

2025 CISO Survey for Third-Party Cyber Risk Priorities

February 2025



Table of Contents

Introduction and Key Findings	3
Introduction & Methodology	4
Key Findings	5
Survey Report Findings	6
Increase in Third-Party Cybersecurity Incidents Over the Past Year	7
Predicted Changes in Third-Party Cybersecurity Incidents in 2025	8
Visibility Into Digital Supply Chain	9
Prioritization of Third-Party Cyber Risk Management in Cybersecurity Strategies	10
Business Management's Understanding of Third-Party Cyber Risk Implications	11
Adequacy of Budgets for Managing Third-Party Cyber Risks	12
Unresolved Third-Party Vulnerabilities Due to Resource Constraints	13
Primary Resource Constraints in Resolving Third-Party Vulnerabilities	14
Platforms Used to Manage Third-Party Cyber Risks	15
Accuracy of Platforms in Representing Third-Party Cyber Risks	16
Use of AI Automation in Third-Party Vendor Assessments	17
Time Savings Achieved with AI Automation for Vendor Assessments	18
Demographics	19
Industry, Company Size	20
About Panorays	21



Introduction and Key Findings

Introduction & Methodology

Third-party cyber risk management (TPCRM) is an ever-evolving challenge for CISOs and security managers. As organizations prepare for 2025, Panorays' annual survey uncovers the key priorities shaping TPCRM strategies and provides actionable insights to help security leaders address emerging risks.

The findings highlight a combination of factors driving the urgency for effective TPCRM solutions. From the rise in supply chain incidents—reported by 91% of CISOs—to the widespread lack of full visibility into third, fourth, and nth-party relationships, the stakes for organizational security have never been higher. Combined with rapid SaaS adoption and emerging regulatory demands, the need for specialized TPCRM platforms has become undeniable.

This report also sheds light on the role of AI as both a transformative tool and a growing challenge in the TPCRM landscape. With its potential to scale cyber risk programs and automate processes, AI offers a dual advantage: enhancing risk management while addressing increasingly sophisticated threats.

Designed for decision-makers navigating these complexities, this report offers guidance on leveraging TPCRM platforms to enhance security, ensure compliance, and build resilience in the face of evolving challenges.

Methodology

To gain insights into third-party risk management, we conducted a survey of 200 full-time CISOs. Participants were strategically sourced from organizations across the United States representing industries such as finance, insurance, professional services, technology, healthcare, and software development. Company sizes ranged from 1,000–5,000 employees, 5,000–10,000 employees, and over 10,000 employees. The survey was conducted in December 2024 in collaboration with Global Surveyz, an independent survey company.

Key Findings

1 **91% of CISOs report rising third-party cyber incidents, but only 3% have full supply chain visibility.**

Despite the sharp rise in third-party cybersecurity incidents, visibility into supply chains remains critically limited. Only 3% of respondents have full insight across their entire supply chain, including fourth and nth parties, while 33% can see only as far as third parties. This lack of comprehensive oversight leaves organizations unable to identify and address vulnerabilities effectively, increasing their risk of breaches.

2 **98% of CISOs admit that most third-party vulnerabilities go unresolved due to lack of resources.**

This widespread resource shortage leaves organizations unable to address critical vulnerabilities, significantly increasing their exposure to risk. To minimize potential losses from breaches, investing in efficient tools and processes is essential for resolving vulnerabilities at scale.

3 **While 90% of CISOs prioritize third-party cyber risk, 51% say business management has limited understanding of its implications.**

A lack of executive understanding limits funding and support for third-party risk management initiatives. Closing this gap is essential to aligning organizational priorities and implementing effective risk mitigation strategies, ultimately reducing long-term costs.

4 **CISOs are rapidly adopting AI automation to manage third-party risks.**

Currently, 27% of CISOs rely on AI automation for vendor assessments, with an additional 69% planning to adopt it within the next 12 months. This reflects a growing recognition of AI's ability to enhance efficiency and scalability, equipping organizations to manage the complexities of modern supply chains.

5 **AI automation transforms vendor assessments with significant time savings.**

AI automation is proving to be a game-changer for vendor assessments, significantly reducing the time and effort required. On average, assessment efforts are reduced by nearly half, with the vast majority of CISOs reporting meaningful time savings. AI-driven automation not only streamlines these processes, but also frees up resources for higher-value tasks, making it an indispensable tool in modern third-party risk management.

6 **GRC platforms fall short in addressing third-party cyber risks.**

Although widely used, GRC platforms often fail to fully address the complexities of third-party cyber risks. While 27% of CISOs rely on GRC platforms as their primary solution, more than half admit these tools only somewhat, minimally, or do not accurately represent third-party risks. This highlights the need for more specialized solutions to improve visibility and risk management.



Survey Report Findings

Increase in Third-Party Cybersecurity Incidents Over the Past Year

The prevalence of third-party cybersecurity incidents has surged, with 91% of respondents reporting an increase in the past year. Among these, 70% experienced a moderate rise, while 21% encountered significant escalation.

Figure 2 reveals a clear correlation between unresolved third-party vulnerabilities and the rise in incidents. Of respondents with 1-25% of vulnerabilities unresolved, 86% reported an increase in incidents, compared to 92% of those with 26-50% unresolved and 97% of those with more than 51%. As the number of unresolved vulnerabilities grows, so does the frequency of third-party-related cybersecurity incidents.

This trend underscores the growing vulnerability of organizations to third-party risks, driven by increasingly complex supply chains and evolving threat landscapes. As third-party relationships expand, so do the opportunities for attackers to exploit weaknesses. The findings highlight an urgent need for enhanced vendor security assessments, continuous monitoring, and comprehensive third-party risk management strategies.

