Panorays

2024 CISO Survey for Third-Party Cyber Risk Priorities

January 2024

Panorays

Table of Contents

Introduction and Key Findings

Panorays

Introduction & Methodology

If strengthening third-party risk management isn't on the agenda for your enterprise in 2024 — you may need to start paying attention. From our vantage point as market leaders in controlling cyber risk, we've noted a number of trends that have converged to make third-party risk management the highest priority for today's security professionals.

Despite measures being taken for due diligence and third-party assessments, third-party cyber breaches are still on the rise. And as the supply chain continues to grow in size and complexity, accelerated digital transformation and SaaS adoption means that visibility into third, fourth and nth parties has become almost impossible. 98% of organizations have integrations with at least one third-party vendor that has experienced a cyberattack during the past two years. Most enterprises simply don't have the technology or the resources to work out whether they are in that 98%, and if so — how to protect their data and their customers.

CISOs recognize that limited resources may not be a valid excuse for much longer. An increase in regulatory attention related to the management of third-party risks and supply chain resilience is putting a burden on organizations and forcing them to rethink where they place budget.

Another critical driver is AI. Artificial Intelligence is both a risk and an opportunity, especially with evolving compliance regulations to consider. Enterprises are asking themselves, what standards of risk management should I employ to securely onboard transformative AI tools within my business? At the same time, AI is also a powerful enabler of third-party risk management, supporting enterprises in protecting against breaches, and in automating and scaling their cyber risk programs.
With the focus on third-party cyber risk management front and center, this report speaks directly to the CISOs themselves, the decision makers who set the priorities and channel both buy-in and budget. The results shine a light on a maturing enterprise landscape, where AI is viewed as a powerful tool, compliance and risk quantification are top priority, and the roadmap towards a dedicated solution for mitigating third-party risk is already well underway.

Methodology

We commissioned a survey of 200 full-time US CISOs who work across all industries, from enterprise companies with between 1k and 15k employees. This report was administered online by Global Surveyz Research, a global research firm. The respondents were recruited through a global B2B research panel, invited via email to complete the survey, and all responses were collected during Dec 2023. The average amount of time spent on the survey was 7 minutes and 29 seconds. The answers to the majority of the non-numerical questions were randomized, in order to prevent order bias in the answers.

Key Findings

1

94% of CISOs are concerned about third-party cybersecurity threats

Nearly all CISOs have third-party cybersecurity threats on their radar as a priority or a cause for concern. The larger the enterprise, the more pronounced that concern becomes. 47% of CISOs in midsize enterprises (under 2k employees) say they are very concerned about their level of risk, compared with 73% of CISOs in very large enterprise (10k-15k employees).

2

There is no silver bullet to manage third-party cybersecurity threats

Whether it's cyber questionnaires, audit and assurance software, compliance management tools or external attack surface monitoring — different tools have different approaches. As a result, each one is effective or highly effective for between 65-73% of organizations. The data proves it's the combination that makes cyber risk management complete.

3

As regulation over Artificial Intelligence grows, CISOs know they need to get prepared

The top challenge for CISOs in 2024 is complying with new regulations for third-party risk management, especially pertinent with the rise of AI. Evolving regulations such as the EU's AI Act, the American Data Privacy and Protection Act, as well as guidance such as NIST's AI Risk Management Framework will soon no doubt be the tip of the compliance iceberg.

4

61% of CISOs believe AI could prevent more than 50% of third-party breaches

Compliance with AI-driven regulations is critical, as 61% of CISOs see AI as the answer for preventing between 50-100% of third-party breaches. AI will shore up enterprise defenses by adding much needed visibility, improving supply chain discovery (23%), and in the discovery of third-party assets (21%).

5

Budget to manage third-party risk is growing, and CISOs have a long wish list

65% of CISOs have increased their third-party cyber risk management budget for 2024. 92% are using this for implementing or planning the implementation of a designated solution for third-party threats. It's no surprise to see 70% of CISOs have at least 9 critical capabilities and considerations on the list. However, top of the list is risk quantification — a tool that can put a dollar value on third-party risk.

Survey Report Findings

Panorays

How Concerned are Companies About Third-Party Cybersecurity Threats?

94% of CISOs are concerned about third-party cybersecurity threats. For 16%, this issue is their top priority.

This is unsurprising, as according to Gartner, 45% of organizations experienced third party-related business interruptions over the past two years.

On average, 65% of CISOs call out third-party cybersecurity threats as an issue they are very concerned about. However, when we break down the answers by the size of the company, a pattern emerges.

While everyone is focused on this issue, **the larger the enterprise, the more concerned they are about third-party cybersecurity threats.** At one end of the scale, 47% of CISOs in companies with fewer than 2,000 employees are very concerned about this issue, with the percentage rising in line with company size.

As a result, when speaking with CISOs responsible for the largest enterprises, (those who employ between 10,000 and 15,000 workers) 73% call third-party cybersecurity threats very concerning or have made the issue their top priority.

Larger enterprises may be more concerned due to a greater number of third parties, or they may need to adhere to more extensive regulations. It's also important to consider the maturity level of the enterprise. The larger the company, the greater the risk and consequence of a third-party breach.

