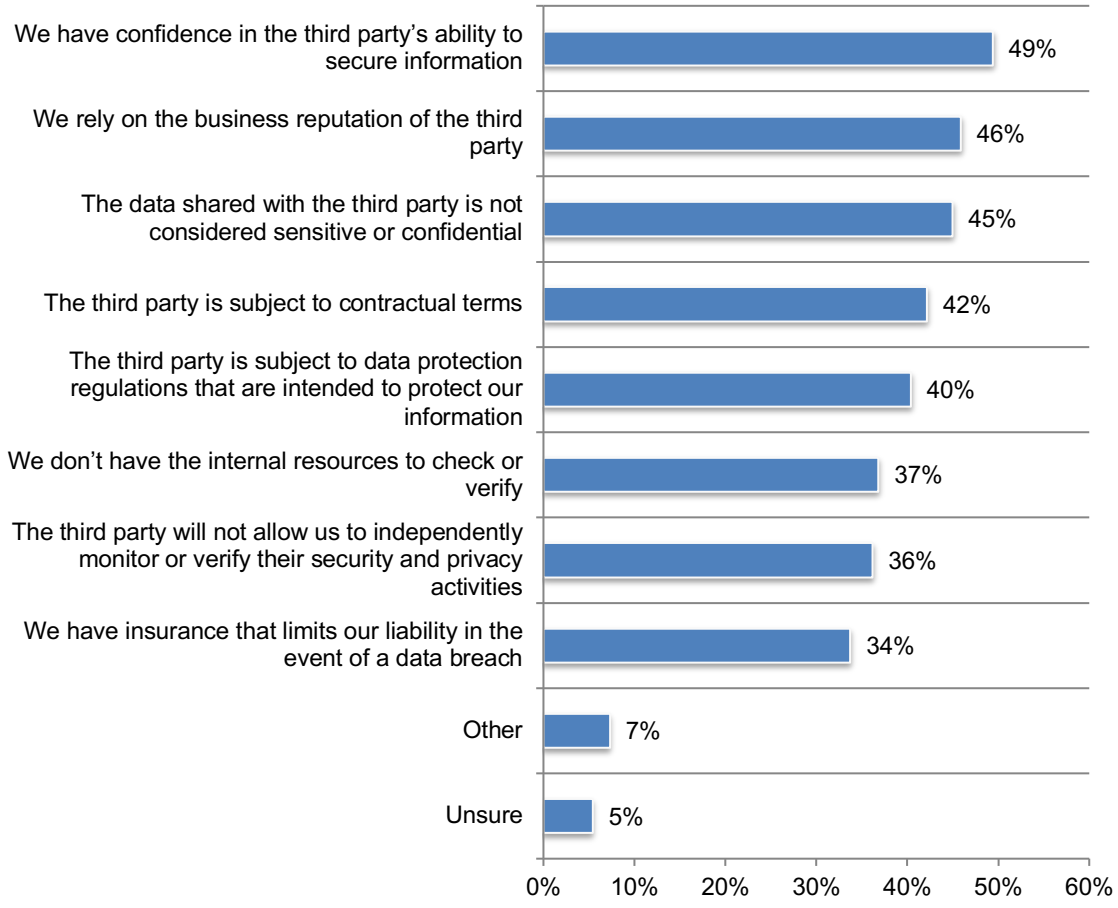
Figure 12. Reasons for not performing an evaluation
More than one response permitted



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

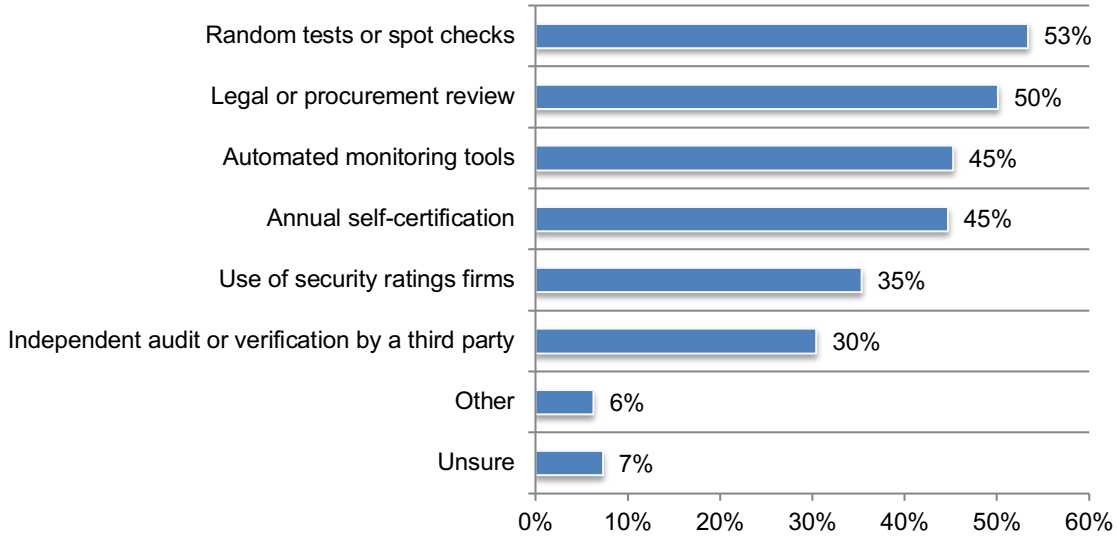
As shown in Figure 13, the primary reasons for not monitoring are: confidence in the third party's ability to secure information (49 percent of respondents), reliance on the business reputation of the third party (46 percent of respondents), data shared with the third party is not considered sensitive or confidential (45 percent of respondents) and contracts (42 percent of respondents). These are similar to reasons for not evaluating third parties before engaging them.