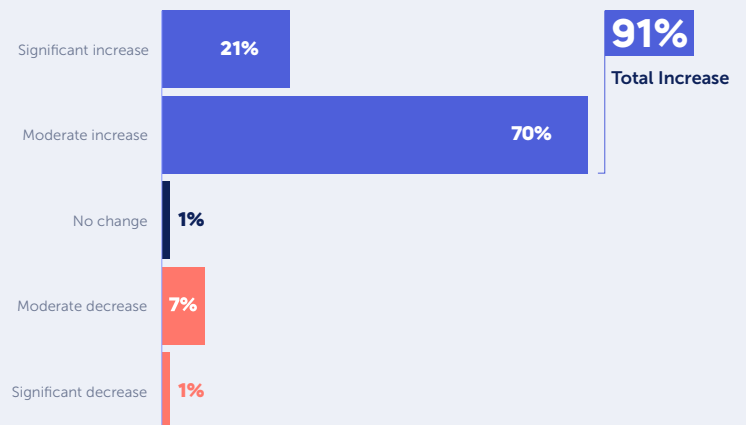


Figure 1: Increase in Third-Party Cybersecurity Incidents Over the Past Year

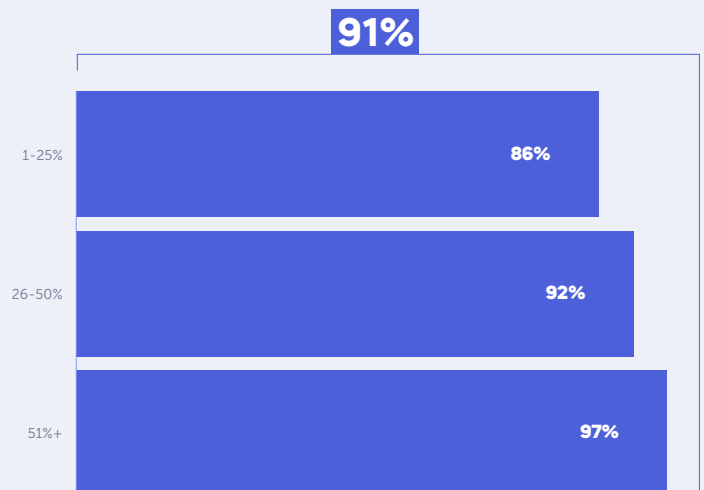


Figure 2: Increase by Percentage of Unresolved Third-Party Vulnerabilities

Predicted Changes in Third-Party Cybersecurity Incidents in 2025

An overwhelming 95% of surveyed CISOs predict a rise in third-party cybersecurity incidents in 2025, reflecting a stark consensus among security leaders. This near-unanimous forecast underscores the escalating challenges organizations face as third-party cyber risks grow in scope and complexity.

The implications are clear: organizations must act now to prepare for this predicted surge. Strengthening third-party risk management strategies, investing in advanced tools for continuous monitoring, and fostering a proactive security posture will be critical to mitigating the impact of these incidents.

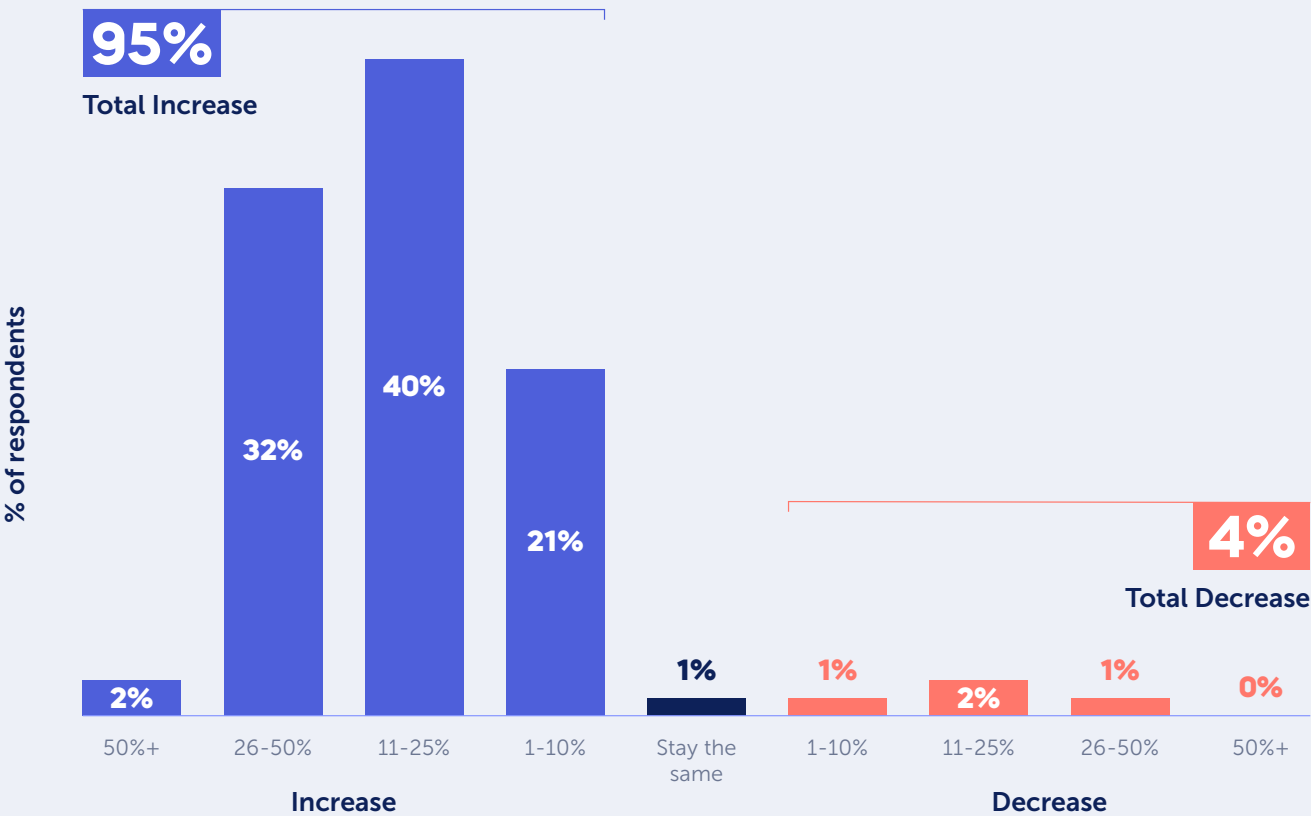


Figure 3: Predicted Changes in Third-Party Cybersecurity Incidents in 2025

Visibility Into Digital Supply Chain

Only 3% of respondents report full visibility into their supply chain, while 39% acknowledge limited visibility into all levels of their supply chain, and 33% maintain insight into third parties but lack visibility into deeper tiers, such as fourth and nth parties.

Figure 5 shows that larger companies face greater challenges in achieving supply chain visibility. Among organizations with 1,000–4,999 employees, 15% report visibility into third parties and most and nth parties. This figure rises to 24% for companies with 5,000–9,999 employees and 36% for those with over 10,000 employees. As supply chains grow more complex with organizational size, identifying and mitigating risks at deeper tiers becomes increasingly difficult.

This lack of comprehensive visibility significantly increases business risk. If companies cannot see the vulnerabilities within their supply chains, they are ill-equipped to address them, leaving themselves exposed to escalating threats. This is particularly concerning given that 91% of CISOs reported a rise in third-party cybersecurity incidents over the past year (Figure 1).

