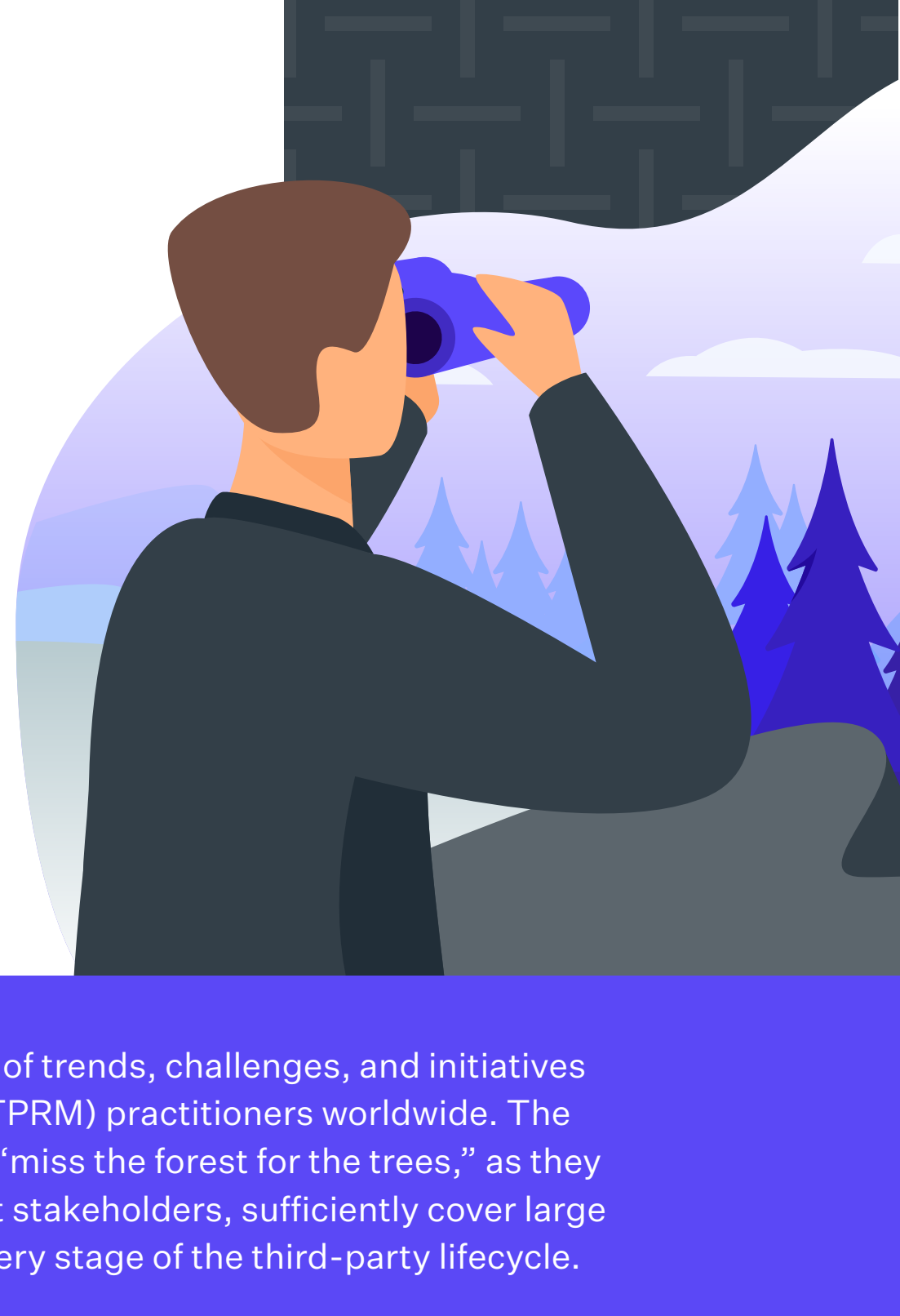


The 2024 Prevalent Third-Party Risk Management Study

Some TPRM programs are still missing the forest for the trees.