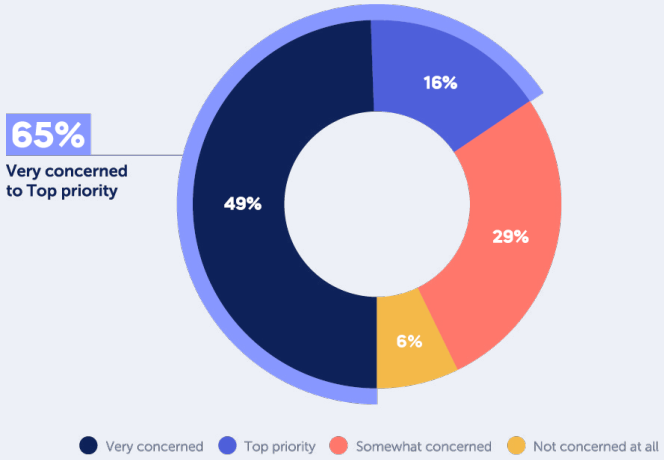

Figure 1: Level of Concern Regarding Third-Party Cybersecurity Threats

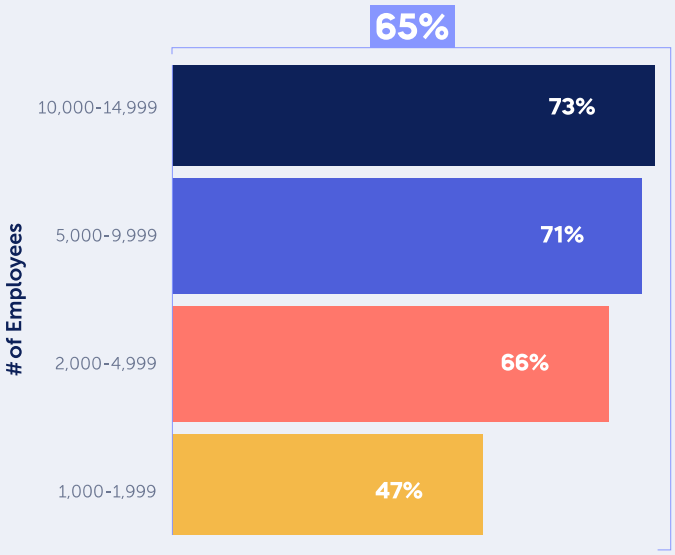

Figure 2: Very Concerned to Top priority, by Company Size

How Effective are Existing Tools in Reducing Third-Party Cyber Risks?

We asked CISOs which tools they find the most effective in reducing third-party cyber risk and found a similar level of impact for all options across the board.

When looking at what percentage of CISOs consider specific tools to be effective or highly effective, there is no one clear winner.

Cyber questionnaires for third parties is ranked as effective or highly effective for 73% of CISOs. Compliance management tools were chosen by 69%, and API monitoring by 68%. Audit and assurance software is considered to be effective or highly effective for 67% of CISOs, and when asking about external attack surface monitoring of third parties – the percentage was 66%. There is just 7% difference between the most and least effective tool on the list.

It's clear that there is no silver bullet that can fully manage the challenge of reducing third-party cyber risk. Instead, combining multiple tools is the most effective route to success.

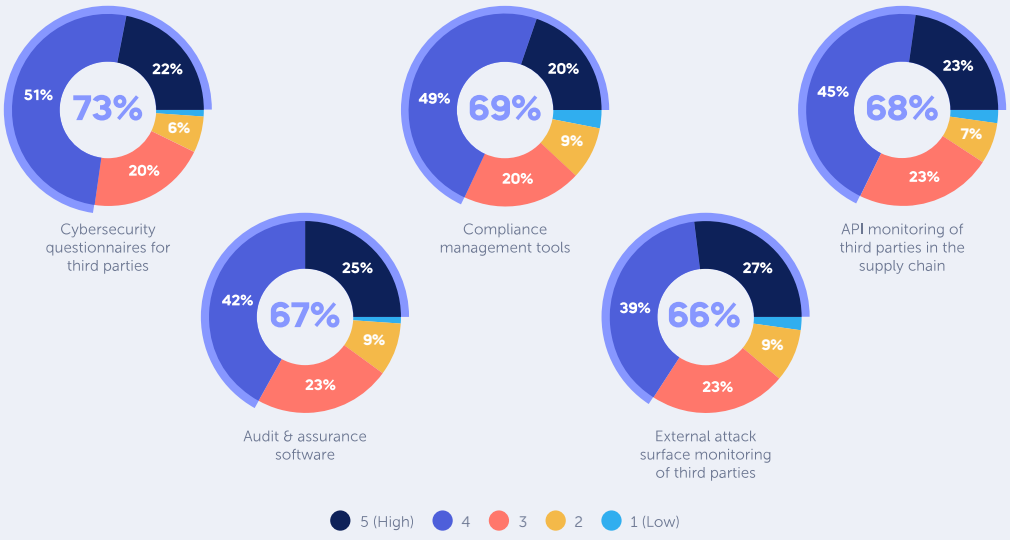

Figure 3: Effectiveness of Tools Reducing Third-Party Cyber Risks

Sue Bergamo
CIO & CISO
BTE Partners

"In 2024, I believe companies will start to pay attention to their 3rd party cyber risk, as all industry indications continue to point to an increase in supply chain attacks. With limited visibility into suppliers and API connections, CISOs need to arm themselves with the necessary tools to defend against cyber criminals."

