cyber GRX

Ponemon INSTITUTE

The Cost of Third-Party Cybersecurity Risk Management

Sponsored by CyberGRX

Independently conducted by Ponemon Institute LLC
Publication Date: March 2019

Table of Contents

Want to learn more?

We sat down with Larry Ponemon, Chairman and Founder, Ponemon Institute and David Monahan, Research Director at Enterprise Management Associates (EMA) to discuss highlights of the study and recommendations to help you tackle your organization's third-party cyber risk management strategy.

WATCH THE WEBINAR

Part 1. Executive Summary

CyberGRX and Ponemon Institute surveyed over 600 IT security professionals to learn more about the cost and efficacy of the tools and processes used to conduct third-party cyber risk management today. The survey respondents come from a variety of industries and are all involved in managing their organizations' third-party cyber risk management programs (TPCRM). All organizations represented in the study have TPCRM programs and believe it is critical to have cybersecurity risk management controls in place.

When it comes to vetting and evaluating third parties...

Third parties are inundated

15,000+ hours
spent on completing assessments each year

Enterprises aren't getting insights

54% say data is only somewhat valuable

Less than 8% of assessments result in action

The cost of failure is high

70% believe cost of failure is **$13 million**
(costs include impact on reputation and brand, decreases in share value, loss of business, etc.)

Quick Stats

$2.1 million is the average annual spend on vetting third parties	However →	64% say the processes used are only somewhat or not effective
40% of organizations use manual procedures, like spreadsheets and 51% employ risk scanning tools, to vet their third parties	However →	34% said results of these tools are only somewhat valuable while 20% said results don't provide any insights
Third parties are spending 15,000 hours a year on completing assessments, at an average cost of $1.9 million annually	However →	Over 55% said these assessments only somewhat or do not accurately reflect their security posture
Only 8% of assessments result in action (eg. disqualification of a vendor or a requirement to remediate gaps)	However →	If assessments revealed gaps, only 26% of respondents say their organizations terminated the relationship

Here are the biggest takeaways for key decision makers:

- Current practices and technologies used to support TPCRM and assess third parties are costly and often inadequate and inefficient.
- Investing in better assessment and vetting tools can increase effectiveness in TPCRM while decreasing the cost of maintaining the program.
- Applying the same approach to all third parties can be costly - taking the time to prioritize third parties and apply an appropriate level of due diligence to them will reduce costs and increase efficiencies in the long run.
- Control over budgets for third-party cybersecurity risk management is dispersed throughout the organization which can make the allocation of resources inefficient because of management interests in the various functions.

Part 2. Overview of Findings

Third-party breaches remain a dominant security challenge for organizations, with over 63%[1] of breaches linked to a third party. To prevent or mitigate the severity of a third-party data breach or cyber exploit, organizations can implement a variety of cybersecurity risk management controls such as assessing compliance with regulations, vetting third-party security practices and establishing data breach and cyber exploit incident response procedures. We created this study to learn if the current processes and controls organizations employ today to mitigate third-party related breaches are effective and provide a return on investment. The results reinforced our hypothesis that the majority of organizations believe their current TPCRM processes are not as effective as they should be. As a result, both organizations and their third parties are wasting critical financial and human resources on programs that aren't optimized to help them reduce cyber risk in their shared ecosystems.

Procedures used to evaluate and vet third-parties' security practices are costly but not effective. As shown in Figure 1, 42% of respondents are spending an average of between $1 million to $10 million annually to vet their organization's business partners, vendors, contractors and other third parties' information security protection capabilities beyond just compliance measures. Figure 2 shows what tools and/or approaches are used to assess third parties.

Figure 1. The estimated annual cost to evaluate and vet third parties' security practices

Measured in US$ | Extrapolated value = $2,096,750

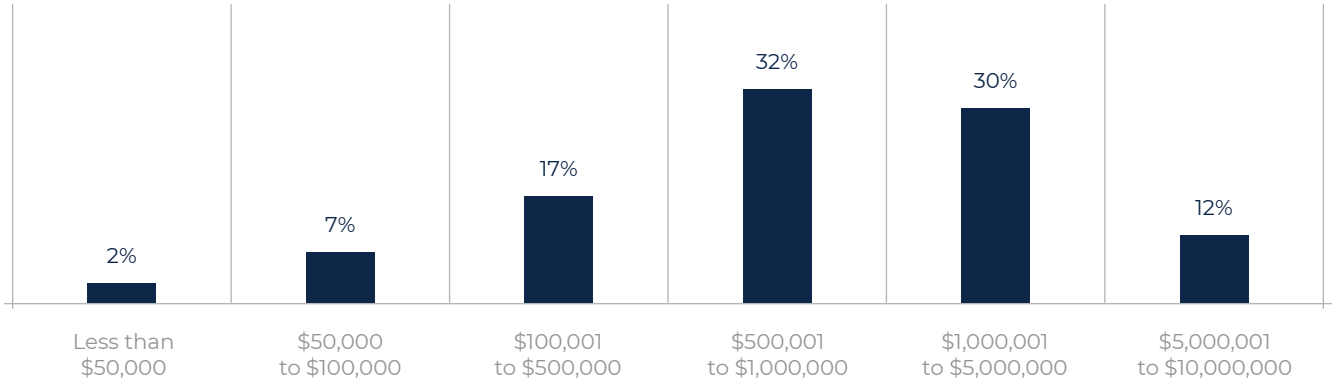
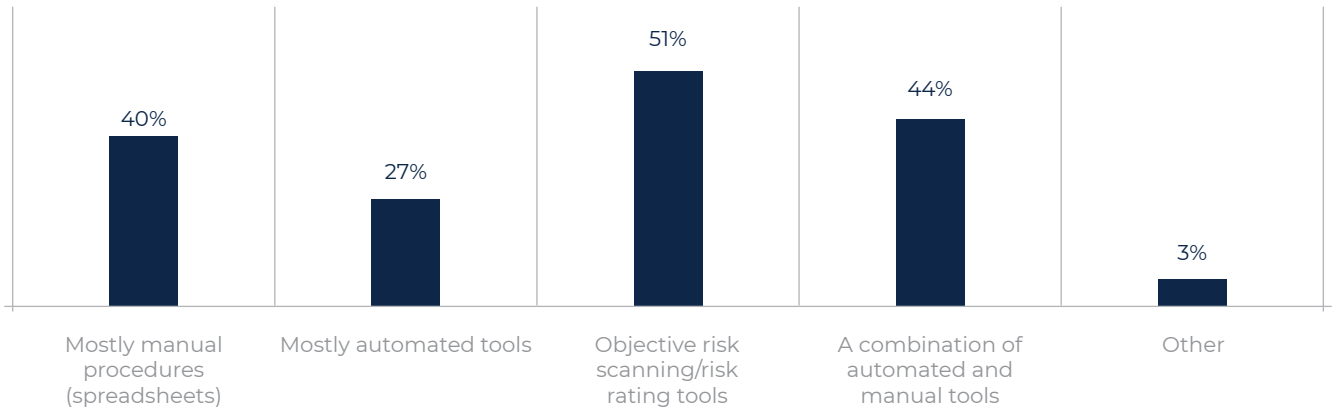


Figure 2. The tools used to assess third parties (select all that apply)

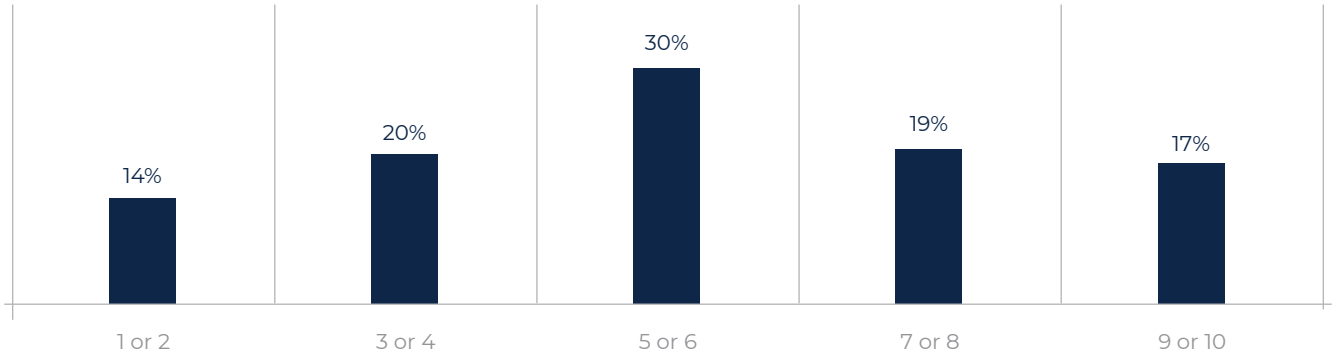


Manual procedures (spreadsheets) and risk rating tools are still the dominant methods for assessing vendors. However, when respondents were asked to rate the effectiveness of vetting third parties' security practices from 1 = ineffective to 10 = very effective, **only 36% of respondents say they are highly effective (7+ ratings) in vetting third parties' security protection capabilities**, as shown in Figure 3.

[1] Soha Systems, Third Party Advisory Group 2016 IT Survey Report

Figure 3. How effective is the evaluation and vetting of third-parties' security practices?

From 1 = ineffective to 10 = very effective
Extrapolated value = 5.60



Industry Insights

This research also highlighted differences in TPCRM practices among the following industries: financial services, health/pharma, public sector, retail, and technology/software. Below are the most notable differences.

In the past two years, financial service companies had more third-party breaches than the overall sample of respondents (56% vs. 53%). This is despite the fact that third-party companies in this sector spend the most time completing assessments of their cybersecurity practices (17,588 hours annually).

- Reducing time spent on those assessments would allow third parties to spend more time on cybersecurity measures.

Health/pharma organizations were less likely to have had a third-party data breach.

- More health/pharma companies are using a combination of automated and manual tools. This combination of tools seems to increase effectiveness as almost half of respondents in these organizations say the results of these assessments are very valuable and are used to report to the C-suite and board of directors.

Third-party organizations in the public sector believe the process for completing assessments is essential or very important and spend an average of 15,327 hours annually completing them.

- Public sector organizations are also more likely to use automated tools or a combination of manual and automated tools to assess their third parties and believe these assessments are very valuable.

Like financial services companies, retail companies reported more third-party data breaches than other industries, despite third parties in this industry spending an average of 16,578 hours annually on assessments of their cybersecurity practices.

- Despite all the time spent on filling in assessment spreadsheets, retail organizations are most likely to rate these assessments as not resulting in an accurate depiction of their security posture.

Technology and software companies were the most likely to have multiple third-party data breaches.

- Third parties in this industry sector are spending 15,543 hours annually on assessments but almost all rate these assessments as not an accurate depiction of their organization's security posture.
- Despite being in the technology/software industry, 41% of respondents say their organizations use mostly manual. procedures to assess their third parties.

Industry Quick Stats

Financial Services	Reported the second most third-party breaches despite their third parties spending the most time on assessments (over 17,000 hours/year)
Health & Pharma	Less likely to have a third-party breach and most likely to use a combination of tools to assess third parties
Public Sector	Use a combination of tools to assess third parties and tend to believe their results are valuable
Retail	Reported the most third-party data breaches despite their third parties spending over 16,578 hours on assessments
Technology & Software	Most likely to have multiple third-party data breaches, and over 41% still use manual procedures to assess third parties

Summary of Findings

The results of this study illustrate a persistent theme that organizations (both third parties and the organizations assessing them) see their third-party cyber risk management procedures as important but ineffective.

- **Third-party breaches remain an expensive problem.**
  Over 53% of respondents have experienced a third-party data breach in the past 2 years at an average cost of $7.5 million.
- **IT security professionals still believe their TPCRM programs are immature.**
  58% of respondents described their TPCRM programs as early (not deployed) or middle stage (only partially deployed).
- **Using a combination of automated tools provides better results.**
  While most organizations still rely on manual spreadsheets or risk ratings tools, industry analysis found that organizations that relied on a combination of tools found their results more valuable.
- **Risk prioritization processes are viewed as critical, but current processes are ineffective.**
  Cloud and payroll providers do this the best (56% and 49% of respondents, respectively). Only 30% of respondents say they prioritize data centers that have access to their information.
- **If third-party security gaps are discovered, organizations are not proactive in mitigating these risks.**
  Only 24% of respondents say their organizations collaborate with third parties to improve their security measures. Most often organizations will request—not require—mitigation of the security gaps.
- **No one function controls the budget for third-party cyber risk management programs (TPCRM).**
  Less than half of respondents say their organizations specifically earmark funds to support their TPCRM. Further, accountability for the allocation of resources to third-party cyber risk management efforts is dispersed throughout the organization.
- **Investing in better assessment and vetting tools can increase effectiveness in TPCRM while decreasing the cost of maintaining the program.**
  Our research shows that there is a correlation between TPCRM effectiveness and the amount of money companies spend on all the activities for the deployment of controls. Effectiveness of these controls not only means better management of third-party risks but also greater efficiencies that lead to lower costs.

Bottom line, there is a massive disparity between the resources invested (both human and financial) and the value received from today's approach to TPCRM.