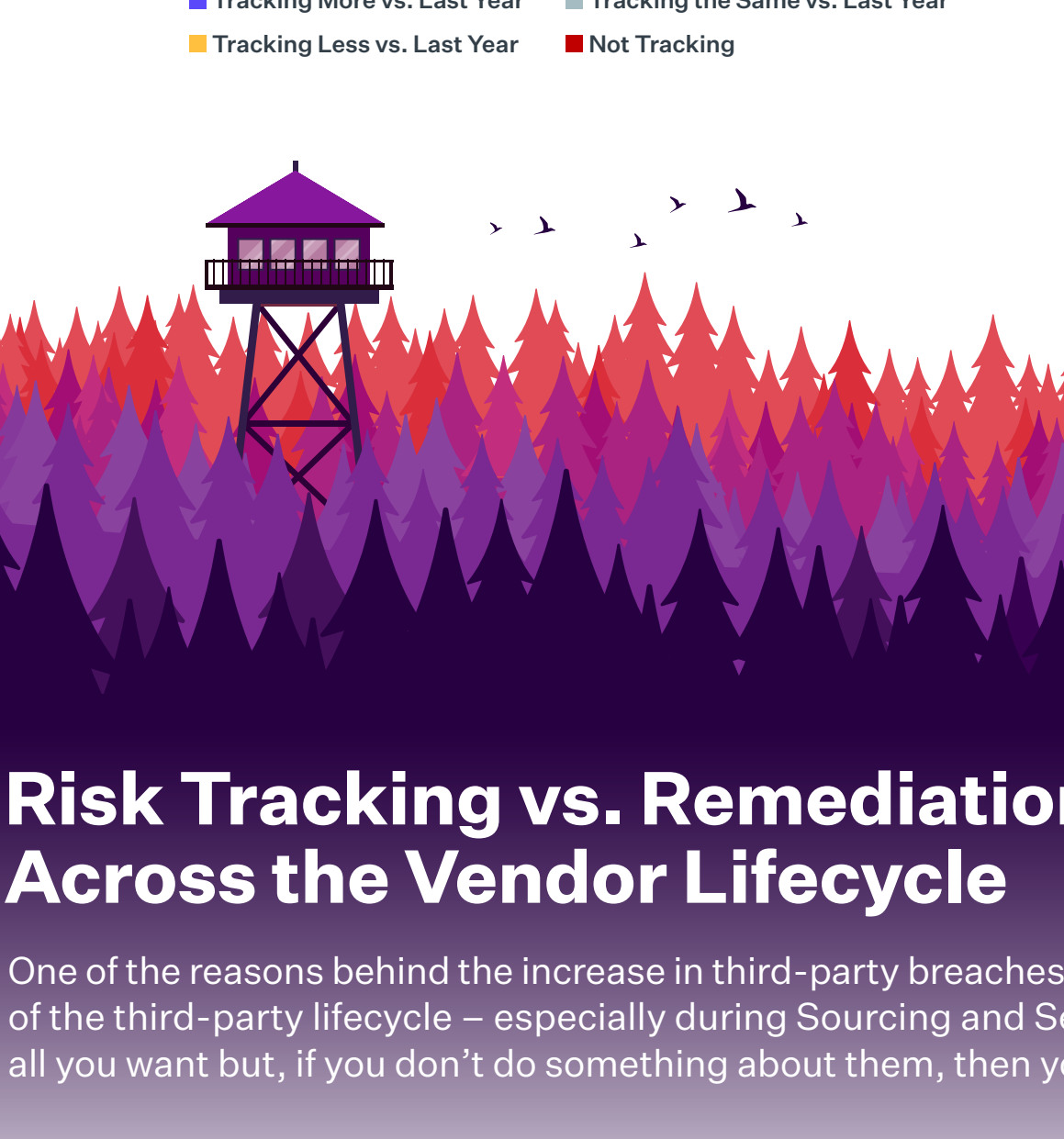


In early 2024, Prevalent conducted a study of trends, challenges, and initiatives impacting third-party risk management (TPRM) practitioners worldwide. The results indicate that many TPRM programs “miss the forest for the trees,” as they struggle to meet the broad needs of different stakeholders, sufficiently cover large vendor ecosystems, and address risk at every stage of the third-party lifecycle.

↑ 49%
YOY Increase

A Record Level of Third-Party Incidents

Third-party data breaches are up 49% year over year, with 61% of companies reporting a breach in the last year.

