Tenchi Security

Executive Report

TENCHI

THIRD-PARTY CYBER RISK MANAGEMENT

Third-Party Cyber Risk Management in Brazil

2nd Edition - 2025

1. Executive Summary

Multiple surveys and a wealth of data have highlighted the relevance of third-party cyber risk. One example of this is found in Verizon's 2025 Data Breach Investigations Report (DBIR): The proportion of breaches that could be attributed to "supply chain interconnections" have reached 30%, doubling in the last period studied by Verizon and reinforcing the trend from the previous year, when the increase had reached 68%.

In addition to quantity, the severity of third-party-related incidents is unequivocal. When including reports of leaks and intrusions into the systems of companies that operate as B2B service providers or which provide critical infrastructure, we noted that 1.3 billion personal data records were exposed over the course of the year 2024.

While this scenario deserves attention, **82%** of our survey participants **stated that they feel that there is a lack of materials and training** that focus on managing and mitigating the risks associated with third-party technology assets. This also applies to materials and training on the relationship between contracting and contracted companies.

Tenchi's **Third-Party Cyber Risk Management Survey** aims to provide visibility into the daily work of professionals responsible for Third-Party Cyber Risk Management (TPCRM) programs and their operation, which represent businesses' efforts to manage third-party cyber risk.
Our focus lies on Brazil, where this information is particularly scarce – and it is this gap that we seek to fill. What we see in the survey is that many still rely on practices and routines that are designed for a simpler, more modern environment. Surveys and certifications made more sense when there was no shared or interconnected cloud infrastructure. Nor were there the numerous consequences – many of them positive – that resulted from the standardization of software and solutions, such as Single Sign-On (SSO) and interfaces for communication between systems (APIs).

A noteworthy fact is that one of the most interesting findings of the survey is that many professionals (87%) acknowledge the need to monitor third-party cloud environments, although most of them (55%) are unable to do so. This is quite understandable, as the traditional methods used to assess third-party risk were not designed for the cloud.

We also see, however, that a large number of companies are already investing in automated assessment methodologies with continuous monitoring. Although these measures are often applied exclusively to critical third parties, this highlights the demand for innovation, particularly when it comes to protecting what matters most to the business.

Our first survey was conducted in 2023. When we repeated the survey in 2024, we felt that this work deserved a report with a more in-depth analysis of the data, highlighting the most interesting observations found. We hope that all cybersecurity professionals can see themselves reflected in this survey and learn more from what others have already achieved in their third-party risk management programs.

Summary

2.Insights ↓

79%

of companies with up to 5,000 employees have a TPCRM program in place

2.1 Who has a TPCRM program in Brazil?

The Third-Party Cyber Risk Management (TPCRM) program is the key pillar of third-party cyber risk management. Without a TPCRM program, this risk tends to be completely ignored, leaving the business exposed and without visibility into events that may cause operational, financial, and reputational damage.

Within the TPCRM program, companies use a number of methods to assess the information security posture of third parties to hire more capable and secure suppliers or coordinate the handling of incidents and vulnerabilities.

Among companies with up to 5,000 employees, 21% stated that they still do not have a structured TPCRM program. This rate drops to 5% among companies with more than 5,000 employees.

2.2 Who manages TPCRM programs in companies?

When a company structures its TPCRM program, it needs to decide who will be in charge of it. In our survey, 70% of respondents reported that their companies assigned the Information Security department to lead the program, while **20% stated that their Risk Management team was responsible.** The remaining respondents cited other departments, most notably the Privacy team (6%).

While it is easy to associate the relationship between third-party cyber risk and corporate information security, business partners can be linked to a wide range of company processes. A cyber incident at a third party can significantly impact the business without having a direct effect on the IT infrastructure or assets that are directly subordinated to the information security department. Third-party cyber risk management tends to be more efficient when the team in charge has the necessary skills to understand the relationship between these risks and the responsibilities to engage in risk mitigation.

70%

of TPCRM programs are managed by the information security team

1 in 5 companies have+3,000 third parties

- **In companies with over 3,000 third parties, 58% have more than 500 that are considered critical.**
- In companies with up to 1,000 employees, 34% have 11 to 50 critical third parties.
- In companies with between 1,000 and 5,000 employees, 36% have at least 50 critical third parties.

2.3 How many third-parties do Brazilian companies have?

Among the survey participants, more than half (54%) of the companies had at least 500 third-party contractors. In addition to a significant number of third-party contractors, many of them are also considered business-critical.

This data demonstrates a reality in which organizations build an ecosystem together with their service providers, suppliers and partners.

