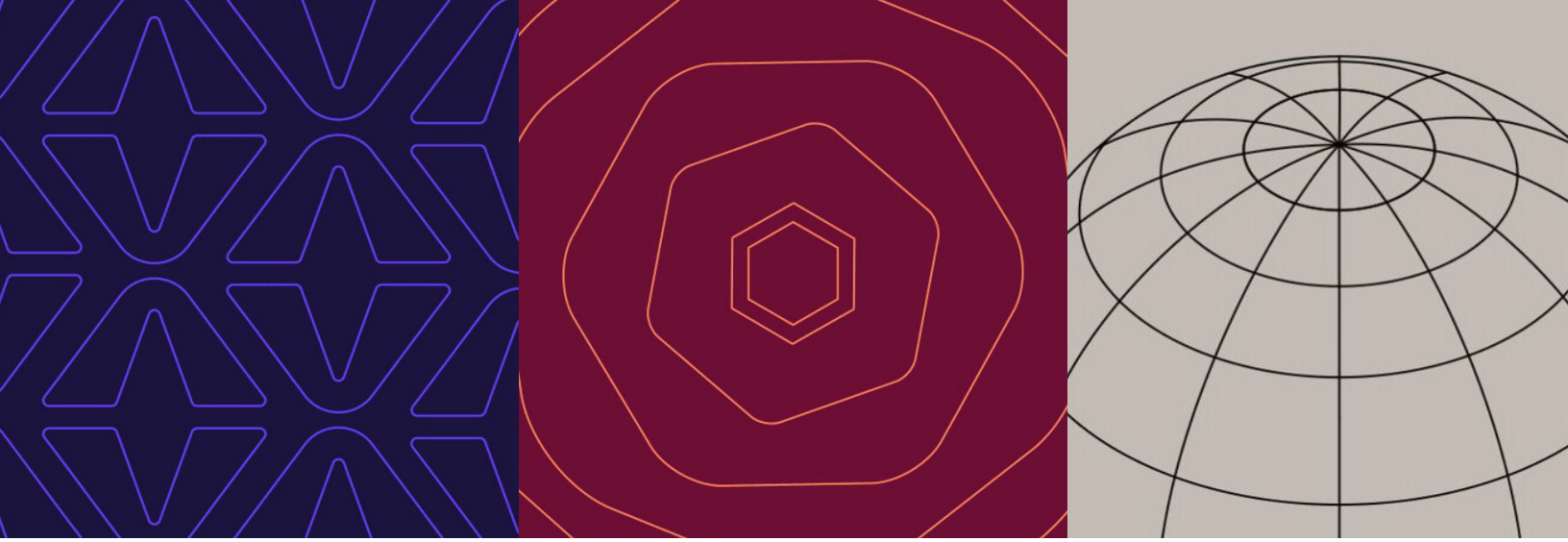


2026 Supply Chain Cybersecurity Trends Report

The paradox of third-party risk: Confidence rises as exposure grows

SecurityScorecard

Executive Summary

Third-party risks are expanding. Mitigation practices aren't evolving fast enough.

For the second consecutive year, SecurityScorecard surveyed leaders who oversee or manage third-party cybersecurity risks within their organization. The results reveal a third-party risk management paradox, defined by a widening gap between leaders' high confidence and the demonstrable deficiencies in their supply chains.

Among the key findings:

Confidence is high, but concern is widespread. Despite 86% of leaders expressing concern about supply chain risks, 90% remain confident that their business could seamlessly continue operations if a vendor suffered a cybersecurity incident.

Massive gaps in vendor oversight exist. Most (78%) organizations admit their internal cybersecurity programs cover less than 50% of their total vendor ecosystem, including third, fourth, and fifth parties, leaving serious blind spots across their growing risk landscape.

Mitigation practices are slow and outdated. More than half (55%) of respondents still depend on manual methods like phone calls, meetings, or emails to collaborate with vendors during a breach. As a result, it takes 60% of organizations 8 days or more to remediate a high-severity issue.