Figure 13. Reasons for not monitoring security and privacy practices
More than one response permitted



Fifty percent of respondents say their companies monitor the security and privacy practices of third parties to ensure the adequacy of these practices. Figure 14 reveals that 53 percent of respondents say their organizations conduct random tests or spot checks. Only 30 percent of respondents say they depend upon independent audit or verification by a third party.

Figure 14. Third-party monitoring procedures used to ensure the adequacy of security and privacy practices
More than one response permitted

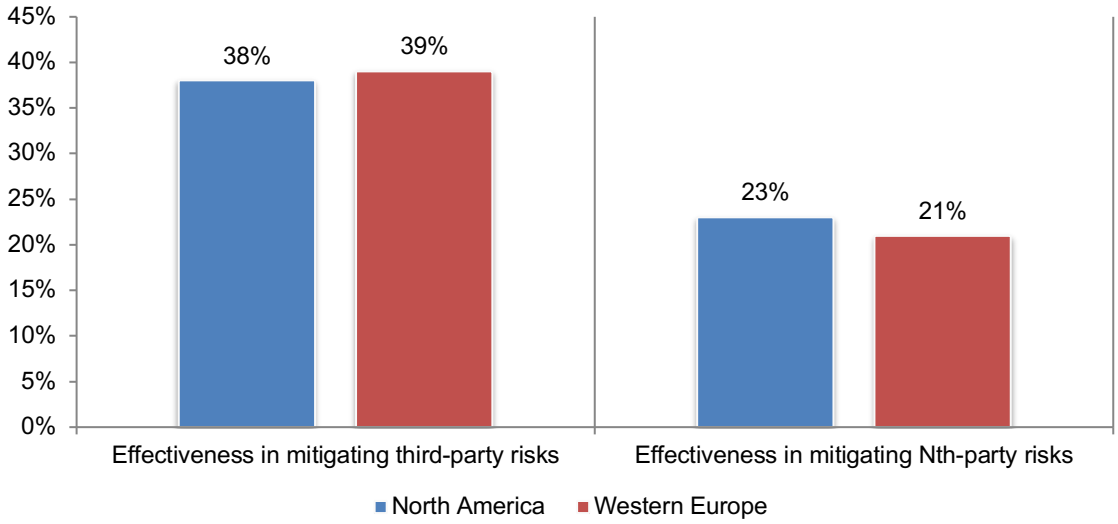


Regional differences: North America and Western Europe

In this section, we present differences in perceptions about third-party data risks between respondents in North America (656) and Western Europe (506). In several findings, respondents' perceptions in these different regions are consistent.

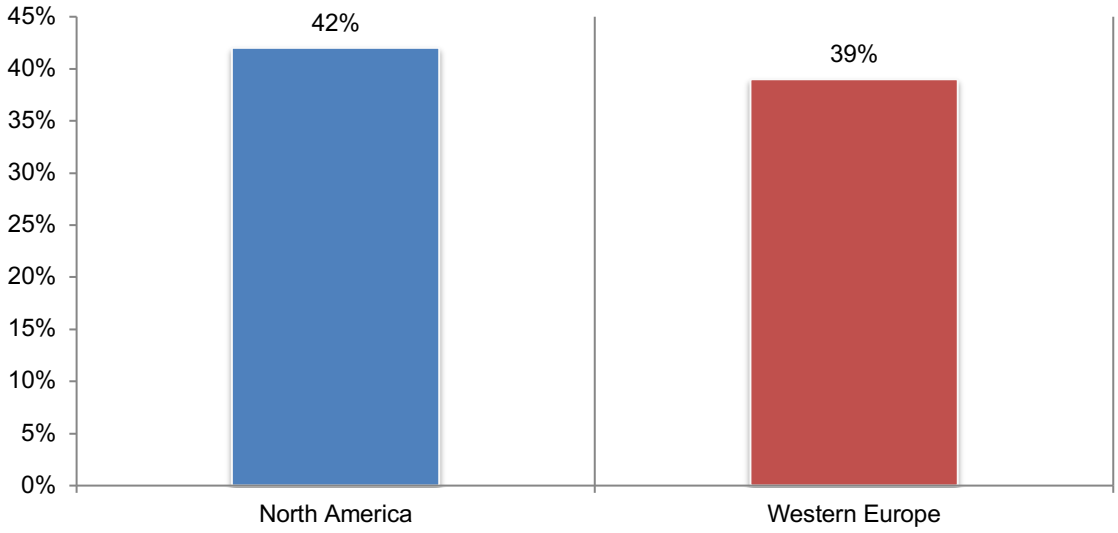
Low effectiveness in mitigating third-party and Nth-party risks exists in both regions. Figure 15 presents the high and highly effective responses (7+ on the 10-point scale). Only 38 percent of respondents in North America and 39 percent in Western Europe report high effectiveness in mitigating these risks. Effectiveness in mitigating Nth-party risks is even lower.