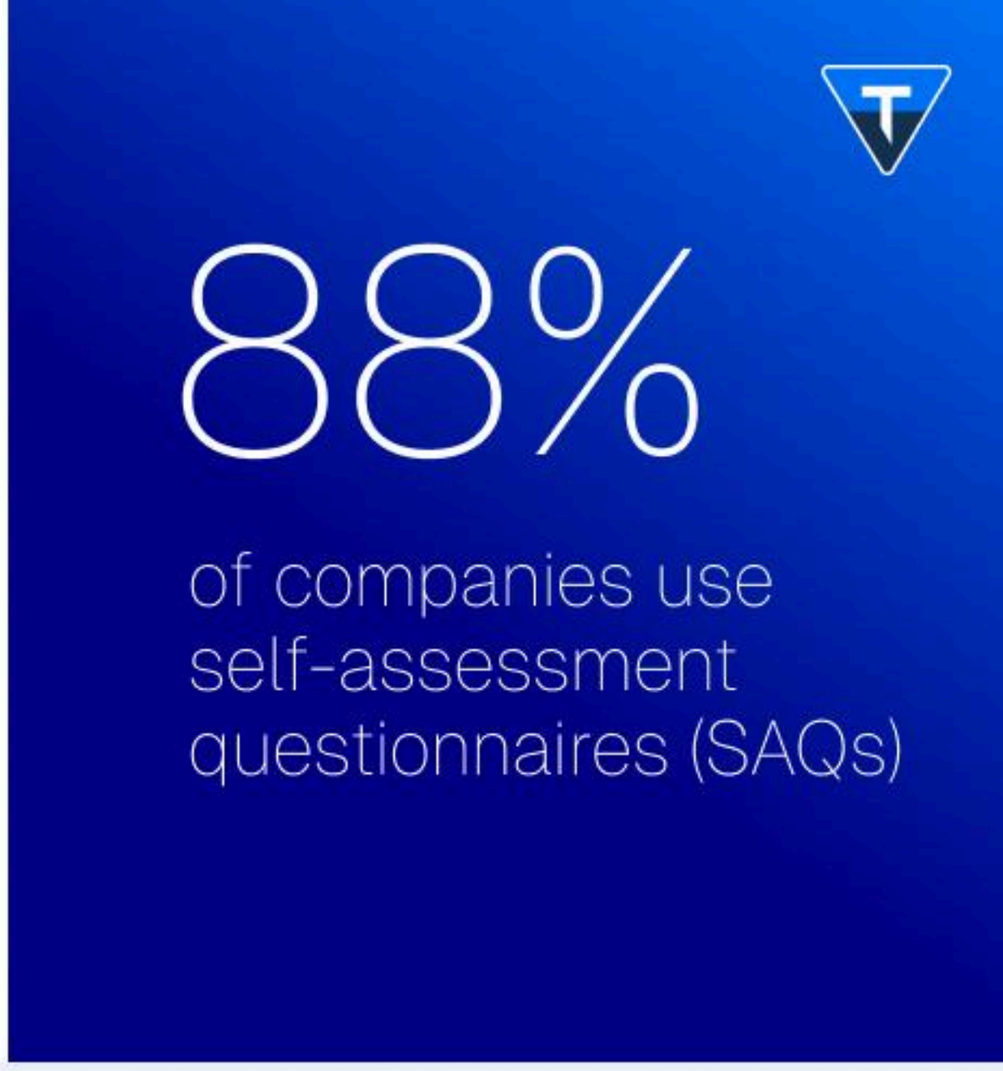
When we talk about digital systems, interconnection is the rule. Thus, the attack surface of all these companies is often interconnected, meaning that a cyber incident at any contracted supplier can trigger a domino effect across this entire digital ecosystem.

2.4 What is the most popular method for third-party assessment?

There are various ways to assess third-party information security postures and managing cyber risk, although the most widely used are still self-assessment questionnaires (SAQs). In our survey, 88% of respondents claimed that their companies use this method.

These questionnaires rely on the supplier's good faith and, therefore, are based more on compliance principles than on practical information security concepts.

While well-intentioned, questionnaires rarely provide an accurate picture of a supplier's security posture. Moreover, they remain frozen in time for a long period (71% of companies only administer questionnaires once a year at most). Because vulnerabilities can emerge at any time, questionnaires tend to quickly become obsolete, even when all responses are accurate and detailed.



2.5 The use of continuous monitoring continues to grow

Along with audits and intrusion tests, continuous monitoring is one of the tools available to improve the visibility of the TPCRM program, with more realistic indicators of the third-party security posture.

Monitoring can be as follows:
Outside-in: It views the third party "from the outside," typically using standardized security tests, often with extremely limited coverage of the third-party's critical infrastructure and security controls;
Inside-out: It views the third party "from the inside," utilizing the existing relationship between a contractor and its supplier to ensure more accurate and comprehensive data collection, including the ability to assess security controls and the cloud environment.

60% of companies reported using some form of continuous monitoring. Monitoring, which must be automated to be continuous, tends to gather information in a quick and easy manner. Additionally, it is not limited to specific occasions, such as contracting and renewal.

2.6 Inside-out monitoring protects what matters mos

Our research found that inside-out monitoring, when adopted by a company, is often used to manage third parties deemed most relevant to the business.

By providing greater visibility into supplier security, inside-out monitoring tends to bring a business closer to its suppliers, creating opportunities for jointly addressing vulnerabilities. Thanks to its continuous approach, this monitoring operates as a regular check-up on supplier security.

The only assessment method used in a similar way is audits performed directly by employees of the contracting company. There is, however, a difference: While these audits are performed at most once a year in 75% of companies, monitoring can occur on a daily basis, depending on the chosen solution.

2.7 What matters most for third-party cyber risk management

"Continuously monitoring cyber risks to identify threats as close to real-time as possible" was the most frequently cited element by respondents when asked what is necessary for effective third-party cyber risk management.
Only continuous monitoring can provide this visibility. Other methods fail to identify vulnerabilities or cannot do so in real time. Penetration tests, for example, are able to identify vulnerabilities, but it is impractical to conduct them regularly for these discoveries to occur in real time.

The least frequently cited element was trust in reports and certifications issued by third parties (17%), which shows that professionals prefer assessments that companies may link to their business routine.

85%

Of professionals also note that rapid threat identification is crucial for third-party cyber risk management.

87%

of professionals highlight the importance of cloud infrastructure monitoring

2.8 Visibility into cloud infrastructure is still a challenge

Cloud infrastructure was the most frequently cited aspect among respondents when asked which third-party infrastructures are most relevant for monitoring risks associated with them. 55% of respondents claim that their companies lack visibility into third-party cloud environments. This rate, however, is reversed in the financial sector, where 56% claim that they do have visibility into third-party clouds. It is often in the cloud environment that third-parties connect directly to the contracting party's infrastructure, whether to share data or to provide SaaS (software as a service) services.