Part 3. Key Findings

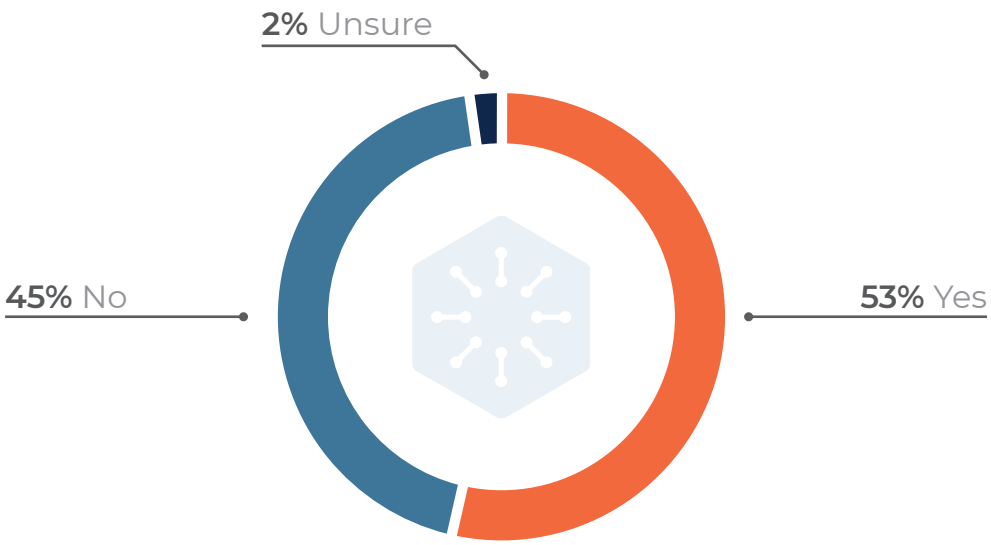
In part 3, we present an analysis of the key findings. The complete audited findings are presented in the Appendix of this report. The findings are organized by the following themes:

The Cost and Effectiveness of Third-Party Cyber Risk Management Controls

The findings in this section highlight that while various TPCRM controls are deployed, deployment and cost do not equal effectiveness. For instance, third party vetting is the most deployed control, but was rated the least effective. In fact, we found that as effectiveness increases, the cost of these controls starts to decline because highly effective companies are better able to manage constrained resources and improve their risk management practices at given levels of spending.

To stop data breaches caused by third parties, rigorous due diligence and assessment of third-parties' security and data protection practices is critical. As shown in Figure 4, third-party data breaches are affecting most organizations. More than half of respondents (53%) say their organizations have experienced one or more data breaches caused by a third party over the past two years. The average cost to remediate these breaches was $7.5 million over the past two years.

Figure 4. Has your organization experienced one or more data breaches caused by a third party over the past two years?



The most common TPCRM practice is evaluation and vetting of third parties.

The study focuses on the following six controls, procedures and practices commonly used to manage third-party cybersecurity risks. Of these controls, the most deployed is the evaluation and vetting of third parties' security practices (85% of respondents) and data breach and cyber exploit incident response procedures (83% of respondents).

The Six Controls by Definition

1. **Regulatory compliance controls.**
   Conduct periodic assessments and monitor third parties to ensure compliance with contractually required security requirements and data protection and privacy regulations, such as the EU's General Data Protection Requirement (GDPR) and the California Consumer Privacy Act (CCPA).

2. **Procedures for enforcing non-compliance with an organization's security requirements.**
   Establish enforcement actions, termination penalties and remediation requirements for third parties that fail to achieve the organization's objective security requirements.

3. **Evaluation and vetting of third-parties' security practices.**
   Establish a process to evaluate and vet the organization's business partners, vendors, contractors and other third parties' information security protection capabilities beyond just compliance measures. This assumes the organization conducts the evaluation using a validated risk assessment and ensures these third parties are vetted against objective security requirements (i.e., NIST, PCI-DSS, ISO).

4. **Third-party liability mitigation.**
   Establish procedures to ensure that contracts with third parties limit the organization's liability should the third party have a data breach or cyberattack that compromises the organization's information assets. Periodically review the third-party's insurance policies to ensure the adequacy of coverage.

5. **Data breach and cyber exploit incident response procedures.**
   Establish procedures to respond to a data breach or cyber exploit caused by one of an organization's third parties. These procedures can include formal documentation of incident response procedures, fire drills to practice response plans and the assignment of responsibility for communicating with customers, regulators, law enforcement and other key stakeholders.

6. **Risk prioritization process.**
   Establish a risk prioritization process for the assessment and due diligence of third parties. Such a process could be based upon the type, value and business criticality of information assets the organization shares with the third party.

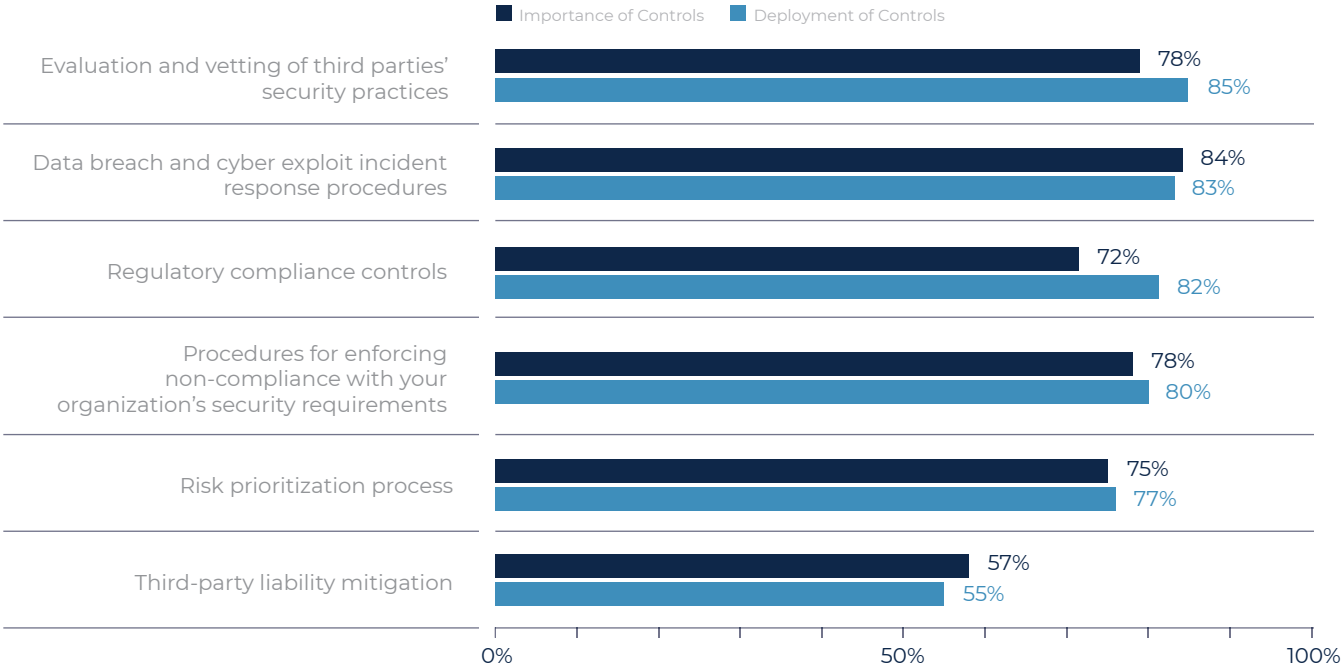
Companies believe these six TPCRM controls are critical and have deployed them in their organization, however deployment does not equal effectiveness.

Figure 5 shows the percentage of respondents who say their organizations are deploying the controls and how important they believe these controls to be. The majority of respondents have TPCRM controls, practices or procedures either fully or partially deployed. The most deployed are evaluation and vetting of third parties' security practices (85% of respondents) and data breach and cyber exploit incident response procedures (83% of respondents).

Respondents were asked to rate the importance of a control from 1 = not important to 10 = very important. Figure 4 also presents the very important responses (7+ on the 10-point scale). As shown, the most important controls are those that help organizations prepare for a data breach or cyber exploit incident (84% of respondents) followed by evaluating and vetting third parties' security practices and enacting procedures for enforcing non-compliance with your organization's security requirements (both 78% of respondents).

Figure 5. The deployment and importance of TPCRM controls

Fully and partially deployed responses combined
From 1 = not important to 10 = very important, 7+ responses presented



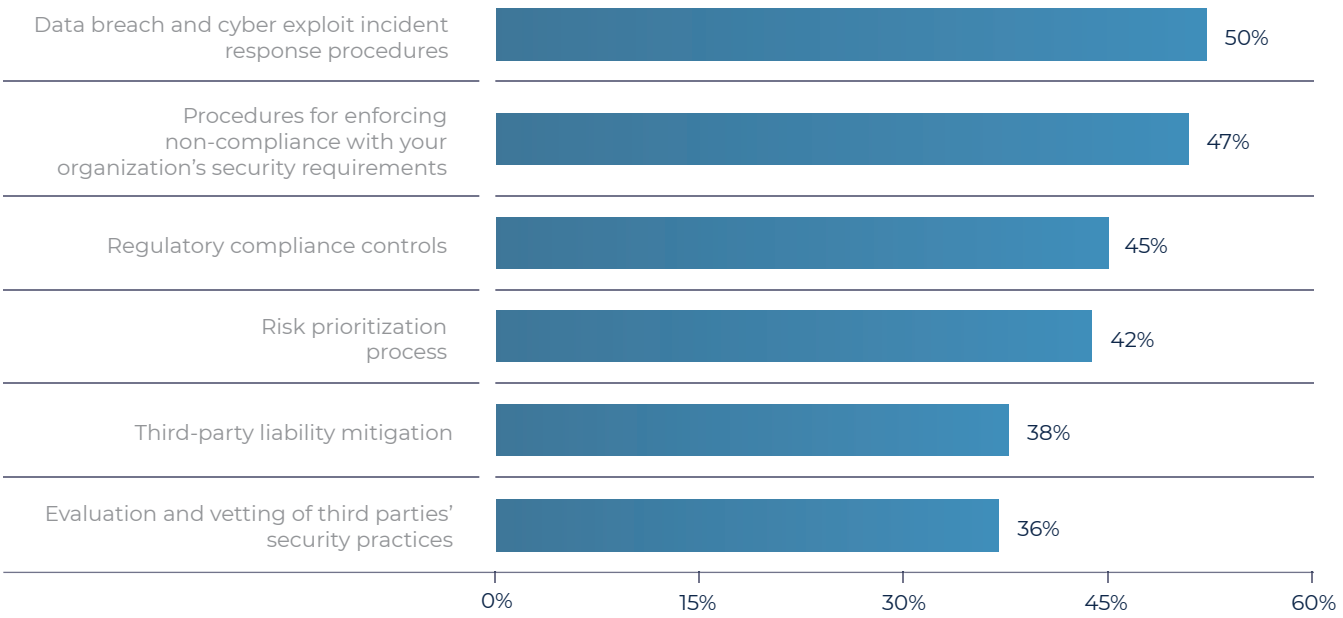
Organizations are least effective at evaluating and vetting third parties and third-party liability mitigation.

Respondents were asked to rate the effectiveness of a TPCRM control in reducing the cost of a third-party data or cybersecurity breach on a scale of 1= ineffective to 10 = very effective. Figure 6 presents the very effective responses (7+ responses).

As shown, 50% of respondents say their organizations are very effective in reducing costs of a third-party data or cybersecurity breach by implementing data breach and cyber exploit incident response procedures. However, only 36% of respondents say their organizations are very effective in reducing the cost of a third-party data or cybersecurity breach through their evaluation and vetting of third-parties' security practices.

Figure 6. How effective is your organization at implementing the following controls or practices in reducing the cost of a third-party data or cybersecurity breach?

From 1 = ineffective to 10 = very effective, 7+ responses presented



The costliest controls to implement and maintain are the ones most often deployed and most important to reducing the risk of a third-party data breach. The most deployed controls are evaluation and vetting of third parties' security practices (85% of respondents) and data breach and cyber exploit incident response procedures (83% of respondents). See Figure 5.

These controls are also the costliest to maintain, according to Table 1. Respondents estimate that the average annual cost to implement and maintain data breach and cyber exploit incident response procedures is $3.4 million and the cost to evaluate and vet third-parties' security practices is $2.1 million. To implement all controls or practices costs an average of $11.3 million.

Table 1. Annual cost to implement and maintain third-party controls or practices	Extrapolated Cost
Regulatory compliance controls	$1,697,250
Procedures for enforcing non-compliance with security requirements	$1,819,000
Evaluation and vetting of third-parties' security practices	$2,096,750
Third-party liability mitigation	$1,031,250
Data breach and cyber exploit incident response procedures	$3,373,500
Risk prioritization process	$1,260,250
Total	$11,278,000

Investing in better assessment and vetting tools can increase effectiveness in TPCRM while decreasing the cost of maintaining the program.

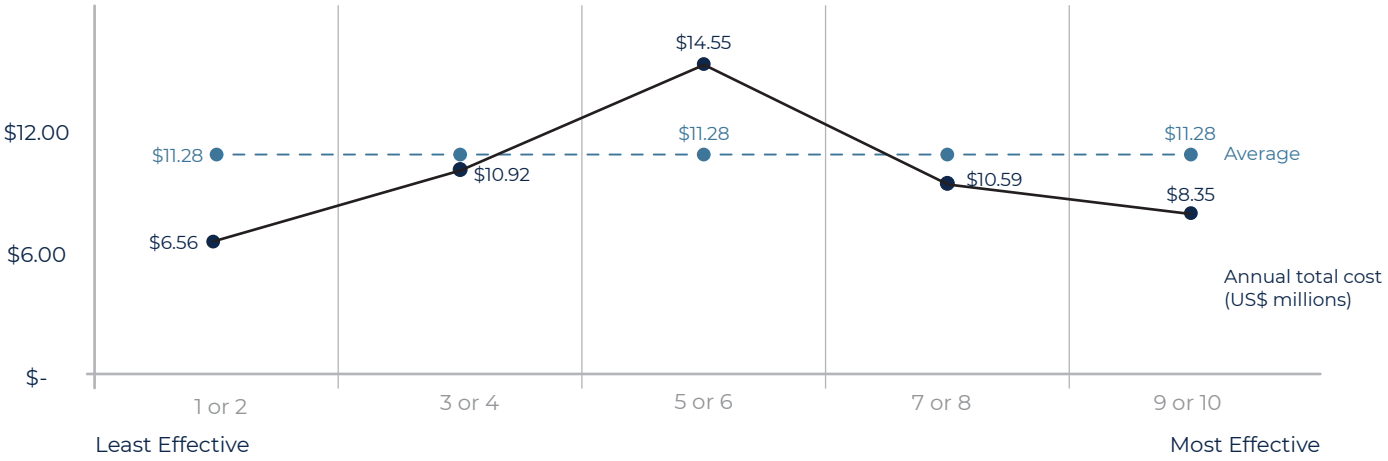
This analysis demonstrates that there is a financial incentive to becoming more effective in managing third-party risk. Figure 7 shows the total cost to implement and maintain all six of the third-party controls at five ascending levels of effectiveness as rated by respondents in this study. The estimated total cost for all six control practices is $11.28 million per annum.