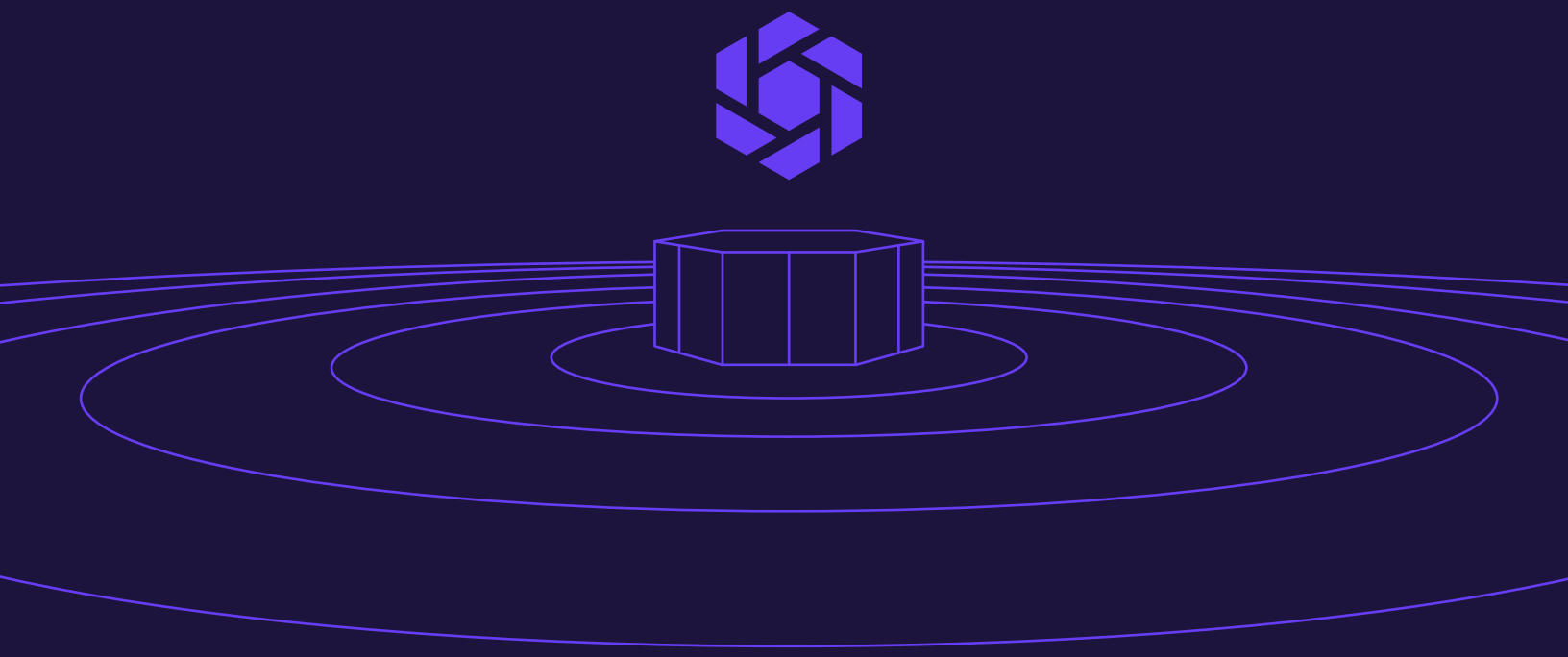
Rising AI threats demand continuous monitoring. Organizations continue to favor static assessments, with 67% using security audits and 46% relying on periodic (monthly/quarterly) monitoring, even though leaders acknowledge the growing risk of AI-driven threats.

The need for automated third-party risk management (TPRM) strategies is growing. The reliance on outdated tactics, coupled with nearly half (49%) of respondents' struggles to keep pace with changing regulations, underscores the urgent need for more mature TPRM approaches.

The supply chain vendor landscape is multiplying rapidly, and AI is accelerating the pace of threats. The question is: Are organizations' third-party risk management (TPRM) strategies keeping up with 2026's threats, or are they relying on risk management practices from the 2010s?

Keep reading to learn the scope of your peers' vendor ecosystems, the challenges they're encountering in securing them, and the plans they're making to reduce their third-, fourth-, and fifth-party risks.

Table of contents



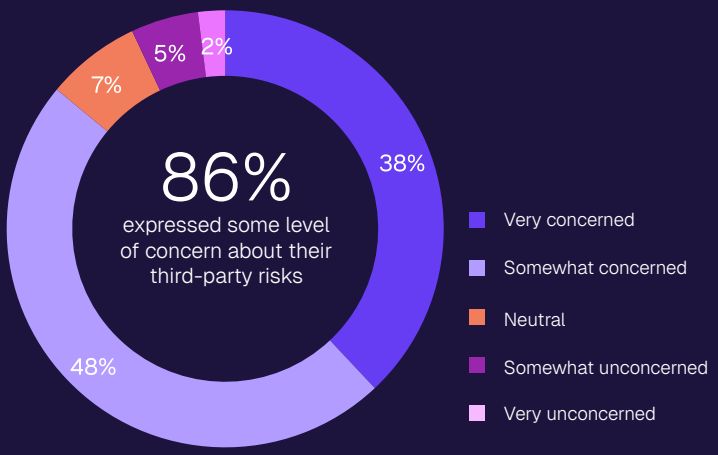
As third-party ecosystems grow, so do the risks

01

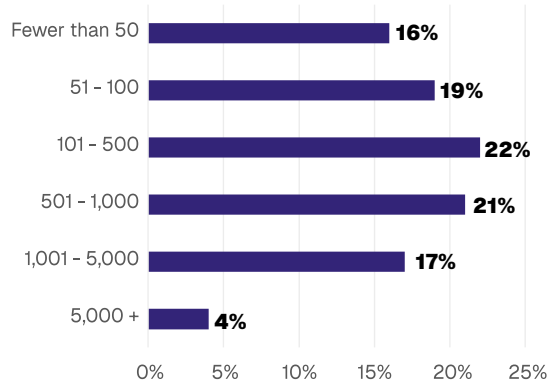
The number of third-, fourth-, and fifth-party vendors keeps expanding, raising supply chain cybersecurity concerns among leaders. This year, **86% of respondents expressed at least some level of concern about their third-party risks**, similar to last year's results. Yet the TPRM practices most organizations follow haven't changed much over the last 12 months.