Although professionals acknowledge the risks involved in the cloud, many risk assessment methods (such as questionnaires and certifications) fail to provide a clear overview of third-party practices in this environment.

35%

of companies already manage all third parties in their TPCRM programs

2.9 More companies manage all third parties

As our survey is now in its second edition, some numbers also stood out for having changed from one year to the next. One of the notable changes is the percentage of companies that manage all third parties. **In 2023, 30% of companies managed all third parties. In 2024, this figure rose to 35%. In the financial sector, the number is even higher: 42%.**

Most companies (64%) still choose to focus risk management on third parties that are considered critical or relevant to the business. This approach, however, limits the company's visibility into other third parties. There is also a risk that a relevant third party may not have been rated as such, leaving it out of the risk management effort. The adoption of highly automated assessment methods, such as continuous monitoring, may facilitate the expansion of the cyber risk management program to reach as many third parties as possible.

2.10 Professionals lack training and information on TPCRM

Our survey was conducted at an event dedicated to third-party cyber risk management. Despite that, 82% of respondents report a lack of training programs focusing on TPCRM.

The expansion of organizations' digital ecosystems has created challenges for third-party cyber risk management. Nevertheless, contractors' responsibilities have been increasing across several countries, both due to consumer demands and the adoption of regulations that hold them accountable for the protection of personal data or the quality of services.

The expansion of digital ecosystems is creating new challenges for third-party cyber risk management. At the same time, contracting organizations face growing responsibilities, driven both by consumer demands and by regulations that hold them accountable for personal data protection and service quality. We are in a period of transition: there is no set formula for structuring TPCRM teams. It is therefore essential to consider how to strengthen third-party cyber risk management programs and adopt methodologies that truly capture the most relevant risks.

82%

of professionals feel that there is a lack of TPCRM training programs

3.Data and analysis ↓

In this chapter, we will take a closer look at the data from the Third-Party Cyber Risk Management survey, highlighting the following questions:

- Which companies have TPCRM programs and how they are organized;
- How third parties expand the attack surface;
- How companies assess third-party security;
- The relevance of cloud risks;
- Security and incident policy;
- Perspectives on TPCRM as governance or security.

3.1 Understanding TPCRM

TPCRM stands for Third-Party Cyber Risk Management. It is a set of measures and technologies that are integrated with other risk management processes so that an organization can gain visibility into cyber risks linked to third parties, including suppliers, business partners, and service providers.

TPCRM can also be described as a derivative of TPRM (Third-Party Risk Management) that focuses on cyber risks.

It is important to consider, however, that cyber risks are often inseparable from operational, financial, and regulatory risks. In the current scenario, a company's technology assets are almost always essential for work to be performed or, at the very least, for achieving the productivity required by the market.

Creating a TPCRM program within an organization is the first step in recognizing the relevance of cyber risks linked to suppliers and partners. This initiative should establish mechanisms to map the third parties on which the company relies and the risks they pose to the business.

The data and insights gathered by the TPCRM program enable companies to justify switching suppliers to more reliable ones, mitigate risks, or even collaborate with their partners to improve the resilience of the services provided. The absence of a TPCRM program exposes companies to operational failures and financial losses resulting from third-party failures, as contractual obligations are insufficient to guarantee compensation for losses resulting from these events.

3.2 Companies with TPCRM programs

TPCRM in Companies

Among the companies analyzed in our research, we found that:

87%

of all companies have a TPCRM program

In companies with up to 5,000 employees, this rate drops to

↓ **79%**

In companies with more than 5,000 employees, the rate rises to

↑ **95%**

39%

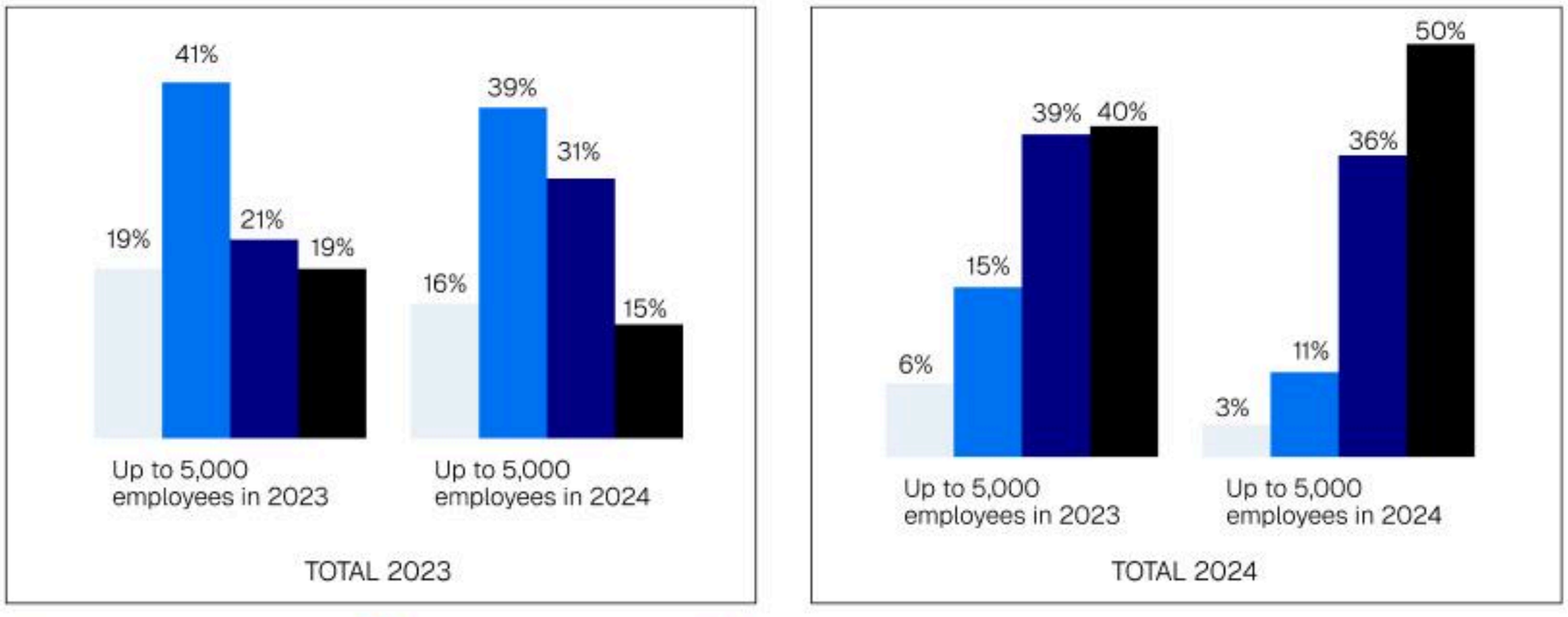
Of companies surveyed indicate that they have a dedicated budget allocated to their TPCRM program.

