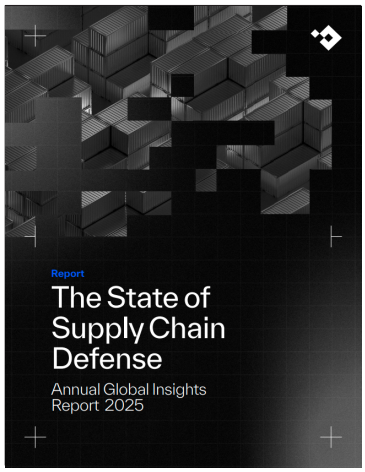


The State of Supply Chain Defense

Annual Global Insights Report 2025

Thank you for downloading this BlueVoyant case study. Carahsoft is the vendor, reseller, and OMG-Vendor for BlueVoyant solutions available via NASA SEWP V, ITES-SW2, NASPO ValuePoint, OMNIA, and other contract vehicles.

To learn how to take the next step toward acquiring BlueVoyant's solutions, please check out the following resources and information:

For additional resources:
carah.io/BlueVoyantResources

For upcoming events:
carah.io/BlueVoyantEvents

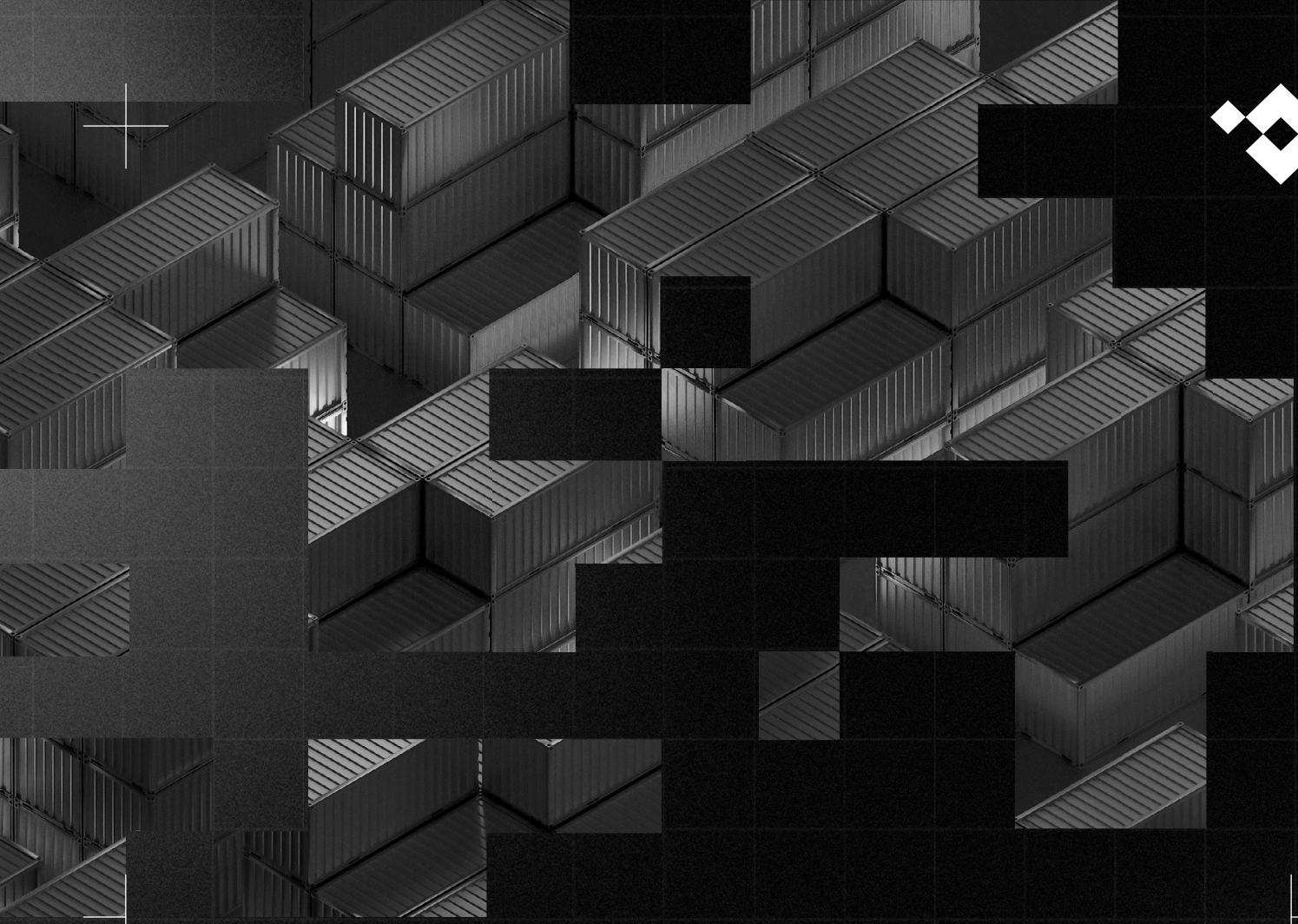
For additional BlueVoyant solutions:
carah.io/BlueVoyantSolutions

