2025 SUPPLY CHAIN CYBERSECURITY TRENDS

Why Visibility Is the Next Competitive Advantage

SecurityScorecard

EXECUTIVE SUMMARY

Cybersecurity now requires more than breach prevention. It demands the ability to survive systemic failure.

A handful of technology giants now control the infrastructure that powers the global economy. When major cloud providers experience outages, airlines ground flights worldwide. When leading software platforms falter, entire sectors go dark. When a single security vendor gets compromised, thousands of customers become victims simultaneously. This unprecedented concentration of digital infrastructure has created a new category of systemic risk that most organizations are unprepared to handle.

Supply chain attacks have become the ultimate force multiplier for cybercriminals and nation-state actors. Traditional cybersecurity threats target individual companies, but today's most devastating attacks exploit the few critical chokepoints that entire industries depend on.

Against this backdrop of rising systemic risk, SecurityScorecard set out to assess how enterprises are managing their third-party risk. The responses from nearly 550 CISOs and cybersecurity leaders worldwide reveal a dangerous gap in organizational preparedness.

Our digital infrastructure becomes more concentrated and interdependent each year, yet our ability to see and manage these risks continues to decline. Organizations are operating under the illusion of security while remaining blind to their most critical vulnerabilities.

Among the key findings:

The concern is real. Eighty-eight percent of respondents say they're "very concerned" or "somewhat concerned" about supply chain cybersecurity risks.

Supply chains are under attack. More than 70% of organizations say they experienced at least one material third-party cybersecurity incident in the past year—and 5% suffered *10 or more* incidents.

Visibility is sorely lacking. Fewer than half of organizations monitor cybersecurity across even 50% of their nth-party supply chains.

Response is passive, not active. Only 26% of organizations incorporate incident response into their TPRM programs. The majority rely on point-in-time, vendor-supplied assessments or cyber insurance.

Responsibilities are misaligned. When a third-party breach occurs, most TPRM teams delegate responsibilities to their Security Operations Center (SOC) colleagues, who are already overworked and at risk for burnout.

Keep reading to see the full picture. Along the way, you'll discover what's keeping your peers up at night and how leading-edge cybersecurity teams are building resilience by integrating real-time response into their risk management strategies.

TABLE OF CONTENTS

Introduction 04

Section 1 05
Complex vendor networks, critical visibility gaps

Section 2 07
The danger is all too real

Section 3 09
Confidence could be an illusion

Section 4 11
TPRM-SOC collaboration shows room for improvement

Section 5 13
Moving from worry to resilience

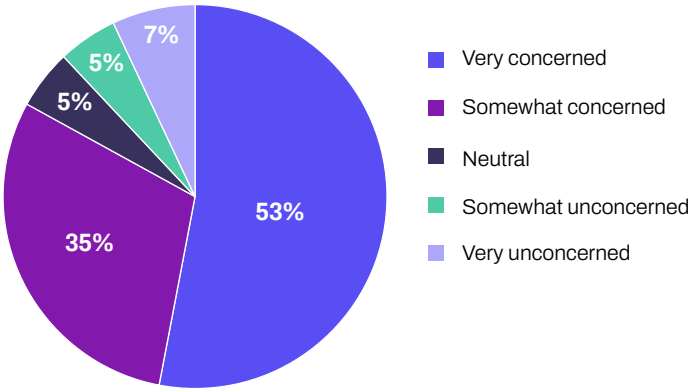
Conclusion 14

INTRODUCTION

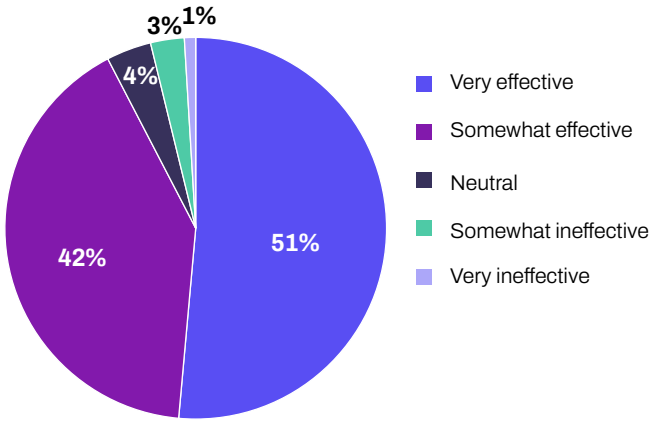
Cybersecurity leaders feel confident in their TPRM programs—so why are they so concerned about supply chain risks?

