STATE OF THIRD-PARTY RISK MANAGEMENT 2020

A collaborative research project between RiskRecon and the Cyentia Institute

riskrecon
mastercard

119
Cyentia
INSTITUTE

50
Median number of third parties assessed each year by TPRM programs

31%
of vendors considered a material risk in the event of a breach

63%
say managing third-party risk is a growing priority for their organization

79%
have formal programs in place to manage third-party risk

5 to 6
Average number of years TPRM programs have been in operation

Introduction

The rise of mass outsourcing of systems and services to third parties is perhaps the largest risk landscape shift in the last 20 years. Data and transactions that were once nestled within the walls of the enterprise have now been scattered across the globe, operated by numerous external organizations. In this reality, protecting assets not only requires watching one's own house, but also watching the house of every third-party to ensure they are properly protecting your risk interests. After all, you can outsource your systems and services, but you cannot outsource your risk.

Third-party risk management (TPRM) professionals are the frontline in managing this important risk reality. And it isn't easy. Managing risk well requires frequent acquisition of good data that reveals the completeness of the risk management activities and the quality of the program outcomes. While internal information security risk teams benefit from having context and complete access to their enterprise systems, third-party risk teams do not. They must execute equally important risk assessments across a wide array of organizations from the disadvantaged point of being an outsider, constraining their access to necessary information.

This study clearly shows that the necessity to manage third-party risk well is not lost on security leaders. While the average third-party risk management program is 6 years old, we observed a wide variance in the number of resources deployed to solving third-party risk. We also observed stark differences in the methodologies of assessing third-party risk. While security questionnaires remain a common program pillar, companies are seeking to achieve better risk outcomes more efficiently by leveraging objective assessment data from services such as security rating solutions. This move towards outcome based third-party risk assessments, focusing on what your program yields as opposed to what your program does, is one that has been rising rapidly over the last few years.

We hope that you find this study helpful in your work to hold third parties accountable to managing risk well. Your work is important to your organization and to the world-at-large. Improving the security of third parties improves the security of the Internet. Thus, TPRM is work done for the greater good. Thank you for doing it well.

50:1
Typical vendor:staff ratio reported by TPRM programs

57%
say staffing levels limit ability to manage third-party risk

34%
believe vendor responses to risk assessment questionnaires

14%
express confidence that vendor security posture meets requirements

81%
of TPRM programs say they rarely require vendors to remediate findings

About the Survey

General Purpose

This study aims to understand the challenges currently faced by third-party security risk management programs, examine what they're doing to meet those challenges, and identify factors that improve their chance of success.

Sampling Method

We vetted and surveyed 154 active third-party risk management professionals using three distinct methods. Many respondents attended workshops hosted by subject matter experts at RiskRecon and completed the survey as part of that event. We also partnered with the Third Party Risk Association to enlist the participation of their members. Finally, we invited members of a large LinkedIn peer group focused on third-party risk. Respondents were offered gift cards as an incentive for their participation.

Sample Firmographics

Approximately two-thirds of respondents work for organizations in the financial services industry. Technology services (10%) and healthcare (7%) round out the top three sectors represented. We identify areas in the study where the findings for the financial sector differ significantly from others. Organizations of all sizes are represented, starting with those greater than 10,000 (34%), 1,000 > 10,000 (29%), 100 > 1,000 (26%), and less than 100 employees (11%).

Thoughts? Questions? Let Us know!

We'd be glad to discuss them. No, really—we love this stuff! Reach out to info@riskrecon.com or @riskrecon on Twitter.

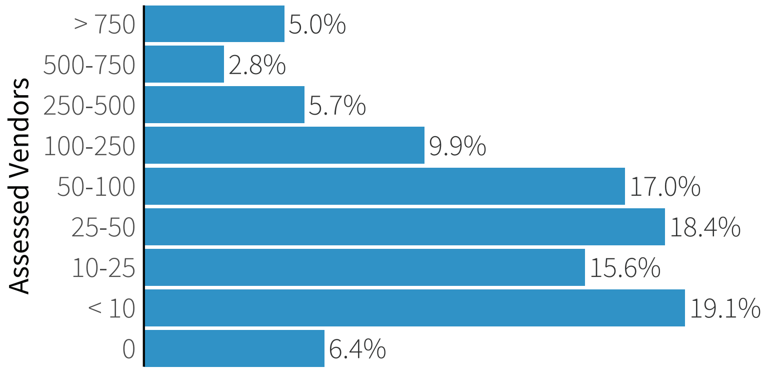
PART 1

The Third-Party Ecosystem

One of the first questions we asked participants was about the number of third parties their organization works with for conducting its business activities. As you might imagine, that answer varied greatly from tens to thousands of vendors. However, this was only a setup question to the one we really wanted to pose: What proportion of vendors require ongoing cyber risk management?