For additional cybersecurity solutions:
carah.io/Cybersecurity

To set up a meeting:
BlueVoyant@carahsoft.com
(888) 662-2724

To purchase, check out the contract vehicles available for procurement:
carah.io/BlueVoyantContracts

For more information, contact Carahsoft or our reseller partners:
BlueVoyant@carahsoft.com | (888) 662-2724



Report

The State of Supply Chain Defense

Annual Global Insights Report 2025

Foreword

Welcome to BlueVoyant's sixth annual report on the State of Supply Chain Defense.

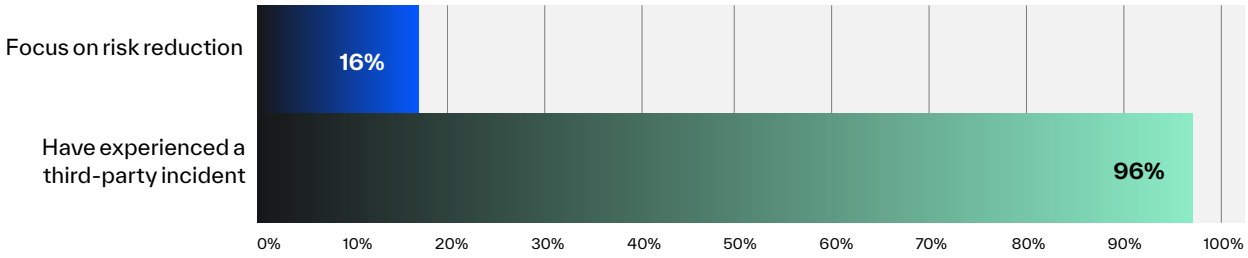
Over the past five years, we've chronicled the ups and downs of third-party risk management (TPRM) as it evolved from an immature awareness program to the established operational function it is today. This year, we refined our survey methodology to better reflect evolving priorities across industries and geographies. It's important to note that all of those surveyed were from organizations that had a risk-owner function.

It's no longer a question of "should we build this program?" but now, "how do we do this effectively?" This year's survey explores not only what organizations are doing, but how, why, and what gaps they're seeing.

The data reveals that as organizations invest heavily in tools, teams, and processes, the gap between program maturity and organizational commitment is widening. While there are bright spots, the overall direction suggests that mature programs don't automatically equal positive outcomes.

This year's report focuses on the following key themes:

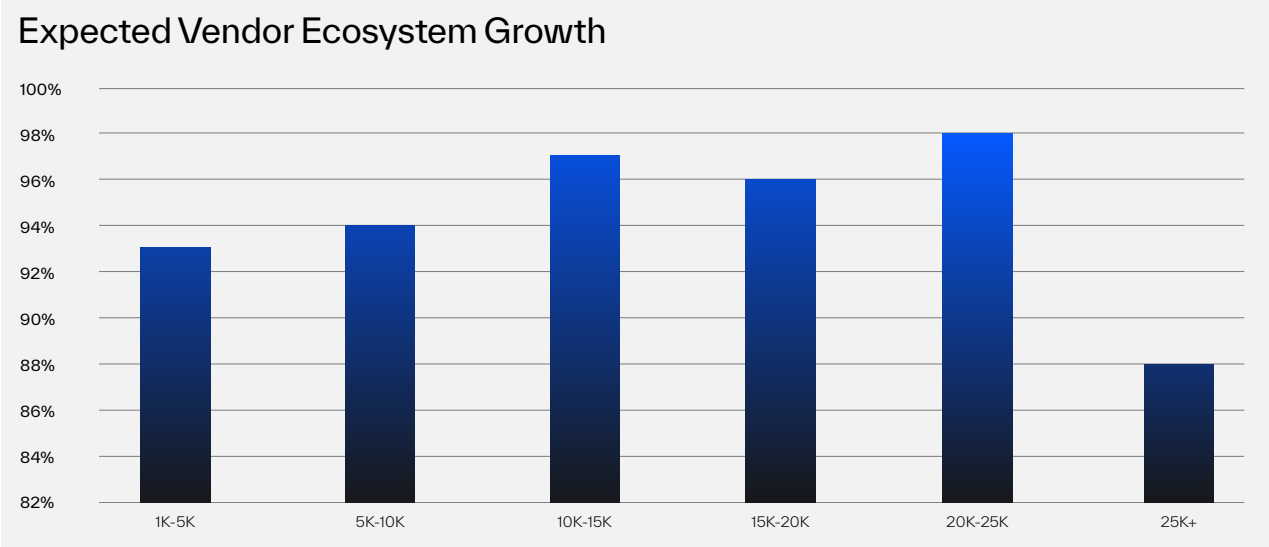
- **Operational challenges:** Despite growing maturity among surveyed organizations, TPRM programs face a widening gap in internal support and alignment. The strategy may be there, but tactically it's hard to execute without far-reaching support. To dive into this thought, we separated our challenge question to focus on both operational and organizational issues. With 60% of organizations citing internal resistance as a top barrier to program maturity and effectiveness, it's no wonder that it's hard to execute.
- **Compliance over risk reduction:** Organizations are building TPRM programs to check a compliance box and not necessarily reduce risk. Only 16% of respondents identified risk reduction as a primary program driver. Instead, they are motivated more by cyber insurance requirements, contractual obligations, and board mandates — all of which support compliance. While meeting minimum compliance requirements is critical, meaningfully reducing risk would lead to the same or better compliance result. Compliance is step one, not necessarily the end goal. The fact that 96% of respondents experienced a cyber incident at one of their suppliers underscores the need to focus on actual risk reduction.