Supply chain risks remain top-of-mind for the vast majority of CISOs and cybersecurity leaders, with 88% reporting that they are somewhat or very concerned about them. At the same time, an even higher majority say they are confident in the effectiveness of their program. These figures represent a subtle but telling disconnect. Why isn't this apparent effectiveness reducing concern?

How concerned are you about supply chain risks?



How effective are your current supply chain cybersecurity measures?



Anxieties are genuine and widespread

CISOs across industries were candid about the underlying reasons behind their crises of confidence. Primary concerns include fraud and abuse, insufficient endpoint security, and a lack of in-house risk management expertise.

"We have problems with hackers and thieves falsifying our company logos and sending it to our potential suppliers with the wrong bank details."

"Operations is always a point of concern and needs to have an endpoint security posture."

"We need more people who understand the cyber space."

"It depends on the extent of the exposure—client data compromise can halt operations."

By digging deeper into the realities of supply chain risk, we can gain some understanding of where this disconnect between concern and confidence may be coming from.

COMPLEX VENDOR NETWORKS, CRITICAL VISIBILITY GAPS

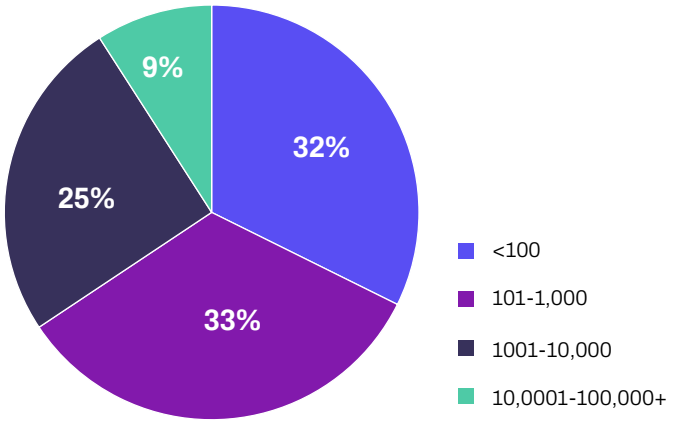
Just 150 companies power 90% of Fortune 500 technology products and services worldwide, creating a scenario where one vulnerable supplier can trigger disruption across multiple industries and countries. Simultaneously, the sprawling network of third-party and *n*th-party vendors is getting larger, more complex, and increasingly fragile.

Vendor volume is expanding exponentially

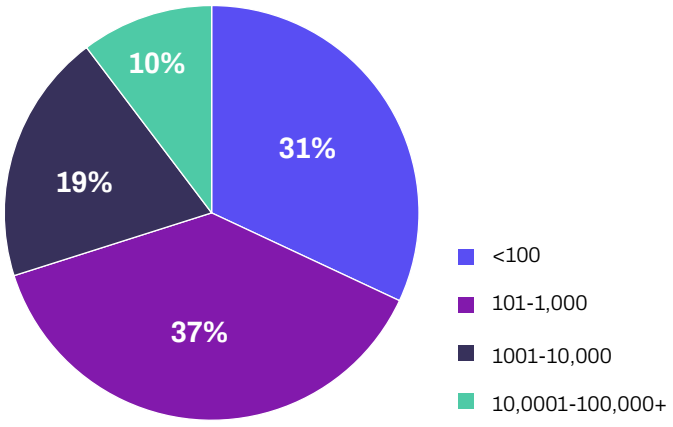
More than one-third of organizations (35%) have over 1,000 third-party suppliers. Another 29% have an equal number of nth-party suppliers, a category that includes their third party's dependencies and their dependencies. In this sprawling yet tightly knit ecosystem, every new connection becomes a potential point of failure.

Supply chain size

Third-party suppliers



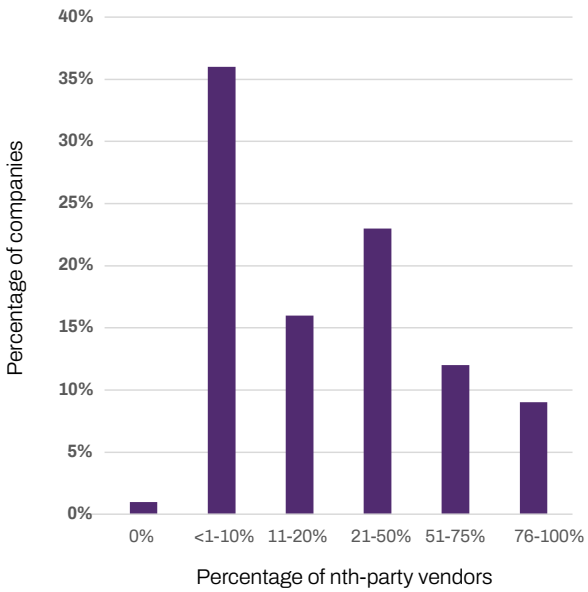
nth-party suppliers



Yet much of the risk remains invisible

Despite clear and present vulnerabilities, 79% of companies say that **less than half of their *n*th-party supply chain is currently overseen by cybersecurity programs.** This means the vast majority of organizations are flying blind when it comes to securing the supply chains that keep their businesses running. In fact, 36% of respondents revealed that only 1%-10% of their supply chain is protected, a sharp indicator amid the rising tide of third-party breaches.