These figures indicate that smaller companies are struggling to create a TPCRM program. While it's possible to speculate that these companies simply have not yet recognized the cyber risk involving third parties, it is a fact that some smaller companies have a greater appetite for risk in general, prioritizing growth and competitiveness.

Conversely, delaying the creation of a TPCRM program can be costly and even derail a company's business, particularly if it is already using third parties to accelerate its scale.

It should be noted that companies that have a TPCRM program may still be exposed to unmanaged risks by contracting with suppliers who do not have a robust TPCRM program or plan to create one in the near future.

How long Companies have had a TPCRM program for:



3.3 The area responsible for the TPCRM program

In companies that have a TPCRM program, it is most common for the Information Security team to be in charge.

70% information security;

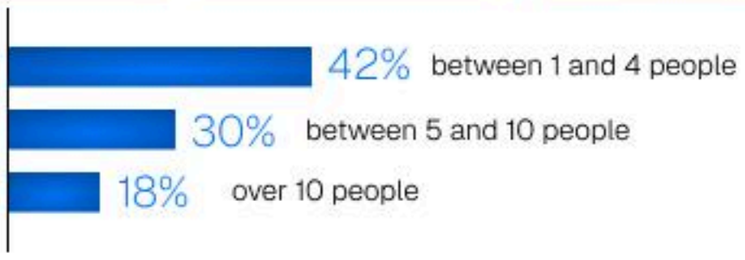
20% risk management;

6% privacy

4% others;

51% of companies have an internal team to take care of the program

Team sizes allocated to the TPCRM program



Since TPCRM is a derivative of third-party cyber risk management, it is understandable that many companies leave the risk management department to handle all aspects of third-party risk. Nevertheless, it is crucial to pay attention to the specificities of cyber risk, particularly regarding the need for incident response and the speed of threats.

It is also understandable that Brazilian companies choose to leave the privacy department in charge of the TPCRM program. For most companies, the Brazilian General Personal Data Protection Act (Lei Geral de Proteção de Dados Pessoais – LGPD) was the first major Brazilian regulation to detail the duties of third-parties (in the role of "operators") and the first or contracting parties (in the role of "controllers").

Conversely, a number of rules related to third-party contracting are already in effect worldwide, particularly in the financial sector. In Europe, the Digital Operational Resilience Act (DORA) came into effect in January 2025, with even stricter and more specific rules for information and communications technology (ICT) service providers.

3.4 Third-party incidents

Third-party cyber incidents pose a complex challenge.

One factor is that these incidents can quickly spread to multiple companies using the same supplier. One prime example were the ransomware attacks involving the file-sharing service MOVEit Transfer, which impacted more than 2,500 organizations in 2023. Companies that failed to use the service were also harmed when their suppliers discovered they had been attacked.

Another factor is visibility. In the event that the contracting company lacks visibility into the third party, it is impossible to know whether that third party has mechanisms to detect access breaches. Moreover, the third party may choose not to report an incident, either because it considers it unimportant or because of fear of reprisal. In the case of MOVEit Transfer, some victims only discovered their data had been stolen when their data was exposed online more than a year after the breaches.