Organizations must prioritize visibility across all tiers of their supply chain to effectively identify and mitigate risks. Without these capabilities, the growing complexity of modern supply chains will continue to outpace risk management efforts.

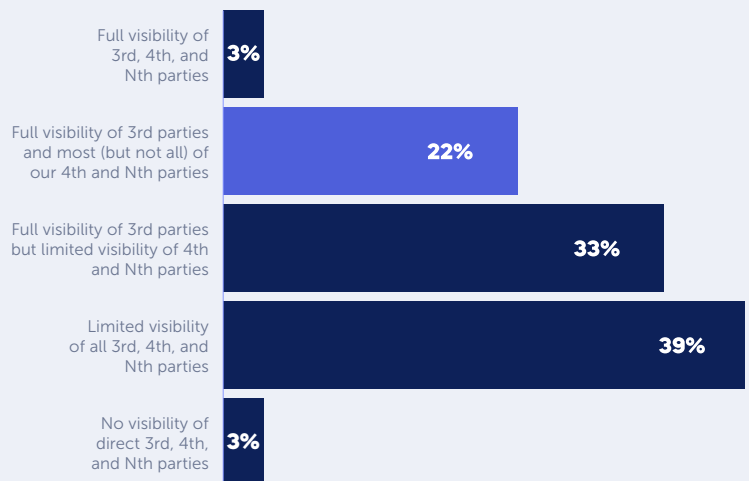


Figure 4: Visibility into Digital Supply Chain

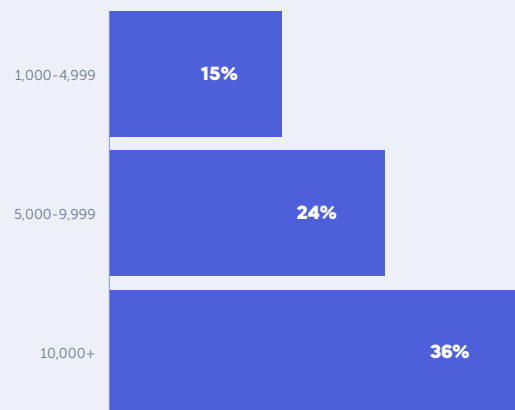


Figure 5: Visibility into Third, Fourth, and Nth Parties by Company Size

Prioritization of Third-Party Cyber Risk Management in Cybersecurity Strategies

Strengthening third-party cyber risk management is firmly at the forefront of CISOs' priorities. 60% of respondents report that third-party cyber risk management is a top or high priority in their overall cybersecurity strategies, with 15% identifying it as a top priority and 45% as a high priority.

Among companies that rank third-party cyber risk management as a high or top priority, 49% are already leveraging AI automation to enhance their strategies and 66% are not yet using AI automation but plan to adopt it. This underscores the growing recognition of AI as a pivotal tool in balancing the complexities and risks of third-party relationships.

As third-party incidents rise and visibility remains limited, organizations must continue to focus on proactive monitoring, enhanced visibility, and innovative solutions like AI to navigate an increasingly complex threat landscape.

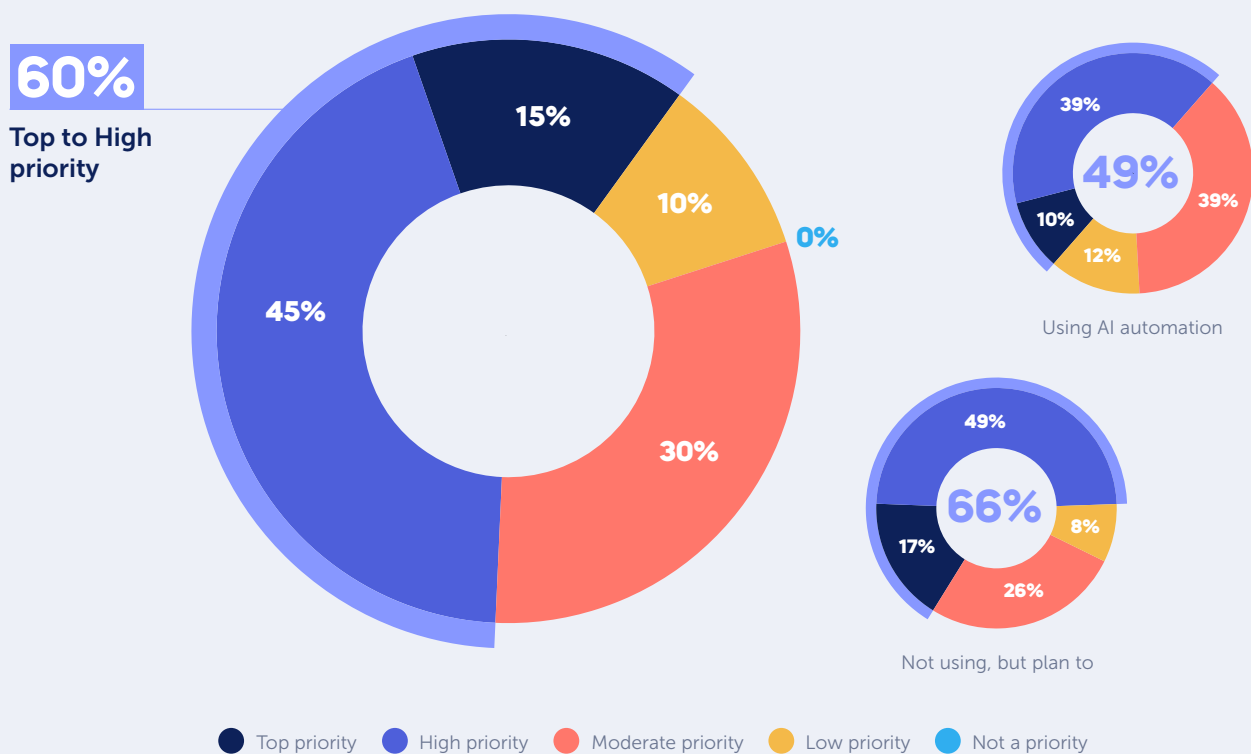


Figure 6: Prioritization of Third-Party Cyber Risk Management in Cybersecurity Strategies

Business Management's Understanding of Third-Party Cyber Risk Implications

A significant gap exists in business management's understanding of third-party cyber risks, with only 17% of respondents rating their management's awareness as complete. 51% report limited understanding, underscoring the challenge CISOs face in communicating the real-world impact of these risks in ways that resonate with business priorities.

This limited understanding can hinder the ability to secure resources and drive proactive measures. Without a clear grasp of the financial, reputational, and operational implications of third-party cyber risks, leadership may underestimate the urgency of investing in robust risk management strategies.