What percentage of your nth-party vendors are overseen by a supply chain cybersecurity program?



36%

of respondents revealed that only 1%-10% of their supply chain is protected

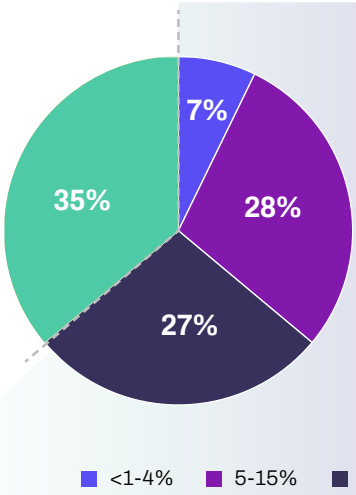
"The same level of concern for third-, fourth-, nth-party risk is multiplied by the number of each one (at least, the ones we know about)."

And vendors' cybersecurity approaches aren't keeping pace

At the very least, you would expect your third-party and nth-party vendors to match your company's security protocols. But that's simply not the case. Sixty-two percent of organizations say that less than half of vendors in their supply chain ecosystem fail to meet their company's cybersecurity requirements.

These findings show that most organizations lack visibility into their supply chain risks—while also facing significant cybersecurity gaps among vendors that expose their organizations to long-term business interruption and the potentially devastating consequences.

What percentage of your vendor ecosystem complies with your cybersecurity requirements?



62%

of organizations say that less than half of vendors in their supply chain ecosystem fail to meet their company's cybersecurity requirements

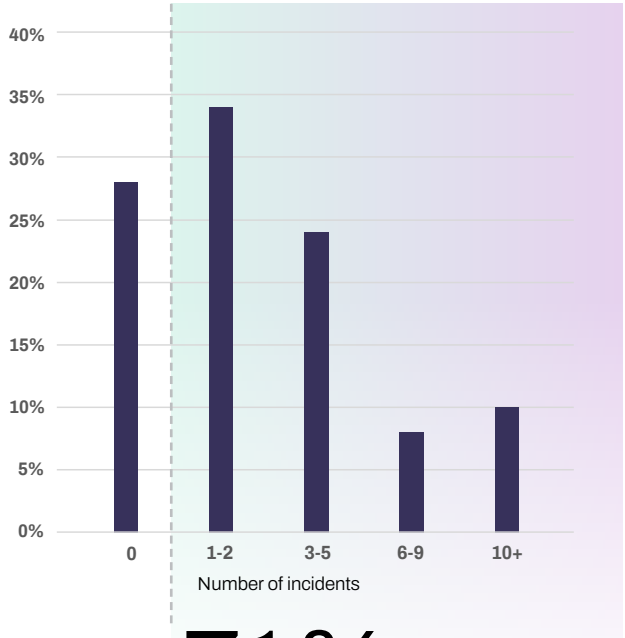
THE DANGER IS ALL TOO REAL

Verizon's most recent Data Breach Investigations Report shows a 100% year-over-year increase in third-party breaches, rising from 15% of all breaches in 2024 to 30% in 2025. And a majority of our respondents are feeling the economic, operational, and reputational effects that system outages leave in their wake.

Supply chain incidents are rising fast

In the past 12 months alone, 71% of survey respondents say they experienced at least one third-party cyber incident that had a material impact on their business. More than one-third (37%) experienced three or more impactful incidents, underscoring the persistent and damaging implications of supply chain breaches.

How many times has a cyber incident had a material impact on your organization in the past 12 months?