As figure 7 shows, increasing effectiveness in managing third-party risk can reduce the average overall cost of having these controls in place. Specifically, those organizations that are only moderately effective (5 and 6 on the ten point scale) are spending the most ($14.55 million), which suggests that there are significant inefficiencies in how they are managing activities associated with the controls. However, as effectiveness increases, the cost of these controls starts to decline because highly effective companies are better able to manage constrained resources and improve their risk management practices at given levels of spending. For instance, as effectiveness increases to the 7+ range the cost for maintaining these controls decreases to $10.59 million. Increasing effectiveness can be achieved through investment in better tools, in-house expertise and more efficient processes.

Understandably, companies that have a low level of effectiveness (1 to 2) are not spending enough to ensure control practices are effective. These companies spend an average of $6.56 million annually on controls that are really not making a difference in protecting them from the possibility of a third-party data breach or security exploit.

Figure 7. Annual total cost to implement and maintain third-party controls or practices

Consolidated view for six controls used to manage third party risk.
US$ millions



When organizations fail to effectively implement a control or practice, the cost of failure can be far more than the cost to implement and maintain.

As shown in Table 2, a control practice that is not implemented effectively becomes costlier as a result of having to deal with potential security incidents and data breaches. The costliest are when data breach and cyber exploit incident response procedures are ineffective ($18.7 million) and when evaluation and vetting of third-parties' security practices are ineffective ($13.4 million).

Table 2. The annual cost if the organization failed to implement the control or practice at a high level of effectiveness	Extrapolated Cost
Regulatory compliance controls	$4,487,250
Procedures for enforcing non-compliance with security requirements	$5,630,250
Evaluation and vetting of third-parties' security practices	$13,413,000
Third-party liability mitigation	$3,083,250
Data breach and cyber exploit incident response procedures	$18,700,500
Risk prioritization process	$4,847,250
Total	$50,161,500

The Assessment and Prioritization of Third-Party Cyber Risk

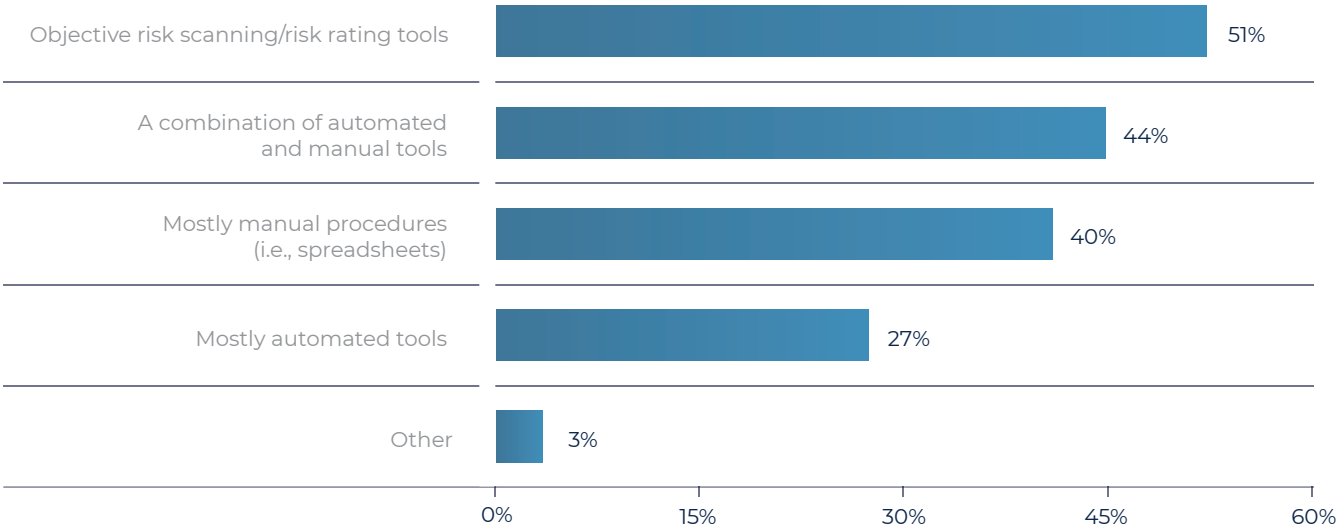
The findings in this section reveal that the current methods used to assess and prioritize third-party risks can prevent companies from making their controls more effective. The successful deployment of TPCRM controls is dependent upon information from assessments about their third parties' security and data protection practices. However, the results of these assessments are considered only somewhat valuable and are not helpful in the prioritization of third-party risks. Moreover, the appropriate allocation of resources is affected by the lack of centralized control over the budget for third-party risk management controls.

Objective risk scanning/risk rating tools are most often used to assess third parties.

Followed closely by a combination of automated and manual procedures, like spreadsheets, risk rating tools are the primary go to when it comes to assessing third parties. The goal of these tools is to help identify and prioritize the potential risk posed by a third party, incorporating industry information and the specific relationships between an organization and a third party. The reality, however, is only 46% of organizations find these tools provide valuable insights.

Figure 8. What assessment tools does your organization use to assess third parties?

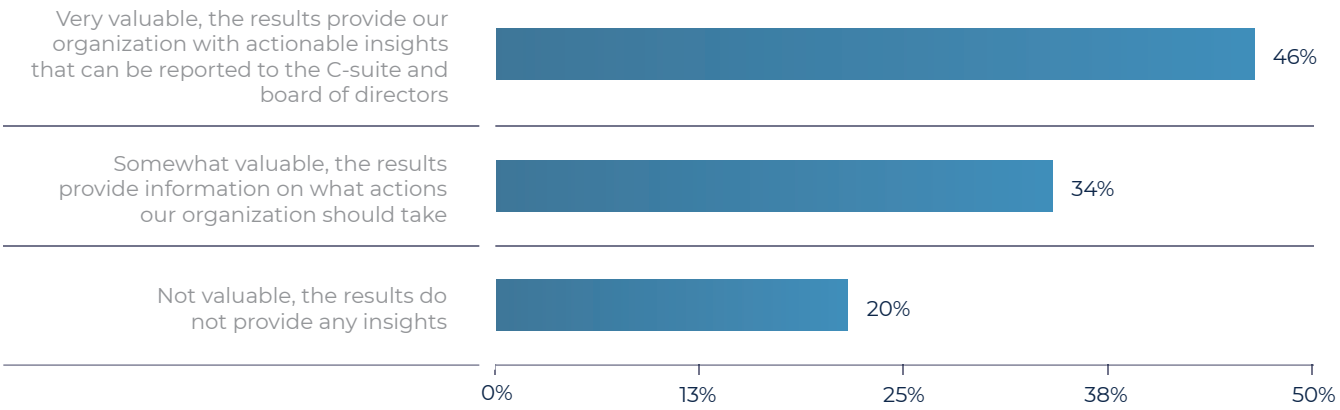
More than one response permitted



54% of respondents believe that information provided from the risk rating and manual assessments is only somewhat or not valuable.

Assessments are conducted to ensure third parties have the necessary security practices in place. They also are intended to assure the company's leadership that any security gaps are revealed and are being addressed. However, as shown in Figure 9, 34% of respondents say the information from third-party assessments is only somewhat valuable and another 20% of respondents say the results do not provide any insights.

Figure 9. How valuable are the results of these assessments?



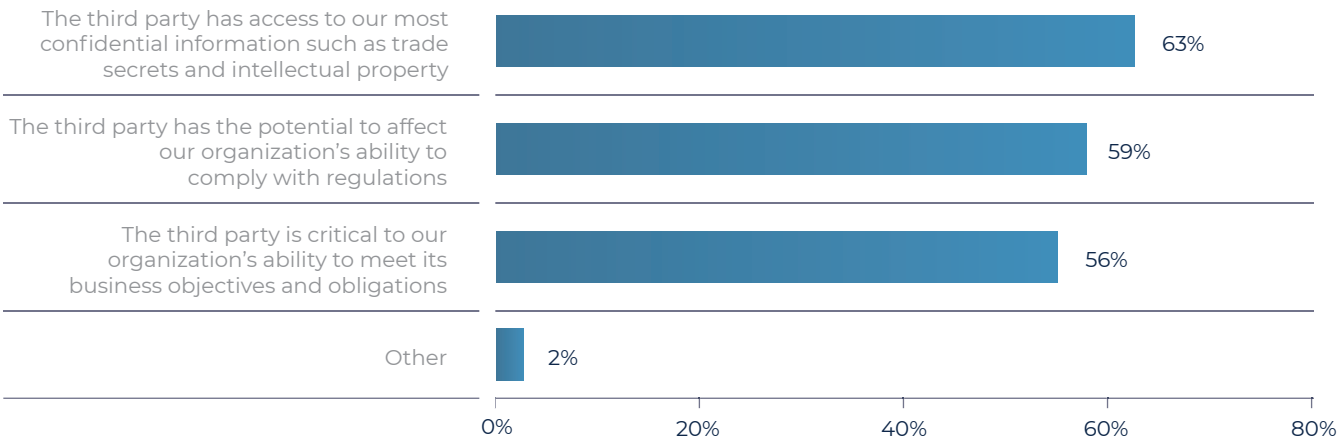
Certain third parties should receive a more comprehensive assessment or level of due diligence than other third parties. 56% of respondents say their organizations require some of their third parties to be subject to a more thorough assessment of their security practices. The remaining 44% apply the same level of due diligence to all their third parties.

The extrapolated cost of not implementing some prioritization process is $4.8 million, which is 4 times the cost of prioritizing third parties. This indicates that taking the time to prioritize third parties and apply an appropriate level of due diligence to them will reduce costs and increase efficiencies in the long run.

For those that do apply different levels of due diligence, Figure 10, illustrates some factors that indicate high priority: third parties that have access to their most confidential information such as trade secrets and intellectual property (63% of respondents), have the potential to affect their organization's ability to comply with regulations (59% of respondents) and are critical to their ability to meet its business objectives and obligations (56% of respondents).

Figure 10. How does your organization determine which third parties should receive due diligence/assessments?

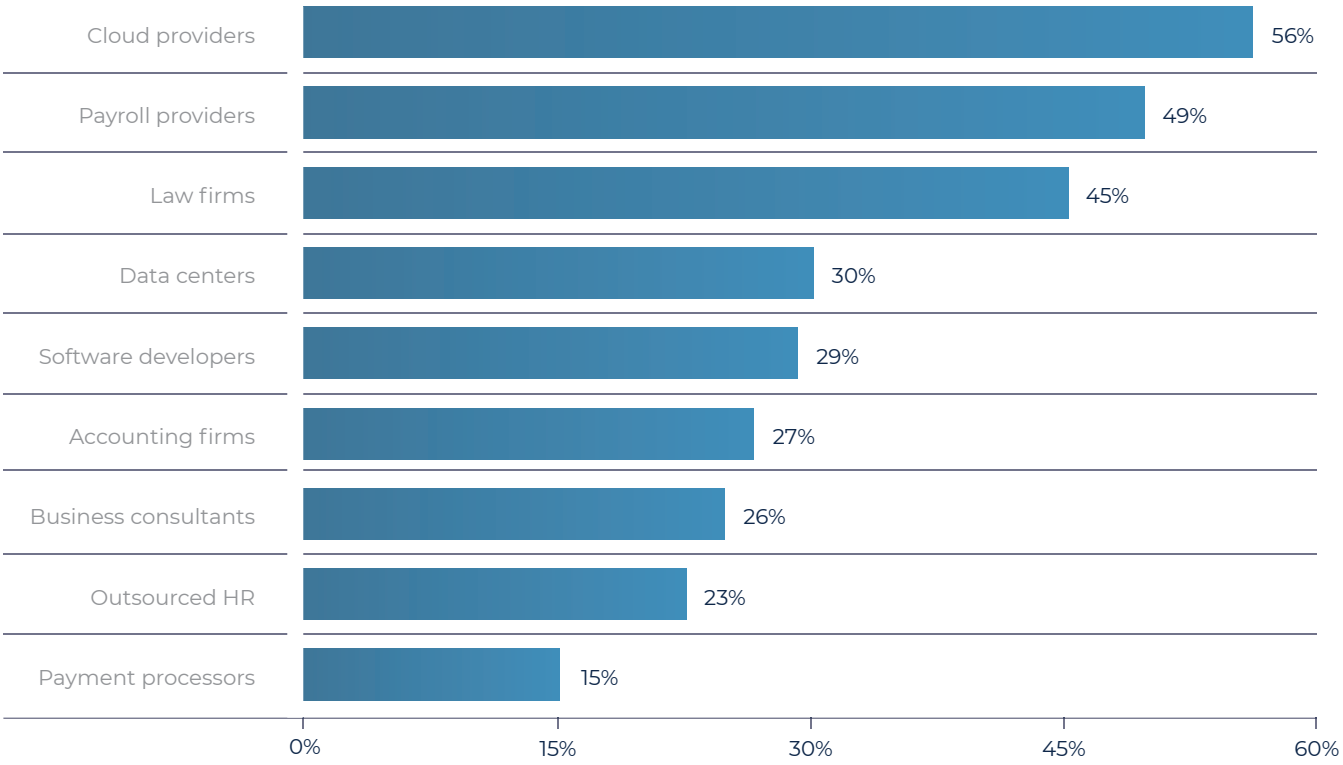
More than one response permitted



Cloud providers are most often selected for a more comprehensive assessment.