Conversely, organizations with leadership that fully understands the implications of third-party risks gain a competitive advantage. These companies are better equipped to prioritize risk reduction, align cybersecurity initiatives with business goals, and mitigate potential fallout from incidents. Strengthening communication and alignment between cybersecurity teams and business leadership is essential to closing this gap and enabling more effective risk management.

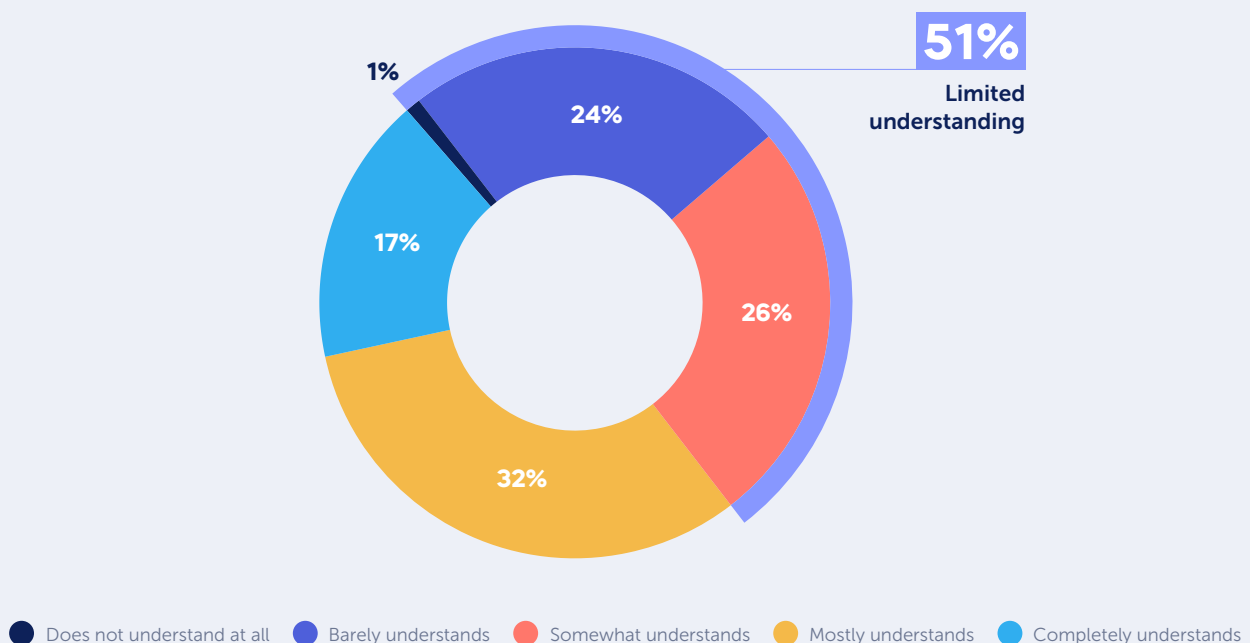


Figure 7: Business Management's Understanding of Third-Party Cyber Risk Implications

Adequacy of Budgets for Managing Third-Party Cyber Risks

Despite the rise of third-party cyber risks, the survey reveals a critical disconnect between the growing threat landscape and the resources allocated to address it. Only 19% of respondents report having adequate budgets to manage these risks effectively, leaving an overwhelming 81% struggling with insufficient funding.

This shortfall is closely tied to the limited awareness of business management regarding the financial, reputational, and operational implications of third-party cyber risks. Without a clear understanding of the potential fallout, leadership may underprioritize budget allocation, leaving organizations vulnerable to escalating threats.

The data underscores the critical need for better communication and alignment between CISOs and business leaders. Demonstrating the tangible impact of third-party cyber risks on overall business objectives could drive more investment in risk management strategies, ensuring organizations are equipped to handle the increasing complexity of today's threat landscape.

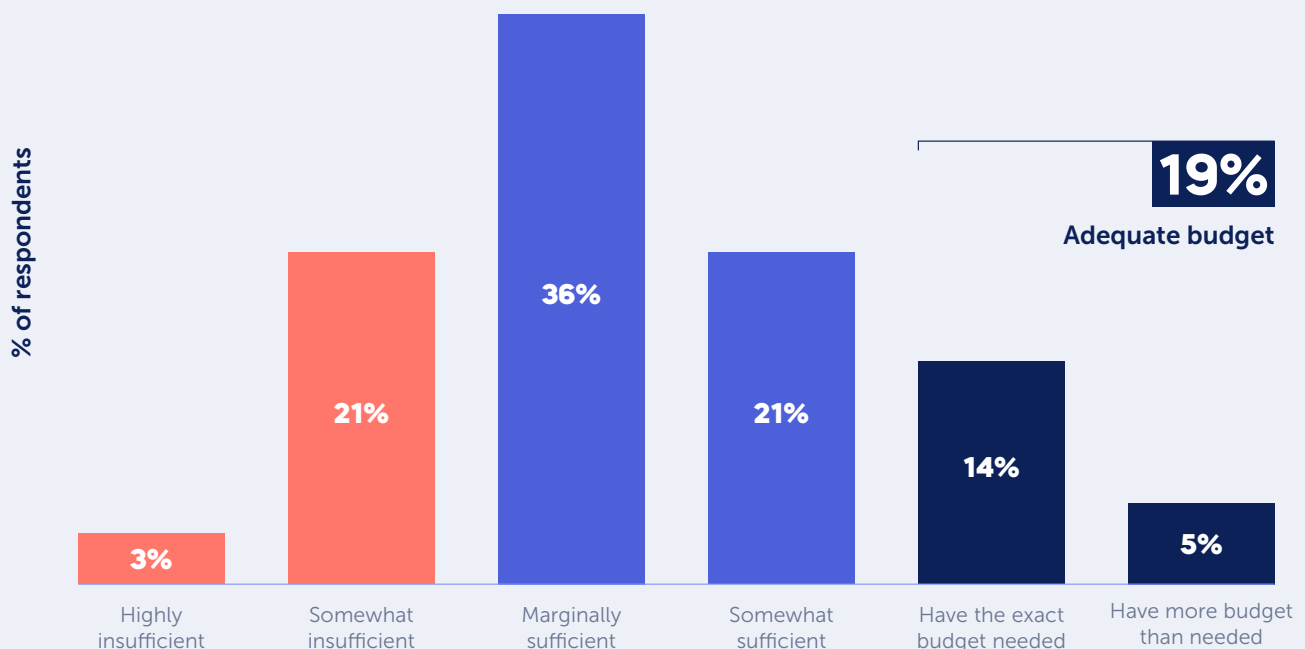


Figure 8: Adequacy of Budgets for Managing Third-Party Cyber Risks

Unresolved Third-Party Vulnerabilities Due to Resource Constraints

Resource constraints present a significant barrier to effective third-party vulnerability management, with 50% of respondents reporting they are unable to resolve between 26% and 50% of identified vulnerabilities. Alarming, **98% of organizations admit they leave at least 10% of third-party vulnerabilities unresolved due to insufficient resources**, with many struggling to address significantly higher percentages.