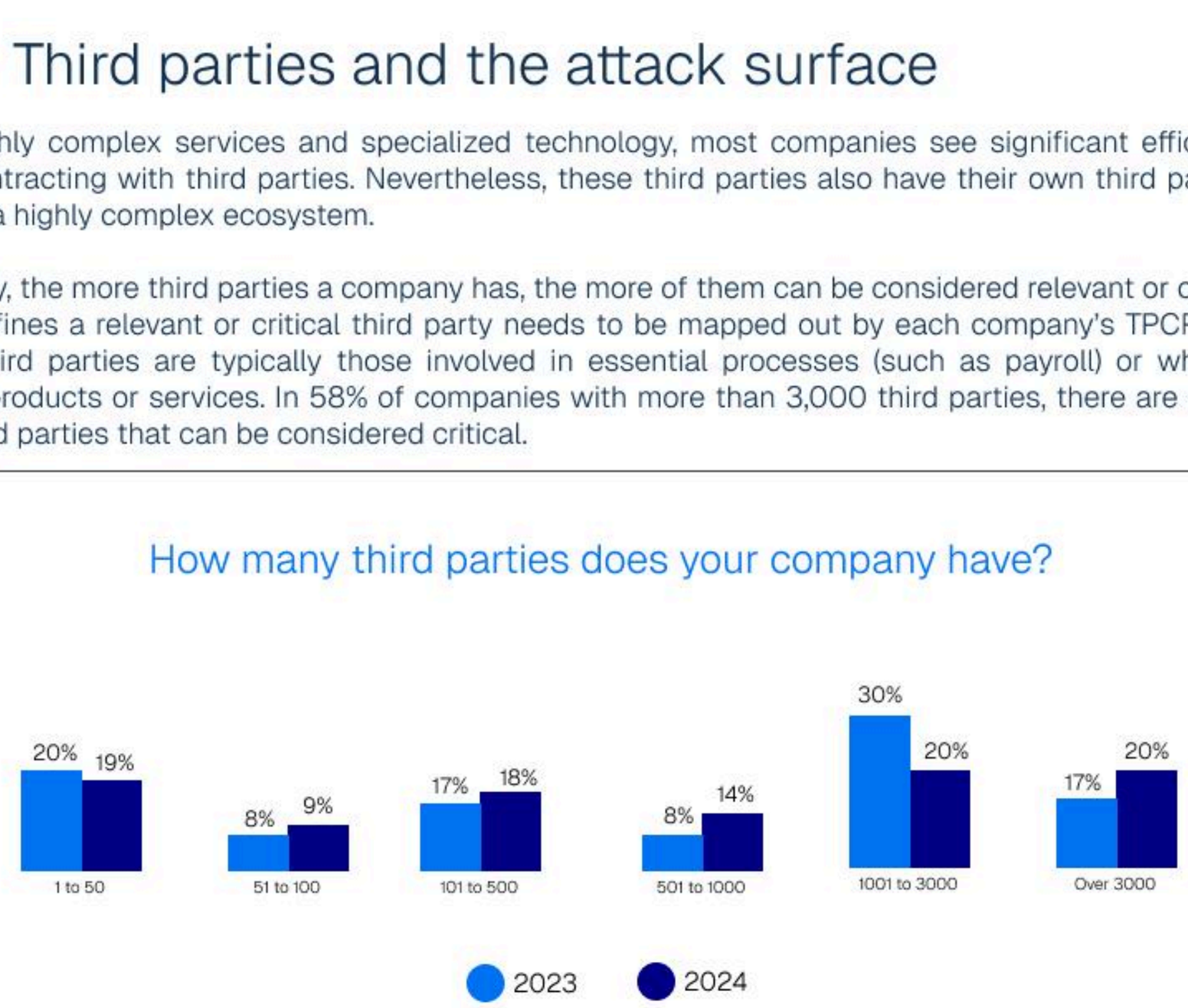
Finally, the third party may be responsible for critical operations and unable to compensate the contractor for all damages. In early 2025, Safe{Wallet}, which provides services to companies in the cryptocurrency sector, was compromised by attackers who used this access to siphon $1.5 billion from Bybit, one of its clients.

3.5 Third parties and the attack surface

With highly complex services and specialized technology, most companies see significant efficiency gains from contracting with third parties. Nevertheless, these third parties also have their own third parties, which creates a highly complex ecosystem.

Generally, the more third parties a company has, the more of them can be considered relevant or critical. While what defines a relevant or critical third party needs to be mapped out by each company's TPCRM program, these third parties are typically those involved in essential processes (such as payroll) or which support certain products or services. In 58% of companies with more than 3,000 third parties, there are also at least 500 third parties that can be considered critical.

How many third parties does your company have?