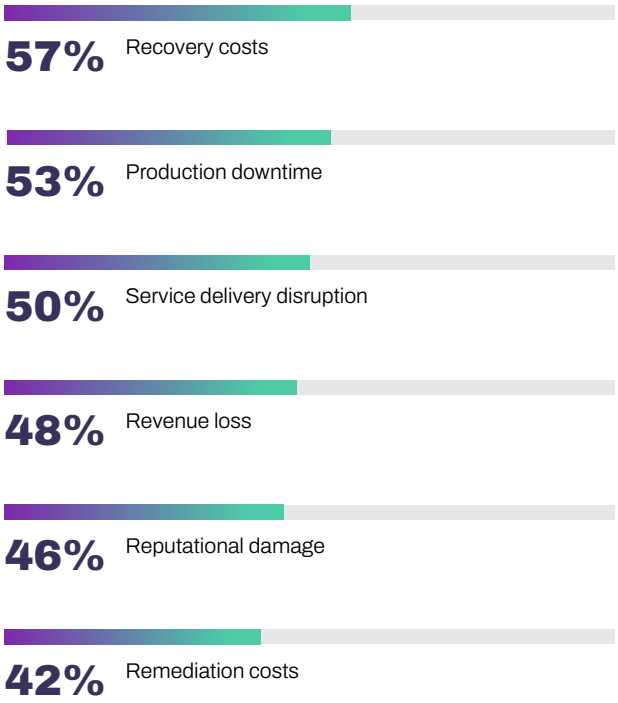
71%

of survey respondents say they experienced at least one third-party cyber incident that had a material impact on their business

Each incident carries a steep price

Supply chain cyber events create a chain reaction of negative consequences across the entire business, including financial (recovery costs and revenue loss) and operational (production downtime and service delivery disruption).

How do you assess the impact of a supply chain cyberattack on your business operations?



"Our organization was recently attacked, and we lost a big amount of data, so our cybersecurity vendors have been a concern since."

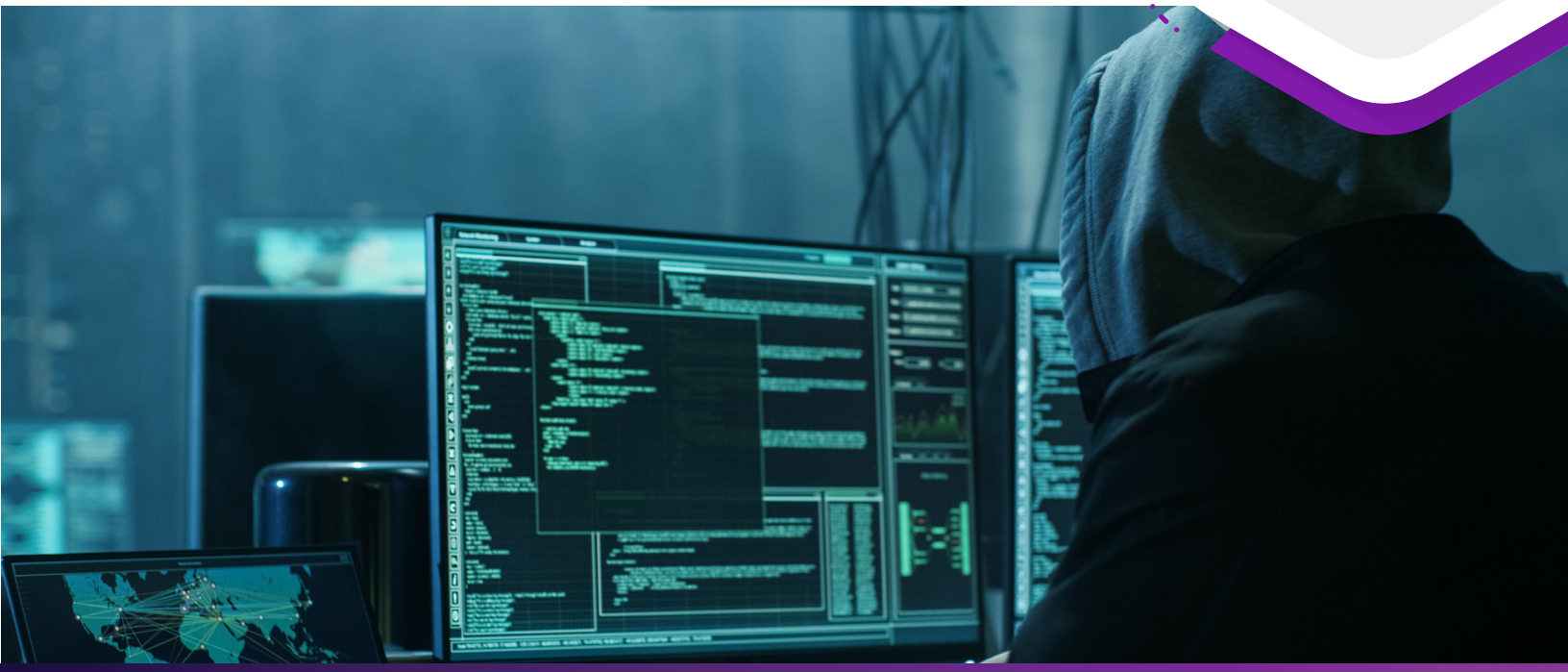
The risks are known, but hard to contain

When asked about their top threats, leaders listed vulnerability exploitation as their No. 1 threat. The next most common concern was the growing reliance on shared software and platforms—such as ERP, SCM, and IAM systems—that create dependencies across vendors.