- **Scale:** With 96% of organizations expecting to grow their vendor ecosystem over the next year, the attack surface continues to widen. But without organizational support and integration across tools and teams, silos will only continue to grow, limiting risk visibility.

One positive trend was the increase in organizations being proactive about working with their third-party vendors. While 19% of organizations rely on vendor attestation alone, 23% use external third-party monitoring, risk ratings, or threat intelligence feeds for verification. And with 45% of organizations working with vendors directly to remediate issues, this collaboration is a step in the right direction.

Ninety-six percent of respondents expect their vendor ecosystems to grow in the next year. Thirty-two percent expect their ecosystem to grow by 11-15%, and 35% expect 6-10% growth. Here's the breakdown by organizational size:



Percentage of global respondents expecting their vendor ecosystem to grow in the next 12 months by organizational size

In positive news, 95% of respondents estimated that their TPRM spending increased over the past 12 months to further support this growth and continue maturing their program.

We found that common challenges have shifted as priorities change. Organizations are fully aware of the risks their third-party vendors pose, but they're less clear on how to tackle the problem because of inconsistent organizational support. While the 2024 challenges were more tactical — knowing how to penalize vendors who don't fix issues and meeting regulatory requirements — this year's signal more of a systemic issue. There's less focus on what to do with vendors who aren't proactive about risk, and more focus on getting the organization in order internally.

Rank	2025 Top Challenges	2024 Top Challenges
1	Lack of integration to broader enterprise risk or GRC tools and processes already in use	Understanding how to penalize third parties/ suppliers when they don't respond or remediate issues
2	Getting suppliers to take remediation action when risks are identified	Meeting regulatory requirements and ensuring third-party cybersecurity compliance
3	Continuous monitoring of supplier risk posture	Enforcing SLAs with all our third parties/suppliers and getting them to comply

When it comes to AI, organizations identify this technology as best suited for continuous monitoring, recognizing that automation will be essential for maintaining visibility as the attack surface expands. Yet technology alone won't solve the fundamental challenges of organizational alignment and strategic prioritization.

For six years now, the goal of this report has been to raise awareness and understanding for building a TPRM program. As organizational attitudes and priorities evolve, we're excited to share our 2025 findings.

Methodology

BlueVoyant commissioned its sixth annual survey undertaken by independent research organization, Opinion Matters, in September 2025.

Eighteen hundred chief information officers (CIO), chief information security officers (CISO), chief operating officers (COO), chief security officers (CSO), chief technical officers (CTO), and chief procurement officers (CPO) responsible for supply chain and cyber risk management were surveyed. The respondents represented organizations with 1,000-plus employees across a range of industries including: financial services, healthcare and pharmaceutical, utilities and energy, retail, manufacturing, and defense. To gain a global perspective, the research was conducted in the following countries/regions: U.S., Canada, DACH (Germany, Austria, Switzerland), the U.K., APAC (including Australia, Malaysia and the Philippines), Japan, and Singapore. The data was collected between September 16 and September 25, 2025.