Which Department Takes Responsibility for Third-Party Cyber Risk Management?

In more than half of cases, (54%) the responsibility for third-party cyber risk management falls under dedicated IT and Risk teams who have specific technology expertise. These include Operations and Logistics teams, Compliance and Privacy, Information Security, Risk Management, and Technology or IT.

In 36% of cases, the Back Office Team is in charge, which includes Legal, Finance and Procurement. This may include tasks like managing cyber questionnaires, onboarding third parties to internal systems, or handling payments.

We also noted that while 10% outsource third-party cyber risk management to external service providers, this is predominantly the case in enterprises with under 5k employees.

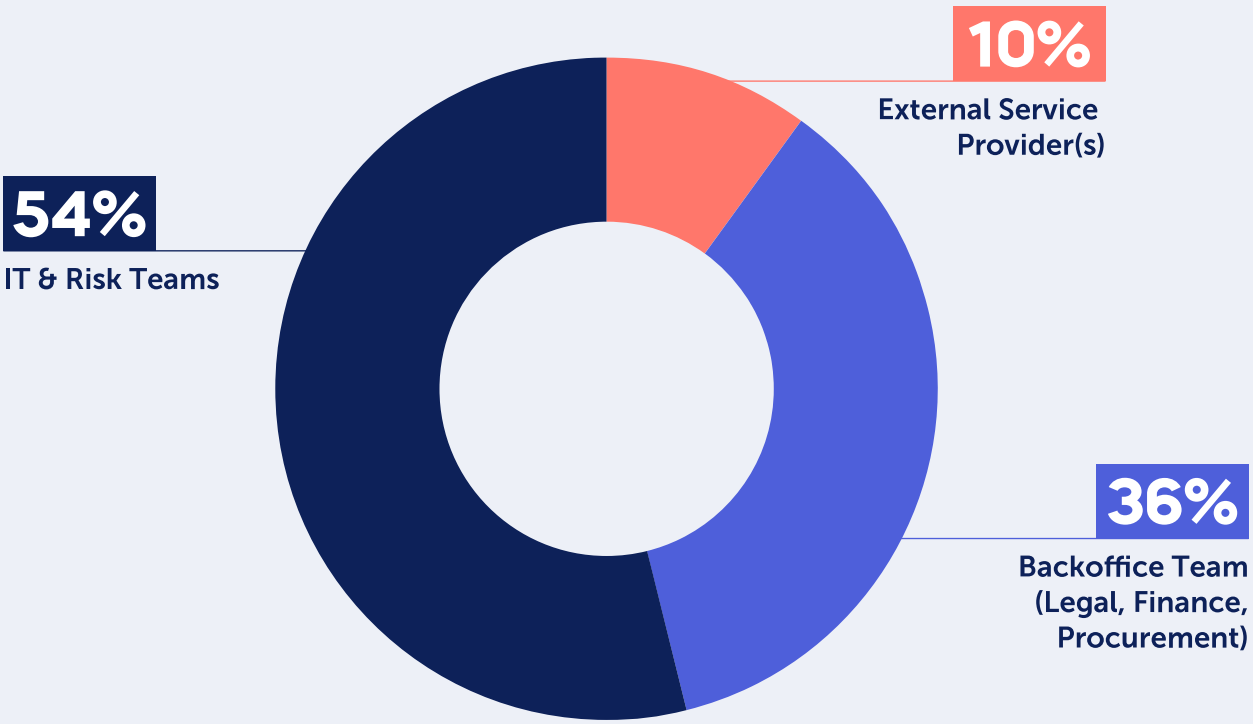

Figure 4: Departments in Charge of Third-Party Cyber Risk Management

What is the Size of the Team Handling Third-Party Cyber Risk Management?

98% of companies have third-party cyber risk management teams of more than three people.

78% have teams of between 6-20 people. In 5% of teams, there are more than 20 members of staff who are responsible for third-party cyber risk management.