What types of supply chain risks concern you the most?

1. **Vulnerability exploitation**
2. **Increased reliance on software shared with third parties**
3. **Shadow IT**
4. **Open-source software usage**
5. **Other**

Clearly, organizations need more effective ways to limit the potential business-busting impacts of supply chain breaches. But are their current risk management methods up to the task?



CONFIDENCE COULD BE AN ILLUSION

Achieving true resilience requires a holistic supply chain cybersecurity strategy that includes third-party risk assessments, continuous monitoring, proactive risk mitigation, and fast, appropriate incident response. The good news is that about one-quarter of respondents say they already include incident response within their supply chain cybersecurity approaches. That means roughly three-quarters of companies have a little catching up to do.

Popular risk-reduction strategies may fall short

When asked to list key components of their cybersecurity programs, leaders' feedback uncovered fundamental weaknesses. While cyber insurance is widely adopted, far fewer organizations are investing in tools designed to actively prevent third-party breaches (such as formal vendor onboarding and offboarding, vendor issue remediation outreach, and joint tabletop exercises with vendors) and tools designed to respond to incidents, (such as distinct third-party incident response plans and escalations to owners of business relationship with vendors).

Additionally, 56% of respondents still rely on self-assessment questionnaires—tools that only offer a point-in-time and somewhat biased evaluation, considering they're often completed by the vendors themselves.

Key components of cybersecurity

63% Cyber insurance coverage for supply chain incidents

60% Employee security awareness training

60% Continuous monitoring

56% Vendor risk assessments

45% Regular reporting to executive management or board of directors

39% Contractual requirements

38% Formal vendor onboarding and offboarding process

37% Vendor issue remediation outreach

37% Distinct third-party incident response plans

31% Escalations to owners of business relationship with vendors

29% Penalties for vendors who don't comply with requirements

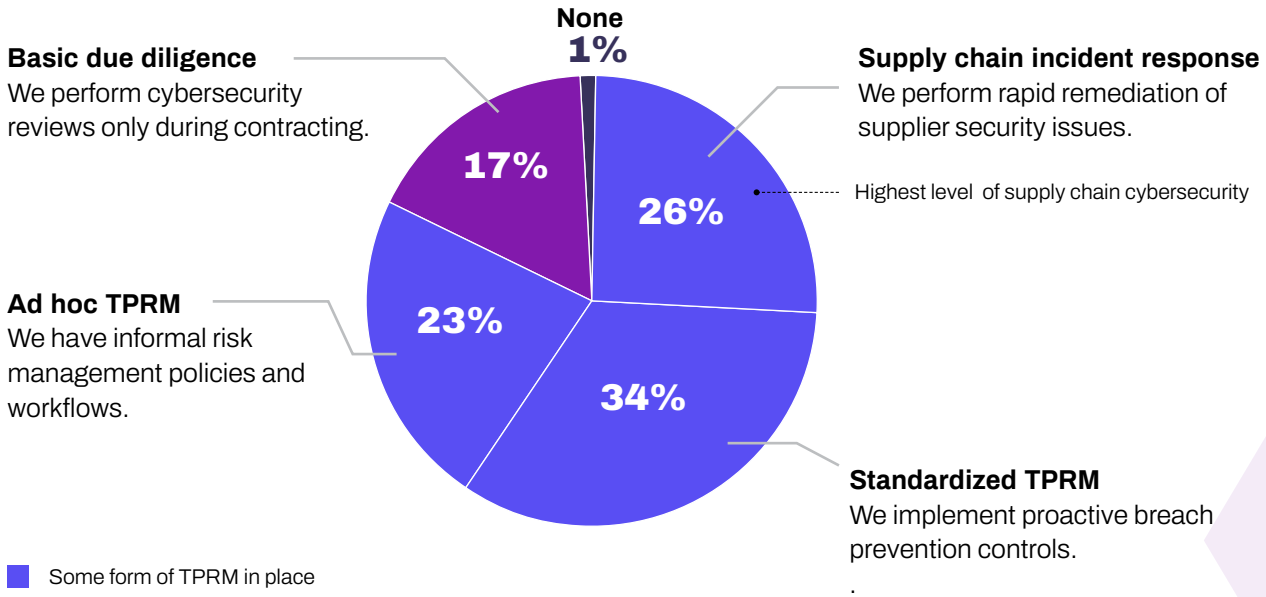
26% Joint tabletop exercises with vendors

1% We do not have a formal supply chain cybersecurity program

But supply chain cybersecurity programs are advancing in maturity

It's encouraging that **83% of companies already have some form of TPRM in place**, with 26% of respondents rating themselves at the highest level of supply chain cybersecurity—incorporating rapid response into their supply chain cybersecurity programs.