According to our results, the typical (median) third-party risk management (TPRM) program assesses about 50 vendors annually. Figure 1 shows the broad range around that median value, with about a third assessing less than 25 vendors each year, another third handling 25 to 100, and the final third managing portfolios of more than 100 vendors. A small number of valiant programs (5%) bear the responsibility for conducting cyber risk assessments across 750+ third parties every year!

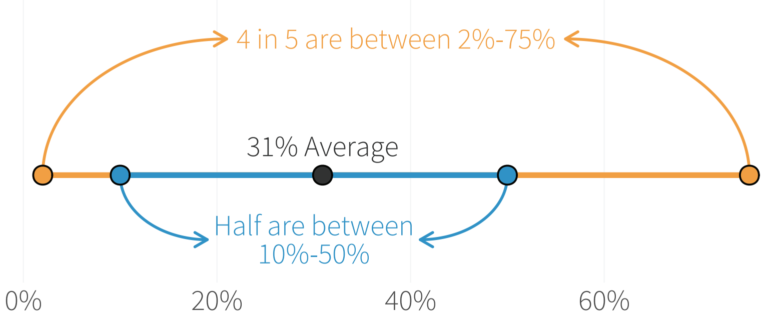
FIGURE 1: NUMBER OF VENDORS RECEIVING CYBER RISK ASSESSMENTS EACH YEAR (PER FIRM)



1 in 3 TPRM programs assess **100+** vendors per year

The number of vendors under management is an important aspect of any TPRM program, but equally (perhaps even more) important is the level of risk those vendors represent. Because of that, we next asked respondents what percentage of vendors could cause a critical impact to their organization if a cyber incident occurred.

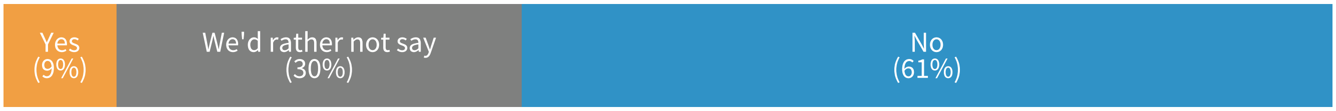
FIGURE 2: PERCENT OF VENDORS THAT COULD CAUSE CRITICAL IMPACT FROM CYBER EVENTS



On average, respondents said that 31% of their vendors pose that kind of potential risk, but Figure 2 indicates this varies widely among TPRM programs. About 1-in-4 claimed that over half of their entire third-party network could trigger severe impacts!

Speaking of "if a cyber event occurred," it appears that's not just a theoretical possibility. Just under 10% of respondents claim their organization experienced a breach due to a third-party compromise during the last three years. Another 30% preferred not to answer the question, which doesn't imply they had a breach...but it makes you wonder, doesn't it? Based on these figures, we suspect the actual proportion of firms in our sample that suffered a vendor-related breach to be somewhere between 10% and 25%.

FIGURE 3: PERCENT OF RESPONDENTS REPORTING VENDOR-RELATED SECURITY INCIDENTS



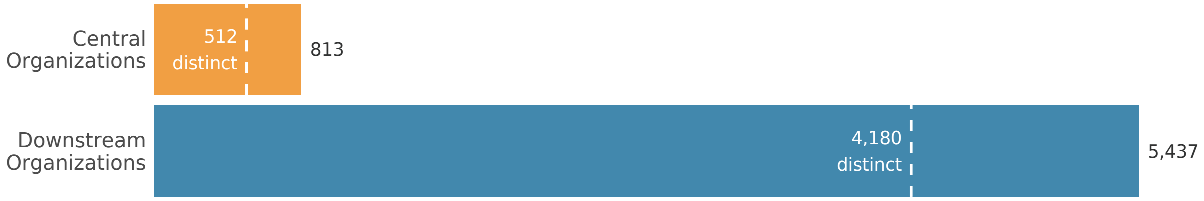
The net of these findings is both perception and reality agree that vendors—whether few or many—represent a significant risk to the business. We'll examine how firms are dealing with that reality by building programs to manage third-party risk in the next section.