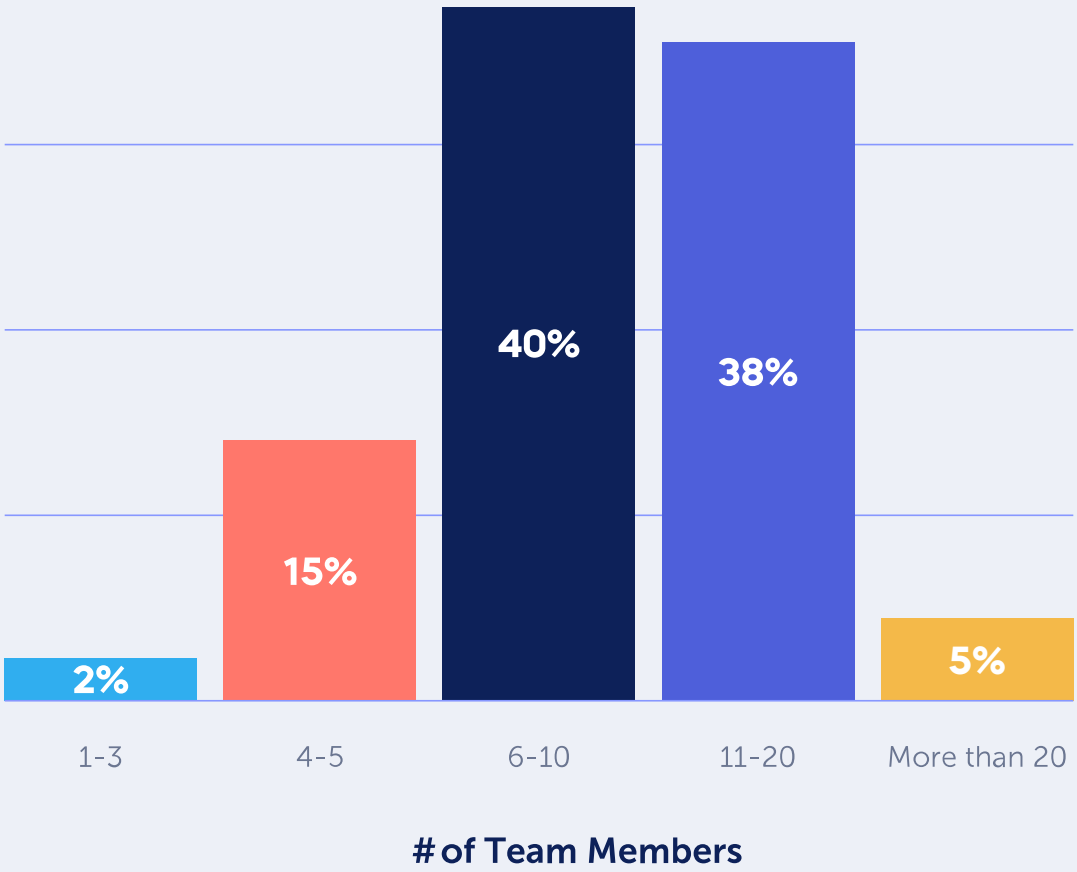

Figure 5: Team Size of Third-Party Cyber Risk Management

How Many Breaches Can Be Prevented Using AI-Driven Solutions?

CISOs are extremely confident that AI can help to prevent third-party data breaches.

61% of CISOs say that AI can prevent between 50-100% of breaches, with an additional 31% reporting AI can protect against at least 10%. Just 2% of CISOs say AI cannot help to prevent breaches from third parties.

CISOs of larger enterprises are far more likely to recognize AI's capabilities in preventing third-party breaches. 43% of CISOs of companies with under 2k employees believe AI can prevent more than half of their breaches, compared with 71% of CISOs in large enterprises, and 60% of CISOs working in very large enterprises.

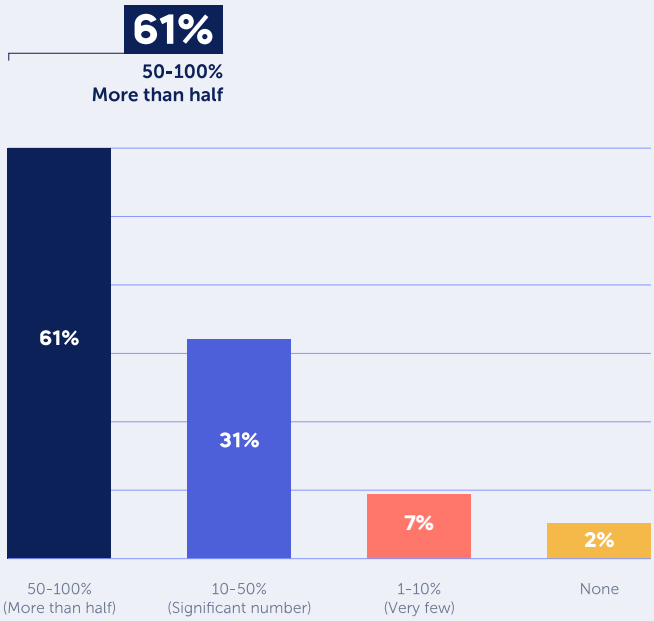

Figure 6: Number of Breaches That Could Be Prevented Using AI-Driven Solutions

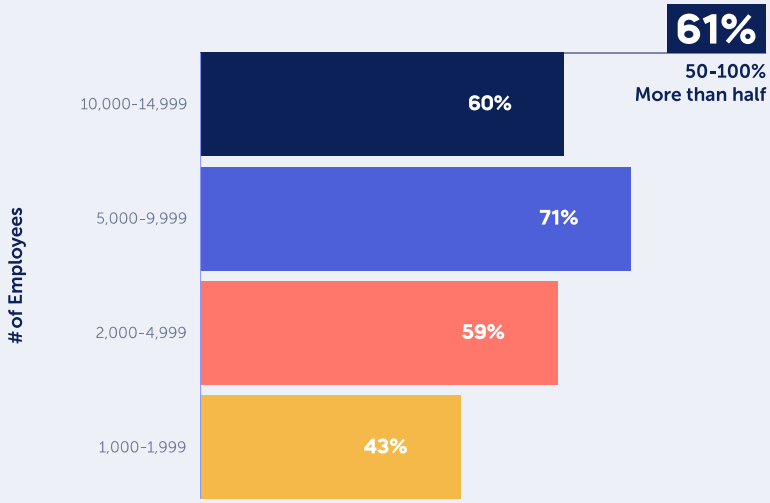

Figure 7: Can Prevent More Than Half of the Breaches (50-100%), by Company Size

What is The Actual Positive Impact of AI-Driven Solutions on Third-Party Security Programs?