What level of risk management do you perform?



These findings show that supply chain cybersecurity isn't failing because leaders lack tools. Instead, it's failing because those tools aren't allowing organizations to perform real-time incident response.

TPRM-SOC COLLABORATION SHOWS ROOM FOR IMPROVEMENT

Who's responsible for supply chain cybersecurity within your organization?

An overwhelming number of survey respondents (92%) say that the SOC plays an integral role, either owning the entire process or sharing responsibility with risk management teams.

The human cost is mounting

Shared ownership requires tight collaboration between TPRM and SOC teams, especially within ad hoc and standardized TPRM models. However, SOC teams are chronically overburdened. One study shows that 71% of SOC analysts report high stress and burnout. Sixty percent say their workload has increased over the past year. And 70% say they're understaffed.

53% of organizations rate their TPRM-SOC collaboration as very effective

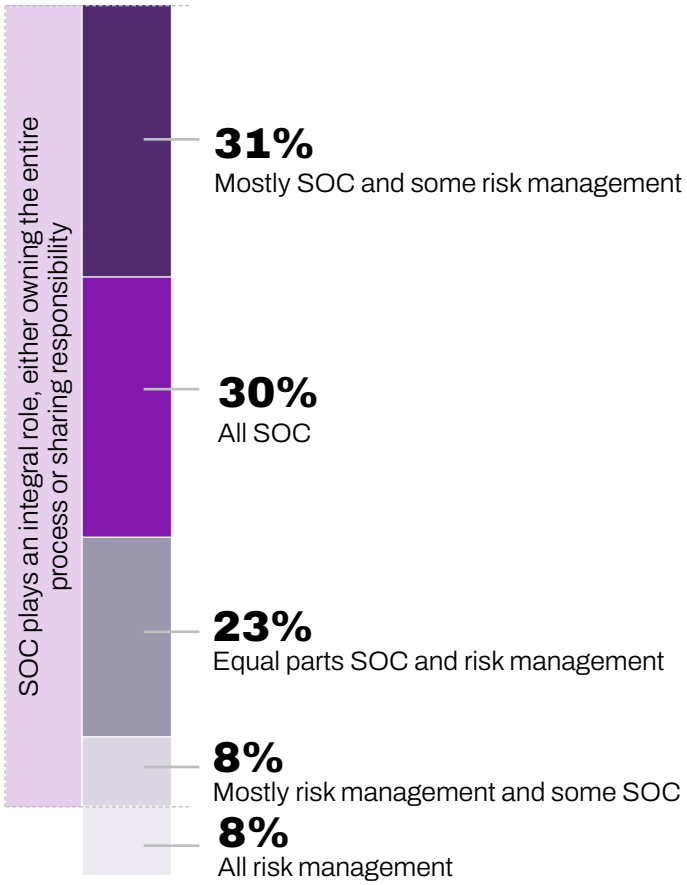
47% of organizations say teamwork could be better

When collaboration falters, performance suffers

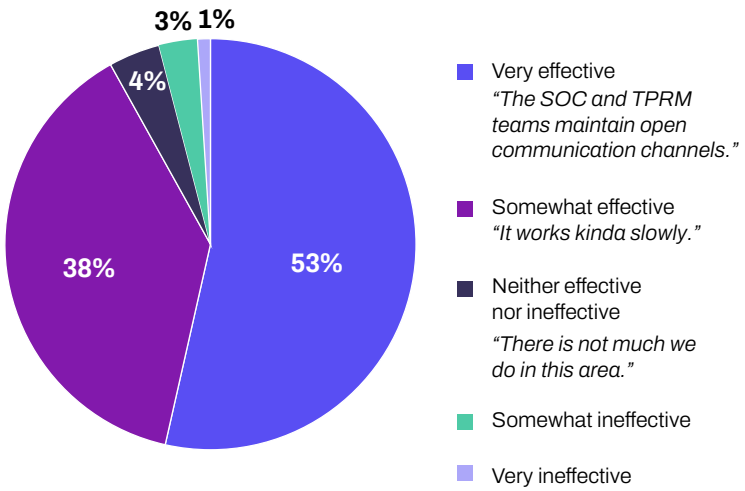
Subpar collaboration creates real-world operational problems. The most common TPRM challenges cited by respondents fall on the shoulders of an already overextended SOC team, including:

- **Data overload and threat prioritization.** SOC analysts are already flooded with a barrage of internal alerts, giving them little time to investigate third-party risks.
- **Resistance or lack of supplier engagement.** Vendors may not respond to self-assessments. But SOC teams do not have enough visibility into a third-party vendor's risk profile to complete their own assessment.