Indirect Third-Party Incidents

RiskRecon and the Cyentia Institute published a report titled "Ripples Across the Risk Surface" that analyzes data gathered on over 800 multi-party cyber incidents observed over the last decade. These so-called "ripple events" are different from traditional security breaches because they don't just impact a single organization, but trigger secondary loss events that ripple across the supply chain. We demonstrate that such incidents are increasing in frequency and that associated losses are much higher than for single-party incidents.

Case in point: the 813 multi-party incidents we analyzed in that report generated a total of 5,437 downstream loss events. Quite a few were repeat victims on both the source and receiving ends of the ripples. Adjusting for that, we identified 512 unique firms central to the incident and another 4,180 unique organizations that experienced losses because of these incidents. This makes for a rather startling comparison—downstream entities affected by multi-party incidents outnumber primary victims by more than 8-to-1!

FIGURE 4: NUMBER OF CENTRAL VS. DOWNSTREAM ORGANIZATIONS AFFECTED IN MULTI-PARTY INCIDENTS



We've known for a long time that cybersecurity management was plagued by externalities, but these findings cast a whole new light on that challenge. From this, it's readily apparent that the ripples from these events spread much wider than where the initial impact breaks the surface. And such incidents become more likely and spread wider as the size of your third-party ecosystem increases.

PART 2

Sizing Up TPRM Programs

Having vendors who experience security breaches and represent a material risk motivates the need to manage that risk. Perhaps that's why two-thirds of respondents told us that TPRM is an increasing priority for their organizations. And it's not as though the rest are disinterested; they report a continued, steady emphasis from their employers. Very few told us that managing third-party risk wasn't a priority at all.

Over three-quarters of respondents say their organizations not only prioritize TPRM but have put formal programs in place around it. We suspect that's substantially higher in our sample than the broader population because those who participated in this study ostensibly work for firms engaged (or at least interested) in TPRM.

FIGURE 5: DOES YOUR FIRM HAVE A TPRM PROGRAM?

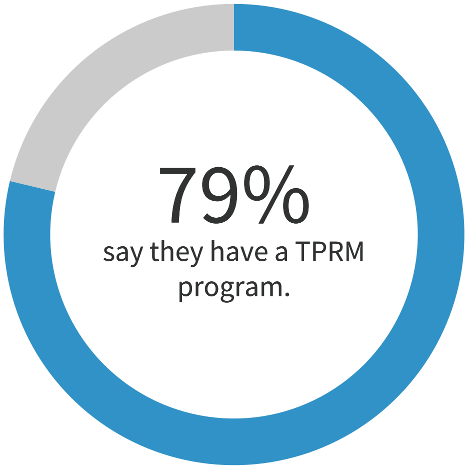
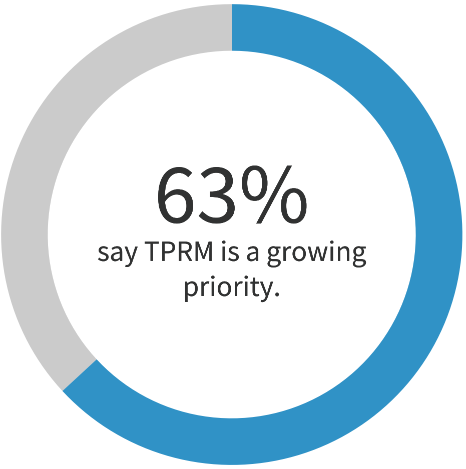


FIGURE 6: IS TPRM PRIORITIZED IN YOUR FIRM?



More than 60% of participants reported that regulatory compliance is a major driver behind the development of their company's TPRM program. Most of the others pointed to executive mandates (22%) or customer requirements (16%). Regulators, executives, and customers hold major sway, which probably has a lot to do with more than two-thirds of respondents saying their organizations report third party risk at the Board level.

What motives drive the formation of TPRM programs?