Most organizations (78%) manage 1,000 or fewer third-party vendors. When you extrapolate that out across fourth- and fifth-party suppliers, however, the complexity grows. Roughly two-thirds (67%) of respondents say they have over 1,001 total vendors in their ecosystem, and 34% have between 10,001 and 100,000+ suppliers.

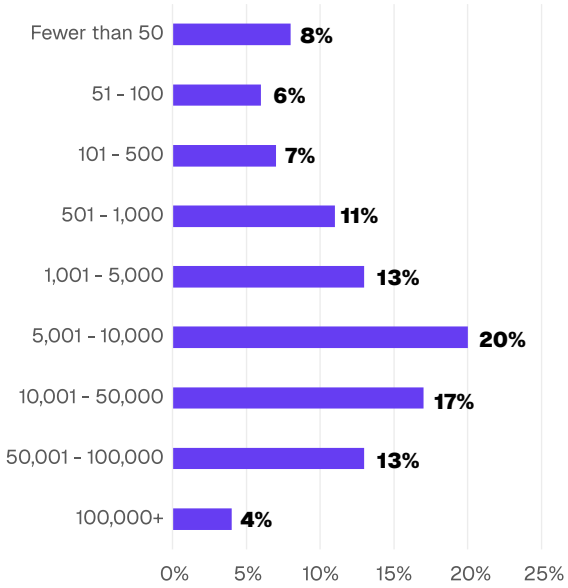
How concerned are you about supply chain cybersecurity?



Approximately how many third-party suppliers does your organization have?



Approximately how large is your total vendor ecosystem (up to the fifth party)?



"What we hear most often from our customers is that when they get out to the fourth and fifth party, they feel even more exposed," says Jeff Barker, VP of Product Marketing at Security Scorecard. "Just one material incident can become a full-blown, five-alarm fire quickly."

The challenge, Barker explains, is trying to oversee and orchestrate tens of thousands of vendors with a relatively small internal team. Survey respondents concur. When asked to name the most significant challenge to their current supply chain cybersecurity program, one respondent said:

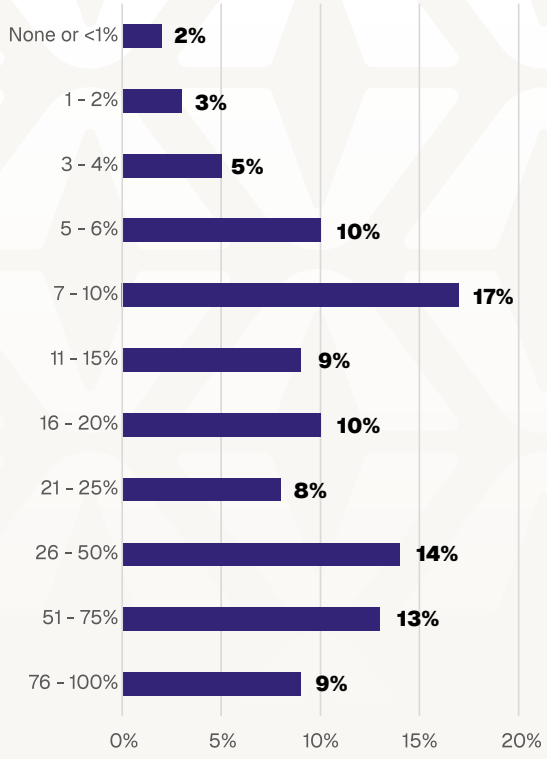
> ***"The biggest blind spot is the lack of coordination and communication between us and our different suppliers…. Sometimes I feel overwhelmed with the large amount of vendors we have."***

As the number of nth-party vendors has increased, so have the risks. Third-party breaches doubled in 2025, according to Verizon's latest Data Breach Investigations Report. Yet internal oversight of supply chain risks remains flat from last year. **Just 9% of respondents say over three quarters of their total vendor ecosystem is overseen by an internal supply chain cybersecurity program**, similar to 2025. More concerning:

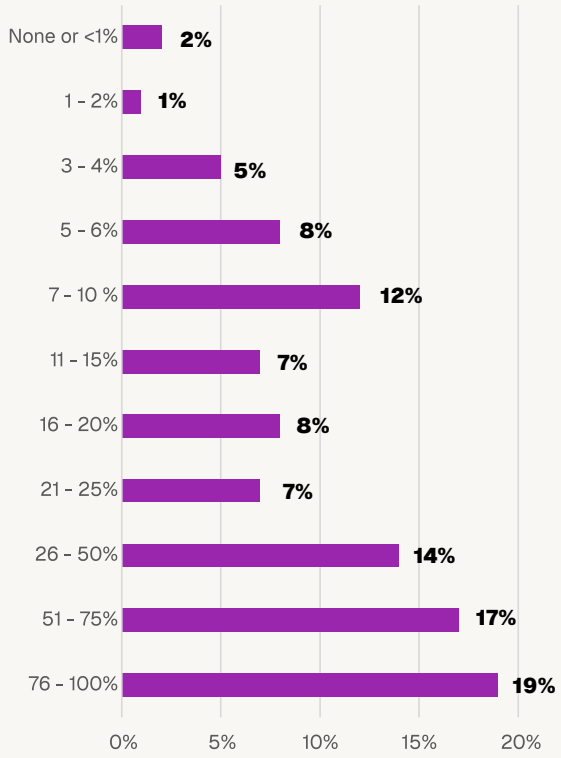
64%

this year's respondents say that fewer than half of their vendors comply with their organization's internal rules