How is supply chain cybersecurity ownership distributed?



How effective is TPRM-SOC collaboration?



What are your biggest supply chain cybersecurity challenges?

39% Data overload; inability to prioritize issues and threats

36% Difficulty in assessing the security posture of third-party vendors

36% Limited resources to dedicate to supply chain security

36% Resistance or lack of supplier engagement to remediate identified issues

33% Lack of visibility into the supply chain

32% Resistance from business units to implement security controls

29% Too many manual processes

27% Lack of cyber expertise

12% No capacity for vendor outreach

9% None of the above

To overcome these challenges, organizations are creating supply chain incident response teams dedicated to anticipating and managing cyber events across the vendor ecosystem. These teams are designed to improve communication and collaboration across departments, including business owners, legal, IT/security, and leadership. As supply chain threats grow, supply chain incident response teams may prove essential for reducing the burden on the SOC and building true resilience.

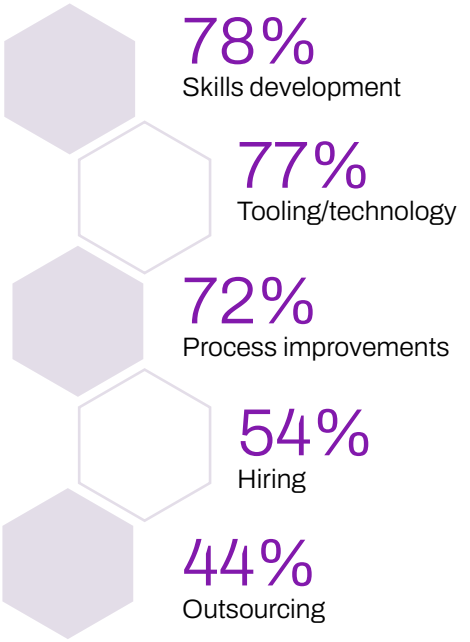
MOVING FROM WORRY TO RESILIENCE

With risks present across every link in the supply chain, should organizations continue investing in traditional risk management approaches, or is it time for something new?

Rethinking where—and how—to invest

Many CISOs are quickly realizing that the status quo doesn't cut it anymore. So, they're doubling down on their investments in people, tools, and training in an effort to build more resilience.

Percentage of organizations increasing cybersecurity investment by type



One of the more popular and promising tools is Supply Chain Detection and Response (SCDR). Rather than relying on static controls and manual reviews, the SCDR framework empowers security teams to actively prevent third-party breaches by enhancing the security posture of both their organization and their suppliers, reducing the time between identifying issues and resolving them.

In fact, true confidence comes when incident response and resilience are factored in. For example, one respondent explained, "I chose 'very confident' because our organization has a comprehensive continuity plan and robust cybersecurity measures in place."

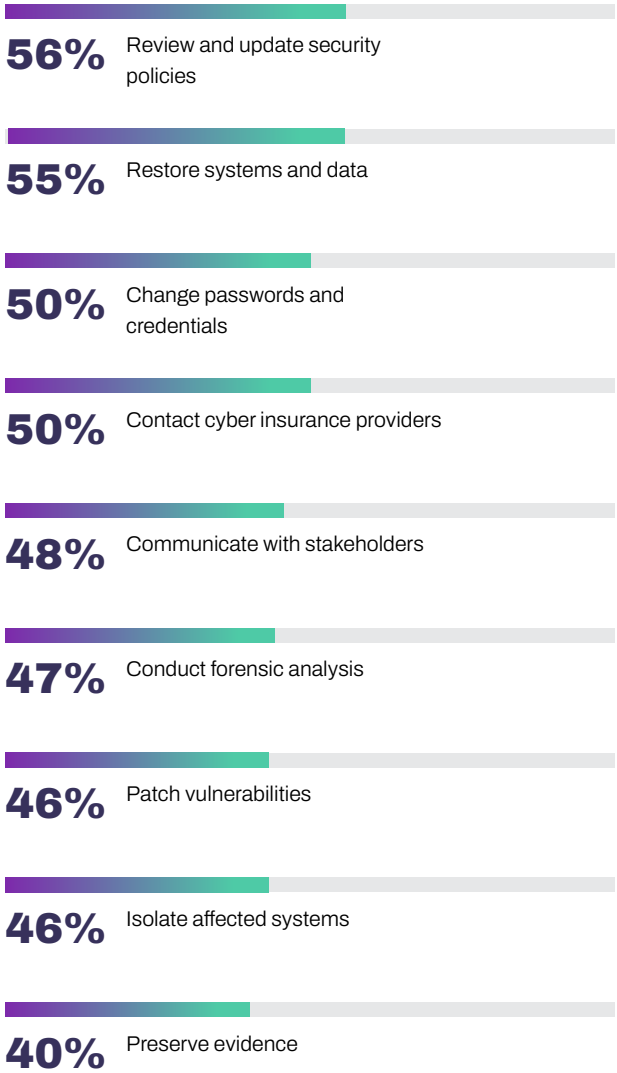
Strengthening security and incident response