Table of Contents

07 — At a Glance

08 — Key Findings

11 — Vertical Market Analysis

- 11 — Financial Services
- 12 — Healthcare and Pharmaceutical
- 13 — Energy and Utilities
- 14 — Retail
- 15 — Manufacturing
- 16 — Defense

17 — Region-Specific Analysis

- 17 — Global insights: Program maturity
- 19 — U.S. and Canada
- 20 — U.K.
- 21 — DACH (Germany, Austria, Switzerland)
- 22 — APAC (Australia, Philippines, Japan, Malaysia, and Singapore)

23 — Final Thoughts

24 — Data Appendix

At a Glance

97%

97% of organizations were negatively impacted by at least one breach in their supply chain

Despite growing budgets and maturity, this is a telling increase from 2024's 81%.

60%

60%* of companies say internal buy-in is a top challenge

Organizations understand the criticality of TPRM programs yet struggle to gain support across the company.

45%

45% are working directly with third parties to remediate issues**

This represents a welcome shift toward collaboration and accountability.

96%

96% of organizations expect their vendor ecosystem to grow

As the attack surface expands, an effective TPRM program is more important than ever.

**60% is a total of three separate answers from the question, "What, if anything, is the top organizational challenge to maturing your organization's Third-Party Risk Management program?": Internal resistance to change that may be required to mature our Third-Party Risk Management program (25%); Collaboration across all the key internal stakeholders (21%); and Executive support (14%).*

***45% is a composite of two responses from the question, "If you find a problem with regards to your Third-Party's cybersecurity, how do you go about remediation?": "We work with the Third Party each step of the way until the issue is rectified" (23%); and "We identify the problem with the Third Party and help them to find a solution" (22%).*

Key Findings

Observation 1: As TPRM programs mature, they're lacking internal support

Program maturity does not guarantee effectiveness. While nearly half (46%) of organizations report established and optimized TPRM programs, we see a troubling gap between maturity and organizational support. Despite years of investment and awareness, TPRM initiatives continue to struggle to gain internal alignment.

One reason could be executive engagement. With only 24% of organizations briefing senior leadership on security matters monthly or more often, the majority (59%) only hold these briefings every three to six months. Without this visibility, executives likely won't throw their support behind a program they don't understand or aren't fully aware of.

With 60% of respondents citing internal challenges — resistance to change, collaboration across all the key internal stakeholders, and executive support — the challenges run deep. One industry that saw big changes in the past year was financial services. Once an industry benchmark, we noted those reporting established or optimized programs at only 36%, and just 17% report briefing senior leadership monthly or more. This tells us that maturity is not a single destination, but rather a living program that requires engagement and support.

Observation 2: Reducing risk may be taking a back seat to compliance

Our data suggests that some organizations are building TPRM programs based on compliance check boxes, rather than truly reducing risk. Only 16% of respondents listed risk reduction as the primary program driver, while cyber insurance requirements, contractual obligations, and board mandates came out on top. Though a compliance-first mentality may feel like the right path, risk reduction efforts would likely get organizations to the minimum compliance baseline, if not better.

Organizations increasingly recognize supply chain risk as a cybersecurity imperative, with 36% of programs now housed within either cyber/information security or information technology teams — a positive shift from previous years. While these teams are naturally risk-oriented, 64% of programs reside in other functions and compliance-focused teams such as legal, finance, and procurement. These departments are structurally oriented toward meeting contractual and regulatory requirements, not proactively reducing exposure. Compliance mandates set a minimum threshold for organizations to achieve. With 97% of organizations experiencing at least one breach in their supply chains, checking the compliance box can lead to a false sense of security. Compliance is step one, but risk reduction should be the ultimate goal.

Observation 3: Gaps in integration lead to silos and inefficiencies

While organizations have made investments into TPRM tools and processes, many have neglected to integrate those into broader enterprise risk frameworks. Sectors like financial services, manufacturing, defense, and retail all listed a lack of integration as a top pain point.

A fragmented program unfortunately leads to fragmented results. When teams operate in silos, the entire organization loses risk visibility. Gaps in integration make for inefficient workflows, disconnected reporting, and slow responses to incidents — all of which makes it difficult to prove value to a potentially skeptical senior leadership team. Fortunately, there have been some positive shifts. Forty-five percent of organizations now report working directly with vendors for remediation, a notable shift from monitoring vendors to partnering with them.

When teams come together with a joint goal of reducing risk, resources work more effectively and value is clearer.

Observation 4: Vendor ecosystem growth often surpasses program maturity

An overwhelming 96% of organizations plan to grow their third-party ecosystems over the next year, with some sectors like healthcare projecting double digit expansion. This begs the question — what are these organizations doing to manage this growth? Unfortunately, many organizations are adding vendors faster than they're adding visibility, validation, or remediation capacity.