Regulatory Compliance	Executive Mandates	Customer Requirements
62%	22%	16%

We then asked about the age of TPRM programs and found that those in our sample have been around for an average of five to six years. About 20% existed for at least twice that long. Financial firms appear to have been at this a little longer than others, so phone a finance friend if you need guidance on building a TPRM program. Whether new or old, it's good to see so many companies developing programs and capabilities to meet the challenge of managing third-party risk.

Typical age of TPRM programs:

5-6 years

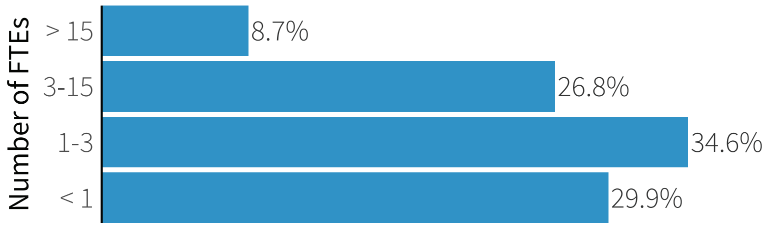
Respondents told us that over half of these TPRM programs sit within the information security organization. About 15% fall under vendor management or procurement, another 15% in compliance or legal, and the remainder are scattered across other areas of the business.

Where does the TPRM program sit within the organization?

InfoSec	Compliance	Vendor Mgt	Other
53%	18%	14%	15%

Beyond where they land in the organization chart, we were very interested to learn more from participants about the size of their TPRM teams. The median number of full-time equivalent staff (FTEs) managing third-party risk among the firms represented is two. The average is 12 FTEs, and the difference between the median and mean indicates broad variation in those summary statistics. Figure 7 illustrates this.

FIGURE 7: NUMBER OF FTEs MANAGING THIRD-PARTY RISK PER FIRM



Median TPRM staff:

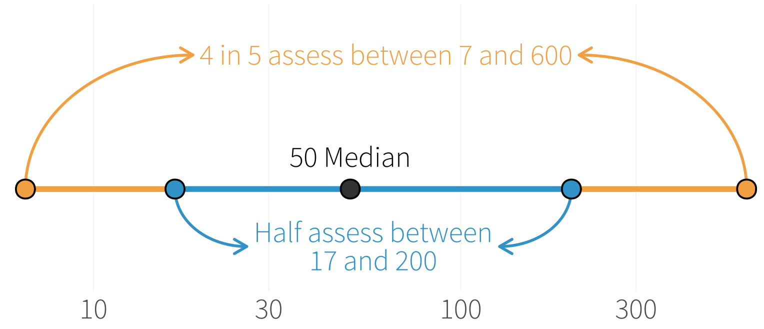
2 FTEs

About 30% of respondents indicated their organizations don't have anyone fully dedicated to managing third-party risk. A little over one-third of programs fall in the one to three FTEs range, and the remaining third claim four or more. As per Figure 7, just under 1-in-10 organizations have the luxury of 15 or more employees working in TPRM.

A count of FTEs is a straightforward way to size up TPRM programs, but the adequacy of that number is relative to the size of the vendor portfolio. Thus, it's arguably more useful to benchmark staffing levels as a ratio of vendors per FTE. We did exactly that across the organizations in our sample, and calculated a median of 50 vendors assessed annually for each staff member dedicated to TPRM.

It's probably not surprising to learn that the vendor-FTE ratio varies a lot from program to program, and Figure 8 offers a more complete picture. Here we see that half the TPRM programs in our study assess between 17 and 200 vendors per FTE. But that ratio must be expanded even further to between 7 and 600 in order to capture 80% of programs.

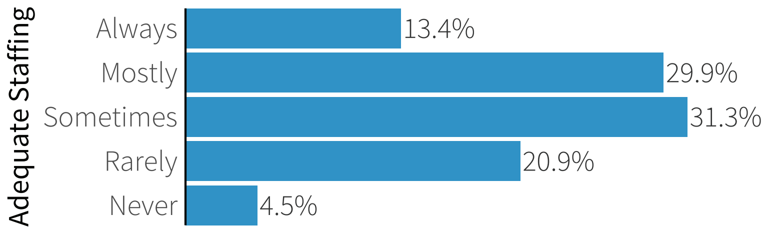
FIGURE 8: NUMBER OF VENDORS ASSESSED ANNUALLY PER FTE



TPRM programs typically manage **50** vendors per FTE

The fact that there's little consistency among vendor-to-staff ratios suggests many are still trying to strike the balance between needs and resources. Whether it's managing 50, 262, or upwards of 600+ vendors (those poor souls), there's no question that TPRM teams have more than their fair share of work cut out for them. That's almost certainly why over half (57%) of respondents say staffing levels regularly limit their ability to keep up with the responsibilities of managing risk across their third-party portfolio. Even worse, over a quarter of programs report severe personnel shortages result in rarely or never getting done what needs to be done.