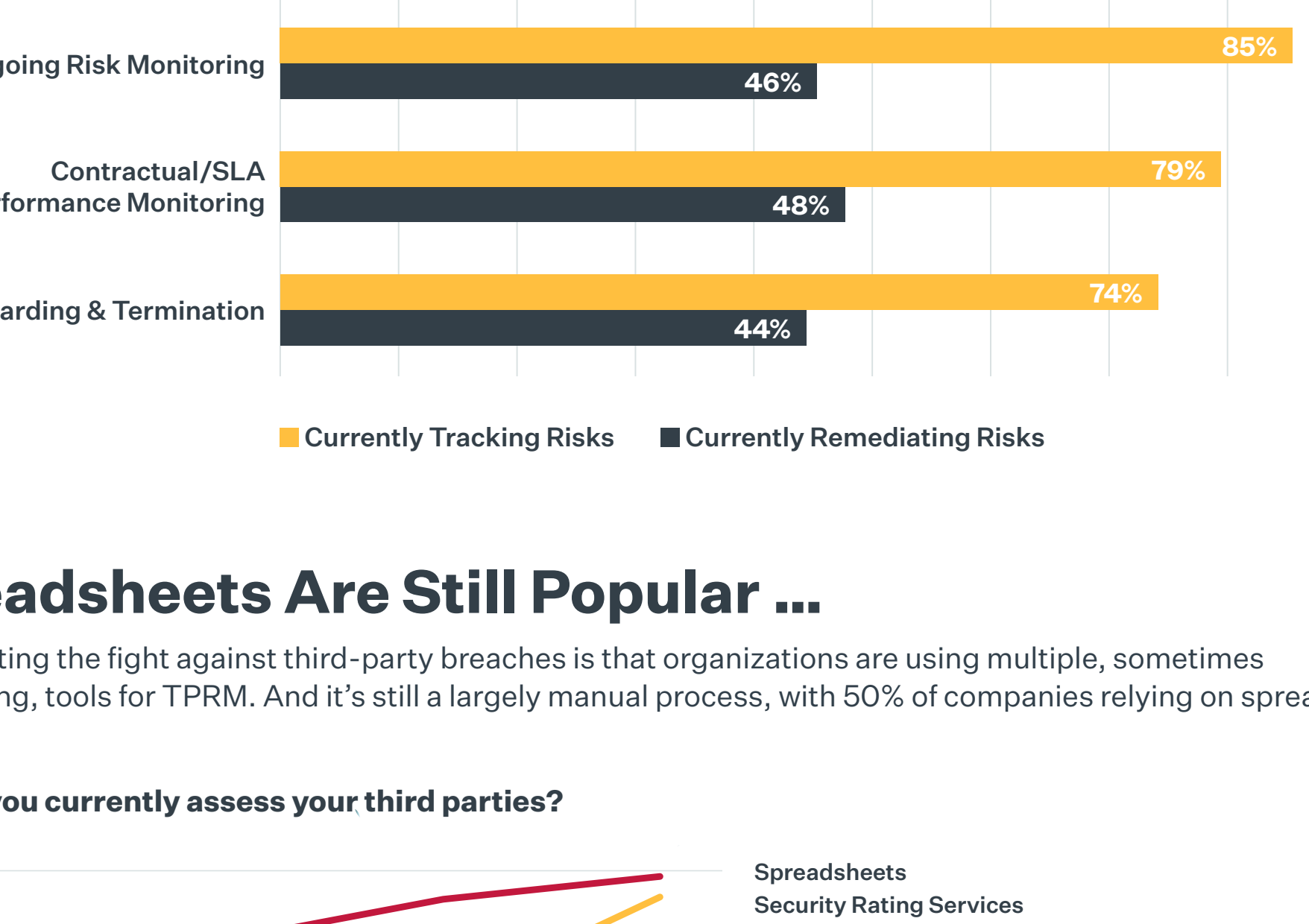


Some Risks Get More Attention Than Others

Those third-party breaches drove greater involvement in third-party risk. So much so that 58% of orgs are now tracking third-party cybersecurity risks more than last year – more than any other risk type.

Risk Tracking vs. Remediation Across the Vendor Lifecycle

One of the reasons behind the increase in third-party breaches might be the lack of risk remediation at key stages of the third-party lifecycle – especially during Sourcing and Selection and Risk Assessment. You can track risks all you want but, if you don't do something about them, then you could end up with a breach on your hands.



Spreadsheets Are Still Popular ...

Complicating the fight against third-party breaches is that organizations are using multiple, sometimes overlapping, tools for TPRM. And it's still a largely manual process, with 50% of companies relying on spreadsheets.

How do you currently assess your third parties?



... and Internal Assessments Are Lagging Behind External Monitoring

Given the increase in breaches, it's not surprising that companies are using security ratings services more vs. last year. But the concerning trend is that companies are monitoring cyber risks more than they are assessing cyber risks. The downfall is that monitoring provides no view of internal controls.