According to Figure 11, 56% of respondents say cloud providers and 49% of respondents say payroll providers are selected for additional assessments. These third parties have access to an organization's most confidential information and are critical to supporting its business objectives and obligations.

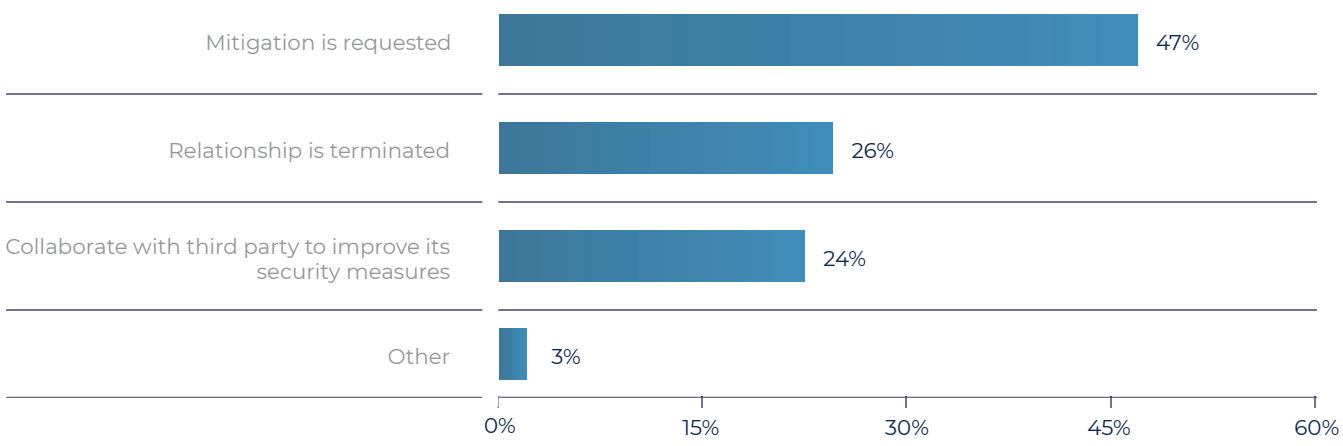
Figure 11. What types of third parties does your organization prioritize and focus its due diligence on?



If third-party security gaps are discovered, organizations take very little action to reduce their vulnerability to a possible data breach.

According to Figure 12, only 24% of respondents say their organizations are proactive in improving the third party's security measures through collaboration. Almost half (47% of respondents) say their organizations request—but do not require—mitigation.

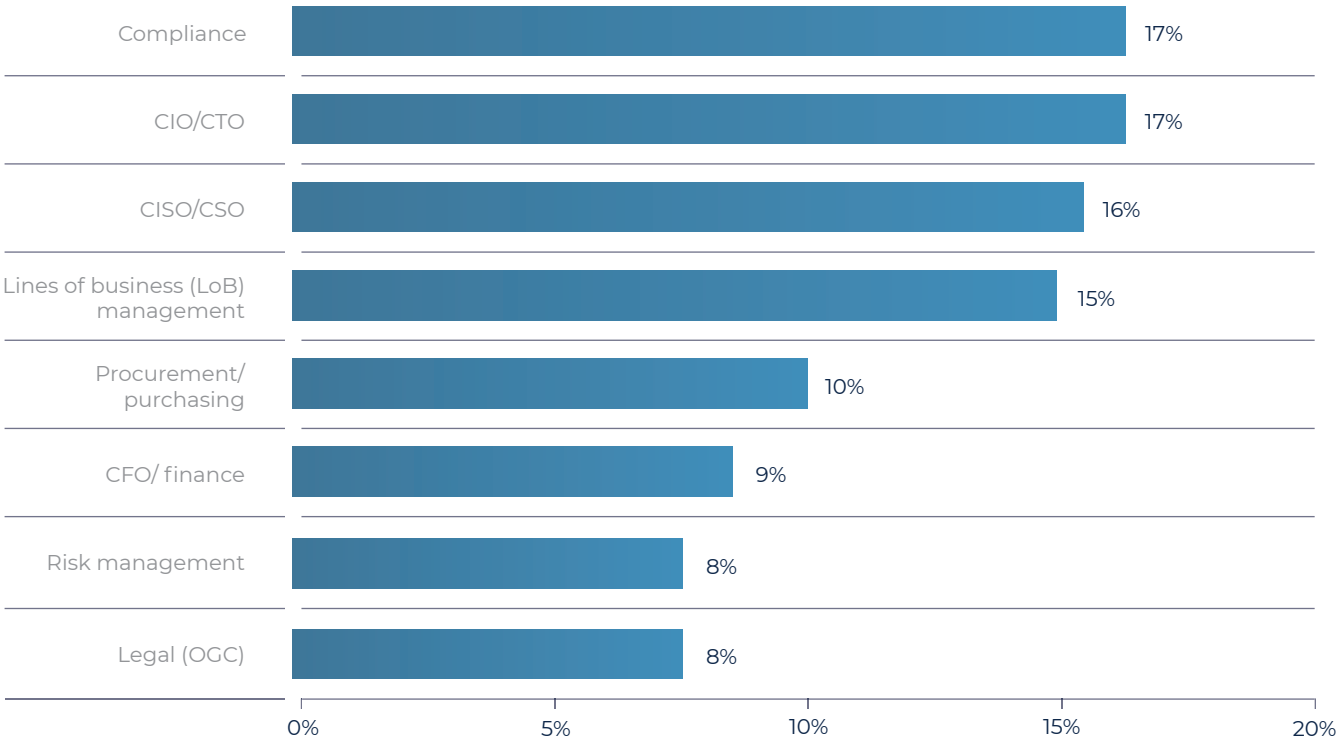
Figure 12. Actions taken if a third party has gaps in its security controls or practices



Control over budgets for third-party cybersecurity risk management is dispersed throughout the organization. Less than half of respondents say their organizations earmark funds to support its third-party cybersecurity risk management program. If they do, the average budget for the program is $7.1 million.

According to Figure 13, not one function clearly owns the third-party risk management budget. The three functions that have the most control are the CIO/CTO and compliance (both 17% of respondents) and the CISO (16% of respondents). The lack of centralized control can make the allocation of resources inefficient because of competing interests in the various functions.

Figure 13. Who controls the budget for third-party cybersecurity risk management?



The Cost and Impact of Assessments on Third Parties

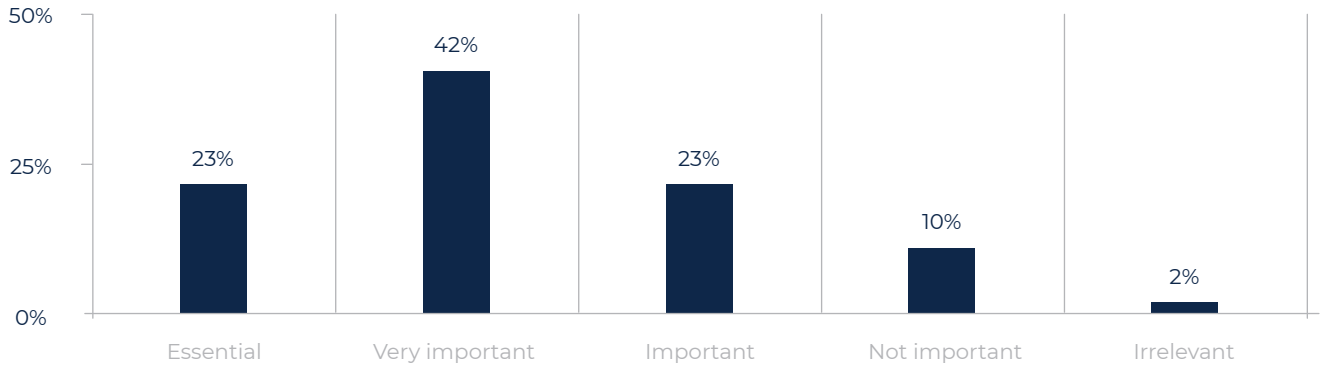
Third parties are devoting an average of more than 15,000 hours annually completing assessments of their security practices because they believe they are important for their customers. Yet, despite the average cost of $1.9 million to complete these assessments, the information they yield is often not considered to be valuable or accurate in their depiction of their security practices and their customers are only taking action on 8% of them.

Third parties believe customer assessments are important, but many believe these assessments do not accurately reflect their security posture. 78% of respondents say their organizations are third parties and are required to complete assessments of their security practices and controls. As shown in Figure 14, almost all respondents in third-party organizations (88%) believe it is important to have a process for completing assessments of their security practices and controls.

Third parties are spending **15,000** hours a year on completing assessments, at an average cost of **$1.9 million** annually.

Only **8%** of assessments result in action (eg. disqualification of a vendor or a requirement to remediate gaps)

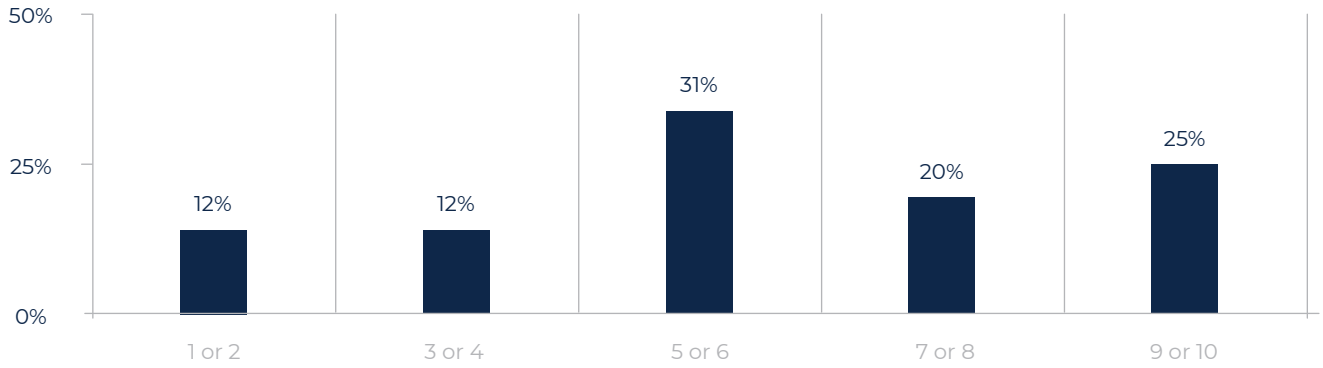
Figure 14. How important is the process for completing customer assessments of your organization?



Despite the investment in time and budget, the majority of respondents say these assessments are not helpful in demonstrating the security controls and practices they have in place. Respondents were asked to rate the accuracy and effectiveness of these assessments on a scale of 1 = not accurate to 10 = very accurate.

As shown in Figure 15, 55% of respondents say these assessments do not accurately reflect their organizations' security posture (responses 1 to 6 on the ten-point scale). This suggests the need for third-party assessments that address the potential damage that a third party could cause based on criticality of the relationship between the organization and the third party.

Figure 15. How effective or accurate are assessments at reflecting your organization's security posture?

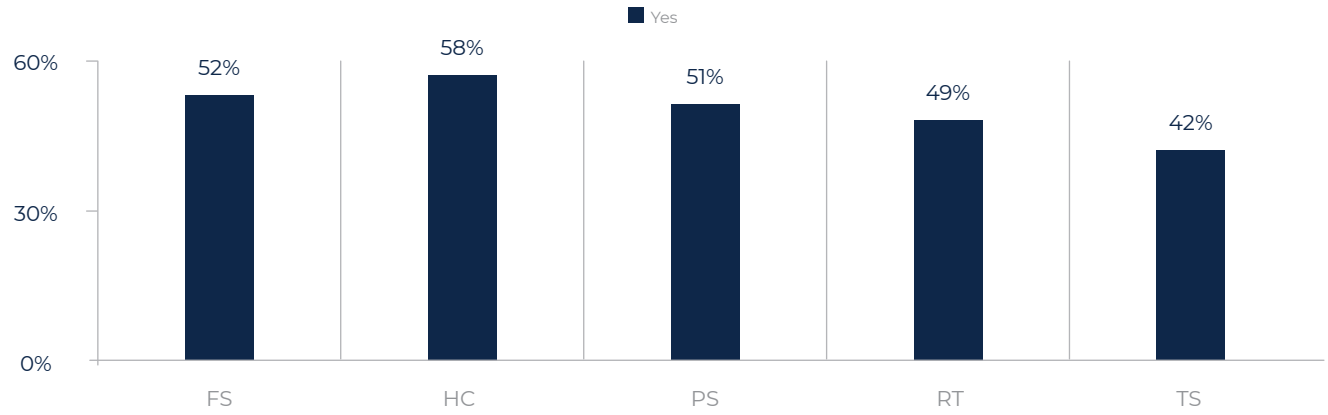


Industry Differences in TPCRM Assessments and Controls

In this section, we provide the most salient differences among the industries represented in this research. These industries include: financial services (FS), health/pharmaceuticals (HC), public sector (PS), retail (RT), technology and software (TS).

Highly regulated industries are more likely to require more comprehensive assessments or level of due diligence than the other industries represented in this research. According to Figure 16, health/pharma (58% of respondents) and financial services (52% of respondents) say some of their third parties receive a more comprehensive assessment or level of due diligence than other third parties. Only 42% of respondents in technology and software identify and require some third parties to be subject to greater due diligence.