FIGURE 9: PERCENT OF RESPONDENTS WHO REPORT TPRM STAFFING IS ADEQUATE



87% report inadequate TPRM staffing

At this point, you might be wondering if there's a relationship between the vendor-to-staff ratio and whether respondents believe their TPRM program is understaffed. We're right there with you! Turns out there's something to that hypothesis, but it's not as clear cut as you might expect. We'll briefly share what we found, add our thoughts on the matter, and leave you to draw your own conclusions as well.

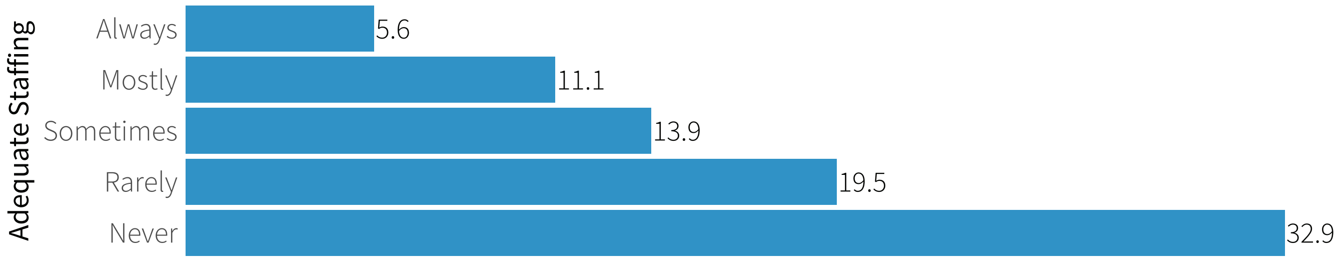
We compared the number of third parties assessed each year with the total number of FTEs managing those vendors, and as you'd expect, there's a correlation. More vendors generally means more TPRM staff (with variation, of course). What we did not expect to find is zero correlation between a program's vendor-to-FTE ratio and whether or not they report staffing levels as adequate to their needs. Some highly-staffed programs feel inadequate to the task and vice versa. We initially planned to add a pretty chart to illustrate that point, but it was a rather confusing mess. So, we'll just use words instead: the data clearly shows that keeping up in TPRM isn't just a matter of hiring more FTEs.

You're probably wondering "What is it a matter of, then?" Well, that's the question we're trying to explore in this study and there's still another (hopefully insightful) section to go yet. But we can give an example based on what we've covered thus far. Queue Figure 10.

Figure 10 combines four variables from the preceding sections: total vendors assessed annually, the percentage of vendors representing critical risk, the number of TPRM FTEs, and respondents' perception of staffing adequacy. You thought it was just another bar chart, didn't you?

While our previous attempt to compare vendor-to-FTE ratio and staffing adequacy showed no obvious correlation, the inclusion of critical-risk vendors in Figure 10 makes the relationship plain as day. Respondents in teams that manage an average of five to six critical-risk vendors per FTE always feel adequately staffed, while those juggling 30 or more never do. And there's an even progression between those extremes.

FIGURE 10: PERCEPTION OF STAFFING ADEQUACY BASED ON AVERAGE NUMBER OF HIGH-IMPACT VENDORS PER FTE



We infer from this that a high ratio of critical vendors is a more effective way to assess strains on TPRM staff capacity than just the raw number of total vendors under management. In other words, critical-risk vendors sap resources and thus deserve special attention. Understanding that should save your staff a lot of stress while also lowering third-party exposure. Everybody wins!

The bottom line is that we find good evidence that organizations are investing in programs and people to manage third-party risk. Some are just getting started on that journey and others are well into it. Most have encountered challenges along the way, and we've seen clues of how they are (or aren't) navigating around them. Overall, we get the sense that organizational drivers and policies are in place but resources and capabilities remain a limiting factor. In the next section, we'll shift from the attributes of TPRM programs to the activities they undertake.