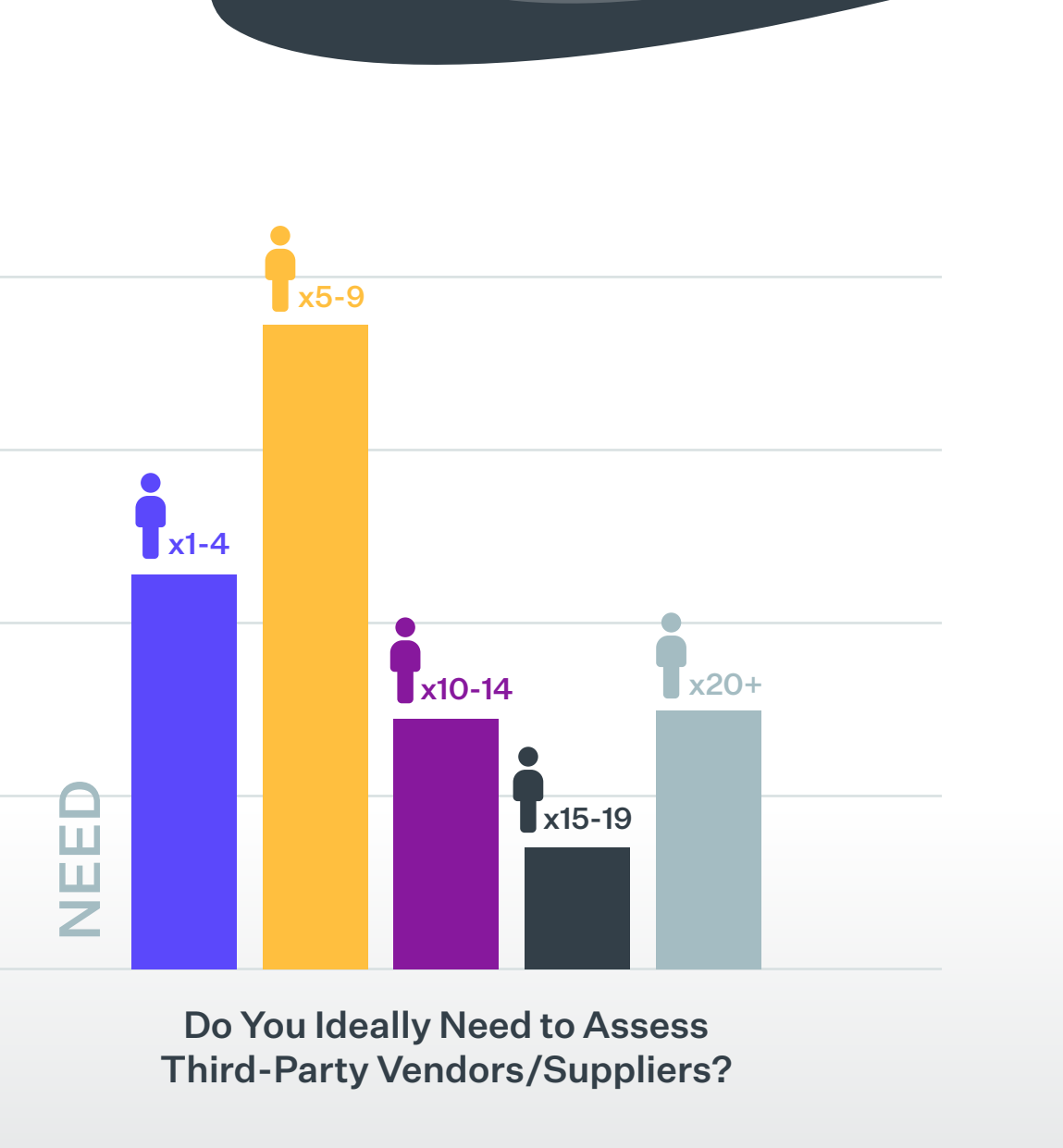