Figure 16. Do some of your organization's third parties receive a more comprehensive assessment or level of due diligence than other third parties?



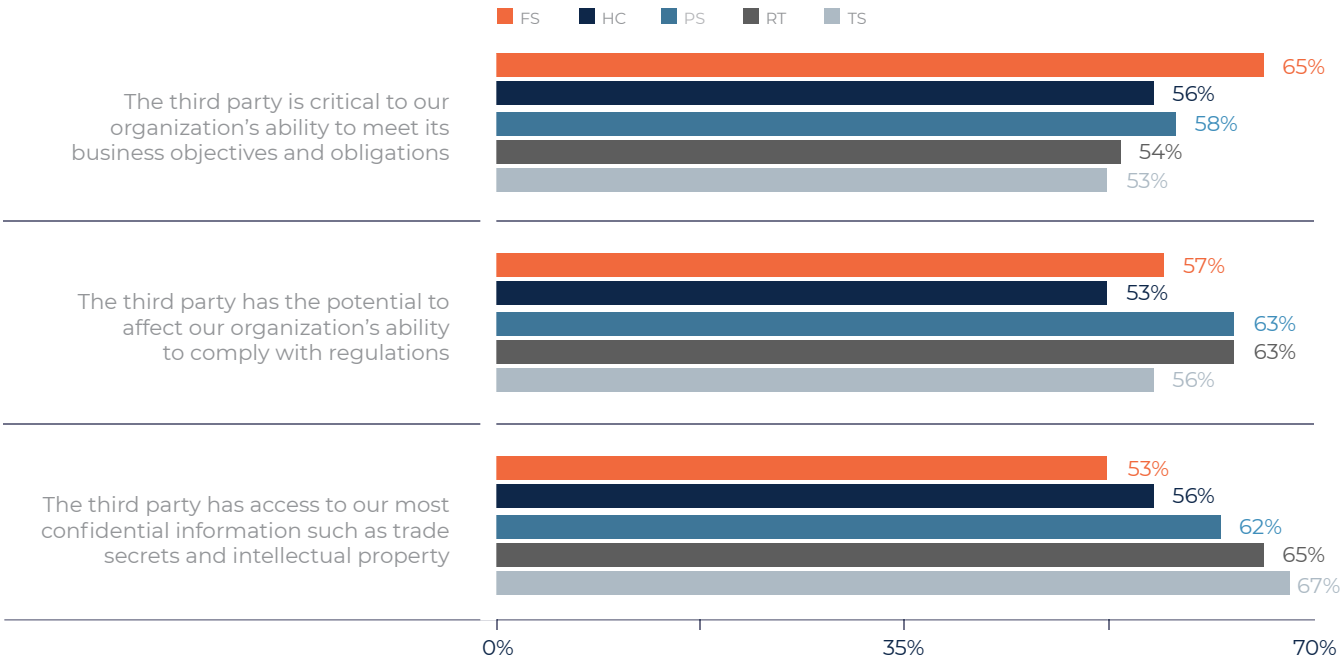
How organizations determine the third parties to prioritize is influenced by the potential damage a third-party can do if a security exploit or data breach occurs. As shown in Figure 17, financial service organizations are most likely to prioritize risks according to how the third party could affect its ability to meet business objectives and obligations.

65% of respondents in financial services prioritize risks based on the potential impact on the ability of their organizations' business objectives and obligations to their customers and other key stakeholders. Specifically, the protection of personal financial information and the assurance customers' will be able to complete transactions in a timely and secure manner.

63% of respondents in the public sector and retail say the potential to affect their ability to comply with regulations is how they prioritize third parties for more in-depth assessment. Retail and technology are concerned about protecting their most confidential information such as trade secrets and intellectual property.

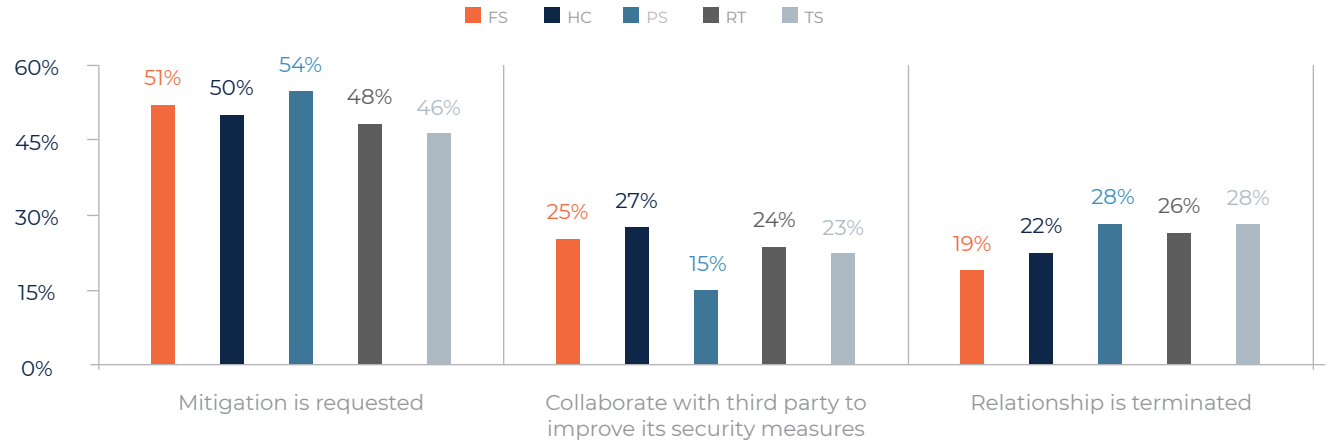
Figure 17. If yes, how do you determine which third parties to prioritize?

More than one response permitted



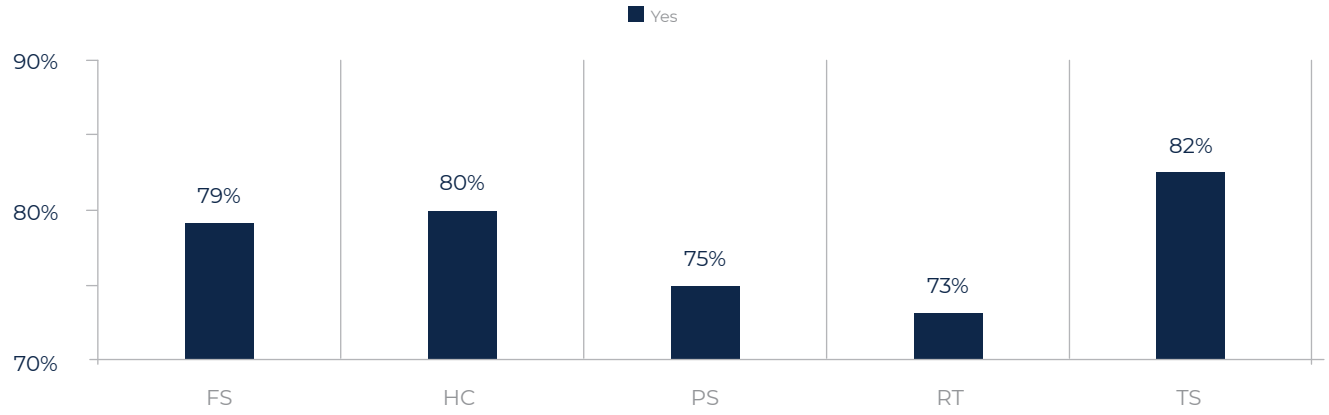
Most respondents in all industry sectors prefer to request mitigation when a third party has gaps in its security controls or practices. Organizations have three possible options when they discover a third party has gaps in its security controls or practices that could put the organization at risk. As shown in Figure 18, all industries represented are far more likely to request, not require, mitigation. Collaboration to improve the third parties' security measures and termination of relationships is rarely pursued.

Figure 18. What actions does your organization take if a third party has gaps in its security controls or practices that could put your organization at risk?



Many organizations in this study are also a third party that is required to complete customer assessments. As shown in Figure 19, 82% of respondents in the technology and software sector are required as a third party to complete customer assessments and 80% in health/pharma complete third-party assessments.

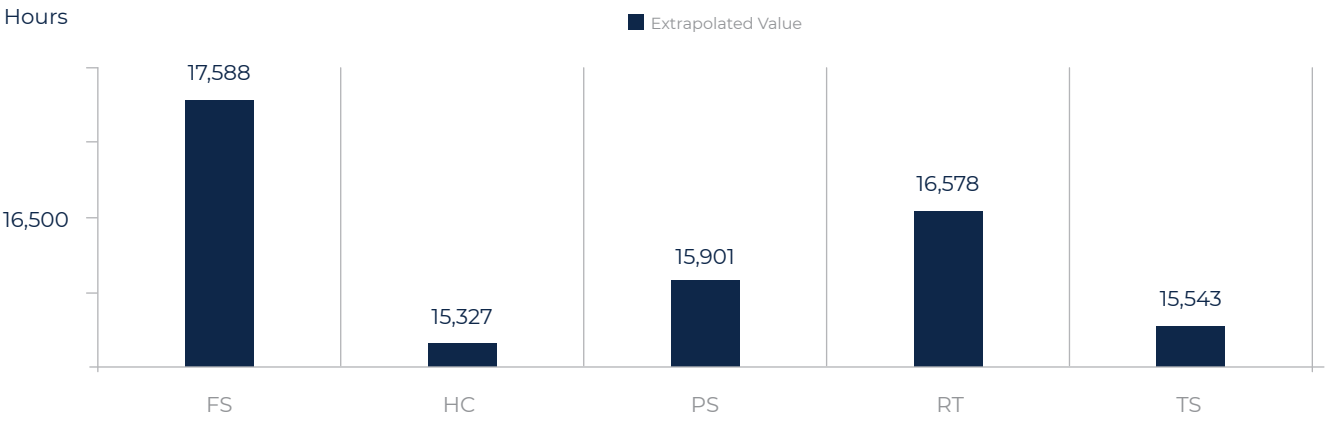
Figure 19. Is your company also a third party that is required to complete customer assessments?



Financial service third parties spend the most time completing customer assessments each year. Figure 20 presents the average hours spent each year completing customer assessments. As shown, financial services companies spend by far the most time on completing these assessments.

Figure 20. How many hours are spent completing customer assessments of your organization annually?

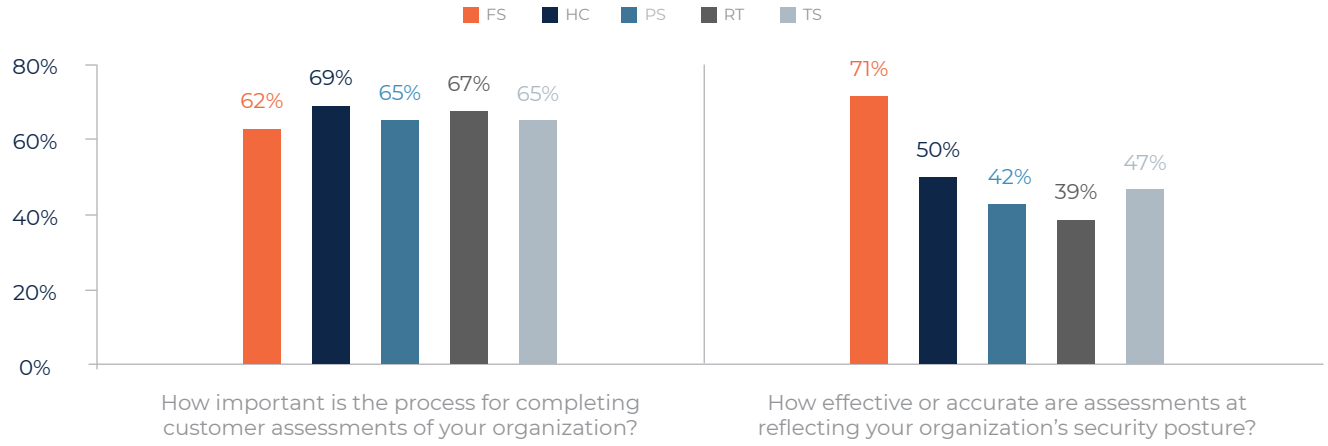
Extrapolated values presented



As shown in Figure 21, financial services organizations are spending the most time on completing these assessments and are most likely among the industry sectors to believe these assessments accurately reflect their security posture. Retail is least likely to believe assessments present an accurate picture of their security posture.