In addition to choosing the right frameworks and tools, leaders can strengthen their supply chain resilience by reviewing what's working and what isn't for other organizations.

Survey respondents shared these key components of their incident response plans that allow them to recover from a supply chain cyberattack and minimize business disruption.

Building resilience is about investing smarter, not necessarily more.

Key components of incident response plans



CONCLUSION

From risk identification to real-time response

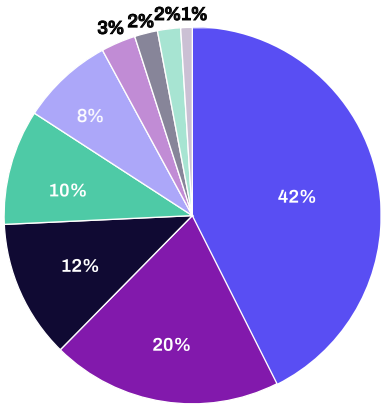
The way most organizations manage supply chain cyber risk isn't keeping pace with the expanding threats. Regaining a true sense of security means investing in not just identifying risk, but in responding to those risks in real time.

While traditional TPRM had its place, it's time for leaders to move beyond prevention and toward resilience. The next wave of third-party cyber incidents won't wait for better processes.

In an era of systemic threats, resilience can't wait. It must be built now—from the inside out. **Learn how at securityscorecard.com.**

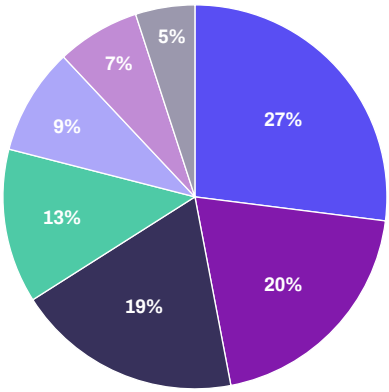
Demographics

Countries represented



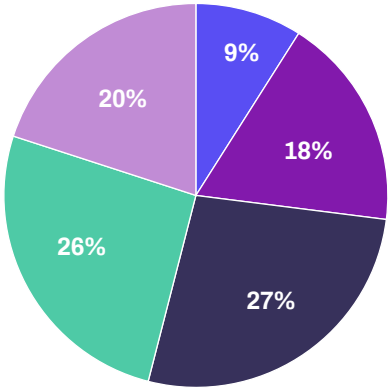
- United States
- Canada
- United Kingdom
- South Africa
- India
- Singapore
- Philippines
- Australia
- New Zealand

Industries represented



- Technology
- Manufacturing
- Financial services/insurance
- E-commerce
- Other
- Healthcare
- Government

Respondents' annual revenue



- >$5B
- $1B-$5B
- $500M-$1B
- $200M-$500M
- <$200M

SecurityScorecard

SecurityScorecard created Supply Chain Detection and Response (SCDR), transforming how organizations defend against the fastest-growing threat vector—supply chain attacks. Our industry-leading security ratings serve as the foundation and core strength, while SCDR continuously monitors third-party risks using our factor-based ratings, automated assessments, and proprietary threat intelligence to resolve threats before they become breaches. MAX enables response and remediation capability, working through our service partners to protect the entire supply chain ecosystem while strengthening operational resilience, enhancing third-party risk management, and mitigating concentrated risk.

Trusted by over 3,000 organizations—including two-thirds of the Fortune 100—and recognized as a trusted resource by the U.S. Cybersecurity & Infrastructure Security Agency (CISA). Backed by Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, NGP, Intel Capital, and Riverwood Capital, SecurityScorecard delivers end-to-end supply chain cybersecurity that safeguards business continuity.

Visit securityscorecard.com for details.