Another area of focus is vendor risk tiering. Our survey found that more than half (57%) of companies consider 30-50% of their suppliers to be critical. When this much of a vendor population is considered "critical," the term loses its meaning. If half your vendors are critical, you may be lacking a strong prioritization strategy. This yields an overwhelming attack surface with no clear way to allocate limited resources.

This lack of a sophisticated tiering system is even more concerning the bigger your ecosystem grows. Basing prioritization on factors like contract value or operational criticality fails to capture the full picture of risk, such as access to sensitive data, security posture, and the potential for cascading failures.

Finally, too narrow a focus on compliance means risk reduction takes a back burner. As organizations grow their third-party ecosystem, knowing where your risks lie is critical.

Observation 5: Positive trends

Despite the gaps between maturity and effectiveness, there are several encouraging trends to note.

Collaborative vendor management remains high, with 45% of organizations working directly with third parties to remediate issues.

Structural improvements are also taking hold as TPRM program ownership consolidates. Thirty-six percent of programs now sit within security-focused teams, such as cyber and information security and IT. While not the majority, this trend is going in the right direction.

Financial commitment across organizations is also increasing. With 95% of organizations estimating that their spending increased this year, leadership is making TPRM a priority.

Finally, the defense sector continues to prove that maturity and internal alignment deliver the best outcomes. With 60% reporting established or optimized programs, 30% conducting monthly or more frequent executive briefings, and 47% collaborating with vendors, this sector sets the standard for risk management.

BlueVoyant's TPRM Recommendations

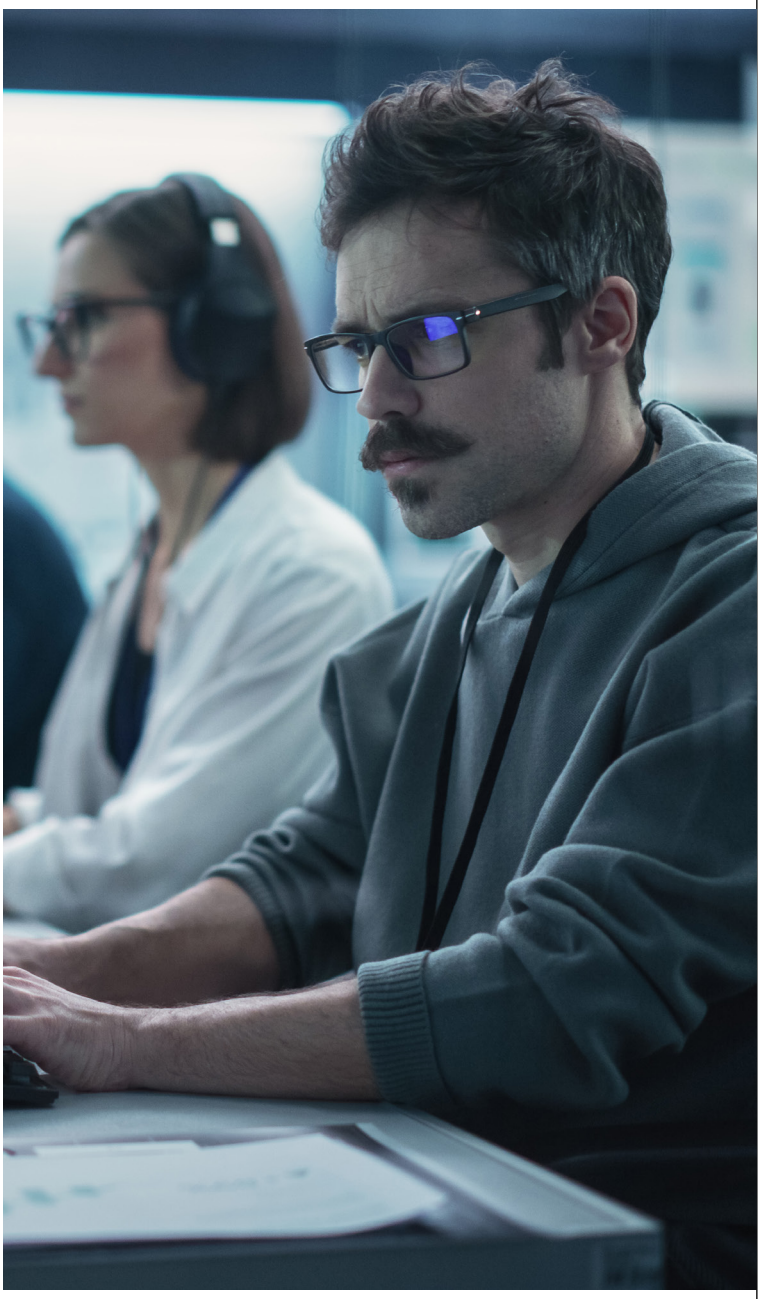
Monitor all vendors continuously and regularly evaluate and refine vendor prioritization and tiering.