Figure 21. The importance and effectiveness of customer assessments

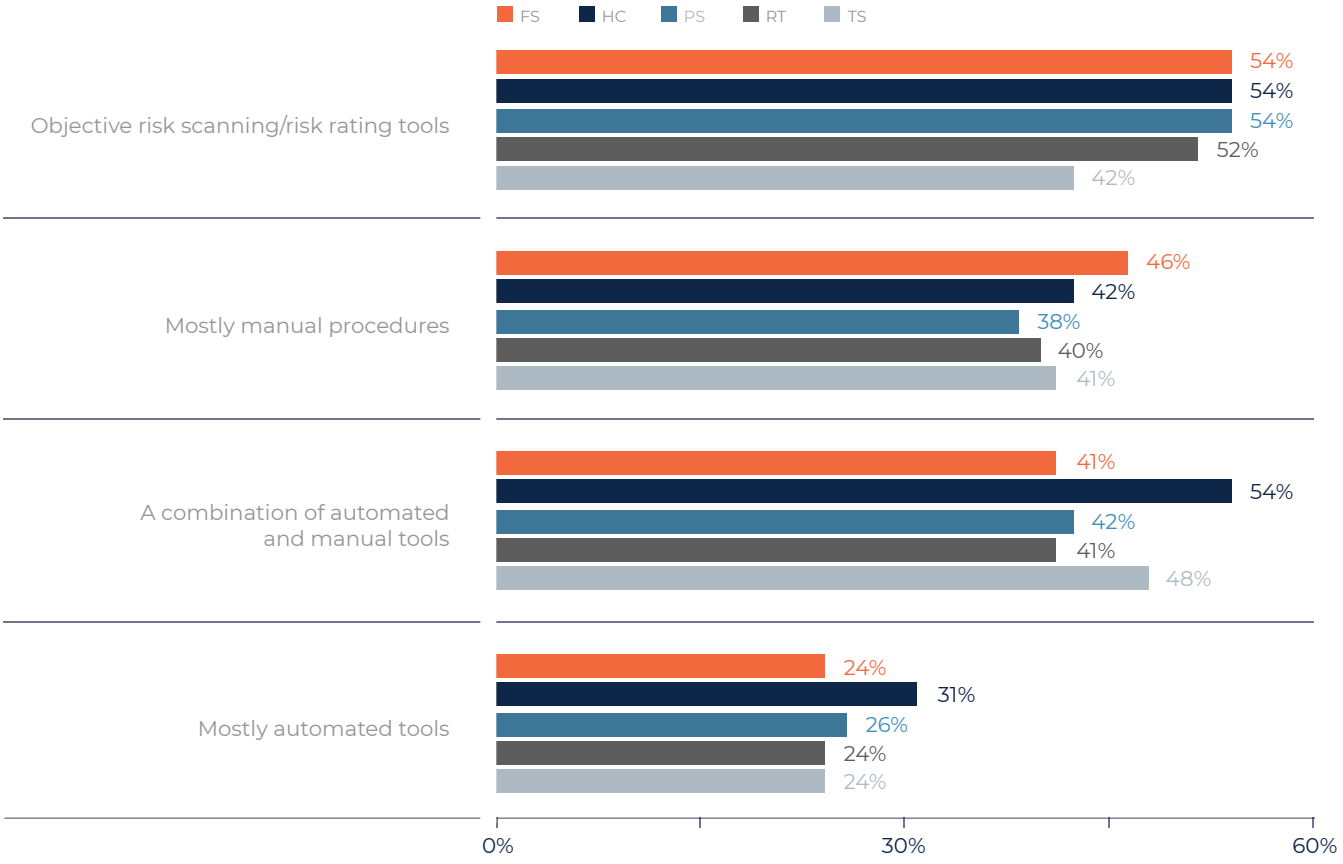
Essential and Very important responses presented, and from 1 = ineffective to 10 = very effective, 7+ responses presented



Very few respondents are automating the assessment of third parties. Health/pharma is most likely to use a combination of automated and manual tools (54% of respondents) followed by technology and software. Technology and software companies are least likely to use objective risk scanning rating tools (42% of respondents), as shown in Figure 22.

Figure 22. What assessment tools does your organization use to assess third parties?

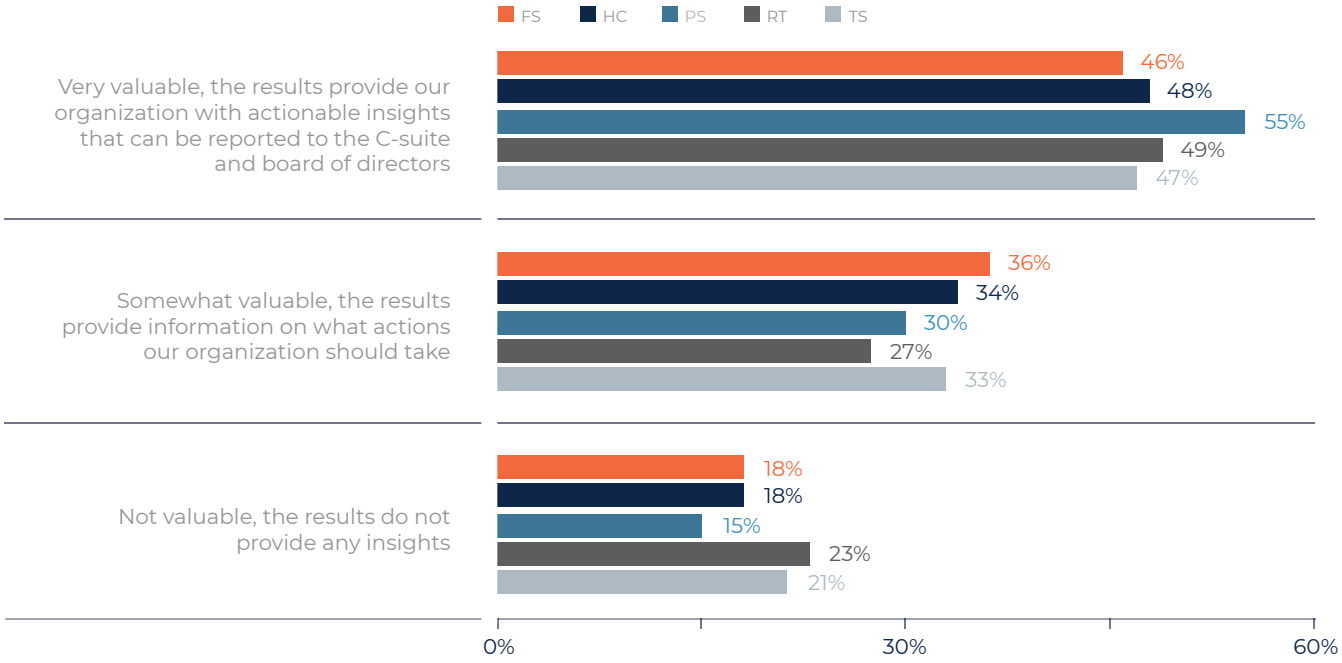
More than one response permitted



The public sector is most likely to believe completion of assessments is valuable. According to Figure 23, 88% of respondents in the public sector say the results are either very valuable and provide actionable insights that can be reported to the C-suite and board of directors or provide information on what actions their organization should take. Retail is least likely to find the information from these assessments valuable.

Figure 23. How valuable are the results of these assessments?

More than one response permitted



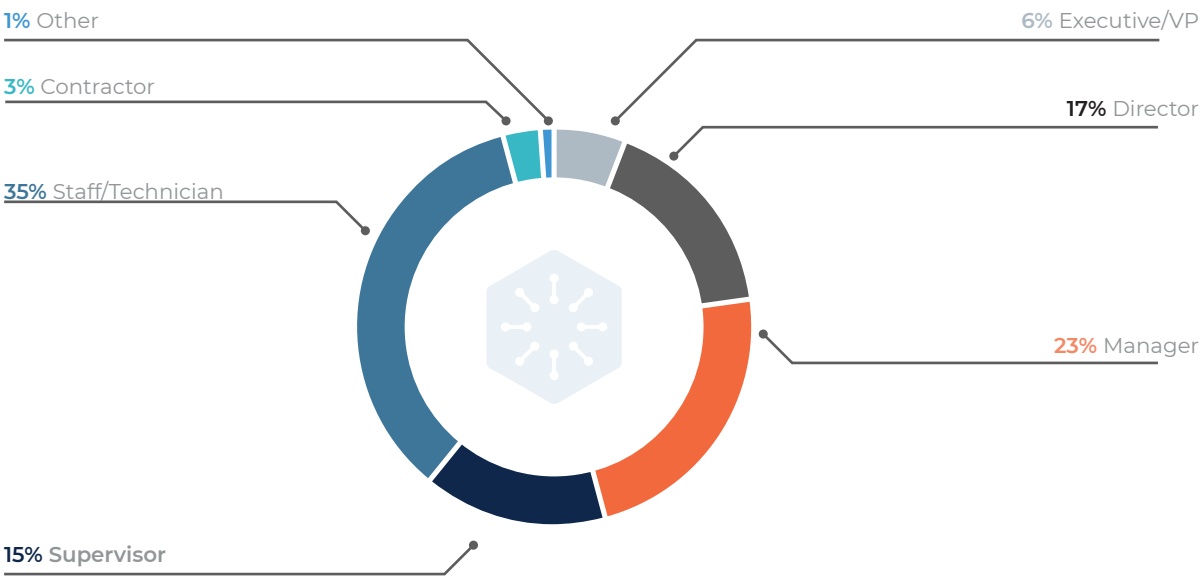
Part 4. Methods

A sampling frame of 16,865 IT and IT security practitioners who are familiar with their organizations' approach to managing data risks created through outsourcing business functions to third parties and have involvement in managing the cyber risks exacerbated by insecure third-party organizations were selected as participants in this survey. Table 1 shows 682 total returns. Screening and reliability checks required the removal of 65 surveys. Our final sample consisted of 617 surveys, or a 3.7% response rate.

Table 1. Sample response	FY2017	Pct%
Sampling frame	16,865	100.0%
Total returns	682	4.0%
Rejected or screened surveys	65	0.4%
Final sample	617	3.7%

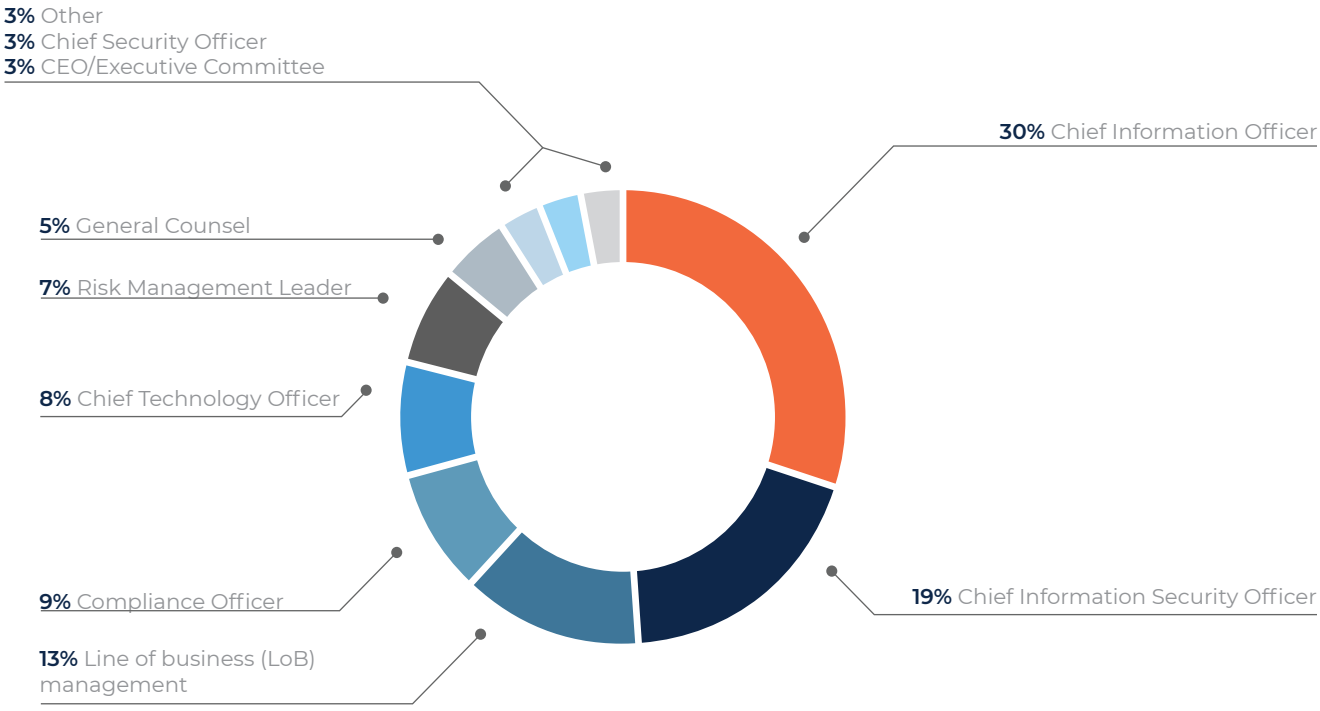
Pie Chart 1 reports the respondents' organizational levels within the participating organizations. By design, more than half of the respondents (61%) are at or above the supervisory levels and 35% of respondents described their position as staff/technician.

Pie Chart 1. Current position within the organization



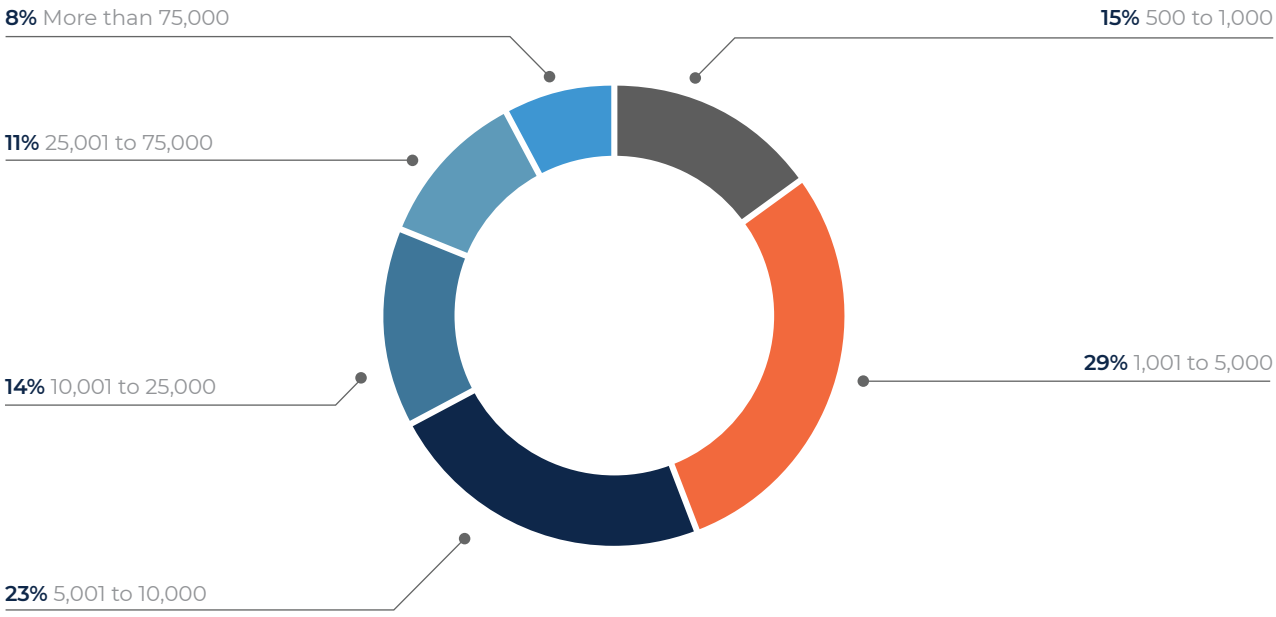
As shown in Pie Chart 2, 30% of respondents report to the Chief Information Officer, 19% of respondents report to the Chief Information Security Officer, 13% of respondents report to the line of business management and 9% of respondents indicated they report to the Compliance Officer.