Figure 15. Effectiveness in mitigating third-party and Nth-party risks
On a scale from 1 = not effective to 10 = highly effective, 7+ responses presented



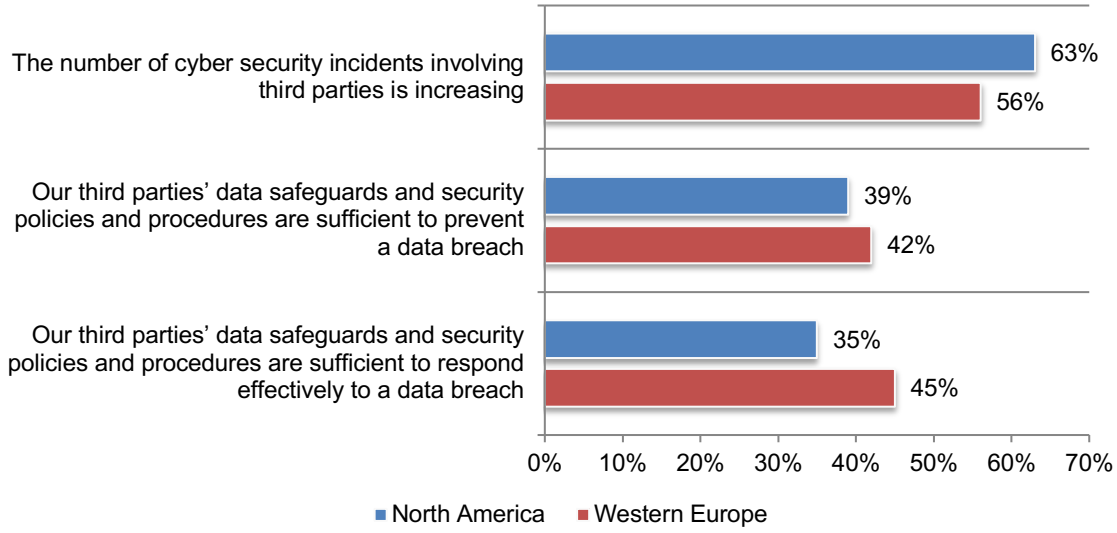
Globally, third-party risk management programs are not effective. However, North American respondents are slightly more likely than Western Europe to say their third-party risk management program is effective (42 percent vs. 39 percent of respondents).

Figure 16. Effectiveness in the organization's third-party risk management program
On a scale from 1 = not effective to 10 = highly effective, 7+ responses presented



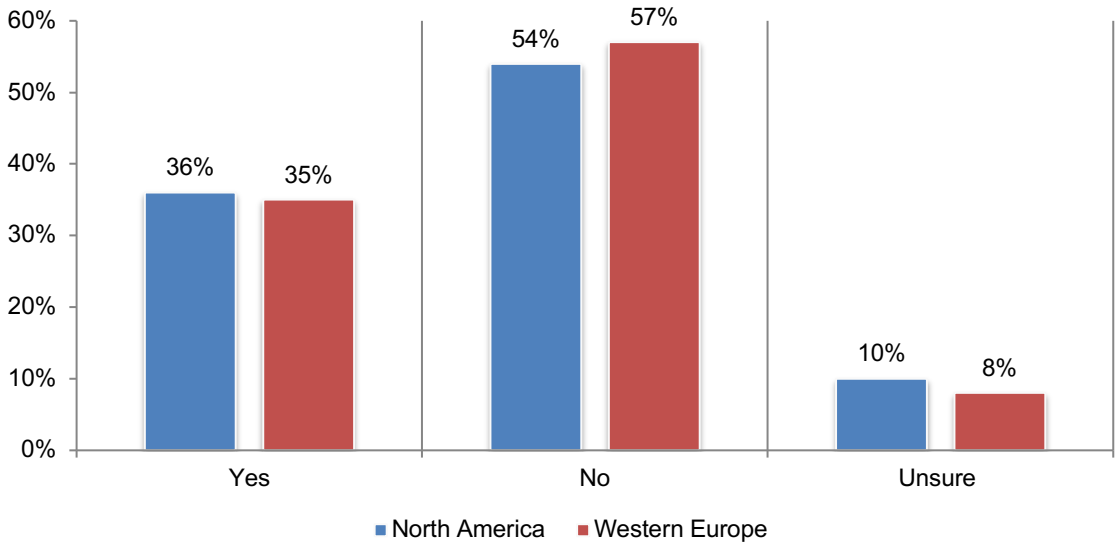
North American respondents are more likely to see increases in cybersecurity incidents involving third parties (63 percent vs. 56 percent of respondents). Western Europe respondents are more positive than North American respondents about the third parties' data safeguards and security policies and procedures are sufficient to respond to a data breach (45 percent vs. 35 percent of respondents), as shown in Figure 17.

Figure 17. Perceptions about third-party risks
Strongly agree and Agree responses combined