What percentage of your total vendor ecosystem (up to the fifth party) is overseen by an internal supply chain cybersecurity program?



What percentage of your vendor ecosystem is complying with your cybersecurity requirements?

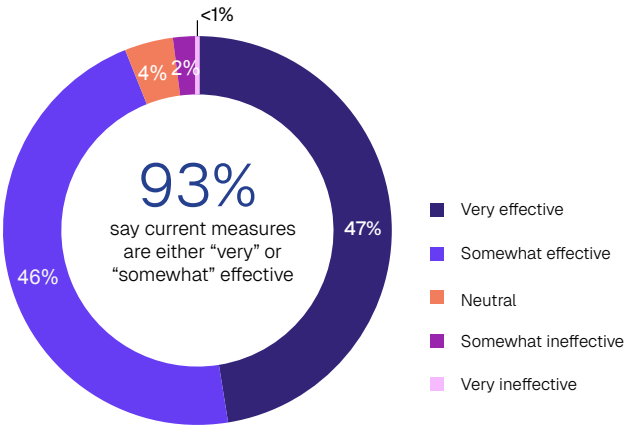


Leaders express confidence, but new threats are emerging

02

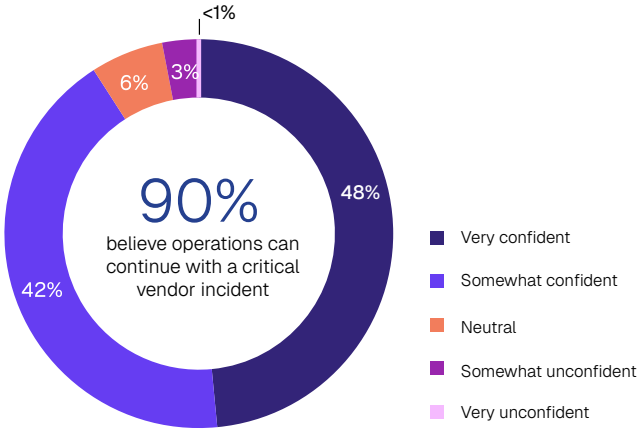
Even with the number of third-party breaches doubling worldwide, risk and security teams believe they have their supply chain risks under control. **Most (93%) respondents say their current measures are either "very" or "somewhat" effective**.

How effective are your organization's current supply chain cybersecurity measures at mitigating risks?



Another 90% believe they can continue operations seamlessly in the event of an incident with a critical vendor. That confidence level is 5 percentage points higher than what leaders told us in last year's survey.

How confident are you that your business could continue operations without disruption if a cybersecurity incident occurred at a critical vendor?



But when asked which dependencies most influence their confidence in maintaining operations during a vendor-related incident, open-ended responses revealed some conflicting viewpoints:

"Very confident:

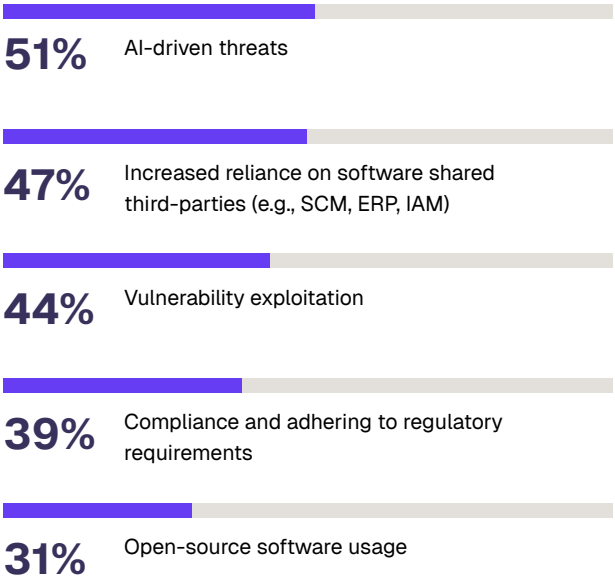
*"What influences this is that we have one of the best crisis relief systems you could get.... Any form of problem or crisis is usually **solved in under an hour."***

"Somewhat unconfident:

*"We are heavily dependent for service delivery on a few critical vendors.... If [one of those vendors] has a global or multi-region outage, **we would be hard down."***

What could shake leaders' confidence even further? The rise of AI-driven threats.