Pie Chart 2. Primary person respondent reports to



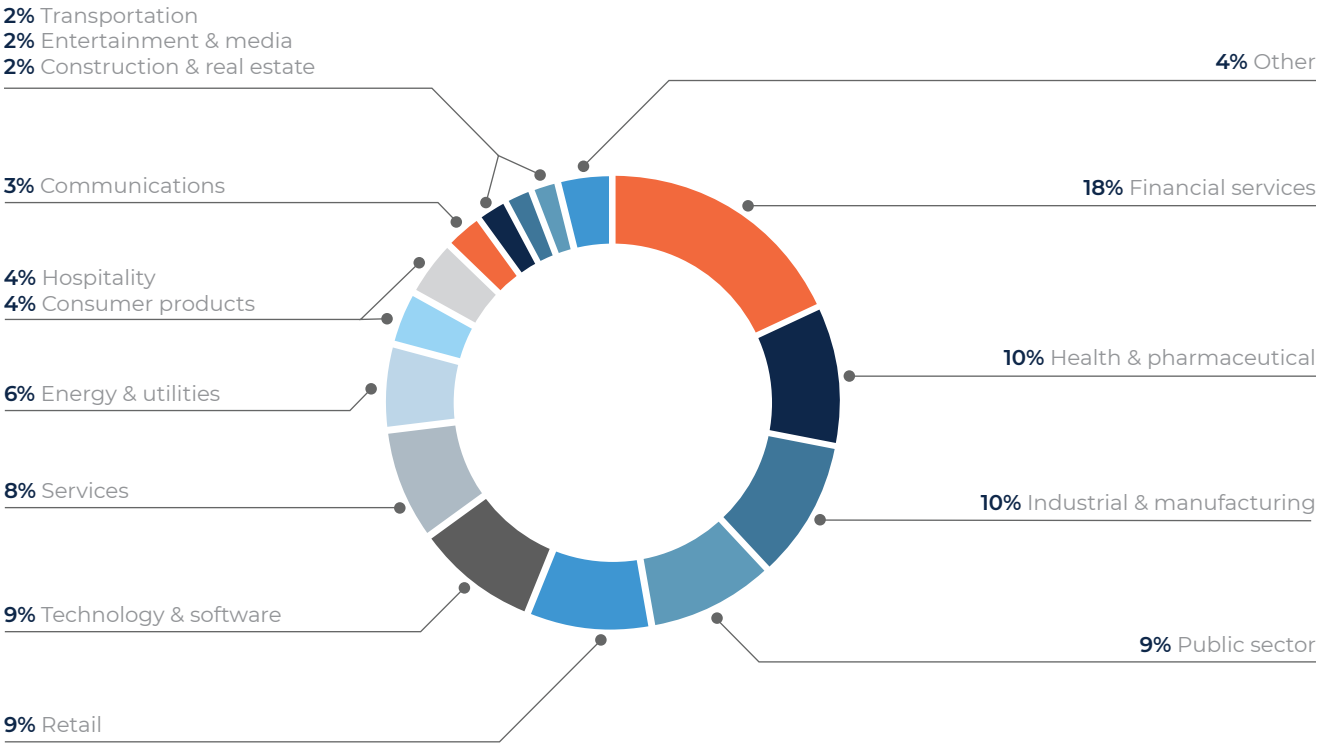
Pie Chart 3 reports the head count of the respondents' global organizations. More than half of respondents (56%) are from organizations with a worldwide head count greater than 5,000 employees.

Pie Chart 3. Head count of respondents' global organizations



Pie Chart 4 reports the industry classifications of respondents' organizations. This chart identifies financial services (18% of respondents) as the largest segment, followed by health and pharmaceuticals (10% of respondents), industrial/manufacturing (10% of respondents), public sector (9% of respondents) and retail (9% of respondents).

Pie Chart 4. Primary industry classification of respondents' organizations



Part 5. Caveats to This Study

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

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

- **Sampling-frame bias:**
  The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners. 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, the possibility remains that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured between October 30, 2018 and November 16, 2018.

Table 1. Sample response	FY2017	Pct%
Sampling frame	16,865	100.0%
Total returns	682	4.0%
Rejected surveys	65	0.4%
Final sample	617	3.7%

Part 1. Screening Questions

S1. How familiar are you with your organization's approach to managing data risks created through outsourcing business functions to third parties?	Pct%
Very familiar	39%
Familiar	41%
Somewhat familiar	20%
No knowledge (Stop)	0%
Total	100%

S2a. Does your company have a third-party data risk management program (TPCRM)?	Pct%
Yes	100%
No (Stop)	0%
Total	100%

S2b. If yes, what best describes the maturity level of your organization's third-party cybersecurity risk management program and related activities?	Pct%
Early stage – Many TPCRM activities have not as yet been planned or deployed (stop)	20%
Middle stage – Many TPCRM activities are planned and defined but only partially deployed	38%
Late-middle stage – Many TPCRM activities are deployed across the enterprise	26%
Mature stage – All TPCRM activities are maintained and refined across the enterprise	16%
Total	100%

S3. Do you have any involvement in managing the cyber risks exacerbated by insecure third-party organizations?	Pct%
Yes, fully involved	38%
Yes, partially involved	41%
Yes, minimally involved	21%
Not involved (Stop)	0%
Total	100%

Part 2. Third-party cybersecurity risk management

Q1. Regulatory compliance controls

Q1a. Does your organization deploy this third-party control or practice?	Pct%
Yes, fully deployed	37%
Yes, partially deployed	45%
No	18%
Total	100%

Q1b. If yes, how important is this control or practice at reducing the risk of a third-party data breach? Please use the following 10-point scale to express your opinion, from 1 = not important to 10 = very important.	Pct%
1 or 2	8%
3 or 4	7%
5 or 6	13%
7 or 8	32%
9 or 10	40%
Total	100%
Extrapolated value	7.28

Q1c. If yes, please provide your best estimate for the annual cost incurred by your organization to implement and maintain this third-party control or practice.	Pct%
Less than $50,000	0%
$50,000 to $100,000	9%
$100,001 to $500,000	26%
$500,001 to $1,000,000	33%
$1,000,001 to $5,000,000	23%
$5,000,001 to $10,000,000	9%
$10,000,001 to $50,000,000	0%
$50,000,001 to $100,000,000	0%
More than $100,000,000	0%
Total	100%
Extrapolated value	1,697,250

Q1d. How effective is your organization at implementing this control or practice in terms of reducing the cost of a third-party cybersecurity breach? Please use the following 10-point scale to express your opinion, from 1 = ineffective to 10 = very effective.	Pct%
1 or 2	12%
3 or 4	13%
5 or 6	30%
7 or 8	22%
9 or 10	23%
Total	100%
Extrapolated value	6.12

Q1e. Please provide your best estimate for the annual cost incurred by your organization if it **failed** to implement the above-mentioned control or practice at a high level of effectiveness. In your estimate, please consider soft costs such as reputation impact, brand damages, decline in share value, etc.	Pct%
Less than $50,000	0%
$50,000 to $100,000	3%
$100,001 to $500,000	20%
$500,001 to $1,000,000	26%
$1,000,001 to $5,000,000	36%
$5,000,001 to $10,000,000	10%
$10,000,001 to $50,000,000	3%
$50,000,001 to $100,000,000	2%
More than $100,000,000	0%
Total	100%
Extrapolated value	4,487,250

Q2. Procedures for enforcing non-compliance with your organization's security requirements.

Q2a. Does your organization deploy this third-party control or practice?	Pct%
Yes, fully deployed	45%
Yes, partially deployed	35%
No	20%
Total	100%

Q2b. If yes, how important is this control or practice at reducing the risk of a third-party data breach? Please use the following 10-point scale to express your opinion, from 1 = not important to 10 = very important.	Pct%
1 or 2	6%
3 or 4	8%
5 or 6	8%
7 or 8	40%
9 or 10	38%
Total	100%
Extrapolated value	7.42

Q2c. If yes, please provide your best estimate for the annual cost incurred by your organization to implement and maintain this third-party control or practice.	Pct%
Less than $50,000	4%
$50,000 to $100,000	10%
$100,001 to $500,000	21%
$500,001 to $1,000,000	33%
$1,000,001 to $5,000,000	20%
$5,000,001 to $10,000,000	12%
$10,000,001 to $50,000,000	0%
$50,000,001 to $100,000,000	0%
More than $100,000,000	0%
Total	100%
Extrapolated value	1,819,000

Q2d. How effective is your organization at implementing this control or practice in terms of reducing the cost of a third-party cybersecurity breach? Please use the following 10-point scale to express your opinion, from 1 = ineffective to 10 = very effective.	Pct%
1 or 2	13%
3 or 4	11%
5 or 6	29%
7 or 8	24%
9 or 10	23%
Total	100%
Extrapolated value	6.16

Q2e. Please provide your best estimate for the annual cost incurred by your organization if it **failed** to implement the above-mentioned control or practice at a high level of effectiveness. In your estimate, please consider soft costs such as reputation impact, brand damages, decline in share value, etc.	Pct%
Less than $50,000	0%
$50,000 to $100,000	5%
$100,001 to $500,000	18%
$500,001 to $1,000,000	29%
$1,000,001 to $5,000,000	26%
$5,000,001 to $10,000,000	13%
$10,000,001 to $50,000,000	7%
$50,000,001 to $100,000,000	2%
More than $100,000,000	0%
Total	100%
Extrapolated value	5,630,250

Q3. Evaluation and vetting of third parties' security practices

Q3a. Does your organization deploy this third-party control or practice?	Pct%
Yes, fully deployed	51%
Yes, partially deployed	34%
No	15%
Total	100%

Q3b. If yes, how important is this control or practice at reducing the risk of a third-party data breach? Please use the following 10-point scale to express your opinion, from 1 = not important to 10 = very important.	Pct%
1 or 2	8%
3 or 4	6%
5 or 6	8%
7 or 8	29%
9 or 10	49%
Total	100%
Extrapolated value	7.60

Q3c. If yes, please provide your best estimate for the annual cost incurred by your organization to implement and maintain this third-party control or practice.	Pct%
Less than $50,000	2%
$50,000 to $100,000	7%
$100,001 to $500,000	17%
$500,001 to $1,000,000	32%
$1,000,001 to $5,000,000	30%
$5,000,001 to $10,000,000	12%
$10,000,001 to $50,000,000	0%
$50,000,001 to $100,000,000	0%
More than $100,000,000	0%
Total	100%
Extrapolated value	2,096,750

Q3d. How effective is your organization at implementing this control or practice in terms of reducing the cost of a third-party cybersecurity breach? Please use the following 10-point scale to express your opinion, from 1 = ineffective to 10 = very effective.	Pct%
1 or 2	14%
3 or 4	20%
5 or 6	30%
7 or 8	19%
9 or 10	17%
Total	100%
Extrapolated value	5.60

Q3e. Please provide your best estimate for the annual cost incurred by your organization if it **failed** to implement the above-mentioned control or practice at a high level of effectiveness. In your estimate, please consider soft costs such as reputation impact, brand damages, decline in share value, etc.	Pct%
Less than $50,000	0%
$50,000 to $100,000	0%
$100,001 to $500,000	6%
$500,001 to $1,000,000	20%
$1,000,001 to $5,000,000	29%
$5,000,001 to $10,000,000	19%
$10,000,001 to $50,000,000	21%
$50,000,001 to $100,000,000	3%
More than $100,000,000	2%
Total	100%
Extrapolated value	13,413,000

Q4. Third-party liability mitigation

Q4a. Does your organization deploy this third-party control or practice?	Pct%
Yes, fully deployed	40%
Yes, partially deployed	15%
No	45%
Total	100%

Q4b. If yes, how important is this control or practice at reducing the risk of a third-party data breach? Please use the following 10-point scale to express your opinion, from 1 = not important to 10 = very important.	Pct%
1 or 2	6%
3 or 4	11%
5 or 6	26%
7 or 8	25%
9 or 10	32%
Total	100%
Extrapolated value	6.82

Q4c. If yes, please provide your best estimate for the annual cost incurred by your organization to implement and maintain this third-party control or practice.	Pct%
Less than $50,000	9%
$50,000 to $100,000	20%
$100,001 to $500,000	23%
$500,001 to $1,000,000	32%
$1,000,001 to $5,000,000	11%
$5,000,001 to $10,000,000	5%
$10,000,001 to $50,000,000	0%
$50,000,001 to $100,000,000	0%
More than $100,000,000	0%
Total	100%
Extrapolated value	1,031,250