We saw in Figure 6 that 60% of CISOs believe AI can be effective in preventing more than half of third-party cyber threats. Now, we turned our attention to how AI can empower TPCRMs.

From the data, we can see that **AI can dramatically improve security by mapping the real-world supply chain accurately to the nth level, and improving asset discovery of third parties** to reduce the number of false positives and false negatives.

There are some notable differences between the impact of AI-driven solutions when we compare CISO responses across various sizes of enterprise.

For example, improving supply chain discovery was chosen as a key capability by 22% of CISOs on average, but 37% of CISOs in medium-sized enterprises. The same jump can be seen for improving asset discovery – chosen by 21% of CISOs altogether, but 33% of those with fewer than 2k employees.

In contrast, AI's ability to automatically map and classify third parties as well as increase the accuracy of assessments and the ability to predict breaches ahead of time are all far less impactful for mid-size enterprises than they are for large and very large enterprises.

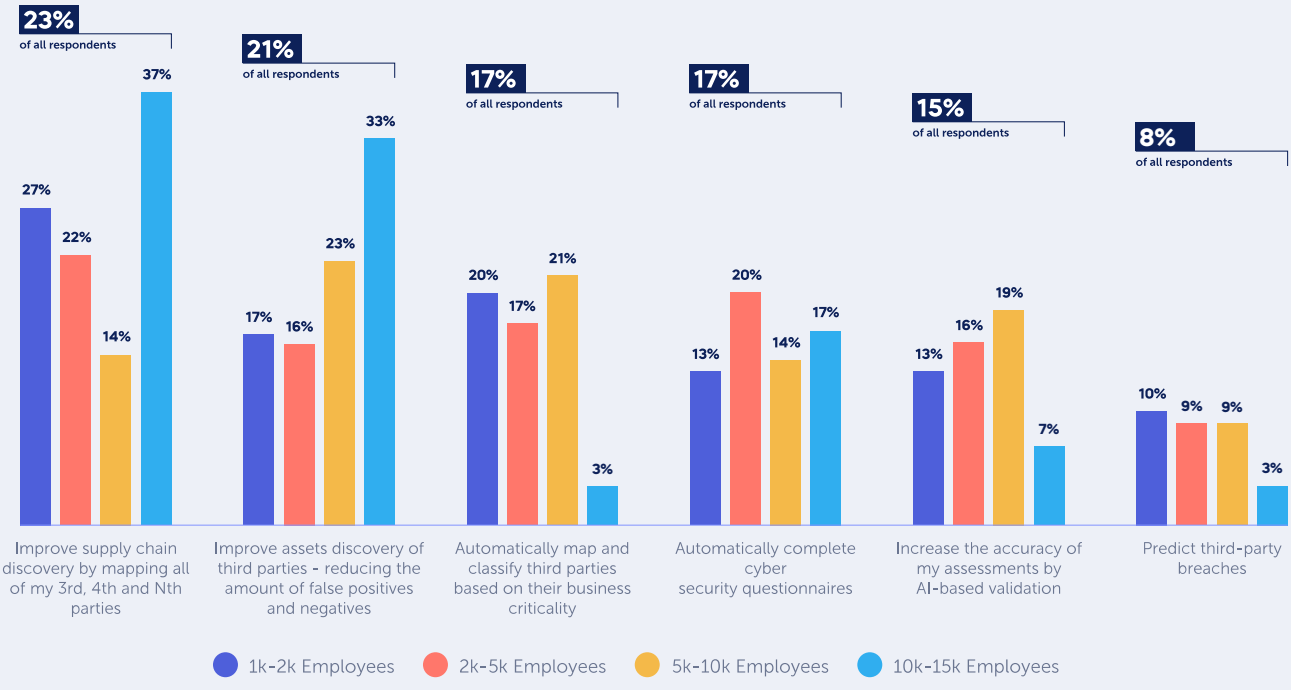

Figure 8: AI-Driven Solutions Impact on Improvement of Third-Party Security Programs

What are the Top Challenges in Third-Party Cyber Risk Management in 2024?

As new waves of regulations arise, for example in regard to AI, it's no surprise that complying with new regulations is a top challenge for 2024, cited by 20% of CISOs.

Other prominent challenges include:

Communicating the business influence of TPRM: 18% of CISOs would like to be able to explain how TPRM positively relates to the business bottom line, in terms of alleviating compliance risk, financial impact and reputational damage.

Resource management: 18% of CISOs feel they need greater resources in place to manage a growing amount of risk in a widening supply chain.

AI: 17% of CISOs recognize that the use of AI in third-party breaches is going to increase in 2024. They would like tools in place to manage this growing threat.

Shadow IT: 15% are worried about Shadow IT, unsanctioned technologies and tools in their business environment, to which they have limited or zero visibility and that could be increasing risk.

Prioritizing risk assessment: 11% of CISOs cite challenges with risk assessment, and would like to receive intelligence that is prioritized based on the level of risk.