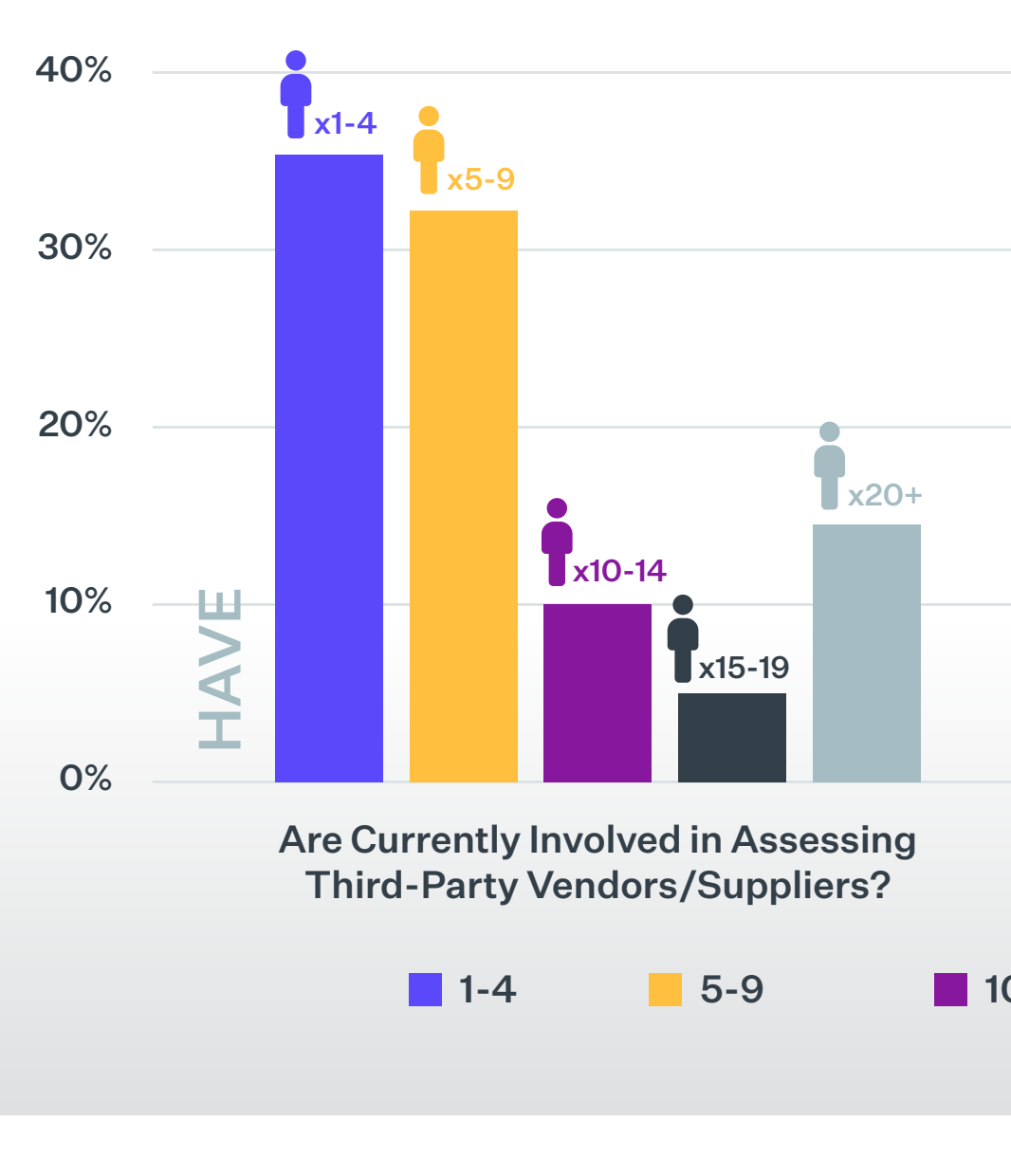