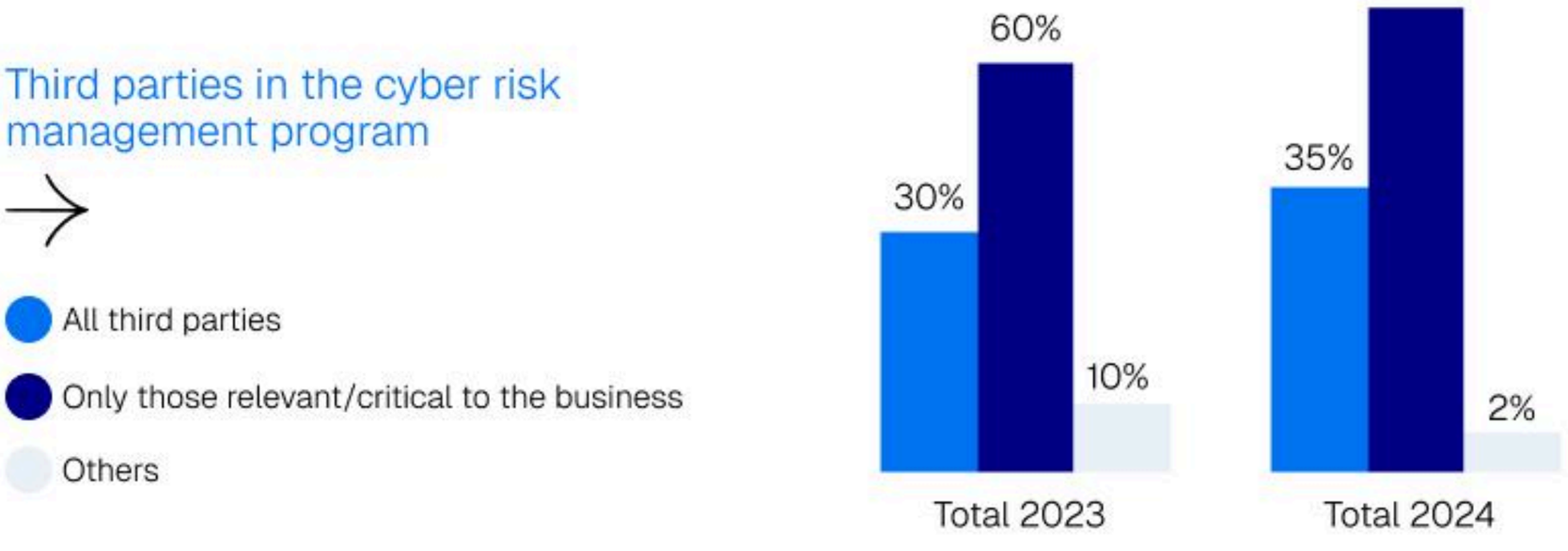


In 58% of companies with more than 3,000 third parties, there are also at least 500 third parties that can be considered critical.

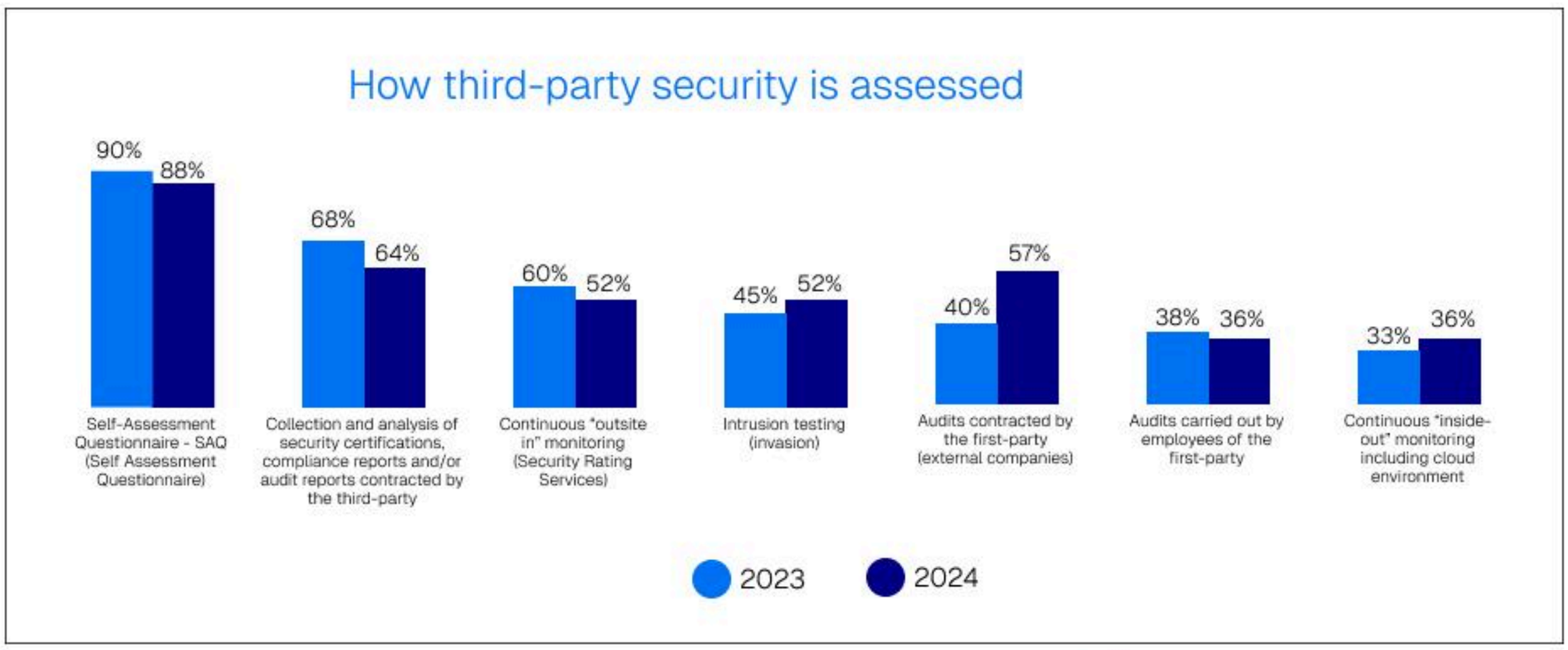
Relevant Third Parties	Total number of third parties					
	1 a 100	51 a 100	101 a 500	501 a 1.000	1.001 a 3.000	+ de 3.000
1 to 100	72%	23%	4%	11%		
11 to 50	28%	69%	54%	33%		
51 to 100		8%	25%	39%	8%	
100 to 250			13%	11%	19%	19%
251 to 500			4%		19%	19%
Over 500				6%	31%	58%

Given the number of third parties, many companies choose not to manage all of them. Nevertheless, our survey found a slight increase in this number: In 2024, 35% of respondents stated that their company manages all third parties. In 2023, this figure was 30%.

Third parties in the cyber risk management program



3.6 How third-party security is assessed



The most widely used method by companies to assess third parties is the Self-Assessment Questionnaire (SAQ), followed by the collection and analysis of security certifications and compliance and audit reports.

Companies' preference for these methods can be explained by the history of TPCRM, which originated as a governance and compliance process. For this reason, it is natural for companies to prioritize documenting third parties and their processes through these mechanisms.

These methods are expected to lose relevance in the coming years, in particular given the regulations that will limit the transfer of responsibility from the contractor to the third party and the perception that cyber threats and events may directly impact company operations, even when the contract holds the third party responsible.

