TENCHI

Third-Party Cyber Risk Management

Challenges and Trends

2025

About Me

Cyber security specialist and entrepreneur for 25+ years.

Cofounder of CIPHER (acquired by ProSegur) and Niddel (acquired by Verizon).

Former Senior Manager of Product for Verizon's global Security Detect and Respond Services.

Internacional speaker at events like Black Hat, DEF CON Cloud Village, FIRST and multiple BSides editions.

Cofounder of MLSec Project. Postgraduate Teacher of AI Applied to Cyber Security at FIA.

Alexandre Sieira

Cofounder and CTO

TENCHI

THIRD-PARTY CYBER RISK MANAGEMENT

About Tenchi Security

We build solutions that to allow security leaders to systematically reduce their Third-Party Cyber Risk.

Trusted by Major First-Parties and Third-Parties

... and many more

”Zanshin is a important and disruptive tool that enables companies to expand their Third Party Risk Management Program.”

IT Security & Risk Management Associate in the Banking Industry

Company Size: 3B - 10B USD

Partnered by Major Security Leaders

FS-ISAC Affiliate

Recognition

2024 LinkedIn TOP STARTUPS

Gartner

2024 CYBER 150

Backed by Major Investors

Gartner and Peer Insights™ are trademarks of Gartner, Inc. and/or its affiliates. All rights reserved.
Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences, and should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.

Third-Party Risk

Cyber security is increasingly dependent on critical third-parties.

41%

of organizations that suffered a material impact from a cyberattack said it originated from a third-party.

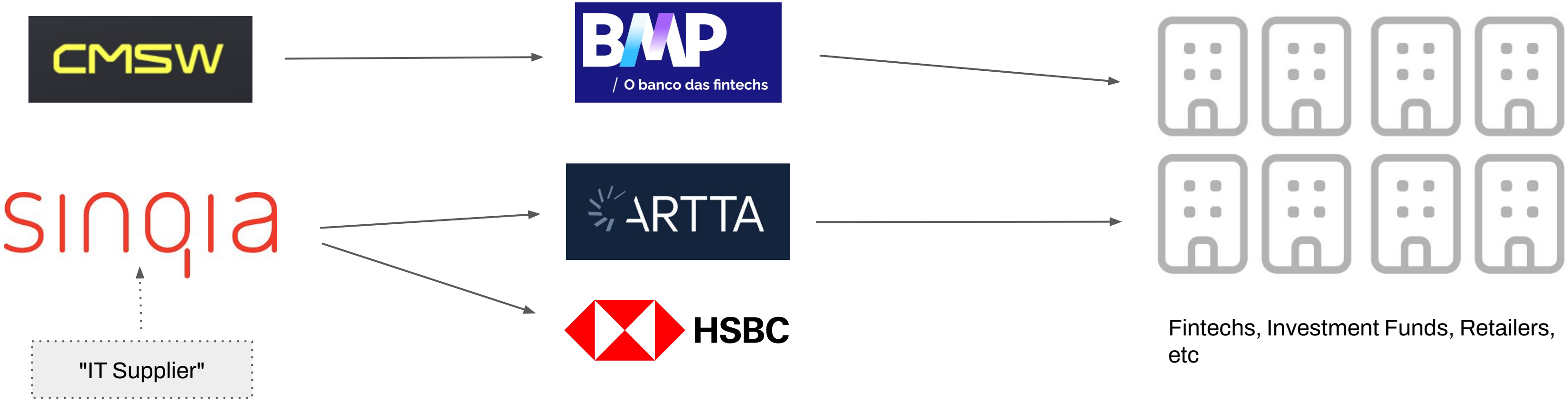
[World Economic Forum Global Cybersecurity Outlook 2024]

2x

YoY growth in third-party involvement in data breaches (15% in 2024, 30% in 2025).

[Verizon 2025 Data Breach Investigations Report (DBIR)]

Growth Drivers - Incidents



CHANGE HEALTHCARE Part of Optum

USD 2.87B in losses

PII leak of 100MM

snowflake

165+ corporations including Santander, TicketMaster, Neiman Marcus impacted, 10+ ransomed.

PII leak of tens of millions

Infosys McCamish

BofA, Fidelity, Newport Group, Union Labor Life Insurance and others

PII leak of of 6MM+

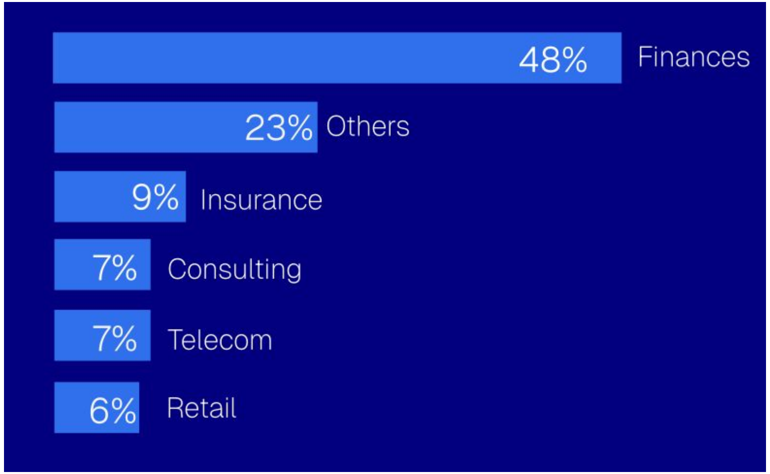
Safe

USD 1.5B of Ethereum stolen from ByBit cryptocurrency exchange. Largest financial theft in history.