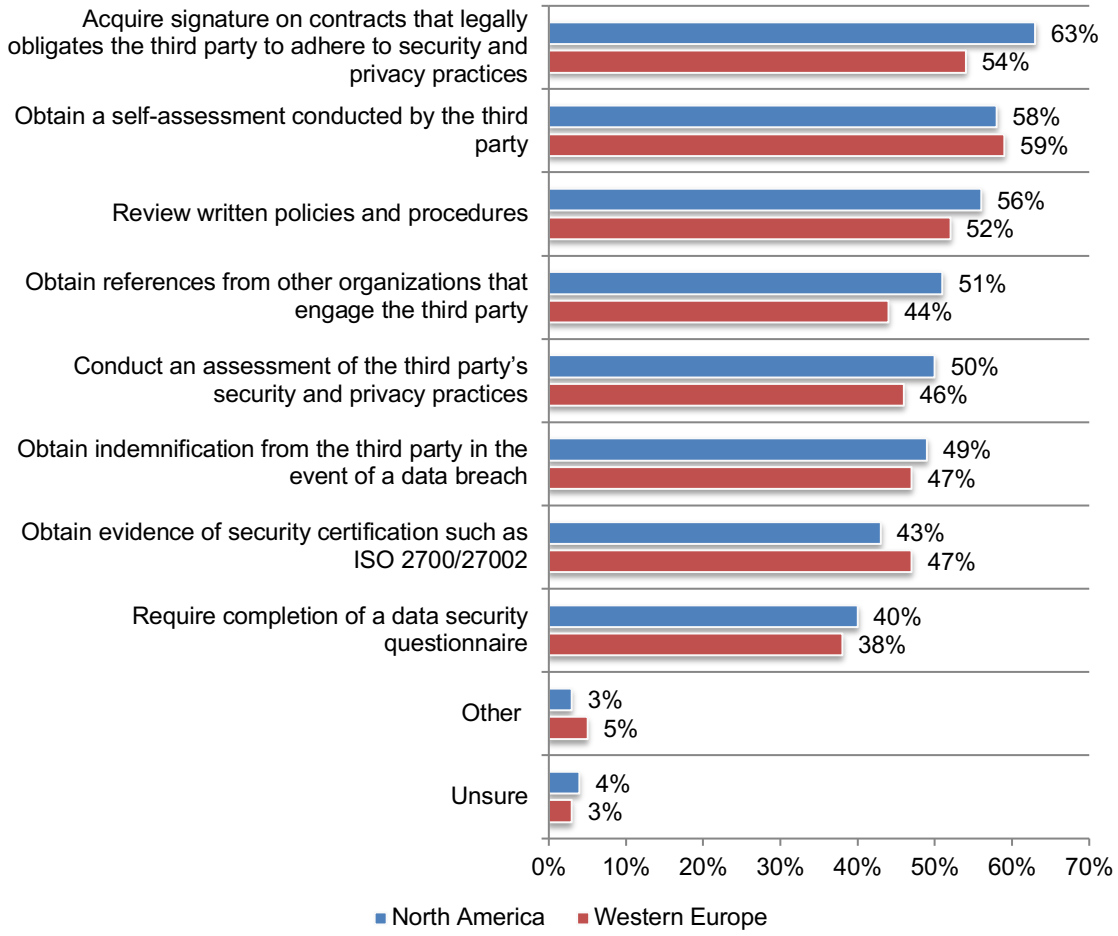
Both North America and Western Europe respondents are not evaluating the security and privacy practices of third and Nth parties, according to Figure 18.

Figure 18. Does your organization evaluate the security and privacy practices of third parties and Nth parties?



North America respondents are more likely to rely upon contracts that legally obligate the third-party to adhere to security and privacy practices (63 percent vs. 54 percent of respondents). Western Europe respondents' primary method of evaluation is to have the third party conduct a self-assessment, according to Figure 19.

Figure 19. If yes, how do you perform this evaluation?
More than one response permitted



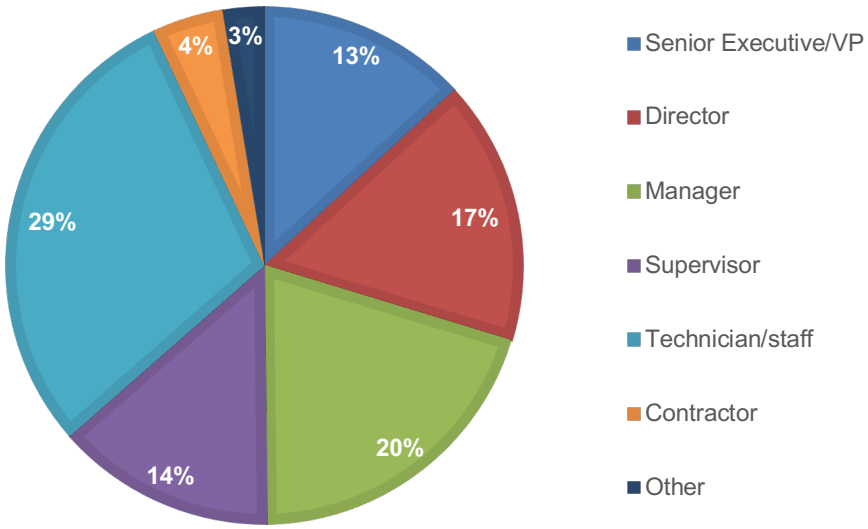
Part 4. Methods

A sampling frame of 30,536 individuals in North America and Western Europe in organizations across multiple industries and who are familiar with their organization's approach to managing data risks created through outsourcing were selected as participants to this survey. All organizations represented in this study have a third-party data risk management program. Table 1 shows 1,270 total returns. Screening and reliability checks required the removal of 108 surveys. Our final sample consisted of 1,162 surveys or a 3.8 percent response.

Table 1. Sample response	North America	Western Europe	Combined
Sampling frame	16,881	13,655	30,536
Total returns	716	554	1,270
Rejected or screened surveys	60	48	108
Final sample	656	506	1,162
Response rate	3.9%	3.7%	3.8%

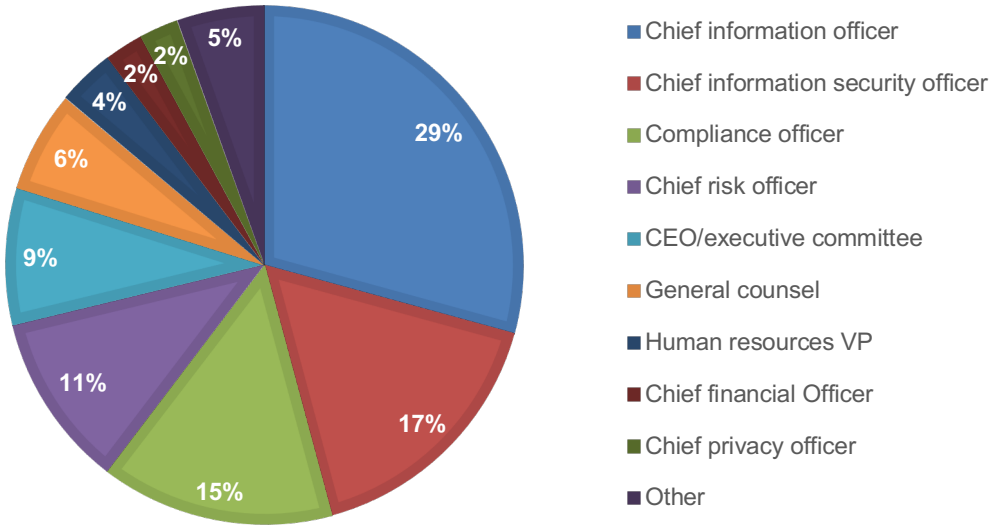
Pie chart 1 reports the respondent's organizational level within participating organizations. By design, more than half (64 percent) of respondents are at or above the supervisory levels. The largest category at 29 percent of respondents is technician or staff.