What types of third-party risks does your organization track?



Understaffed Teams Are Managing Only 33% of Vendors

With all those breaches to manage, infosec teams are overwhelmed – so much so that they're only managing a third of vendors due to understaffing by a factor of two!



How many people in your organization:



Barriers to TPRM Growth

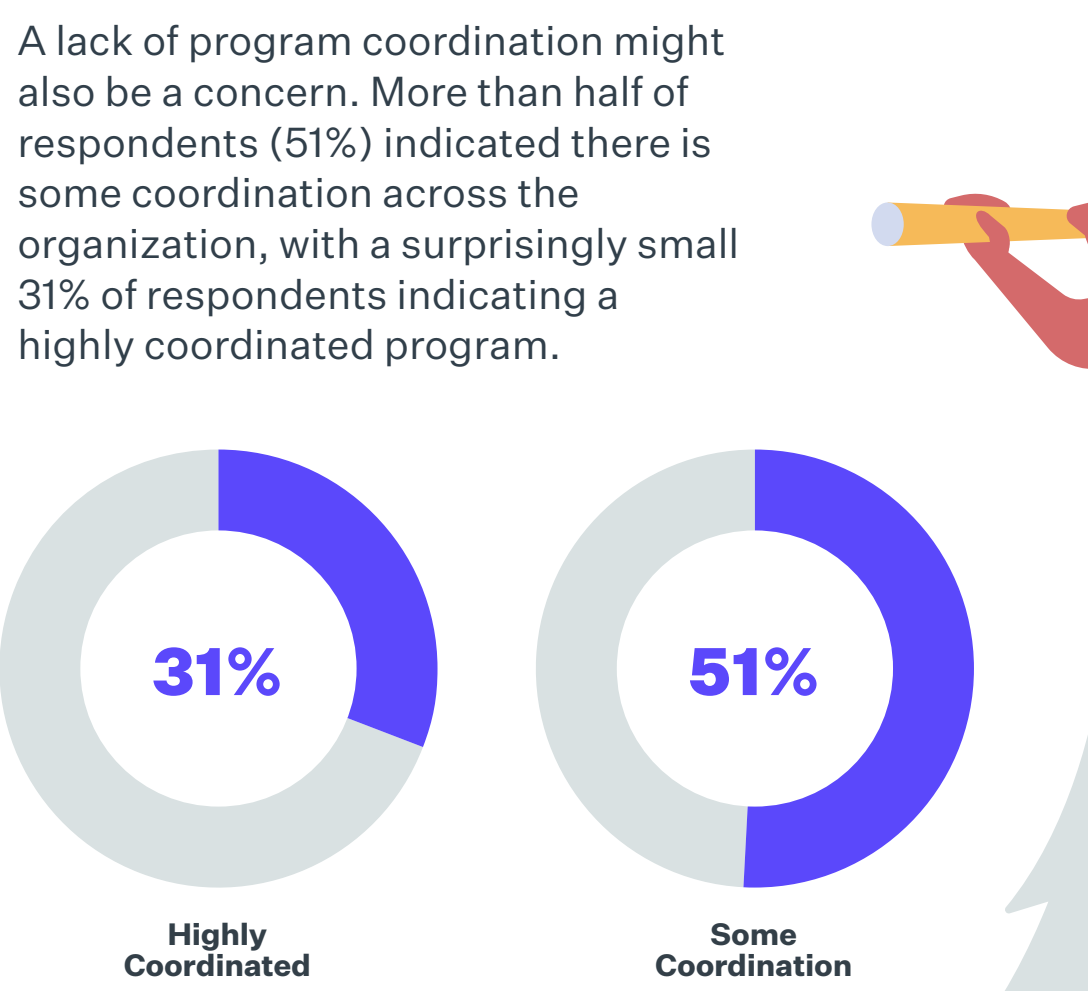
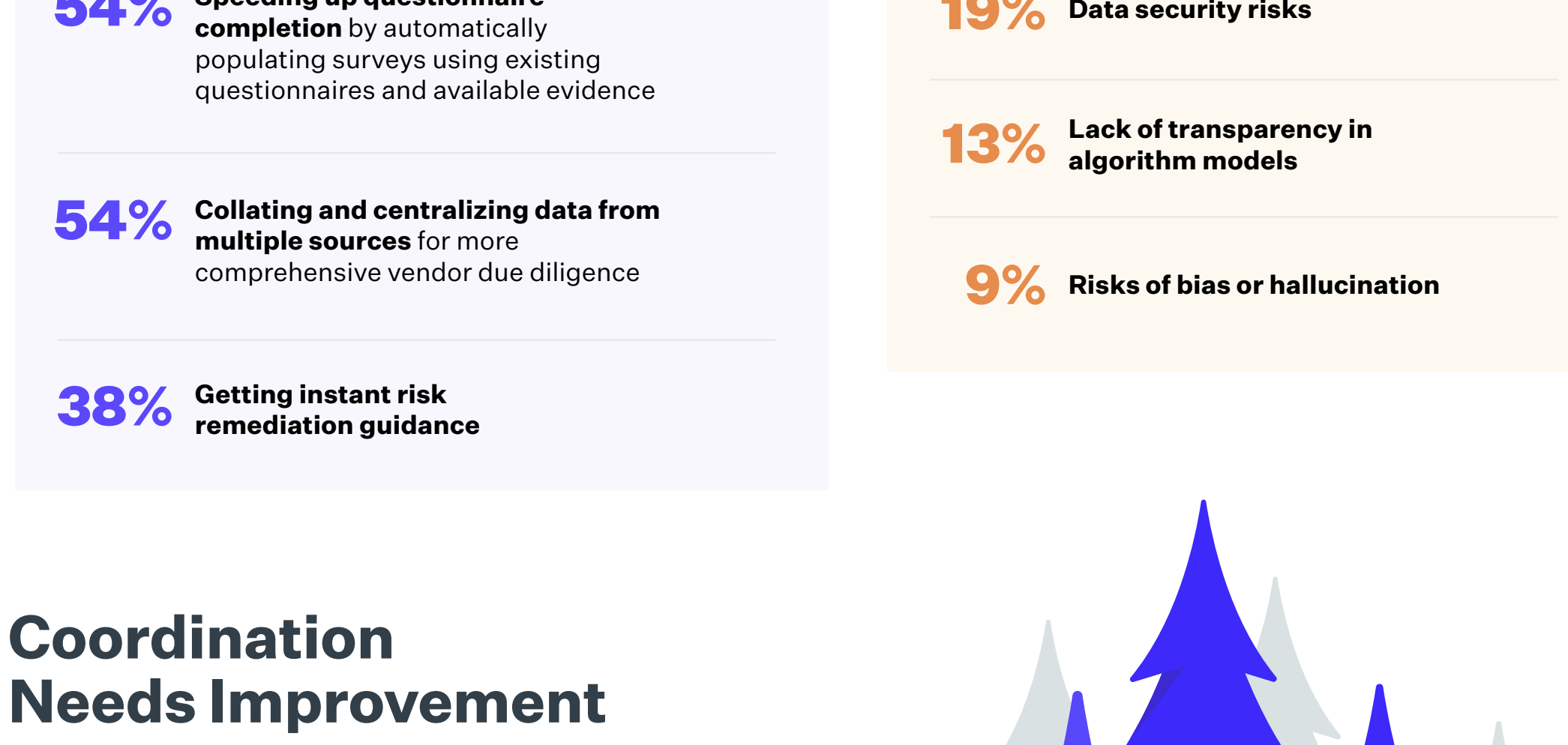
In fact, companies say a lack of resources is the number one barrier to growing their TPRM programs.