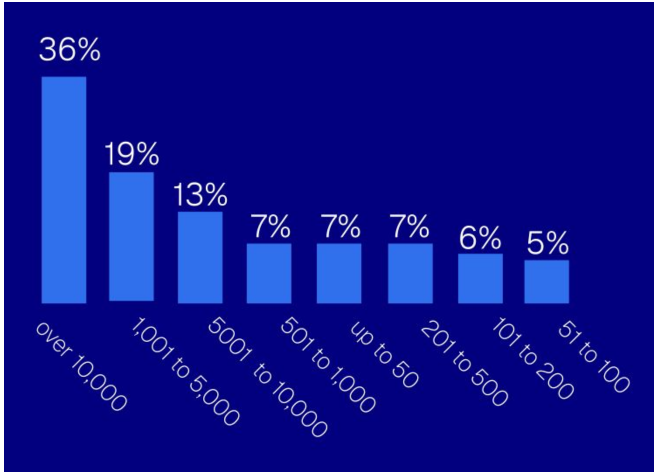
Tenchi Security - Third-Party Cyber Risk Management in Brazil 2025 Report

172 corporate security and privacy professionals interviewed at Tenchi Conference, in November of 2024.

Industry Sector



Company Size (# employees)



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.

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

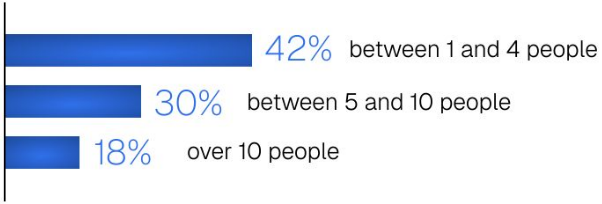
4%

others;

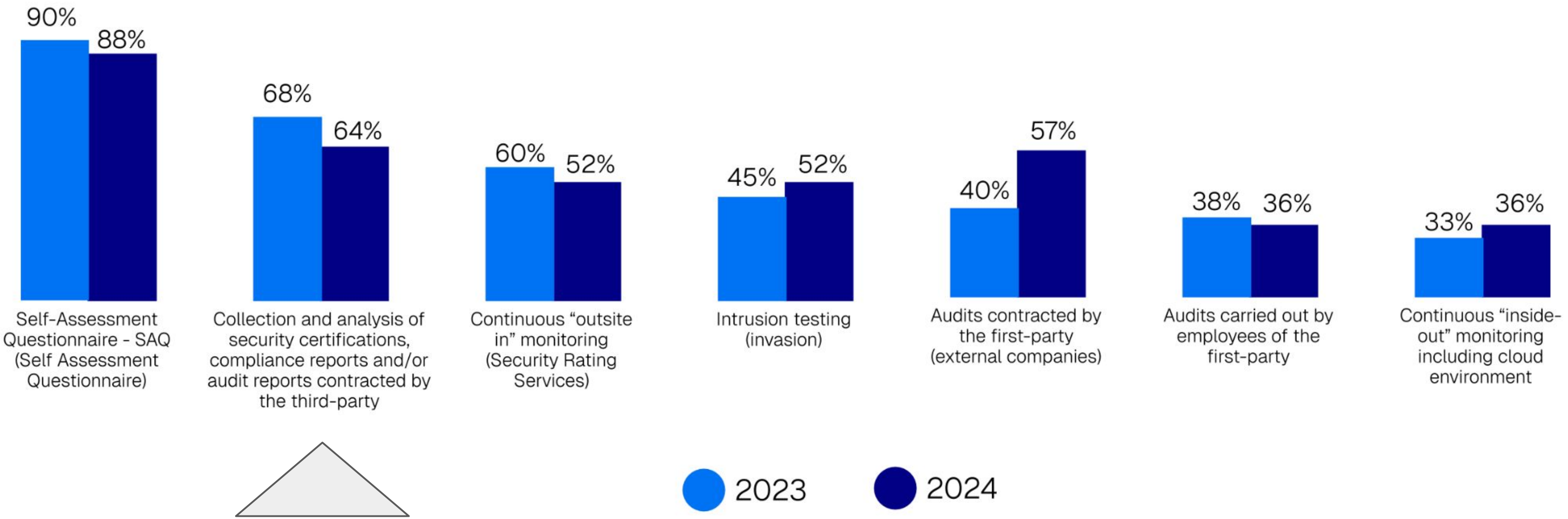
51%

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

Team sizes allocated to the TPCRM program



[Tenchi Security - Third-Party Cyber Risk Management in Brazil 2025 Report]