> "We infer from this that a high ratio of vendors that could materially harm the company strains TPRM staff much more than just the raw number of vendors under management. In other words, risky vendors sap resources and thus deserve special attention."

PART 3

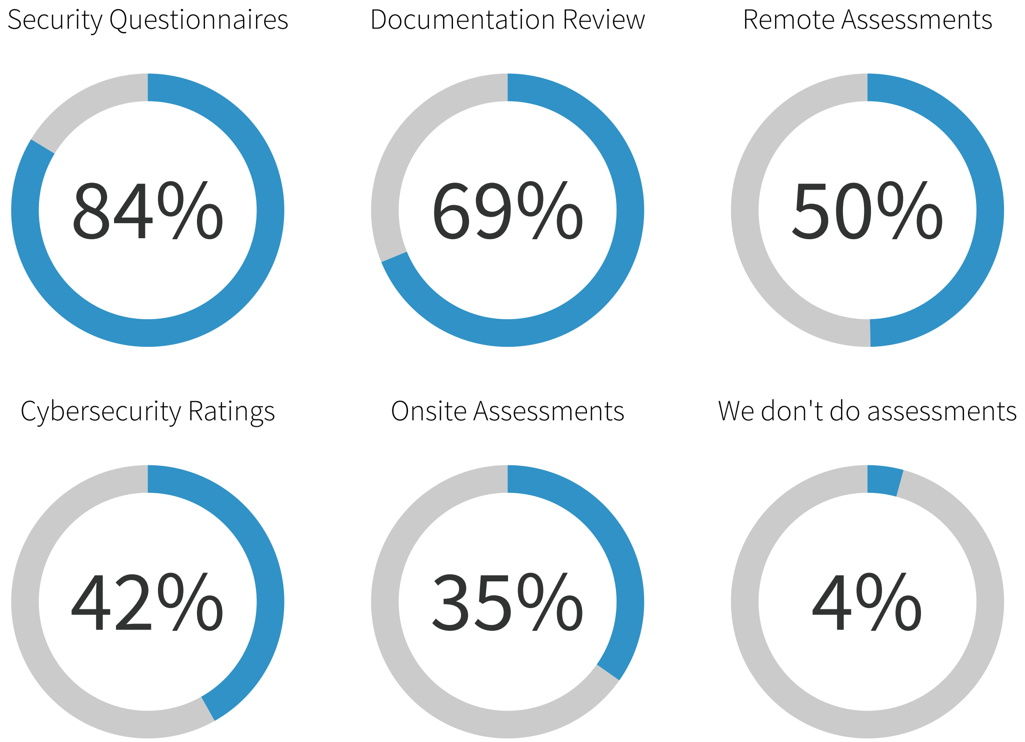
Reviewing TPRM Assessments

There's a lot of conflicting opinions across the cybersecurity industry on a host of issues, but a dislike for security assessment questionnaires might be one of the few things that unite us all. Whether you're the one answering the questions or validating the answers—nobody enjoys the process. Yet questionnaires have long been a staple of TPRM programs and Figure 11 makes it clear they're still the modus operandi.

Respondents pointed to questionnaires (84%) and documentation reviews (69%) as the most common risk assessment methods used by their organizations. Half report using remote assessments or cybersecurity ratings (42%) to bolster those techniques. An unexpectedly high proportion of TPRM programs incorporate onsite security evaluations (34%), but the majority (60%) do so for only a very small percentage (<10%) of vendors.

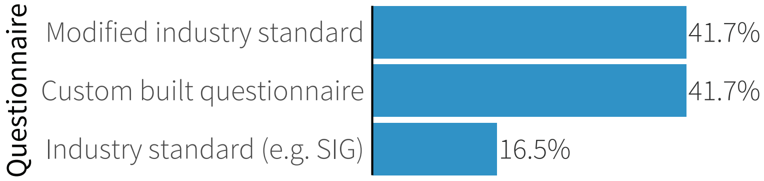
Participants were able to check more than one type of assessment, so we were keen to learn which combinations form the repertoire of TPRM programs. The most common response (from 16% of firms) was "all the above." Sounds like a lot of work! Interestingly, the second-most cited option isn't a combo at all—12% rely on questionnaires alone. Cybersecurity ratings, document review, and questionnaires were the only other assessment mix used by at least 10% of programs. This hints that organizations are innovating away from reliance on questionnaires alone and adopting more advanced techniques like ratings.