Base vendor tiering on risk (rather than other considerations like contract value), with a specific focus on remediation for critical vendors.

Increase reporting and collaboration across different organizational functions and ramp up regular briefings to senior management to build visibility and program buy-in.

Collaborate directly with third parties on remediation to more effectively close the loop on resolving issues and mitigating risk.

Codify AI-driven vendor assessment workflows that tailor actions and analysis by vendor type, improving efficiency, scalability, and coverage across the vendor portfolio.



Vertical Market Analysis

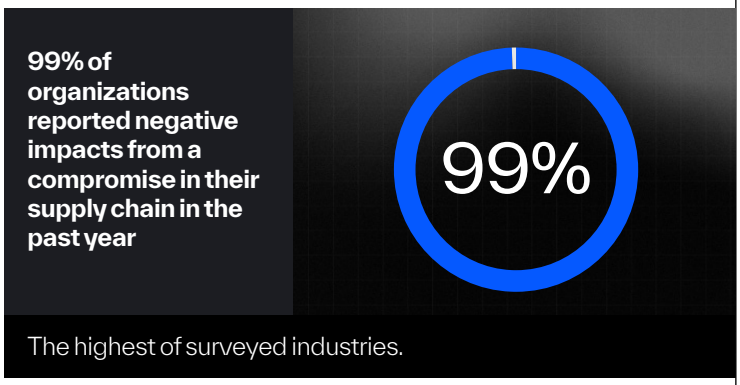
Financial Services

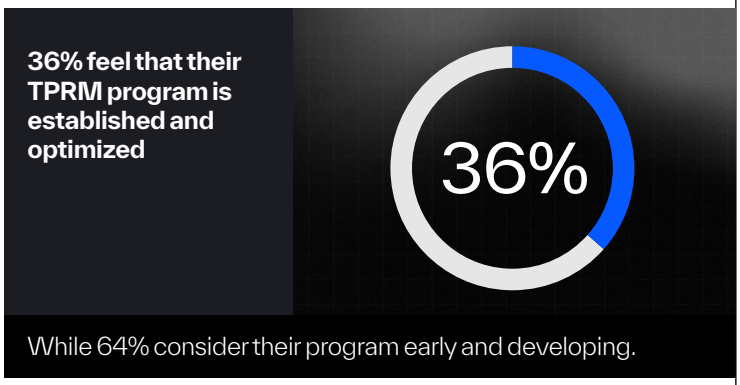
At a Glance

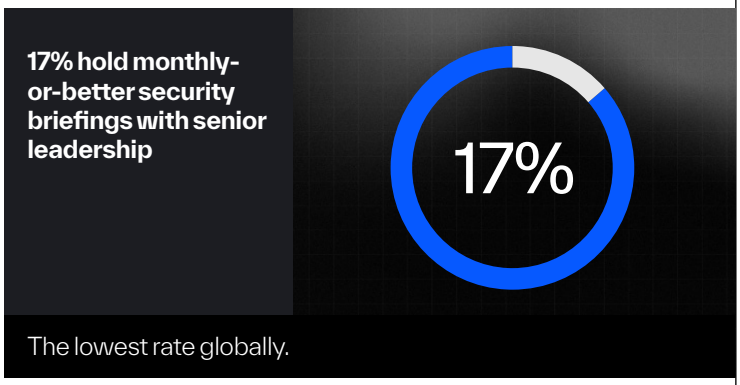
- **Most frequently used tools:** Software Bill of Materials (SBOM) (35% frequently); Risk questionnaires (34% frequently); External security ratings (31% frequently)
- **Risk tiering most commonly based on:** Yearly contract value
- **Department most likely to own third-party cyber risk:** Finance
- **Top 3 challenges and pain points:**
  1. Internal resistance to change
  2. Collaboration across key stakeholders
  3. Lack of integration to broader enterprise risk or GRC already in use

The financial services sector saw a major shift in its TPRM posture this year. With 64% of organizations calling their programs early or in developing stages, organizations may be feeling the effects of siloed teams and low internal support. With 34% citing internal resistance to change as their biggest challenge, it seems that the internal situation is rocky.

One area of concern is the low percentage of organizations — just 17% — reporting that they brief senior leadership on security on a monthly-or-better basis. Ninety-nine percent of organizations experienced breaches in the past year, the highest among surveyed industries and a clear sign of systemic issues. With TPRM ownership mostly sitting in finance departments rather than a security function, and programs driven by yearly contract value, a check the box approach doesn't seem to be delivering meaningful outcomes.