AI May Help, but Adoption Is Slow

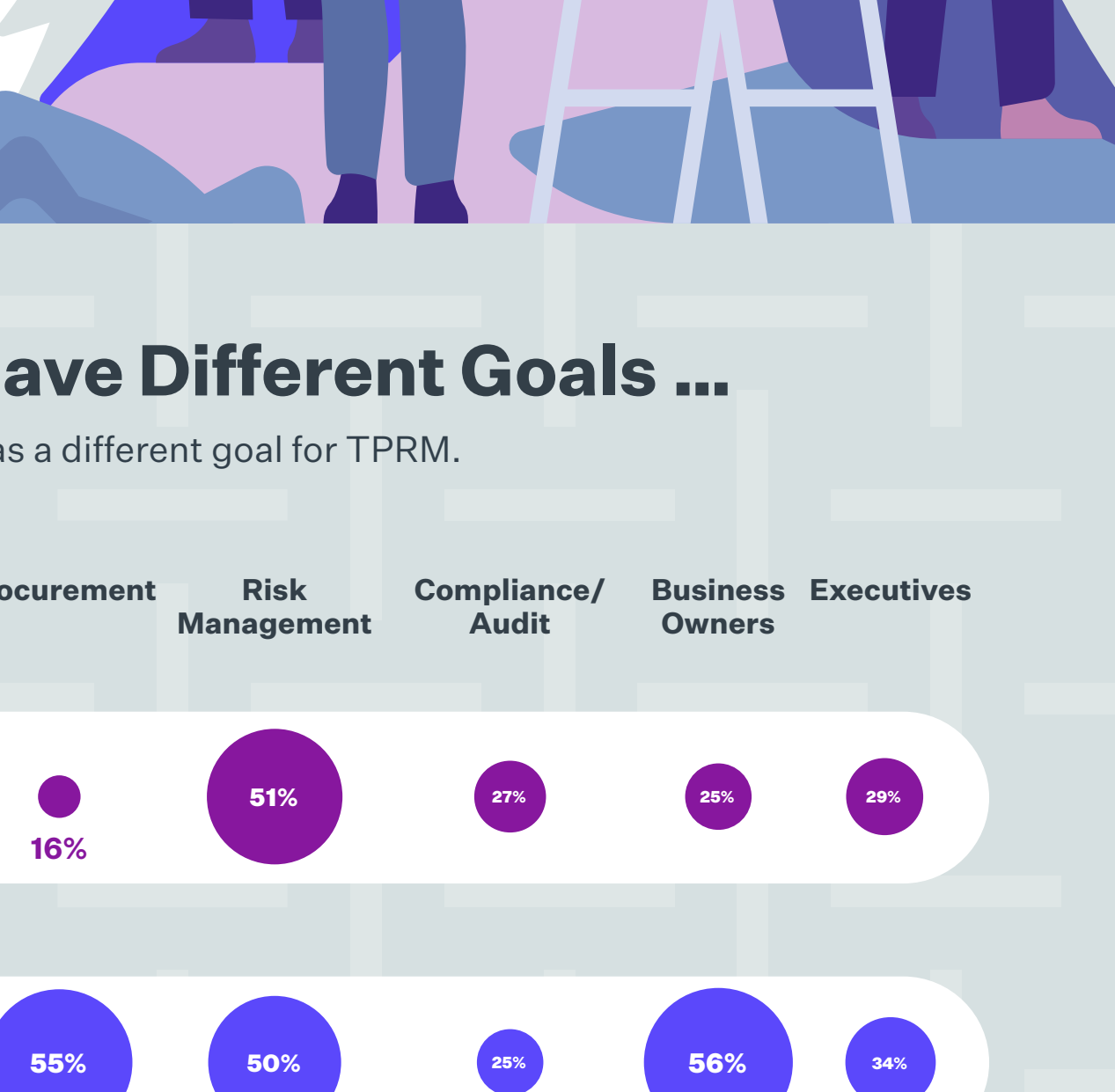
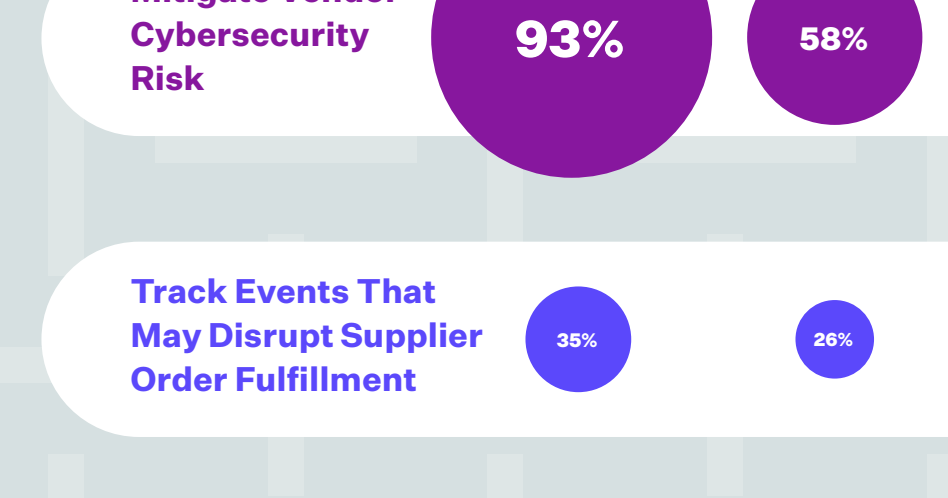
Only its automations and analytics, AI can help alleviate resourcing concerns. But for most companies they're only just starting to investigate its use cases – if at all.