FIGURE 11: PREVALENCE OF THIRD-PARTY RISK ASSESSMENT METHODS



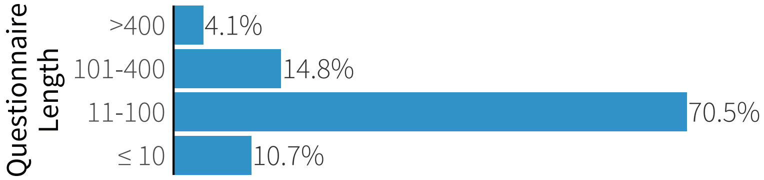
Since questionnaires are so common, let's dig a little deeper into them. Under 20% of programs leverage an industry-standard question set such as SIG, SIG Lite, or CAIQ. About 40% started with one of these standards and tailored the questions to suit their needs. The remaining ~40% claim to have built their own fully customized questionnaire, but we find that rather dubious. It's more likely that a predecessor of the respondent started with a standard template and that evolved over time without preserving the lineage.

FIGURE 12: PERCENT OF RESPONDENTS USING STANDARD, MODIFIED, AND CUSTOM QUESTIONNAIRES



Setting aside origins, let's take a quick look at how many questions are thrust upon vendors deemed risky enough to receive the full battery. We learned that 11% of programs base their assessment on 10 questions or less. Their partners undoubtedly appreciate the brevity. About 70% of questionnaires fall in the 11 to 100 range, and the rest (~20%) ask over 100 questions.

FIGURE 13: PERCENT OF TPRM PROGRAMS USING QUESTIONNAIRES OF VARIOUS LENGTHS



While security questionnaires are the primary information source for third-party risk assessments, they don't appear to yield much actionable insight. As shown in Figure 14, 81% of programs report that at least 75% of their vendors pass their security questionnaires with no exceptions, claiming perfect compliance to requirements. In contrast, only 14% of professionals are highly confident that vendor security performance truly does meet the requirements outlined in the questionnaire.

FIGURE 14: DO YOU REQUIRE VENDOR REMEDIATION?

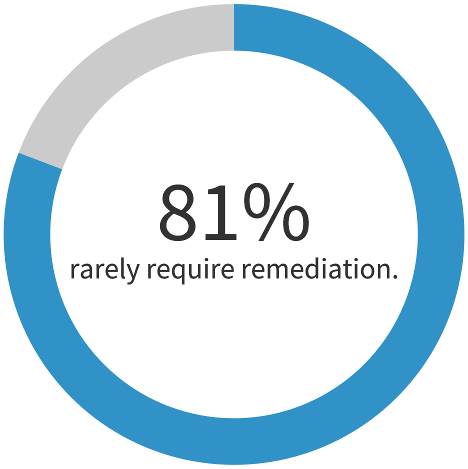
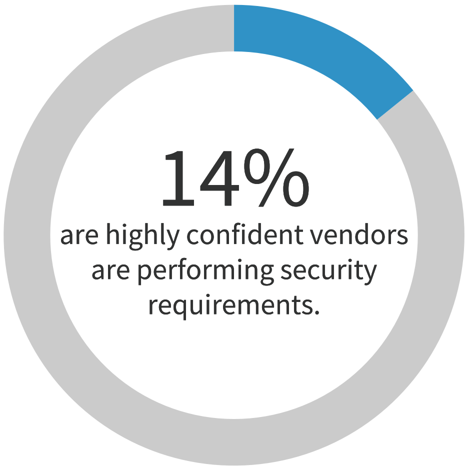
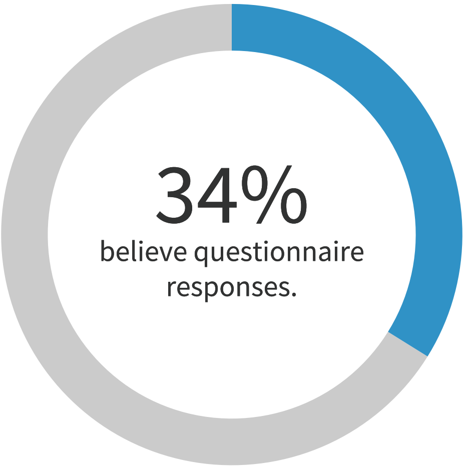


FIGURE 15: DO VENDORS MEET SECURITY REQUIREMENTS?