Pie chart 1. Current position within the organization



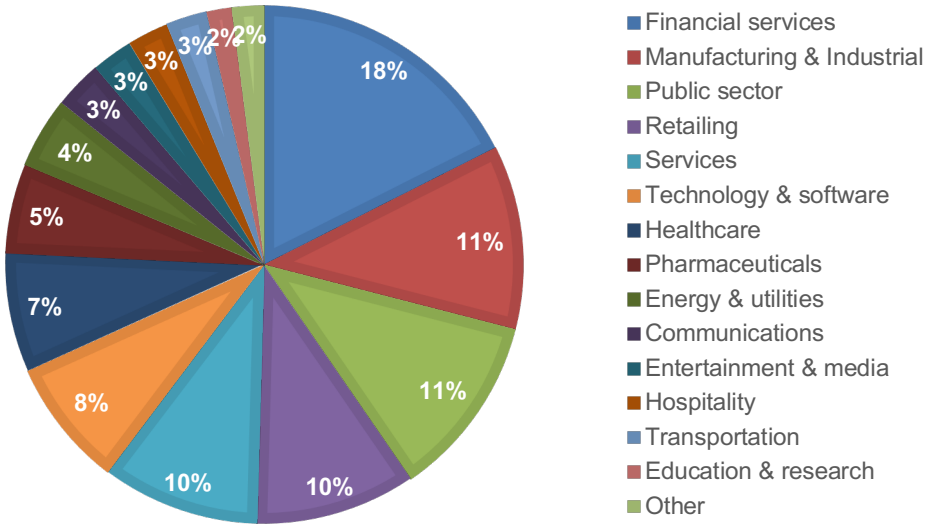
As shown in Pie chart 2, 29 percent of respondents report to the chief information officer, 17 percent of respondents report to the chief information security officer, 15 percent of respondents report to the compliance officer, 11 percent of respondents report to the chief risk officer and 9 percent of respondents report to the CEO/executive committee.

Pie chart 2. Direct reporting channel



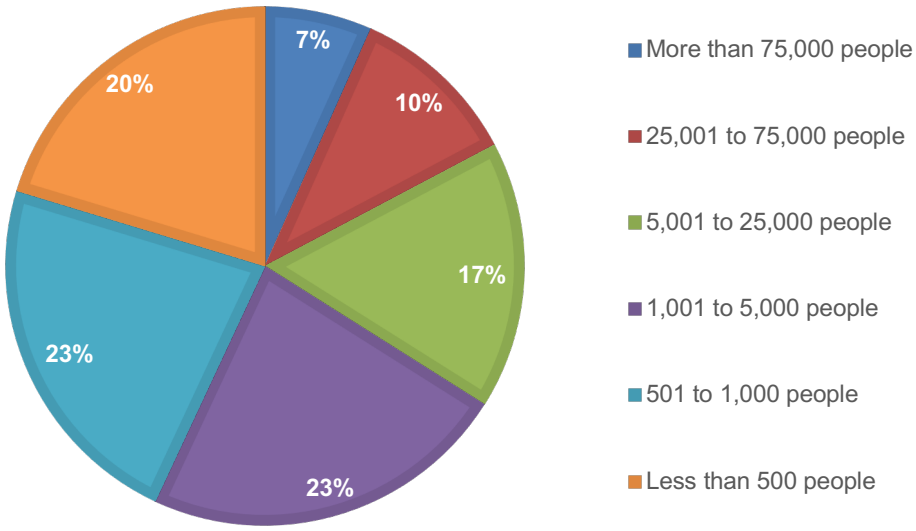
Pie chart 3 reports the industry focus of respondents' organizations. This chart identifies financial services (18 percent) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by manufacturing and industrial (11 percent of respondents), public sector (11 percent of respondents), retailing (10 percent of respondents), services (10 percent of respondents), and technology and software (8 percent of respondents).

Pie chart 3. Primary industry focus



As shown in Pie chart 4, 57 percent of respondents are from organizations with a global headcount of more than 1,000 employees.

Pie chart 4. Global full-time headcount



Part 5. Caveats

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 are managing the data risks created by outsourcing. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in June 2022.

Survey Response	North America	Western Europe	Combined
Total sampling frame	16,881	13,655	30,536
Total survey responses	716	554	1,270
Rejected surveys	60	48	108
Final sample	656	506	1,162
Sample weights	3.9%	3.7%	3.8%

Screening questions

S1. How familiar are you with your organization's approach to managing data risks created through outsourcing?	North America	Western Europe	Combined
Very familiar	41%	39%	40%
Familiar	38%	36%	37%
Somewhat familiar	21%	25%	23%
No knowledge (Stop)	0%	0%	0%
Total	100%	100%	100%

S2. Does your company have a third-party data risk management program?	North America	Western Europe	Combined
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?	North America	Western Europe	Combined
Yes, full involvement	36%	34%	35%
Yes, partial involvement	39%	39%	39%
Yes, minimal involvement	25%	27%	26%
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?	North America	Western Europe	Combined
Yes	63%	54%	59%
No	30%	41%	35%
Unsure	7%	5%	6%
Total	100%	100%	100%