What types of supply chain risks most concern you? (Select up to three)



03

Keeping up with regulations is an ongoing challenge

The 2025 rollout of the Digital Operations Resilience Act (DORA) in the EU is the latest example of the patchwork of ever-changing regulations that supply chain cybersecurity teams must meet. But while staying compliant is *necessary*, it doesn't always mean that a company's supply chain security is *effective*.

Regulation is the main driver of TPRM programs, according to 47% of our survey respondents. However, **49% say that the busywork required to stay compliant impedes their teams**.

Which factors most strongly drive your supply chain cybersecurity or TPRM program? (Select up to three)

- **46%** Regulatory requirements
- **42%** Cyber insurance requirements
- **41%** Risk reduction goals
- **35%** Industry best practices
- **28%** Customer requirements
- **27%** Recent security incidents

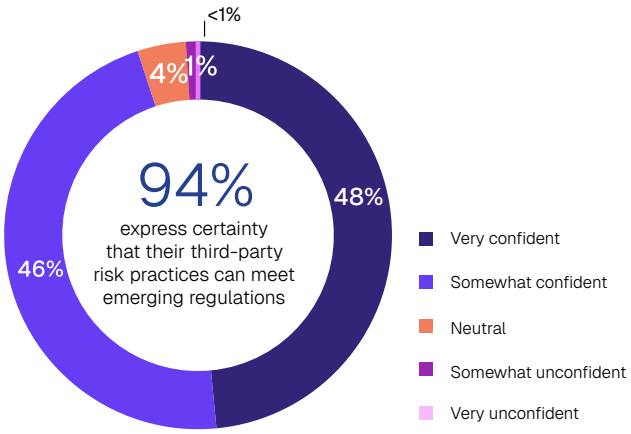
Which areas of third-party or supply chain compliance present the greatest challenges? (Select up to three)

- **49%** Keeping pace with changing regulations
- **40%** Aligning with multiple regulatory frameworks
- **38%** Varying vendor remediation
- **34%** Evidence documentation requirements
- **34%** Incident reporting requirements
- **32%** Demonstrating ongoing monitoring

A majority (94%) of respondents express certainty that their third-party risk practices can meet emerging regulations.

Yet despite their spoken confidence, **38% of leaders list regulatory pressures as a greater concern than talent shortages or a lack of supply chain visibility**. These findings show that compliance remains a major pain point that many organizations have yet to solve.

How confident are you that your third-party risk practices meet emerging supply chain cybersecurity regulations?



What specific events, challenges, or gaps most influence your level of concern?
(Select one)

38% Increasing regulatory pressure

22% Recent high-profile breaches

16% Lack of internal resources/tools

13% Lack of visibility into my own vendors

11% Merger, acquisition, or other change of ownership

Beyond compliance, the challenges in risk mitigation reveal notable year-over-year trends. In 2025, data overload and an inability to prioritize issues and threats ranked as the top barriers. This year, data overload fell to No. 3. **The new No. 1: Difficulties assessing vendors' security posture**. This comment from one survey respondent explains the reason behind the concern:

> *"Vendors are not answerable to us, and **we have no control over lack of or slow responses from them**. We have no visibility into investigations and remediations done by the vendor."*

What are your biggest challenges in managing supply chain cybersecurity risk?
(Select up to three)

35% Difficulty assessing security posture of vendors

32% Limited resources to dedicate to supply chain cybersecurity

30% Data overload; inability to prioritize issues and threats

28% Resistance or lack of engagement to remedy issues

27% Lack of visibility into the supply chain

23% Too many manual processes

Yesterday's supply chain security practices aren't strong enough

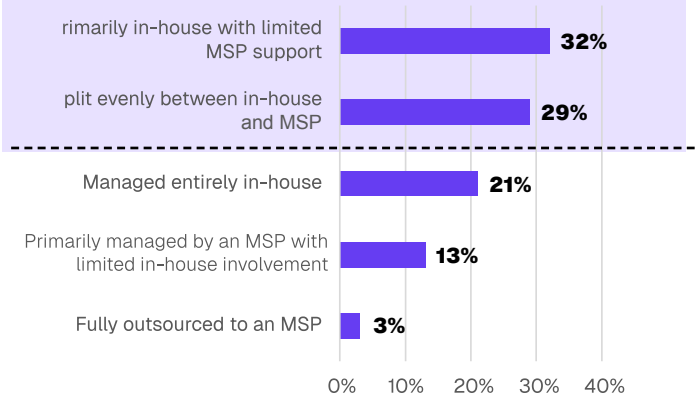
04

In an environment where bad actors can use AI tools to spin up attacks against third-party vendors at machine speed, relying on outdated practices like point-in-time assessments creates serious vulnerabilities. Yet while leaders say they're confident in their supply chain security postures, their actual practices don't match their level of assurance—further underscoring the third-party risk management paradox.

One possible reason for leaders' confidence is trust in their managed service providers (MSPs), with **79% either fully or partially relying on MSPs to manage their vendor ecosystem**.

79% either fully or partially relying on MSPs to manage their vendor ecosystem

Does your organization manage supply chain cybersecurity internally or via an external managed service provider?