These findings align with prior insights on inadequate budgets and limited management understanding. Without sufficient resources and leadership support, CISOs are unable to fully address the growing volume of vulnerabilities, further exacerbating the frequency and impact of third-party cybersecurity incidents.

The data highlights an urgent need for organizations to invest in comprehensive risk management strategies that address resource gaps, streamline vulnerability resolution processes, and prioritize third-party cybersecurity as a critical business concern. Without these measures, unresolved vulnerabilities will continue to pose a significant threat to organizational security.

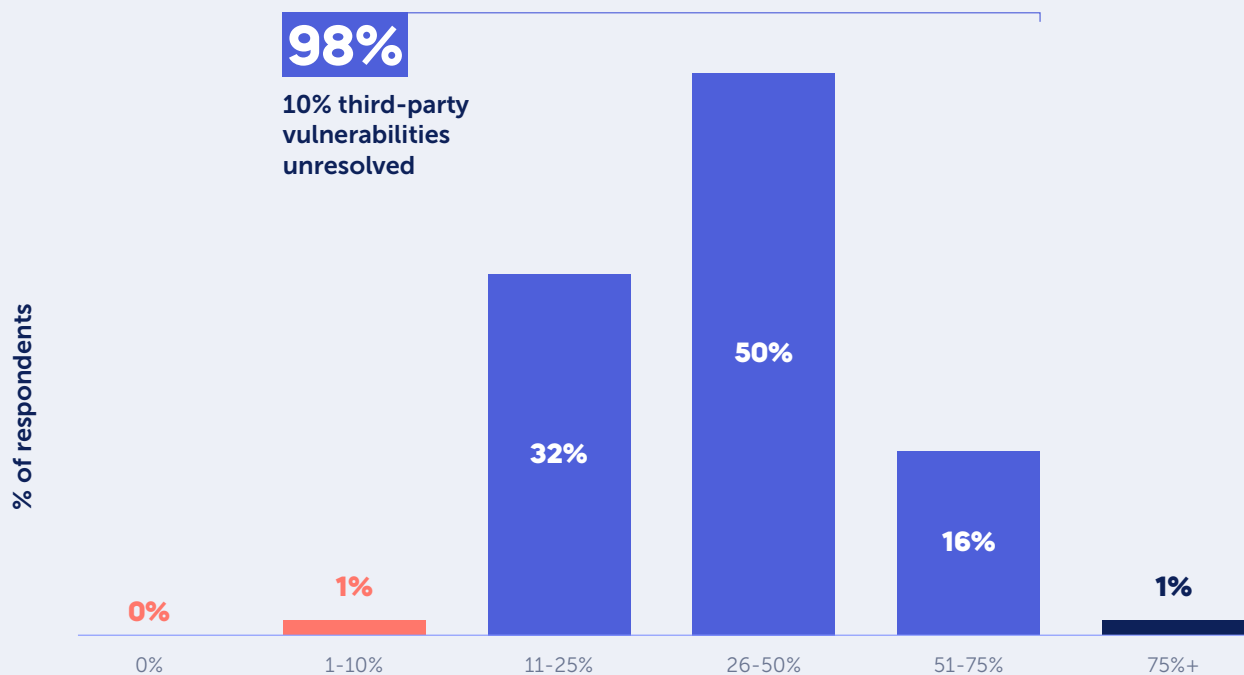


Figure 9: Unresolved Third-Party Vulnerabilities Due to Resource Constraints

Primary Resource Constraints in Resolving Third-Party Vulnerabilities

The survey reveals a wide range of constraints hindering the resolution of third-party vulnerabilities, with no single issue standing out as the dominant challenge. Respondents cite limited time or competing priorities (29%), lack of visibility into third-party risks (27%), and lack of executive or board support (27%) as the top constraints.

This even distribution of challenges highlights a systemic problem: organizations face obstacles at nearly every level of their third-party cyber risk management process. Rather than addressing a single issue, businesses require a comprehensive approach to overcome these multi-faceted constraints.

Implementing an all-in-one platform designed to enhance visibility, streamline processes, and centralize third-party risk management can be a game-changer. Such solutions enable organizations to tackle diverse challenges efficiently, ensuring vulnerabilities are managed and risks mitigated across the board.