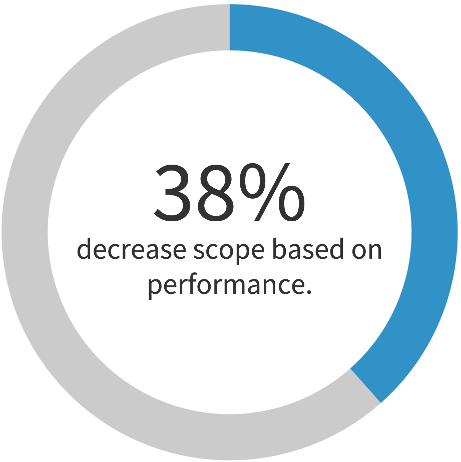
Why do so many vendors pass the questionnaire assessments with perfection while so few professionals believe the results? Perhaps it's more a reflection of the inherent shortcomings of questionnaires. Sure, vendors are probably "doing" vulnerability management—but are they doing it well enough to minimize our risk exposure? Most don't think so.

FIGURE 16: DO YOU REQUIRE VENDOR REMEDIATION?



The inevitable outcome of this questionnaire response-reality disparity is waning trust in assessment outcomes. As evidence of this, Figure 16 reveals that only about one-third of respondents say they believe responses vendors provide to TPRM questionnaires. And that suspicion remains consistent no matter how many questions are included. If there's a bright spot in all of this, it's that firms leveraging cybersecurity ratings and other assessment methods expressed higher confidence than those relying on questionnaires alone.

FIGURE 17: DO YOU DECREASE SCOPE BASED ON GOOD PERFORMANCE?



In addition to the lack of action on questionnaire results, we also read between the lines that TPRM programs are generally struggling to conduct reliable, actionable assessments at scale. As circumstantial evidence of this, it's fairly common among TPRM programs (38% of those in our study) to reduce the assessment scope of vendors with historically strong security performance. Interestingly, we note a divergence between financial firms (32%) and other organizations (49%) on that practice. That's possibly due to their traditionally more risk-averse nature and/or stringent regulatory obligations.

This de-scoping is, of course, a tactic to divert strained resources toward vendors that represent higher risk and therefore require more attention. But given what we learned above, it's unlikely that questionnaires provide a reliable mechanism for focusing those resources. This goes back to the notion of how to operationalize TPRM at scale without sacrificing quality. We have some thoughts on that key challenge to share with you in the concluding section of this study.

> "If there's a bright spot in all of this, it's that firms leveraging cybersecurity ratings and other assessment methods expressed higher confidence than those relying on questionnaires alone."

PART 4

Conclusion & Recommendations

Third-party risk management is arguably the most exciting and impactful area of information security. Practitioners are facing three massive risk factors that will drive powerful innovation over the next few years. First, enterprises have outsourced a massive amount of systems and services to third-parties, placing their sensitive data and their ability to operate in the care of other organizations. Second, professionals increasingly don't trust that questionnaires yield sufficient information for them to properly understand and act on their third-party risk. And third, third-party risk teams are having difficulty keeping up with demand for their services.

To solve these challenges companies are increasingly migrating to a data-driven third-party risk program, following patterns well-established in managing their internal security risk teams. By combining data gathered from a wide range of sources - questionnaires, security rating services, news feeds, financial ratings, and so forth - they are reinventing the way they understand and act on their third-party risks. On this foundation of the capability to rapidly collect and analyze relevant data, they are making new vendor decisions faster, they are intelligently allocating risk engagement resources towards known poor-performing vendors and away from strong-performing vendors, and their assessment engagements result in greater transparency and accountability.

Summing it up, the state of third-party risk management is rapid change and innovation. It is in the companies that are building data-driven TPRM programs where the future patterns and practices of third-party risk management will be defined.

riskrecon
mastercard

RiskRecon enables clients to easily understand and act on their third-party risk through cybersecurity ratings and continuous security control assessments.

www.riskrecon.com

119
Cyentia
INSTITUTE

The Cyentia Institute produces compelling, data-driven research with the aim of improving knowledge and practice in the cybersecurity industry.

www.cyentia.com

A collaborative research project between RiskRecon and the Cyentia Institute

STATE OF THIRD PARTY RISK MANAGEMENT