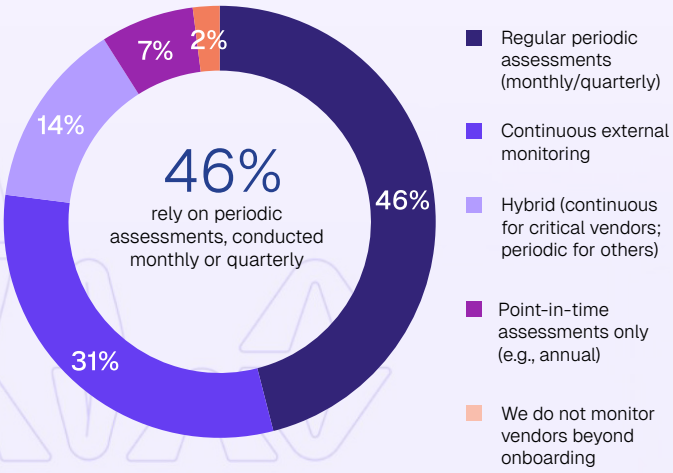


Annual audits and penetration testing are the most popular methods respondents use to ensure vendor compliance. **Another 46% of leaders rely on periodic assessments, conducted monthly or quarterly**. The encouraging news: Shared remediation or security platforms, which can help manage third-party risk in real time, are growing in popularity, with 37% of respondents using one.

Which methods does your organization use to ensure vendor compliance with cybersecurity requirements? (Select up to three)

- **53%** Annual audits or penetration tests
- **49%** Direct advisory support from our team
- **43%** Accepting vendor attestations (SOC 2, ISO)
- **38%** Contractual clauses (penalties/termination)
- **37%** Shared remediation or security platforms

Which best describes your approach to monitoring third-party cyber risk?



Respondents seem to agree that continuous monitoring is a priority, with 52% saying it's an integral part of their programs. **Yet 67% still list static security audits as their top risk-assessment method**, with tools and monitoring second and third. The disconnect could be caused by a lack of capacity or skills to do more frequent monitoring, or it could be that continuous monitoring is spread across teams. It also might mean that organizations' supply chain security postures are in the early stages of maturity.

Which components are part of your supply chain cybersecurity program? (Select all that apply)

- **52%** Continuous monitoring
- **50%** Employee security awareness training
- **45%** Cyber insurance coverage for supply chain incidents
- **44%** Vendor risk assessments
- **41%** Regular reporting to executive management/board
- **36%** Formal vendor onboarding and offboarding process

Which methods do you use to assess third-party risk? (Select all that apply)

67% Security audits

63% Third-party risk assessment tools

55% Continuous external monitoring

46% Penetration testing

41% Self-assessment questionnaires

1% We do not currently assess third-party risk

The conflicts in risk mitigation methods come down to where organizations stand on the TPRM maturity curve.

Level 1 **(least mature): Basic due diligence.** Performing cybersecurity reviews only during contracting

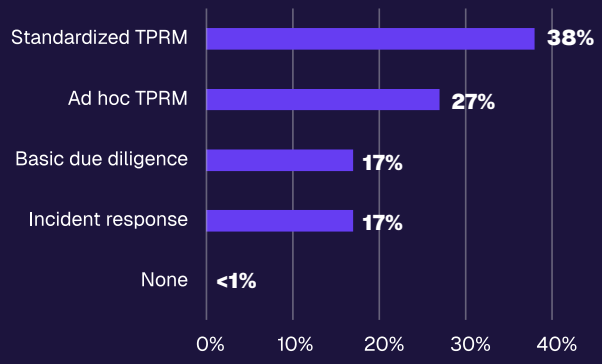
Level 2: Ad hoc (or periodic) TPRM. Following informal risk management policies and workflows

Level 3: Standardized (or continuous) TPRM. Implementing proactive breach prevention controls, including automated monitoring

Level 4 (most mature): Incident response (threat-informed TPRM). Performing rapid remediation of supplier security issues

While 43% of respondents are early in their maturity (basic due diligence and ad hoc TPRM), another **55% are more mature (standardized TPRM and incident response)**. What's interesting, however, is that the percentage of respondents using the highest levels of maturity dropped by 5 percentage points from 2025 to 2026, which shows there is plenty of work yet to be done.

What level of supply chain risk management does your organization perform?



Other response plan measures used by respondents underscore the importance of moving higher on the TPRM maturity curve. According to one leader:

*"Shifting from annual questionnaires to continuous, data-driven monitoring allows teams to **identify third-party risks, rather than relying on outdated, point-in-time reports**."*

Which supply chain incident response capabilities does your organization have? (Select all that apply)