Healthcare and Pharmaceutical

At a Glance

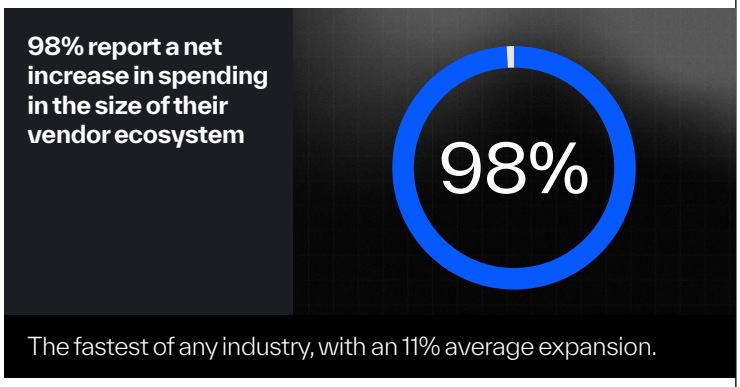
- **Most frequently used tools:** Software Bill of Materials (SBOM) (35% frequently); External security ratings (35% frequently); Penetration tests of Third-Party systems or applications (32% frequently)
- **Risk tiering most commonly based on:** Level of access to critical data
- **Department most likely to own third-party cyber risk:** Cyber or information security
- **Top 3 challenges and pain points:**
  1. Internal resistance to change
  2. Collaboration across key stakeholders
  3. Getting suppliers to take action to remediate risks we identify

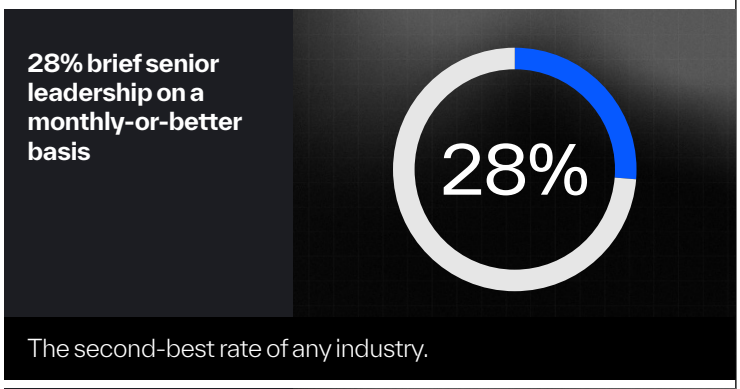
The healthcare and pharmaceutical sector demonstrates improvements across the board in its approach to TPRM. Though the sector struggled in the past with technology limitations, organizational buy-in, and operational maturity, organizations are making the right changes to strengthen TPRM initiatives. And this progress arrives just in time: healthcare faces the fastest ecosystem growth of any industry at an average of 11% over the next 12 months.

One positive indicator is the second highest rate of monthly-or-better senior leadership briefings at 28%. When leadership is aware and bought in, the program is more likely to thrive. With 98% of organizations reporting an expected net increase in spending with vendors, having a mature program in place will be more important than ever. This growth can likely be attributed to the digitalization of the industry and continued reliance on third-party services, from cloud infrastructure and telehealth platforms to pharmaceutical supply chains.

Unfortunately, this industry also averaged 4.1 breaches that negatively affected their supply chain in the past year, the highest rate among the sectors surveyed. The top reported pain point — getting suppliers to remediate identified risks — signals an ongoing challenge with vendor accountability and responsiveness.

With a focus on tiering vendors based on level of access to critical data, the industry is prioritizing protecting sensitive healthcare information. This approach will help the industry keep up with evolving regulatory requirements and privacy regulations.





Energy and Utilities

At a Glance

- **Most frequently used tools:** Software Bill of Materials (SBOM) (28% frequently); Onsite assessments (28% frequently); TPRM module as part of a GRC platform (28%)
- **Risk tiering most commonly based on:** Criticality to operations
- **Department most likely to own third-party cyber risk:** Cyber or information security
- **Top 3 challenges and pain points:**
  1. Collaboration across all key internal stakeholders
  2. Internal resistance to change
  3. Volume and complexity of third-party relationships

The energy and utilities sector manages some of the largest and most complex supply chains around the world. As critical infrastructure, building a successful TPRM program requires not only integrated tools, but support from across the organization.