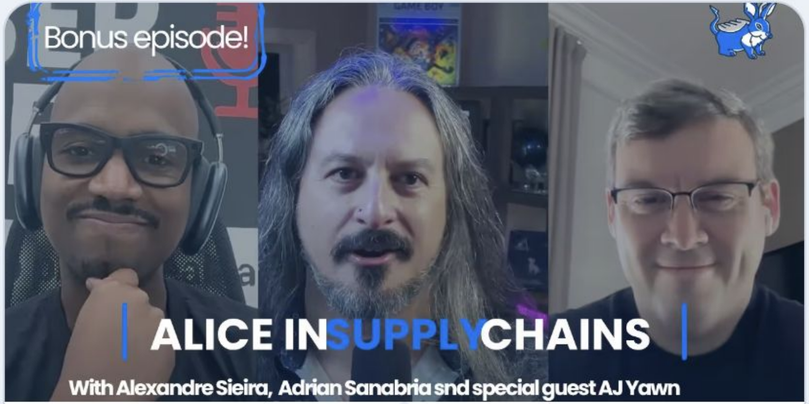


68% ISO 27001
30% SOC 2

71%

of organizations assess their third-parties' security **at most once a year.**

"Independent" Audits and Reports



Bonus Episode - The Limitations of SOC 2 with AJ Yawn

In this special bonus episode, Alexandre Sieira, CTO and Co-founder of Tenchi Security, and Adrian Sanabria,...

LAWFARE

Enforcement of Cybersecurity Regulations: Part 2

Jim Dempsey | Friday, March 24, 2023, 12:29 PM

While a valuable part of a cybersecurity program, “third-party audits” are too often not audits and not done by true third parties.

In a 2002 article, business school professors Max H. Bazerman and Don A. Moore and economist George Loewenstein outlined why external auditors selected and paid by the audited entity often perform bad audits. It begins with “attachment bias”—the internalized concern of auditors that “client companies fire accounting firms that deliver unfavorable audits.” Other factors identified by Bazerman and his colleagues are remarkably pertinent to auditing in the cybersecurity context. For one, they concluded that bias thrives in a context of ambiguity. In the cybersecurity context, where outcomes are by and large unmeasurable, security is inherently risk based and contextual, leaving a lot of room for ambiguity. Throw in the fact that auditors may hesitate to issue critical audit reports because the adverse consequences of doing so—damage to the relationship, potential loss of the contract—are immediate, while the costs of a report glossing over deficiencies—the chances of a breach occurring due to defects that were not called out and remediated—are distant and uncertain, and you have a recipe for overly generous assessments.

https://www.tenchisecurity.com/en/alice-in-supply-chains/episode-7-hoxz2

https://www.lawfaremedia.org/article/enforcement-cybersecurity-regulations-part-2

[Tenchi Security - Third-Party Cyber Risk Management in Brazil 2025 Report]

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.

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

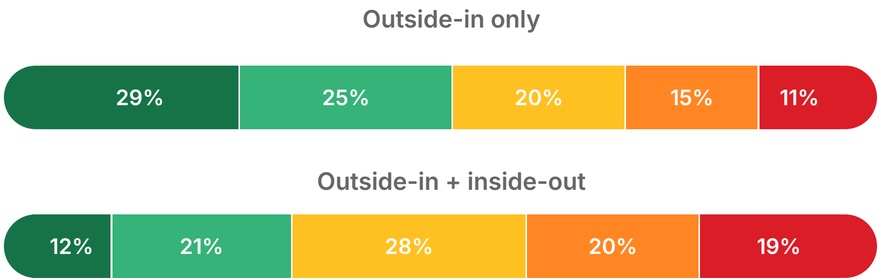
Zanshin Score Reseach (NEW)

74%

74% of organizations with an A score on outside-in scans cannot maintain that performance when their inside-out environments are assessed.

30%

of above-average organizations (A, B, C) with outside-in only scanning become laggards (D, F) when inside-out data is added.



Organizations find it easier to keep high outside-in scores (most frequent is A) than total score (most frequent is C).

What is the point?

1. **Transfer risk to the third-party**
   Outsourcing responsibility does not eliminate enterprise risk.

2. **Select third-parties with the lower risk level**
   Might create friction with the business and still not be enough to bring the risk down to an acceptable level.

3. **Mitigate risks represented by critical third-parties**
   Partner with strategic partners to improve the business' resilience.

Kind Request

Answer this year's survey!

https://form.jotform.com/253133548483662

TENCHI

¡Muchas Gracias!

> **Alexandre Sieira**
asieira@tenchisecurity.com
infosec.exchange/@AlexandreSieira

November 12th, 2025

FS-ISAC Mexico Member Forum