3.7 The main third-party assessment methods

Self-Assessment Questionnaires (SAQs) : This questionnaire can contain hundreds of questions, asking the third party to provide clarification regarding their

Certification and report analysis collection : The contracting company requests that the third party demonstrate information security certifications. ISO certifications (68%) are the most widely requested, especially ISO 27001. Another certification mentioned by various participants was SOC 2 (30%).

Outside-In Monitoring : Outside-in monitoring is performed automatically using tests and information exposed online, whether directly linked to the third party's infrastructure or other risk factors.

Inside-Out Monitoring : Inside-out monitoring utilizes the existing link between organizations to perform an in-depth security check, auditing specific controls that are not covered by other detection methods.

Penetration Testing: In penetration testing, a team specializing in simulating cyberattacks attempts to find a way to attack the company to validate the effectiveness of its security measures.

Auditing : Auditing is similar to a self-assessment questionnaire, but the answers must be documented and justified. Audits can be conducted by a company contracted for this purpose or by the contracting company's employees, but they tend to be laborious.

"Snapshot" or "Video" approach

Many security assessment methods provide only a snapshot of a company ar a given moment - a "frozen" view that may not be updated for months or even over a year.

In contrast, continuous monitoring acts like a "video", tracking the company's security posture over time. This approach offers deeper visibility into the third party's daily operations, providing a more accurate understanding of how security issues are detected and how long they take to be resolved.

3.8 Cloud visibility and risks

A total of 87% of respondents agreed that monitoring the cloud environment is one of the most important ways to track potential risks. Nevertheless, 55% note that they lack visibility into third-party cloud environments.

Given these numbers, we understand **there is a discrepancy between what companies would like to monitor and what is currently being monitored by their TPCRM programs.**

The most relevant infrastructures for monitoring	
Cloud infrastructure	87%
On-premises infrastructure	66%
User Endpoint	51%
SaaS Solutions	70%
Attack Surface Management	61%

55% of those interviewed say they have no visibility into third-party cloud

36% of the companies that monitor third-party cloud do so daily

Many companies that already have adequate visibility into their cloud environments are also able to monitor them frequently: **36%** do so on a daily basis, and more than half **(56%)** do so at least on a monthly basis.

The methods used to evaluate third-party vendors can help explain this difference between companies. Permanent and effective monitoring of the cloud environment requires a continuous inside-out monitoring solution.

Assessment questionnaires and certifications fail to provide visibility into the cloud. An audit is able to document the cloud environment, particularly if the auditor is given the appropriate permissions for this task. Frequent manual audits, however, can be impractical.
Visibility into the infrastructure carried out “from the inside” is the defining characteristic of the inside-out method.

In a sense, this is a missed opportunity for those who do not yet perform this type of monitoring. The cloud opens up many possibilities for sharing information and security and audit policies with mechanisms that are offered by the largest cloud infrastructure providers (Amazon for AWS, Google for GCP, and Microsoft for Azure).

In this sense, the lack of visibility into the cloud cannot be explained by a supposed lack of resources. A change in approach could easily close this gap and provide the desired visibility into third-party cloud environments.

3.9 Security policies and incidents

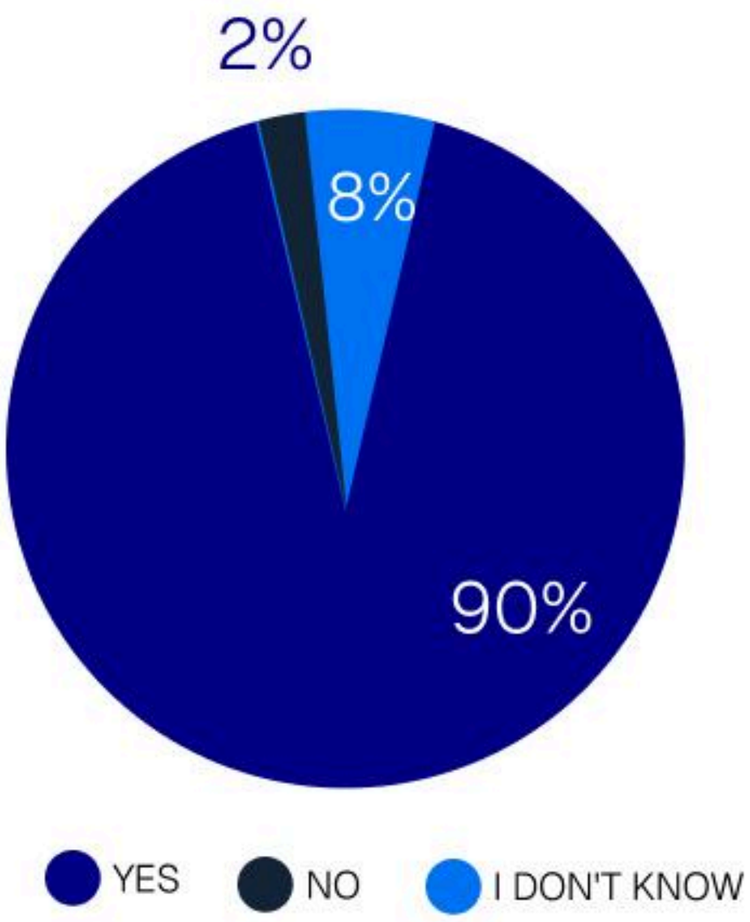
While details may vary from company to company, hiring a third party to provide technology services almost inevitably results in an expansion of the organization’s attack surface. That is because incidents with the third party can translate into impacts for the contracting party.

In some companies that participated in our survey, incidents involving third parties already account for more than half of the incidents experienced.

Even so, some companies may still face difficulties knowing when an impact can be attributed to a third party – either due to a lack of coordination in incident response or the absence of effective mechanisms to detect suspicious activity.