Q1b. If yes, 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?	North America	Western Europe	Combined
Yes	57%	50%	54%
No	37%	45%	40%
Unsure	6%	5%	6%
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?	North America	Western Europe	Combined
Yes	31%	47%	38%
No	58%	43%	51%
Unsure	11%	10%	11%
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?	North America	Western Europe	Combined
Yes	42%	40%	41%
No	53%	51%	52%
Unsure	5%	9%	7%
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)	North America	Western Europe	Combined
1 or 2	12%	8%	10%
3 or 4	28%	29%	28%
5 or 6	29%	25%	27%
7 or 8	19%	23%	21%
9 or 10	12%	15%	13%
Total	100%	100%	100%
Extrapolated value	5.32	5.66	5.47

Q2b. How confident are you that a 4th or 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)	North America	Western Europe	Combined
1 or 2	30%	25%	28%
3 or 4	17%	28%	22%
5 or 6	32%	28%	30%
7 or 8	11%	10%	11%
9 or 10	10%	9%	10%
Total	100%	100%	100%
Extrapolated value	4.58	4.50	4.55

Q3. Who is most accountable for the correct handling of your organization's third-party risk management program?	North America	Western Europe	Combined
General counsel/compliance officer	20%	16%	18%
Chief technology officer (CTO)	6%	5%	6%
Chief information officer (CIO)	21%	23%	22%
Chief information security officer (CISO)	19%	16%	18%
Chief security officer (CSO)	4%	3%	4%
Head of business continuity management	3%	3%	3%
Chief privacy officer (CPO)	2%	2%	2%
Data protection officer (DPO)	0%	0%	0%
Head of human resources	1%	1%	1%
Head of procurement	9%	12%	10%
Chief risk officer (CRO)	9%	10%	9%
No one person/department is accountable	6%	8%	7%
Unsure	0%	1%	0%
Total	100%	100%	100%

Q4a. Does your company have a comprehensive inventory of all third parties with whom it shares sensitive and confidential information?	North America	Western Europe	Combined
Yes (proceed to Q5.)	34%	30%	32%
No	60%	63%	61%
Unsure	6%	7%	6%
Total	100%	100%	100%

Q4b. If no or unsure, why? Please check all that apply	North America	Western Europe	Combined
Lack of resources to track third parties	45%	38%	42%
No centralized control over third-party relationships	64%	62%	63%
Complexity in third-party relationships	50%	56%	53%
Cannot keep track due to frequent turnover in third parties	36%	43%	39%
Not a priority	11%	12%	11%
Total	206%	211%	208%

Q5. How many third parties are in this inventory?	North America	Western Europe	Combined
Less than 10	2%	5%	3%
11 to 50	3%	6%	4%
51 to 100	5%	6%	5%
101 to 250	6%	9%	7%
251 to 500	7%	12%	9%
501 to 1,000	15%	23%	18%
1,001 to 2,500	18%	19%	18%
2,501 to 5,000	21%	16%	19%
More than 5,000	23%	4%	15%
Total	100%	100%	100%
Extrapolated value	,637	1,412	2,103

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?	North America	Western Europe	Combined
Yes	34%	30%	32%
No	57%	62%	59%
Unsure	9%	8%	9%
Total	100%	100%	100%

Q7. What percentage of all third parties do you believe are sharing your sensitive and confident data with Nth parties?	North America	Western Europe	Combined
None	6%	5%	6%
Less than 10%	9%	9%	9%
11% to 20%	14%	12%	13%
21% to 50%	10%	29%	18%
51% to 75%	30%	27%	29%
More than 76%	31%	18%	25%
Total	100%	100%	100%
Extrapolated value	51%	44%	48%

Q8. Do third parties notify your organization when your data is shared with the Nth parties?	North America	Western Europe	Combined
Yes	38%	33%	36%
No	50%	57%	53%
Unsure	12%	10%	11%
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)?	North America	Western Europe	Combined
Yes	29%	30%	29%
No	63%	62%	63%
Unsure	8%	8%	8%
Toral	100%	100%	100%

Q9b. If yes, how do you achieve visibility? Please check all that apply.	North America	Western Europe	Combined
Monitoring third-party data handling practices with Nth parties	37%	33%	35%
Audits and assessments of third-party data handling practices	46%	41%	44%
Reliance upon the third party to notify our organization when our data is shared with their Nth parties	50%	56%	53%
Reliance upon contractual agreements	54%	58%	56%
Use of technology solutions, such as IT threat or security rating feeds	39%	35%	37%
Other (please specify)	2%	3%	2%
Total	228%	226%	227%

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)	North America	Western Europe	Combined
1 or 2	11%	12%	11%
3 or 4	21%	26%	23%
5 or 6	30%	23%	27%
7 or 8	20%	19%	20%
9 or 10	18%	20%	19%
Total	100%	100%	100%
Extrapolated value	5.76	5.68	5.73

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)	North America	Western Europe	Combined
1 or 2	29%	26%	28%
3 or 4	27%	23%	25%
5 or 6	21%	30%	25%
7 or 8	10%	11%	10%
9 or 10	13%	10%	12%
Total	100%	100%	100%
Extrapolated value	4.52	4.62	4.56

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)	North America	Western Europe	Combined
1 or 2	7%	5%	6%
3 or 4	19%	13%	16%
5 or 6	33%	31%	32%
7 or 8	20%	33%	26%
9 or 10	21%	18%	20%
Total	100%	100%	100%
Extrapolated value	6.08	6.42	6.23

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)	North America	Western Europe	Combined
1 or 2	12%	12%	12%
3 or 4	25%	21%	23%
5 or 6	29%	30%	29%
7 or 8	18%	20%	19%
9 or 10	16%	17%	16%
Total	100%	100%	100%
Extrapolated value	5.52	5.68	5.59