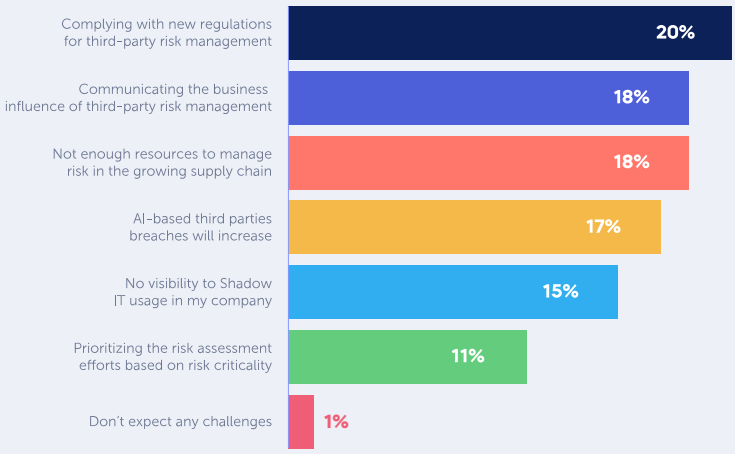

Figure 9: Top Challenges in Third-Party Cyber Risk Management in 2024

David Neuman
Senior Analyst
TAG Cyber LLC

> Looking ahead to 2024, the challenge of managing diverse third-party cyber risks will be met with more sophisticated risk assessment tools and strategies. We expect a rise in sector-specific security frameworks and an increased focus on supply chain transparency. Businesses will likely adopt a more granular approach to risk management, differentiating between critical and non-critical vendors based on the nature and extent of their risk.

Are Enterprises Planning the Implementation of a Third-Party Cyber Risk Management Solution?

Third-party risk management solutions are evolving in line with enterprise maturity.

At the moment, just 2% of companies have implemented a designated tool for third-party cyber risk management. However, as we saw in Figure 3, there is no silver bullet for handling third party risk, and in Figure 1 — 94% of CISOs are worried about this risk.

As a result, we can see here that 92% of enterprises are either in the process of implementing a designated solution for third-party risk or are in the planning stages.

The message is clear: if you're not currently in that 94% — you're falling behind.

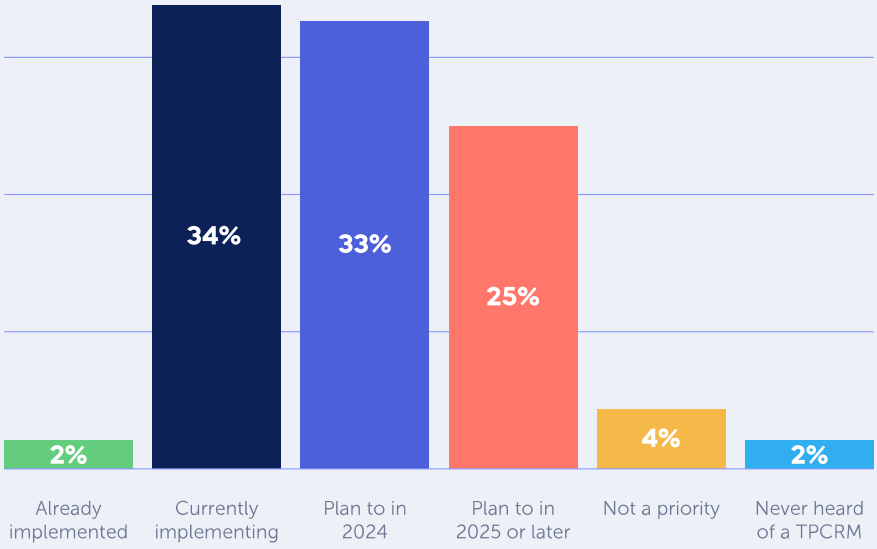

Figure 10: Future Implementation of a Third-Party Cyber Risk Management Solution

Matan Or-El
CEO and Co-Founder
Panorays

"CISOs understand the threat of third-party cybersecurity vulnerabilities, but a gap exists between this awareness and implementing proactive measures. Empowering CISOs to swiftly fortify defenses by analyzing and addressing gaps is crucial in navigating the current cyber landscape. After all, with the speed of AI development, bad actors will continue to leverage this technology to create data breaches, operational disruptions, and more."

How Has Your Budget Changed for Third-Party Cyber Risk Management in 2024?

As third-party cyber risk management becomes a greater priority, and companies move along the maturity model towards implementation of a designated solution, the data confirms there is an increase in budget to meet those requirements.

Despite a challenging macroeconomic environment, just 11% of CISOs have decreased their budget in this area over the past 12 months.

On the other end of the scale, **63% of CISOs report an increase in budget set aside specifically to tackle third-party risk.** Almost a quarter (24%) have increased the money at their disposal by more than 10%.