- **Among companies that have experienced a security incident, 1 out of 5 companies states that at least half of the incidents were caused by a third party.**
- **Only 14% of companies that have experienced an incident state that none of the incidents involved a third party.**

Does your company have a security incident policy shared with third parties?



Most companies share an incident response policy with third parties, including instructing them to report incidents that occur in their environments.

This is a sensible measure, although it relies on the third party's good faith to comply with this requirement. Even considering these caveats, there is still a group of companies (8%) that do not make this attempt to coordinate incident response.

3.10 The balance between governance and security in TPCRM

9 out of 10 companies have contractual clauses that hold third parties accountable;

6 out of 10 companies offer security guidance to third parties;

Half of these companies only offer this guidance at most once a year.

Many organizations assume that third parties are solely responsible for their own security. In this regard, the Tenchi Third-Party Cyber Risk Management Survey found that more companies hold third parties accountable for failures than offer security guidance to them.

When third-party cybersecurity posture is evaluated solely as a legal or compliance issue, it is natural to favor processes that document the guarantees offered by the third party itself. We believe this explains why so many companies continue to opt for questionnaires and certifications.

Nevertheless, it is prudent to acknowledge that third parties are linked to the company's ecosystem, which creates risks that did not previously exist. The damage resulting from negligence or a breach in the security of technology assets should not be limited to the third party, particularly if initial access allows the attacker to exploit other vulnerabilities.
A real-life case that illustrates this risk took place in November 2013, when U.S.-based retailer Target had its corporate network accessed by attackers who stole credentials from a HVAC service provider.

The third-party's credentials were used to steal data from millions of Target customers' credit and debit cards – which was unrelated to the nature of the contract. This was possible because any connection opens an opportunity for an attacker to attempt lateral movement to reach initially inaccessible assets.

From this perspective, it is appropriate for the TPCRM program to help improve security controls related to assets that need to be shared or connected with the third party. More than that, the third party can also benefit from this process, considering that switching suppliers can be much more costly or even detrimental to business efficiency.
The greater the frequency and effectiveness of this collaboration, the greater the potential for real results in improving daily information security practices.

4.Our Research ↓

4.1 Learn more about our research

The 2nd Third-Party Cyber Risk Management Survey was conducted on November 6, 2024, by Interação, a company specializing in market and opinion research, coordinated by Tenchi Security. Participants were interviewed in person by interviewers during the Tenchi Conference – our event focusing on third-party cyber risk management.

The survey was structured with approximately 40 distinct questions.

We designed this survey to better understand how Brazilian companies are addressing cyber risk arising from their commercial and operational relationships with partners, suppliers, service providers, and any other companies or entities on which the company depends in some way.

Compared to the first edition of the survey, the 2nd edition had a significantly larger sample. Furthermore, respondents are distributed across more sectors – in 2023, 59% of the professionals interviewed were in the financial sector.

4.2 Research purpose

To explore how large organizations are addressing third-party cyber risk management in Brazil and what the main challenges and opportunities are.

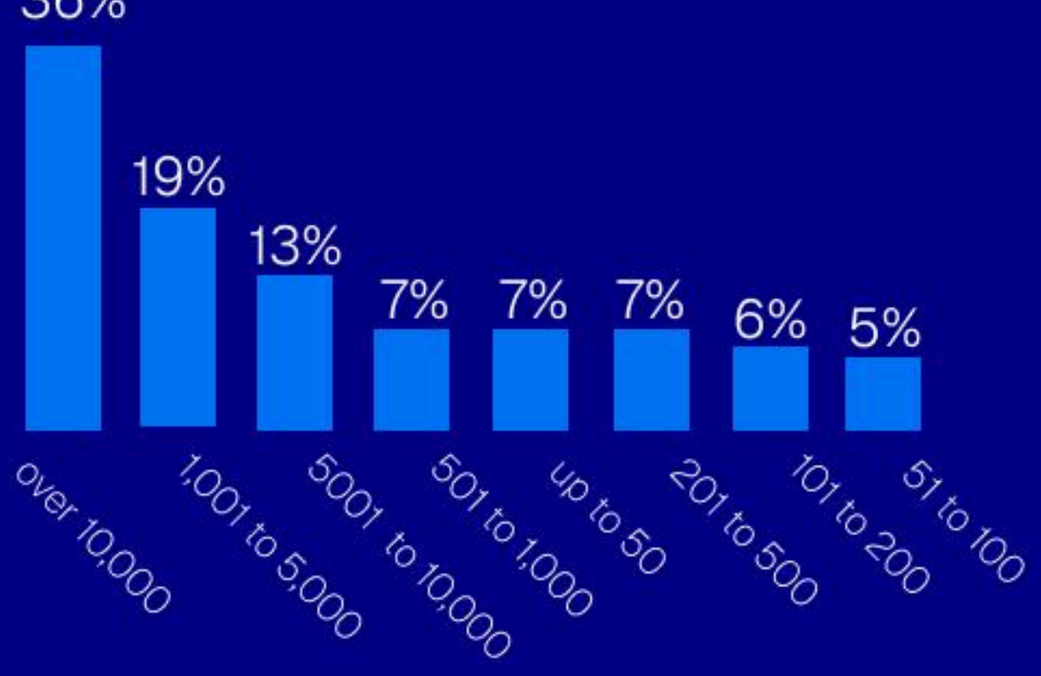
4.3 Profile of interviewees in 2024

172

interviewed

Industry Sector

Company Size
(by # of Employees)



TENCHI

THIRD-PARTY CYBER RISK MANAGEMENT