Q4d. How effective is your organization at implementing this control or practice in terms of reducing the cost of a third-party cybersecurity breach? Please use the following 10-point scale to express your opinion, from 1 = ineffective to 10 = very effective.	Pct%
1 or 2	19%
3 or 4	16%
5 or 6	27%
7 or 8	22%
9 or 10	16%
Total	100%
Extrapolated value	5.50

Q4e. Please provide your best estimate for the annual cost incurred by your organization if it **failed** to implement the above-mentioned control or practice at a high level of effectiveness. In your estimate, please consider soft costs such as reputation impact, brand damages, decline in share value, etc.	Pct%
Less than $50,000	0%
$50,000 to $100,000	5%
$100,001 to $500,000	14%
$500,001 to $1,000,000	27%
$1,000,001 to $5,000,000	32%
$5,000,001 to $10,000,000	21%
$10,000,001 to $50,000,000	1%
$50,000,001 to $100,000,000	0%
More than $100,000,000	0%
Total	100%
Extrapolated value	3,083,250

Q5. Data breach and cyber exploit incident response procedures

Q5a. Does your organization deploy this third-party control or practice?	Pct%
Yes, fully deployed	67%
Yes, partially deployed	16%
No	17%
Total	100%

Q5b. If yes, how important is this control or practice at reducing the risk of a third-party data breach? Please use the following 10-point scale to express your opinion, from 1 = not important to 10 = very important.	Pct%
1 or 2	3%
3 or 4	4%
5 or 6	9%
7 or 8	32%
9 or 10	52%
Total	100%
Extrapolated value	8.02

Q5c. If yes, please provide your best estimate for the annual cost incurred by your organization to implement and maintain this third-party control or practice.	Pct%
Less than $50,000	0%
$50,000 to $100,000	8%
$100,001 to $500,000	25%
$500,001 to $1,000,000	19%
$1,000,001 to $5,000,000	30%
$5,000,001 to $10,000,000	14%
$10,000,001 to $50,000,000	4%
$50,000,001 to $100,000,000	0%
More than $100,000,000	0%
Total	100%
Extrapolated value	3,373,500

Q5d. How effective is your organization at implementing this control or practice in terms of reducing the cost of a third-party cybersecurity breach? Please use the following 10-point scale to express your opinion, from 1 = ineffective to 10 = very effective.	Pct%
1 or 2	15%
3 or 4	14%
5 or 6	21%
7 or 8	27%
9 or 10	23%
Total	100%
Extrapolated value	6.08

Q5e. Please provide your best estimate for the annual cost incurred by your organization if it **failed** to implement the above-mentioned control or practice at a high level of effectiveness. In your estimate, please consider soft costs such as reputation impact, brand damages, decline in share value, etc.	Pct%
Less than $50,000	0%
$50,000 to $100,000	0%
$100,001 to $500,000	1%
$500,001 to $1,000,000	13%
$1,000,001 to $5,000,000	25%
$5,000,001 to $10,000,000	30%
$10,000,001 to $50,000,000	19%
$50,000,001 to $100,000,000	10%
More than $100,000,000	2%
Total	100%
Extrapolated value	18,700,500

Q6. Risk prioritization process

Q6a. Does your organization deploy this third-party control or practice?	Pct%
Yes, fully deployed	44%
Yes, partially deployed	33%
No	23%
Total	100%

Q6b. If yes, how important is this control or practice at reducing the risk of a third-party data breach? Please use the following 10-point scale to express your opinion, from 1 = not important to 10 = very important.	Pct%
1 or 2	5%
3 or 4	7%
5 or 6	13%
7 or 8	31%
9 or 10	44%
Total	100%
Extrapolated value	7.54

Q6c. If yes, please provide your best estimate for the annual cost incurred by your organization to implement and maintain this third-party control or practice.	Pct%
Less than $50,000	10%
$50,000 to $100,000	23%
$100,001 to $500,000	26%
$500,001 to $1,000,000	21%
$1,000,001 to $5,000,000	11%
$5,000,001 to $10,000,000	9%
$10,000,001 to $50,000,000	0%
$50,000,001 to $100,000,000	0%
More than $100,000,000	0%
Total	100%
Extrapolated value	1,260,250

Q6d. How effective is your organization at implementing this control or practice in terms of reducing the cost of a third-party cybersecurity breach? Please use the following 10-point scale to express your opinion, from 1 = ineffective to 10 = very effective.	Pct%
1 or 2	20%
3 or 4	17%
5 or 6	21%
7 or 8	22%
9 or 10	20%
Total	100%
Extrapolated value	5.60

Q6e. Please provide your best estimate for the annual cost incurred by your organization if it **failed** to implement the above-mentioned control or practice at a high level of effectiveness. In your estimate, please consider soft costs such as reputation impact, brand damages, decline in share value, etc.	Pct%
Less than $50,000	0%
$50,000 to $100,000	1%
$100,001 to $500,000	23%
$500,001 to $1,000,000	21%
$1,000,001 to $5,000,000	29%
$5,000,001 to $10,000,000	20%
$10,000,001 to $50,000,000	5%
$50,000,001 to $100,000,000	1%
More than $100,000,000	0%
Total	100%
Extrapolated value	4,847,250

Q7a. Do some of your organization's third parties receive a more comprehensive assessment or level of due diligence than your other third parties?	Pct%
Yes	56%
No, all third parties receive the same level of due diligence (Skip to Part 3)	44%
Total	100%

Q7b. How do you determine which third parties to prioritize for due diligence/assessments? Please select all that apply.	Pct%
The third party is critical to our organization's ability to meet its business objectives and obligations	56%
The third party has access to our most confidential information such as trade secrets and intellectual property	63%
The third party has the potential to affect our organization's ability to comply with regulations	59%
Other (please specify)	2%
Total	180%

Q7c. What types of third parties does your organization prioritize and focus its due diligence on? Please select your top three choices.	Pct%
Law firms	45%
Business consultants	26%
Cloud providers	56%
Accounting firms	27%
Payroll providers	49%
Outsourced HR	23%
Software developers	29%
Payment processors	15%
Data centers	30%
Other (please specify)	0%
Total	300%

Q7d. What actions does your organization take if a third party has gaps in its security controls or practices that could put your organization at risk? Please select one top choice.	Pct%
Relationship is terminated	26%
Mitigation is requested	47%
Collaborate with third party to improve its security measures	24%
Other (please specify)	3%
Total	100%

Part 3. Cost of third-party data breaches

Q8a. Has your organization experienced one or more data breaches caused by an insecure third-party (such as a business partner, vendor or contractor) over **the past 2 years?**	Pct%
Yes	53%
No	45%
Unsure	2%
Total	100%

Q8b. If yes, how many separate data breach incidents did your organization experience?	Pct%
One	45%
2 to 5	41%
6 to 10	10%
More than 10	4%
Total	100%
Extrapolated value	3.17

Q8c. If yes, how many records were lost or stolen as a result of all third-party data breaches experienced over the past two years?	Pct%
Less than 100	32%
100 to 1,000	30%
1,001 to 5,000	15%
5,001 to 10,000	11%
10,001 to 100,000	9%
100,001 to 1,000,000	3%
1,000,001 to 10,000,000	0%
More than 10,000,000	0%
Total	100%
Extrapolated value	22,906

Q8d. If yes, please provide your best estimate for the total cost of all third-party data breaches experienced by your organization over **the past 2 years?**	Pct%
Less than $50,000	4%
$50,000 to $100,000	7%
$100,001 to $500,000	15%
$500,001 to $1,000,000	19%
$1,000,001 to $5,000,000	25%
$5,000,001 to $10,000,000	21%
$10,000,001 to $50,000,000	5%
$50,000,001 to $100,000,000	3%
More than $100,000,000	1%
Total	100%
Extrapolated value	7,468,750

Q8e. Please provide your best estimate for the likelihood (probability) of a third-party data breach involving 10,000 or more records containing sensitive or confidential information over **the next 2 years?**	Pct%
Less than 1%	10%
1% to 5%	11%
6% to 10%	13%
11% to 20%	16%
21% to 30%	20%
31% to 40%	13%
41% to 50%	12%
More than 50%	5%
Total	100%
Extrapolated value	21.9%

Part 4. Completing customer assessments

Q9. Is your company also a third party that is required to complete customer assessments?	Pct%
Yes	78%
No	22%
Total	100%

Q10. On average, how much time (hours) is spent completing customer assessments of your organization on an annual basis?	Pct%
Less than 100 hours	0%
100 to 500 hours	3%
501 to 1,000 hours	7%
1,001 to 5,000 hours	13%
5,001 to 10,000 hours	23%
10,001 to 25,000 hours	24%
More than 25,000 hours	30%
Total	100%
Extrapolated value	15,377

Q11. How important is the process for completing customer assessments of your organization?	Pct%
Essential	23%
Very Important	42%
Important	23%
Not Important	10%
Irrelevant	2%
Total	100%

Q12. On average, what is the total cost incurred by your organization to complete these assessments on an annual basis.	Pct%
Less than $50,000	2%
$50,000 to $100,000	9%
$100,001 to $500,000	19%
$500,001 to $1,000,000	33%
$1,000,001 to $5,000,000	26%
$5,000,001 to $10,000,000	11%
$10,000,001 to $50,000,000	0%
$50,000,001 to $100,000,000	0%
More than $100,000,000	0%
Total	100%
Extrapolated value	1,916,750

Q13. How effective or accurate are assessments at reflecting your organization's security posture? Please use the following 10-point scale to express your opinion, from 1 = ineffective to 10 = very effective.	Pct%
1 or 2	12%
3 or 4	12%
5 or 6	31%
7 or 8	20%
9 or 10	25%
Total	100%
Extrapolated value	6.18

Q14. Please provide your best estimate for the annual cost incurred by your organization if it **failed** to perform third party assessments at a high level of effectiveness. In your estimate, please consider soft costs such as reputation impact, brand damages, decline in share value, etc.	Pct%
Less than $50,000	0%
$50,000 to $100,000	3%
$100,001 to $500,000	8%
$500,001 to $1,000,000	13%
$1,000,001 to $5,000,000	35%
$5,000,001 to $10,000,000	23%
$10,000,001 to $50,000,000	15%
$50,000,001 to $100,000,000	2%
More than $100,000,000	1%
Total	100%
Extrapolated value	10,098,750

Part 5. Requesting third-party assessments

Q15. What assessment tools does your organization use to assess third parties? Please select all that apply.	Pct%
Mostly manual procedures (i.e. spreadsheets)	40%
Mostly automated tools	27%
Objective risk scanning/risk rating tools	51%
A combination of automated and manual tools	44%
Other (please specify)	3%
Total	165%

Q16. As part of your organization's TPCRM process, what% of third party assessments result in disqualification or a requirement to remediate prior to doing business with them?	Pct%
Less than 1%	13%
1% to 5%	28%
6% to 10%	43%
11% to 20%	10%
21% to 30%	4%
31% to 40%	2%
41% to 50%	0%
More than 50%	0%
Total	100%
Extrapolated value	7.7

Q17. How valuable are the results of these assessments?	Pct%
Very valuable, the results provide our organization with actionable insights that can be reported to the C-suite and board of directors	46%
Somewhat valuable, the results provide information on what actions our organization should take	34%
Not valuable, the results do not provide any insights	20%
Total	100%

Part 6. Budget questions

Q18a. Does your organization budget (earmark) funds to support its third-party cybersecurity risk management program?	Pct%
Yes	48%
No	50%
Unsure	2%
Total	100%

Q18b. If yes, who "owns" or controls this budget within your organization? Please select one best choice.	Pct%
CEO/COO	0%
CIO/CTO	17%
CISO/CSO	16%
CFO/ finance	9%
Legal (OGC)	8%
Compliance	17%
Procurement/purchasing	10%
Lines of business (LoB) management	15%
Risk management	8%
Other (please specify)	0%
Total	100%

Q19. Please provide your best estimate for the total budget dedicated for your organization's third-party risk management program this year?	Pct%
Less than $50,000	0%
$50,000 to $100,000	0%
$100,001 to $500,000	14%
$500,001 to $1,000,000	30%
$1,000,001 to $5,000,000	36%
$5,000,001 to $10,000,000	11%
$10,000,001 to $50,000,000	4%
$50,000,001 to $100,000,000	5%
More than $100,000,000	0%
Total	100%
Extrapolated value	$7,122,000

Part 7. Organizational characteristics

D1. What best describes your position level within the organization?	Pct%
Executive/VP	6%
Director	17%
Manager	23%
Supervisor	15%
Staff/Technician	35%
Contractor	3%
Other (please specify)	1%
Total	100%

D2. To whom do you report to within the organization?	Pct%
CEO/Executive Committee	3%
Chief Operating Officer	1%
Chief Financial Officer	1%
Chief Information Security Office	19%
Chief Security Officer	3%
Chief Information Officer	30%
Chief Technology Officer	8%
General Counsel	5%
Compliance Officer	9%
Risk Management Leader	7%
Line of Business (LoB) Management	13%
Other (please specify)	1%
Total	100%

D3. What range best describes the full-time headcount of your global organization?	Pct%
Less than 500	0%
500 to 1,000	15%
1,001 to 5,000	29%
5,001 to 10,000	23%
10,001 to 25,000	14%
25,001 to 75,000	11%
More than 75,000	8%
Total	100%

D4. What best describes your organization's primary industry classification?	Pct%
Agriculture & food services	1%
Communications	3%
Construction & real estate	2%
Consumer products	4%
Defense & aerospace	1%
Education	1%
Energy & utilities	6%
Entertainment & media	2%
Financial services	18%
Health & pharmaceutical	10%
Hospitality	4%
Industrial & manufacturing	10%
Public sector	9%
Retail	9%
Services	8%
Technology & Software	9%
Transportation	2%
Other (please specify)	1%
Total	100%

For more information about this study, please contact Ponemon Institute by sending an email to **research@ponemon.org** or call at **1.800.887.3118**.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.