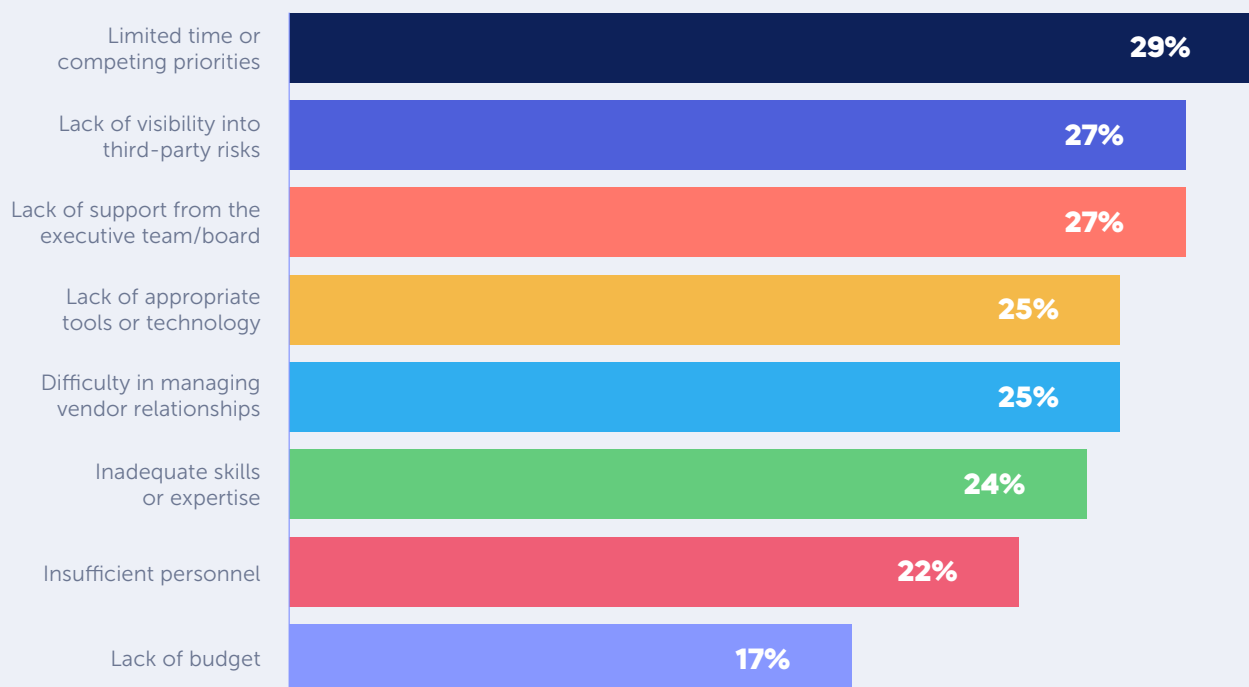


Figure 10: Primary Resource Constraints in Resolving Third-Party Vulnerabilities

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

Platforms Used to Manage Third-Party Cyber Risks

TPRM and TPCRM platforms lead the way as the preferred solutions for addressing third-party cyber risks. With 45% of respondents identifying these platforms as their primary tools, their adoption underscores their effectiveness in targeting the unique challenges of third-party cybersecurity. Purpose-built for this domain, TPRM/TPCRM platforms provide the focused capabilities necessary to tackle these risks comprehensively.

In contrast, Governance, Risk, and Compliance (GRC) platforms, while used as primary solutions by 27% of respondents, lack the specialized focus of TPRM/TPCRM platforms. Their broader scope often fails to fully address the complexities of third-party cyber risk, leaving critical gaps in visibility, monitoring, and resolution capabilities.

The data highlights the importance of selecting a solution tailored specifically for third-party cyber risk management. TPRM/TPCRM platforms not only provide the most targeted approach but also help organizations strengthen their overall cybersecurity posture in a rapidly evolving threat landscape.

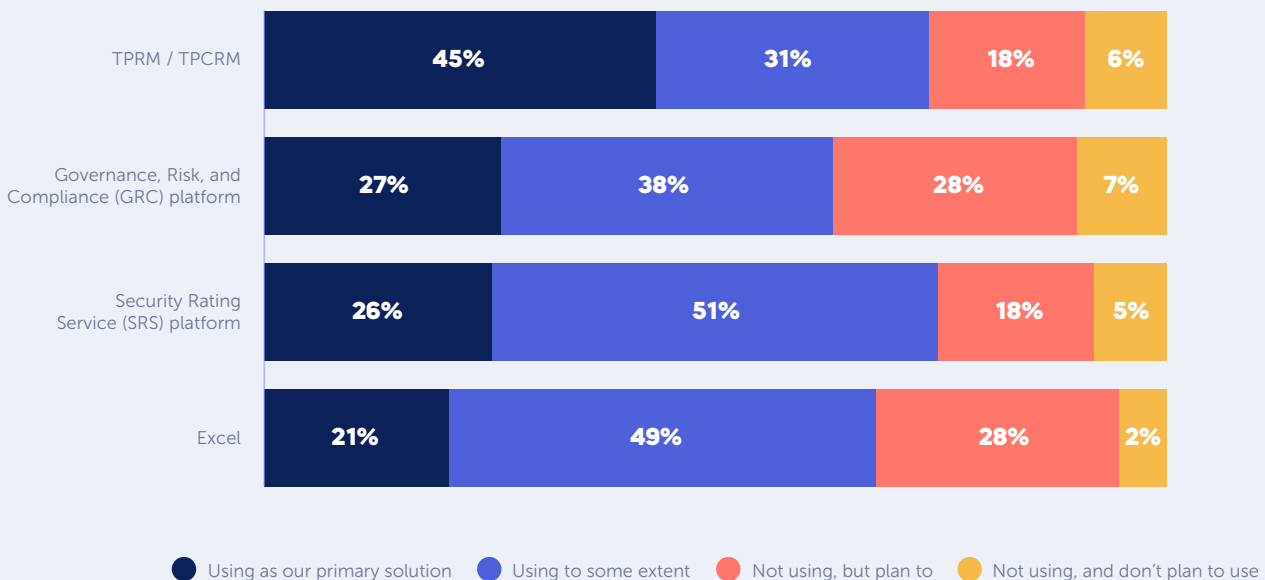


Figure 11: Platforms Used to Manage Third-Party Cyber Risks

Accuracy of Platforms in Representing Third-Party Cyber Risks

TPRM and TPCRM platforms are widely regarded as the most accurate and trusted solutions for managing third-party cyber risks, with 56% relying on them as their primary platform. Among these, 35% rated them "very accurate" and 21% "extremely accurate." Their tailored focus on third-party risk management ensures comprehensive insights, continuous monitoring, and specialized capabilities that address today's complex cybersecurity challenges.

In contrast, GRC platforms, used by 27% of CISOs as a primary solution, often fall short. While 27% find them "very accurate," 54% admit these platforms only somewhat, minimally, or do not accurately represent third-party risks. Designed for broader governance and compliance, GRC platforms lack the specialization needed for effective third-party cyber risk management.

Excel's continued use highlights the limitations of manual processes in managing third-party risks. While 24% of respondents rate it "very accurate," its lack of automation and real-time capabilities prevents organizations from effectively tracking vulnerabilities and risks.

These findings highlight the critical advantage of TPRM/TPCRM platforms, purpose-built to address the complexities of third-party risks with unmatched accuracy and focus.