58% Real-time threat intelligence feeds

56% Automated detection of high-risk vendor activity

48% Remediation tracking with evidence

43% Automated triage or escalation workflows

40% Correlation across multiple vendor issues

38% Shared vendor remediation platform

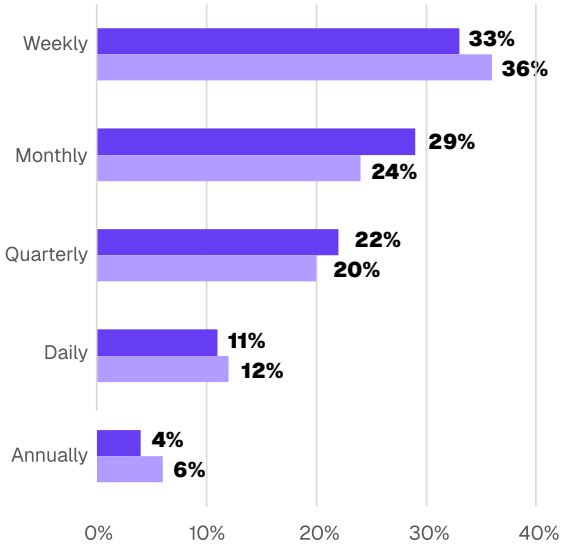
With incident response, time is not on your side

05

Supply chain incidents differ in size and scope. While organizations may have time to solve a newly discovered vulnerability or adapt to a change in a vendor's risk profile, critical incidents require fast remediation. But finding and responding to risks doesn't always happen quickly, respondents say.

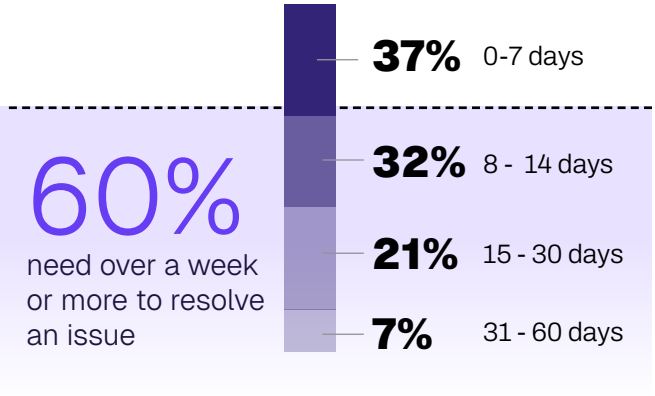
While 44% of leaders say they conduct third-party risk assessments daily or weekly, another 51% only conduct them monthly or quarterly. Additionally, 44% say they only update or re-evaluate their risk assessments of critical Tier 1 vendors monthly or quarterly.

- How often does your organization conduct third-party risk assessments?
- How often is your organization's risk assessment of its critical Tier 1 vendors updated or re-evaluated?

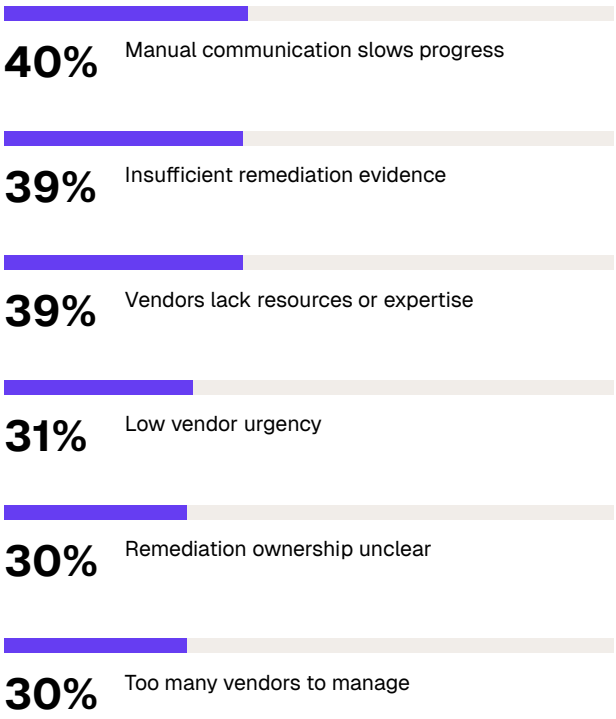


How quickly can respondents remedy a high-severity issue? While 37% of respondents can do it within 0 - 7 days, 60% need 8 - 60 days. **The No. 1 reason for slow response is poor, manual communication methods, cited by 4 in 10 respondents.**

What is the average time it takes a critical vendor to remediate a high-severity security issue?

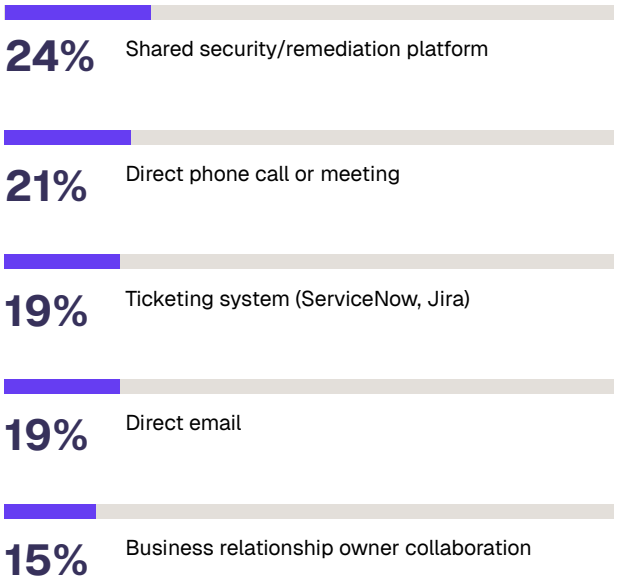


What are the biggest barriers to timely vendor remediation? (Select all that apply)