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)	North America	Western Europe	Combined
1 or 2	12%	14%	13%
3 or 4	23%	24%	23%
5 or 6	26%	26%	26%
7 or 8	16%	15%	16%
9 or 10	23%	21%	22%
Total	100%	100%	100%
Extrapolated value	5.80	5.60	5.71

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)	North America	Western Europe	Combined
1 or 2	10%	12%	11%
3 or 4	24%	23%	24%
5 or 6	33%	30%	32%
7 or 8	17%	18%	17%
9 or 10	16%	17%	16%
Total	100%	100%	100%
Extrapolated value	5.60	5.60	5.60

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)	North America	Western Europe	Combined
1 or 2	11%	14%	12%
3 or 4	20%	19%	20%
5 or 6	27%	28%	27%
7 or 8	25%	23%	24%
9 or 10	17%	16%	17%
Total	100%	100%	100%
Extrapolated value	5.84	5.66	5.76

Part 2. Attributions

Please rate the following statements using the five-point scale provided below each item. **Strongly Agree & Agree** response combined.	North America	Western Europe	Combined
Q14. Managing outsourced relationship risk is a priority in our organization.	43%	40%	42%
Q15. Our organization allocates sufficient resources to managing outsourced relationships.	42%	38%	40%
Q16. The number of cyber security incidents involving third parties is increasing.	63%	56%	60%
Q17. Our third parties' data safeguards and security policies and procedures are sufficient to prevent a data breach.	39%	42%	40%
Q18. Our third parties' data safeguards and security policies and procedures are sufficient to respond effectively to a data breach.	35%	45%	39%
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.	41%	46%	43%

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?	North America	Western Europe	Combined
Yes	36%	35%	36%
No	54%	57%	55%
Unsure	10%	8%	9%
Total	100%	100%	100%

Q20b. If yes, how do you perform this evaluation? Please check all that apply.	North America	Western Europe	Combined
Review written policies and procedures	56%	52%	54%
Acquire signature on contracts that legally obligates the third party to adhere to security and privacy practices	63%	54%	59%
Obtain indemnification from the third party in the event of a data breach	49%	47%	48%
Conduct an assessment of the third party's security and privacy practices	50%	46%	48%
Obtain a self-assessment conducted by the third party	58%	59%	58%
Obtain references from other organizations that engage the third party	51%	44%	48%
Obtain evidence of security certification such as ISO 2700/27002	43%	47%	45%
Require completion of a data security questionnaire	40%	38%	39%
Other (please specify)	3%	5%	4%
Unsure	4%	3%	4%
Total	417%	395%	407%

Q20c. If no, why don't you perform an evaluation? Please check all that apply.	North America	Western Europe	Combined
We don't have the internal resources to check or verify	31%	29%	30%
We have confidence in the third party's ability to secure information	48%	45%	47%
We rely on the business reputation of the third-party	56%	53%	55%
We have insurance that limits our liability in the event of a data breach	34%	38%	36%
The third party is subject to data protection regulations that are intended to protect our information	48%	45%	47%
The third party is subject to contractual terms	51%	45%	48%
The data shared with the third party is not considered sensitive or confidential	28%	31%	29%
Other	5%	4%	5%
Total	301%	290%	296%

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?	North America	Western Europe	Combined
Yes	26%	23%	25%
No	25%	63%	42%
Unsure	10%	14%	12%
Total	61%	100%	78%

Q21b. If yes, how do you perform this evaluation? Please check all that apply.	North America	Western Europe	Combined
Require third parties to disclose any subcontractors with whom they will share your sensitive or confidential information	39%	34%	37%
Use technologies that can reveal the identity of your third party's subcontractors	42%	39%	41%
Require third parties to obtain your specific approval before they share sensitive or confidential information with a subcontractor	47%	51%	49%
Require signatures on contracts that legally obligate the third party's subcontractors to adhere to security and privacy practices	50%	45%	48%
Obtain indemnification from the third party's subcontractors in the event of a data breach	34%	36%	35%
Conduct an assessment of the third party's subcontractors' security and privacy practices	46%	52%	49%
Obtain references from other organizations that engage the third party's subcontractors	52%	55%	53%
Obtain evidence that third party's subcontractors have a security certification such as ISO 2700/27002	33%	39%	36%
Require completion of a data security questionnaire	40%	44%	42%
Obtain evidence of security certification such as ISO 2700/27002	45%	41%	43%
Require completion of a data security questionnaire	23%	27%	25%
Other (please specify)	6%	9%	7%
Unsure	5%	7%	6%
Total	462%	479%	469%

Q22. What percentage of your third parties do you require to fill out security questionnaires and/or conduct remote or on-site assessments?	North America	Western Europe	Combined
None	4%	7%	5%
Less than 10%	9%	10%	9%
11% to 20%	21%	23%	22%
21% to 50%	27%	25%	26%
51% to 75%	26%	21%	24%
More than 76%	13%	14%	13%
Total	100%	100%	100%
Extrapolated value	40%	37%	39%

Q23a. Do you monitor the security and privacy practices of third parties that you share sensitive or confidential consumer information on an ongoing basis?	North America	Western Europe	Combined
Yes	52%	48%	50%
No	40%	45%	42%
Unsure	8%	7%	8%
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.	North America	Western Europe	Combined
Legal or procurement review	51%	49%	50%
Independent audit or verification by a third party	30%	31%	30%
Automated monitoring tools	47%	43%	45%
Random tests or spot checks	56%	50%	53%
Annual self-certification	46%	43%	45%
Use of security ratings firms	34%	37%	35%
Other	5%	8%	6%
Unsure	6%	9%	7%
Total	275%	270%	273%