Is your organization currently leveraging AI in its third-party risk management program?



Coordination Needs Improvement

A lack of program coordination might also be a concern. More than half of respondents (51%) indicated there is some coordination across the organization, with a surprisingly small 31% of respondents indicating a highly coordinated program.



Different Departments Have Different Goals ...

Coordination can be challenging when everyone has a different goal for TPRM.



... And Own Different Pieces of the Third-Party Management

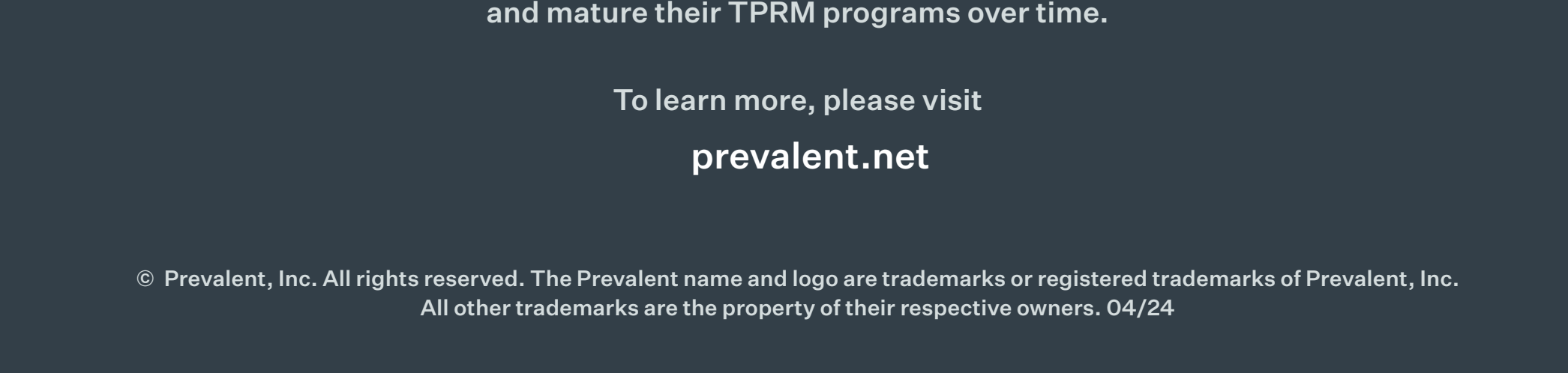
And there's a pretty complex ownership arrangement between Information Security, Business Owners, and Procurement in place in most companies.

In your organization, which department primarily:



Recommendations

Third-party risk management is achieving enterprise-level visibility and importance in the face of growing third-party cybersecurity challenges, but many programs struggle with manual processes that limit risk, lifecycle, and vendor coverage. Here are three actionable steps to improve TPRM.



- Create cross-functional teams and establish clear TPRM ownership to ensure that remediations are enforced
- Automate TPRM processes around a single platform to unify teams, data, and the risk lifecycle
- Close the resource and skill gap with outsourced managed services or artificial intelligence capabilities

Download the complete 26-page report for additional results, detailed analysis, and in-depth recommendations.

[Download the Study](#)