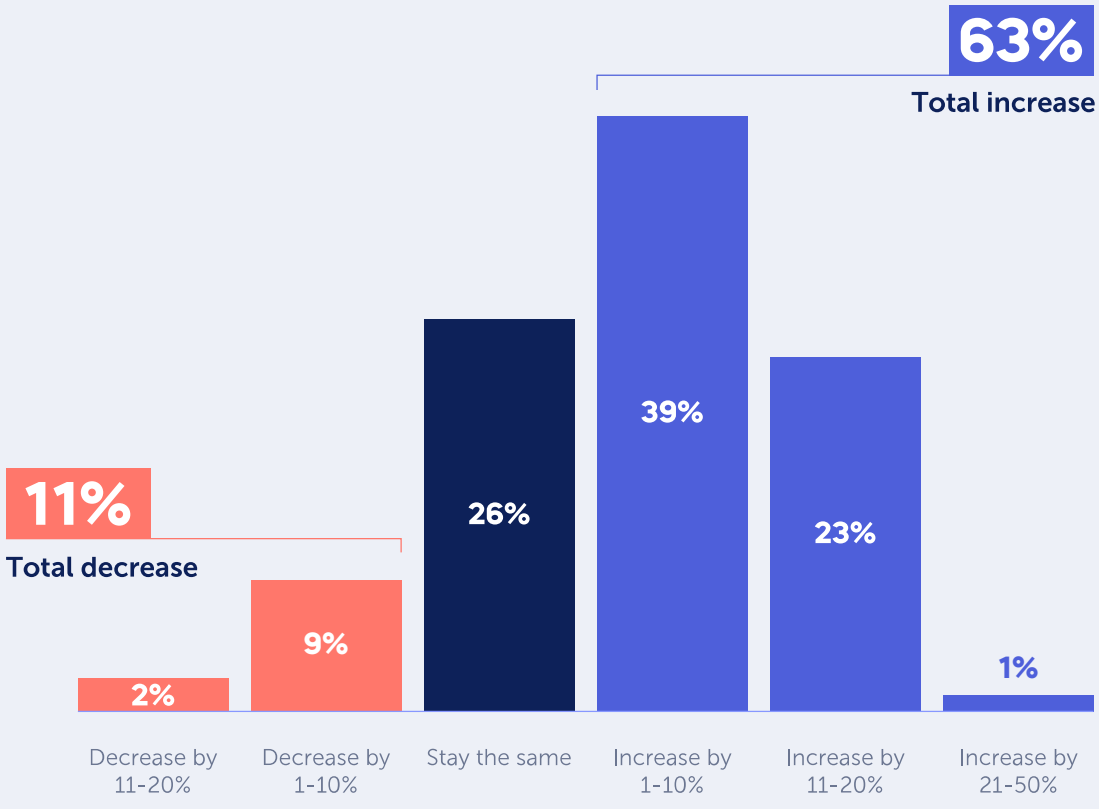

Figure 11: Budget in 2024, Compared to 2023 for Third-Party Cyber Risk Management

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

What Considerations are Important for Choosing a Third-Party Cyber Risk Management Solution?

It's clear that if you're not already implementing a dedicated solution for third-party risk, it's time to get started. With that in mind, it's interesting to see what considerations are very important for CISOs when they are choosing the right technology.

44% call out risk quantification which quantifies third-party cyber risk exposure in dollar values. The ability to quantify risk gives visibility and communicates cyber risk as business risk.

Other important features that CISOs are looking for are actionable remediation tips (40%), threat intelligence (39%), and integration to other systems (38%). However, all the features on the list, including real-time alerts, assessing risk based on risk pillars, reporting business influence, automation, and continuous monitoring are all rated very important or important for more than 70% of CISOs.

CISOs aren't looking to compromise on keeping their business safe. They demand a tool that encompasses all the capabilities on their wish list.