Q23c. If no, why doesn't your organization monitor the third parties' security and privacy practices? Please check all that apply.	North America	Western Europe	Combined
We don't have the internal resources to check or verify	39%	34%	37%
We have confidence in the third party's ability to secure information	52%	46%	49%
We rely on the business reputation of the third party	45%	47%	46%
We have insurance that limits our liability in the event of a data breach	32%	36%	34%
The third party is subject to data protection regulations that are intended to protect our information	43%	37%	40%
The third party is subject to contractual terms	40%	45%	42%
The data shared with the third party is not considered sensitive or confidential	48%	41%	45%
The third party will not allow us to independently monitor or verify their security and privacy activities	34%	39%	36%
Other	6%	9%	7%
Unsure	5%	6%	5%
Total	344%	340%	342%

Q24. What information security control standard(s) does your organization use or plan to use? Please check all that apply.	North America	Western Europe	Combined
NIST	54%	39%	47%
ISO 27001/27002	48%	56%	51%
PCI-DSS	41%	41%	41%
HIPAA/HiTrust CSF	25%	12%	19%
COBIT	28%	25%	27%
None of the above	21%	24%	22%
Other (please specify)	9%	11%	10%
Total	226%	208%	218%

Q25a. Does your third-party management program define and rank levels of risk?	North America	Western Europe	Combined
Yes	59%	54%	58%
No	33%	36%	33%
Unsure	8%	10%	9%
Total	100%	100%	100%

Q25b. If yes, what are indicators of risk? Please check all that apply.	North America	Western Europe	Combined
Failed IT security audits, verification or testing procedures	47%	42%	45%
Overall decline in the quality of the third party's services	44%	42%	43%
Discovery that the third party is using a subcontractor that has access to our company's information	36%	39%	37%
Complaints from customers about privacy or security	29%	34%	31%
History of frequent data breach incidents	55%	52%	54%
Legal actions against the third party	29%	28%	29%
Negative media about the third party	24%	28%	26%
IT glitches, operational failures and stoppages	35%	41%	38%
Poorly written security and privacy policies and procedures	42%	45%	43%
Lack of security or privacy training for the third party's key personnel	39%	48%	43%
Lack of screening or background checks for key personnel hired by the third party	43%	49%	46%
High rate of identity fraud, theft or other cybercrimes within the third party's home country	49%	54%	51%
Lack of data protection regulation within the third party's home country	45%	49%	47%
Turnover of the third party's key personnel	51%	52%	51%
Outdated IT systems and equipment	37%	33%	35%
Other	4%	5%	4%
Total	609%	641%	623%

Q25c. If yes, how often are the risk levels updated?	North America	Western Europe	Combined
Never	0%	0%	0%
As needed	19%	18%	19%
Every six months	34%	31%	33%
Annually	30%	28%	29%
Every two years	12%	16%	14%
Unsure	5%	7%	6%
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?	North America	Western Europe	Combined
Yes	41%	38%	40%
No	50%	54%	52%
Unsure	9%	8%	9%
Total	100%	100%	100%

Q26b. If no, why? Please select all that apply.	North America	Western Europe	Combined
Not a priority for the board	36%	33%	35%
Decisions about the third-party risk management program are not relevant to board members	45%	41%	43%
We only provide this information if a security incident or data breach has occurred involving a third party	56%	60%	58%
Unsure	4%	6%	5%
Total	141%	140%	141%

Part 4. Demographics and organizational characteristics

D1. What organizational level best describes your current position?	North America	Western Europe	Combined
Senior Executive/VP	14%	12%	13%
Director	17%	16%	17%
Manager	21%	19%	20%
Supervisor	12%	16%	14%
Technician/staff	29%	30%	29%
Contractor	4%	5%	4%
Other	3%	2%	3%
Total	100%	100%	100%

D2. Check the Primary Person you report to within the organization.	North America	Western Europe	Combined
CEO/executive committee	9%	8%	9%
Chief financial Officer	2%	3%	2%
General counsel	5%	8%	6%
Chief privacy officer	2%	3%	2%
Chief information officer	31%	27%	29%
Compliance officer	15%	14%	15%
Human resources VP	4%	3%	4%
Chief information security officer (CISO)	17%	16%	17%
Chief risk officer	10%	12%	11%
Other	5%	6%	5%
Total	100%	100%	100%

D3. What industry best describes your organization's industry focus?	North America	Western Europe	Combined
Aerospace & defense	1%	0%	1%
Agriculture & food services	1%	2%	1%
Communications	3%	3%	3%
Education & research	2%	1%	2%
Energy & utilities	4%	5%	4%
Entertainment & media	3%	2%	3%
Financial services	18%	17%	18%
Healthcare	7%	8%	7%
Hospitality	3%	2%	3%
Manufacturing & Industrial	11%	12%	11%
Pharmaceuticals	6%	5%	6%
Public sector	11%	12%	11%
Retailing	10%	10%	10%
Services	9%	11%	10%
Technology & software	8%	8%	8%
Transportation	3%	2%	3%
Total	100%	100%	100%

D4. What is the worldwide headcount of your organization?	North America	Western Europe	Combined
Less than 500 people	19%	22%	20%
501 to 1,000 people	21%	25%	23%
1,001 to 5,000 people	23%	23%	23%
5,001 to 25,000 people	18%	15%	17%
25,001 to 75,000 people	11%	10%	11%
More than 75,000 people	8%	5%	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 hold 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.

RiskRecon, a Mastercard Company

RiskRecon, a Mastercard Company, enables you to achieve better risk outcomes for your enterprise and your digital supply chain. RiskRecon's cybersecurity ratings and assessments make it easy for you to understand and act on your risks, delivering accurate, risk-prioritized action plans custom-tuned to match your risk priorities. Learn more about RiskRecon and request a demo at www.riskrecon.com