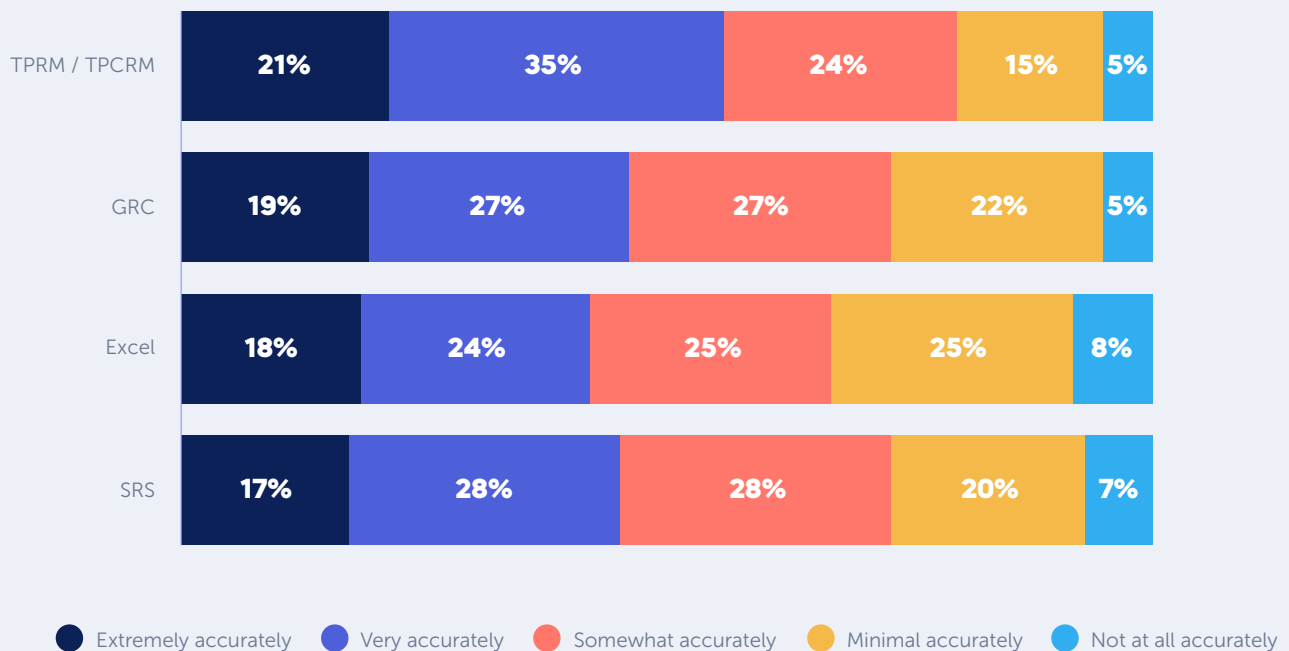


Figure 12: Accuracy of Platforms in Representing Third-Party Cyber Risks

Use of AI Automation in Third-Party Vendor Assessments

CISOs are increasingly recognizing the need to adapt to the complexities of modern supply chains, with AI automation emerging as a key tool for improving vendor assessment processes. 27% of respondents are already leveraging AI automation, with an additional 69% plan to implement it within the next 12 months.

This rapid shift reflects the growing importance of adapting to new technology when managing third-party cyber risks. By adopting AI, organizations aim to streamline vendor assessments, enhance efficiency, and better address the scale and complexity of today's supply chain challenges. The strong intent to embrace AI automation underscores a proactive approach by CISOs to stay ahead of evolving risks and optimize third-party cyber risk management strategies.

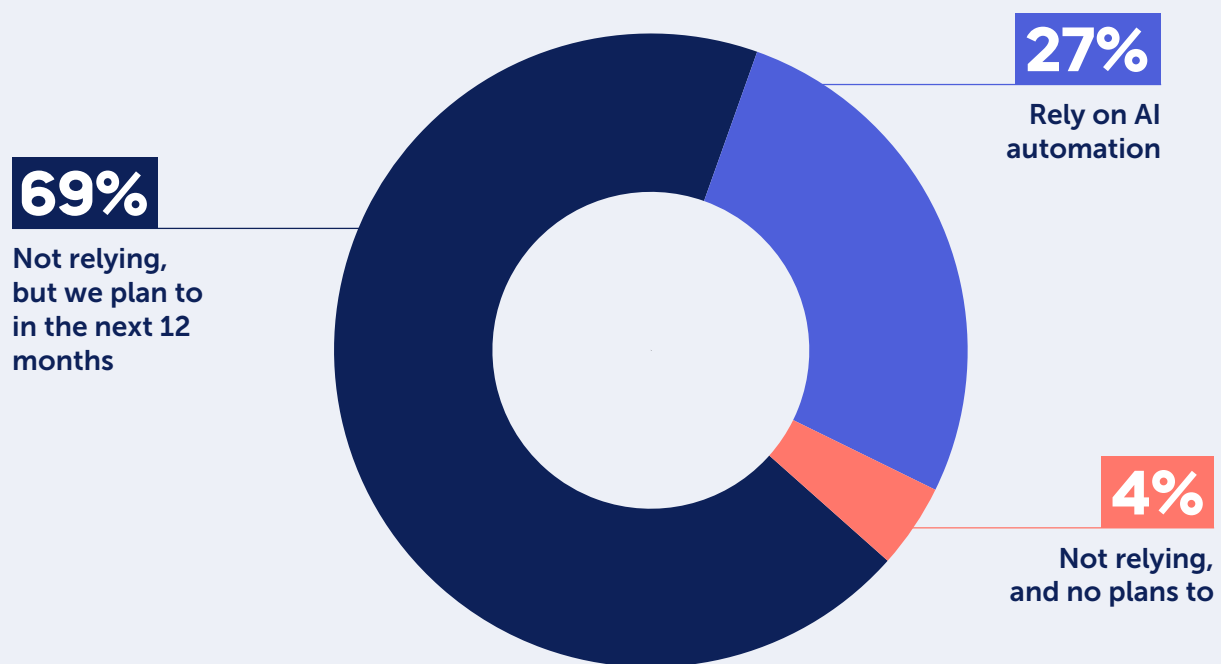


Figure 13: Use of AI Automation in Third-Party Vendor Assessments

Time Savings Achieved with AI Automation for Vendor Assessments

AI automation is revolutionizing third-party vendor assessments, with 94% of CISOs reporting a time savings of over 25% and an average reduction of 44% overall in vendor assessment efforts.

These results directly address the resource constraints highlighted in Figure 8. Limited time or competing priorities (29%) and challenges in managing vendor relationships (25%) were identified as key barriers to resolving third-party vulnerabilities. By significantly reducing the time spent on assessments, AI not only alleviates these challenges but also enables organizations to reallocate resources toward higher-value tasks.

For businesses grappling with inadequate tools or strained resources, AI automation represents a transformative solution. It streamlines workflows, enhances efficiency, and equips teams to better manage the complexities of modern supply chains.