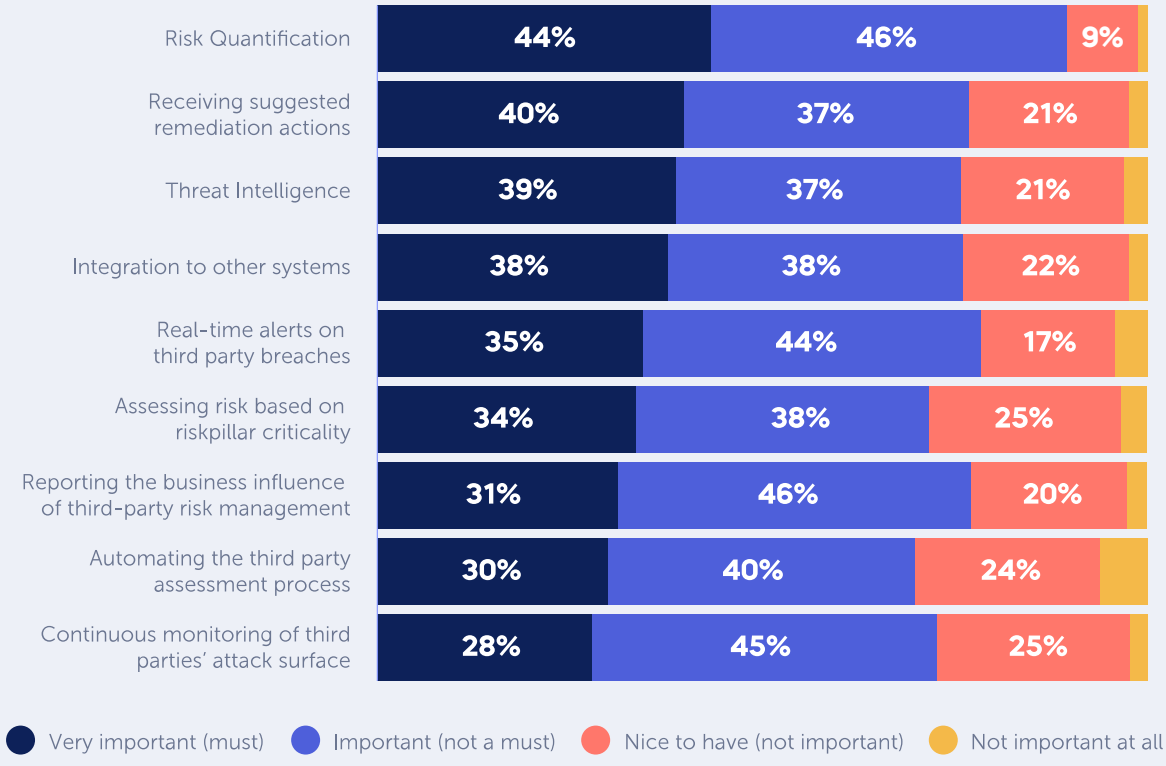

Figure 12: Importance of Considerations for Choosing a Third-Party Cyber Risk Management Solution

Demographics

Panorays

Industry and Company Size

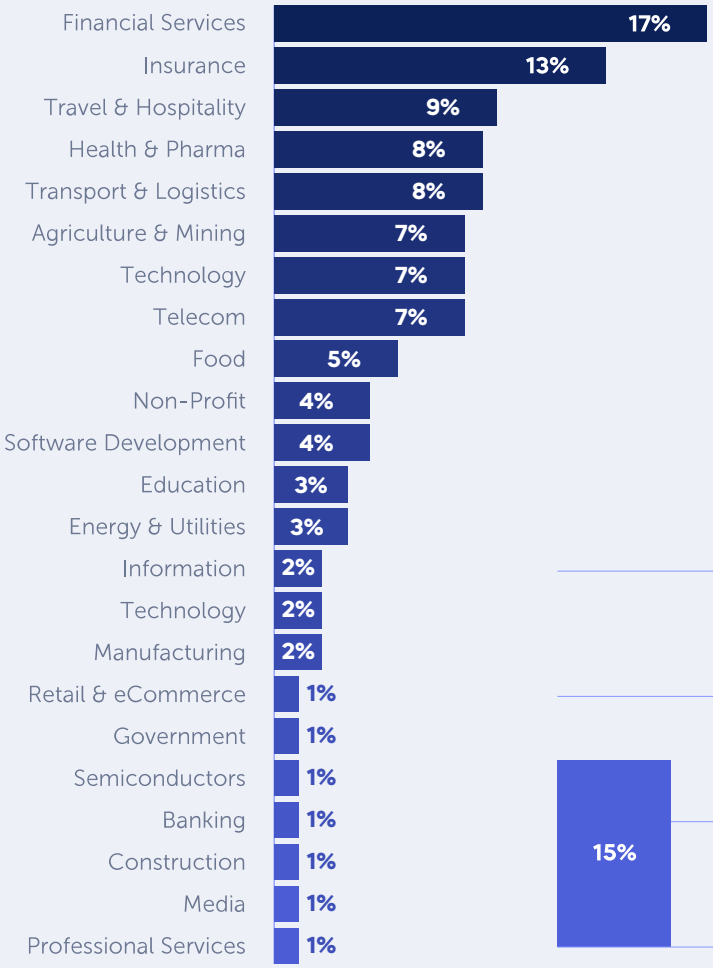

Figure 13: Industry

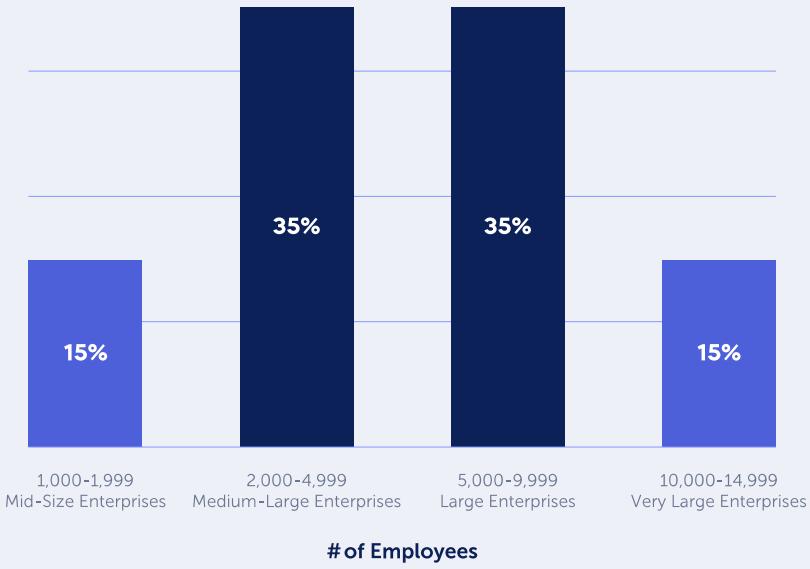

Figure 14: Company Size

Panorays

About Panorays

Panorays offers a comprehensive solution for your organization's third-party cyber risk management with a fast, easy, and secure way to discover, manage and maintain third to nth parties within your digital supply chain. Coupled with continuous monitoring and threat intelligence, Panorays gives you the tools to understand suppliers' risk profiles and stay ahead of any emerging threats.

Request a Demo

For more information, please visit us:

Email: info@panorays.com

Copyright © 2024, Panorays. All rights reserved.