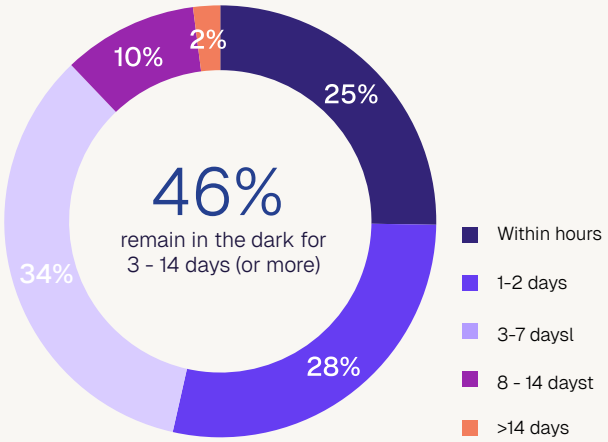
A closer look at vendor collaboration methods shows the disconnect. Among respondents, 24% leverage a shared security and remediation platform for streamlined, in-the-moment incident communication. **But 55% still rely on calls, meetings, emails, or key business contacts to remediate incidents—all of which take too long**. "If you wait to write an email, a bad actor has already encrypted, infiltrated, and ransomed the vendor's system before you even hit send," says SecurityScorecard's Barker.

How does your organization primarily collaborate with vendors during remediation? (Select one)



It also takes many organizations way too long to determine whether a critical vulnerability affects any of their third-party vendors. **While 25% of respondents know within hours, 46% remain in the dark for 3 - 14 days (or more)**.

How long does it typically take your organization to determine whether a newly announced critical vulnerability (e.g., zero-day) affects any of your third-party vendors?



Faster response requires better communication, as one respondent explains:

"Ensuring continuous feedback and reports from both ends, and also during a breach, SOC and TPRM should follow a single plan. If there is overall poor communication, it causes hours of delay."

Conclusion

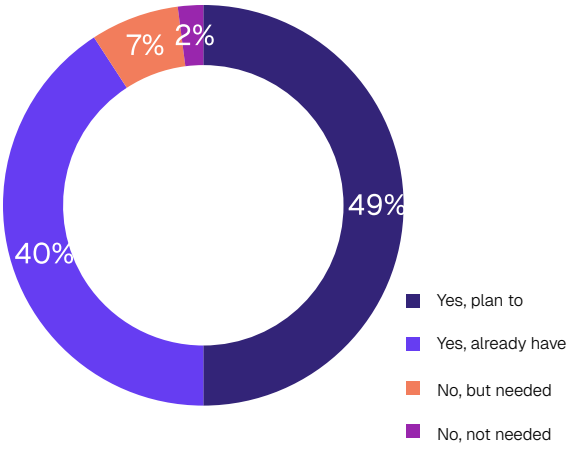
Close the confidence-protection gap with stronger threat intelligence

Annual audits, periodic assessments, and manual communication won't protect organizations against modern, fast-moving supply chain risks. To keep up, businesses need to adopt AI-enabled TPRM strategies that can automate insights and streamline workflows for detection and remediation tracking in minutes, not days or weeks.

The message is already being received by the **40% of respondents who have implemented a dedicated supply chain incident response function**. Another 49% say they "plan to develop one." But good intentions alone won't remediate supply chain risks. Organizations must act now to move their way up the maturity curve and close the gap between misplaced confidence and intelligence-led threat detection.

SecurityScorecard can help. Explore the power of actionable insights, AI, and automation for your supply chain cybersecurity. Learn more about our TITAN AI platform and sign up for a 14-day free trial.

Do you plan to develop a dedicated supply chain incident response function?



Firmographics

Countries represented

U.S.	58%
Canada	11%
UK	11%
South Africa	9%
Singapore/ Philippines/ Australia/New Zealand	7%
India	4%

Industries represented

Technology	27%
Manufacturing	24%
Financial services/ insurance	18%
Retail/ e-commerce	16%
Healthcare	7%

SecurityScorecard is the global leader in threat-informed third-party risk management (TPRM), securing the world's supply chains. The company delivers a modern, threat-informed approach to TPRM that enables organizations to drive out risk at the source. Through continuous visibility, AI-accelerated intelligence, and predictive insights, the platform transforms third-party risk into a competitive advantage, empowering organizations to proactively reduce risk before incidents occur and respond with confidence when they do, delivering measurable supply chain resilience.

Trusted by over 3,300 organizations, including 70% 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, Google Ventures, NGP Capital, Intel Capital, and Riverwood Capital, SecurityScorecard delivers end-to-end supply chain cybersecurity that safeguards business continuity.

Protect the supply chain behind your business.

Learn more at securityscorecard.com.