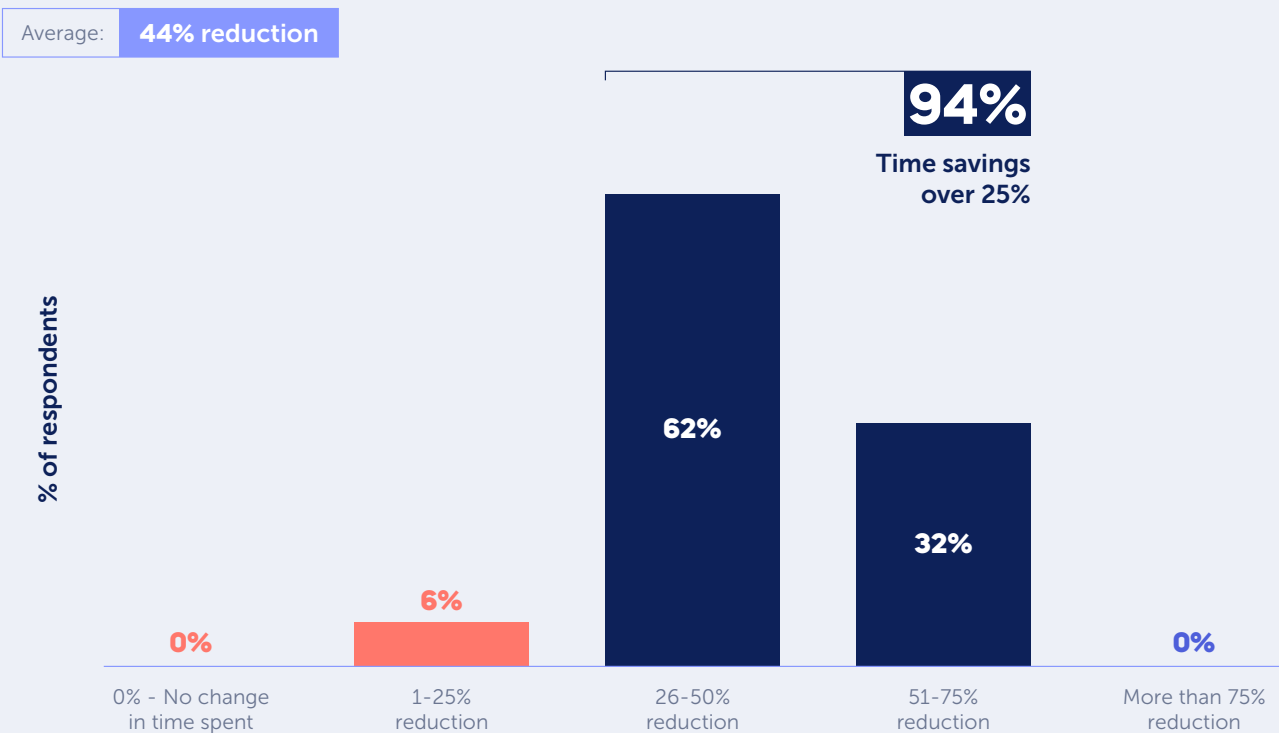


Figure 14: Time Savings Achieved with AI Automation for Vendor Assessments



Demographics

Industry, Company Size

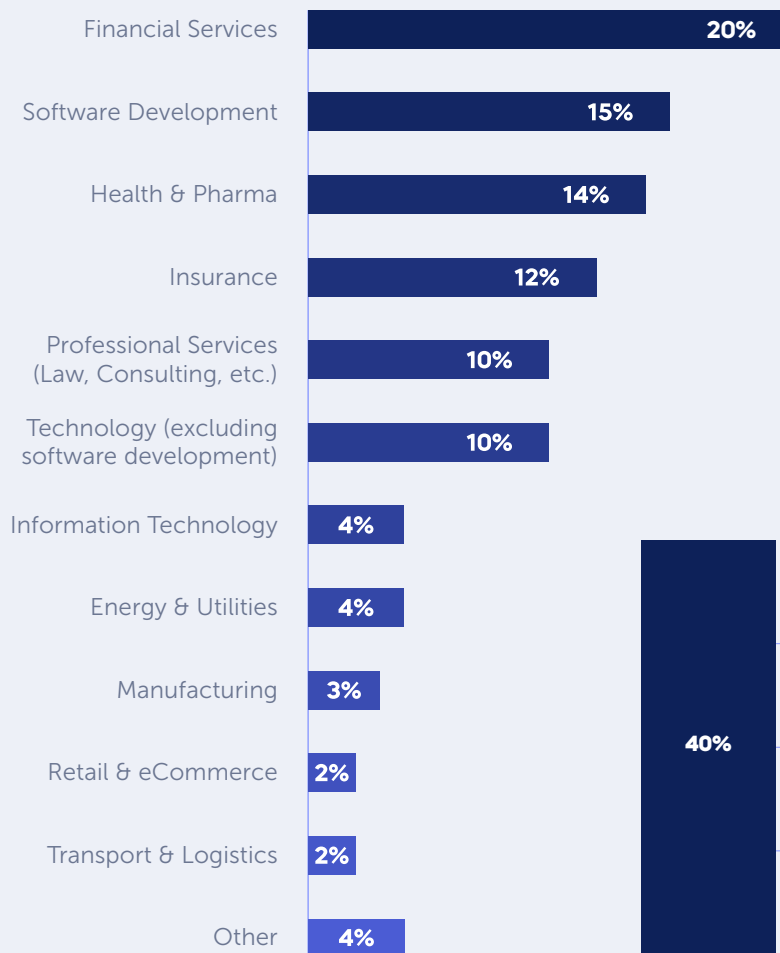


Figure 15: Industry

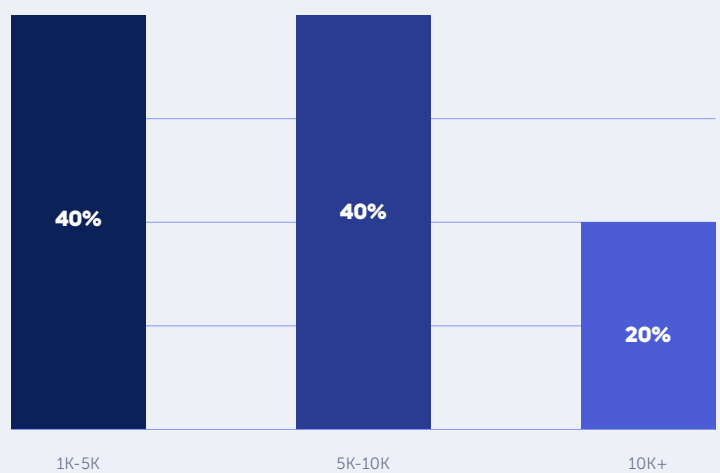


Figure 16: Company Size (Employees)

About Panorays

Panorays is a leading provider of third-party cyber risk management solutions, helping businesses optimize their defenses for each unique third-party relationship. Trusted by the most complex supply chains in the world, Panorays goes far beyond the generic third-party risk management solution with its AI-powered platform making assessments adaptable and more personalized. Panorays provides businesses the tools to stay ahead of emerging third-party threats and delivers actionable remediations that provide strategic advantages

Request a Demo

For more information, please visit us:



Email: info@panorays.com