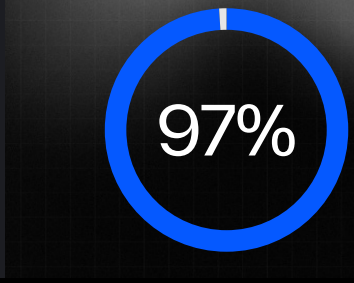
This year, energy and utilities reported the lowest rate of supply chain compromises among all sectors, with 95% negatively impacted by a breach. While still a high number, the data reflects meaningful progress for an industry faced with constant, sophisticated attacks.

Another positive note is the industry's oversight of its vendors. With 44% outsourcing remediation and vendor engagement activities, companies can focus on managing their most critical suppliers and ensuring issues are quickly addressed.

One of the industry's top challenge is the volume and complexity of third-party relationships. Energy and utilities organizations rely on a complex web of equipment manufacturers, suppliers, and technology vendors. When combined with distribution of assets across the world and operations, that complexity is only compounded.

Respondents marked cyber insurance requirements as the primary driver of TPRM programs. As insurers have tightened underwriting standards and increased scrutiny of supply chain security practices (often following high-profile incidents), organizations have responded by strengthening their TPRM capabilities to meet coverage requirements and manage premiums.

97% expect their third-party ecosystem to grow over the next 12 months

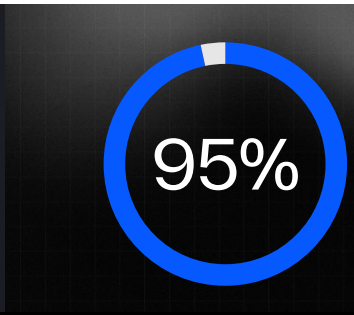


A continued trend of expanding vendor networks.

3.6 average data breaches negatively affecting their supply chain

Among the lowest across sectors.

95% negatively impacted by a breach



The lowest rate among surveyed industries.

Retail

At a Glance

- **Most frequently used tools:** TPRM module as part of a GRC platform (37% frequently); Risk questionnaires (36% frequently); Onsite assessments (34% frequently); Continuous monitoring (34% frequently)
- **Risk tiering most commonly based on:** Criticality to operations
- **Department most likely to own third-party cyber risk:** Cyber or information security
- **Top 3 challenges and pain points:**
  1. Collaboration across internal stakeholders
  2. Executive support
  3. Lack of integration to broader enterprise risk or GRC already in use

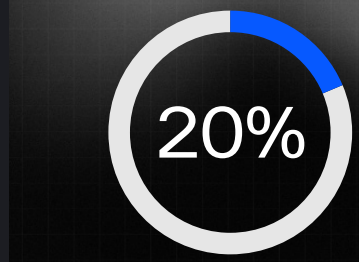
The retail sector presented strong results in breach prevention, while maintaining practices that signal a more hands-off, trust-based approach to TPRM than other industries.

Though historically vulnerable to payment card breaches or point-of-sale compromises, this year the industry reported an average of 3.1 supply chain breach incidents. This could signal improving maturity after years of data breach headlines plagued the industry.

On the vendor management side, there are a few concerning trends. Retail demonstrated the lowest rate of working directly with third parties to remediate issues at 43% collaborating with vendors on remediation, and just 19% working directly with the vendors. Notably, 20% of respondents that use risk questionnaires as part of their TPRM said they rely on vendor attestation alone to validate third-party responses to security questionnaires, the highest among surveyed industries. This reliance on self-reporting without outside verification represents a concerning gap.

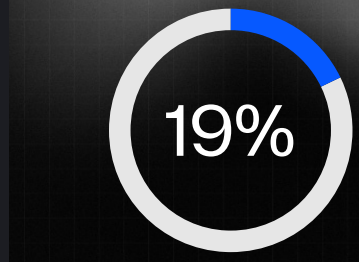
Like financial services and manufacturing, retail identified a lack of integration with broader enterprise risk or GRC tools and processes as a top challenge. When managing a web of suppliers like logistics, payment processors, e-commerce platforms, and merchandise suppliers, gaps in integration can significantly impair risk visibility.

20% rely solely on vendor attestation to validate security questionnaires



Other industries lean on external monitoring, risk ratings, and vendor system assessments.

Just 19% work directly with their vendors all the way through remediation



Among the lowest rates for direct vendor engagement.

3.1 average supply chain breaches in the past year

The lowest average among surveyed industries.

Manufacturing

At a Glance

- **Most frequently used tools:** External security ratings (38%); Risk questionnaires (37%); TPRM module as part of a GRC platform (36%); Software Bill of Materials (SBOM) (36%); Breach reporting services (35%); Continuous monitoring (35%)
- **Risk tiering most commonly based on:** Level of access to critical data
- **Department most likely to own third-party cyber risk:** IT
- **Top 3 challenges and pain points:**
  1. Internal resistance to change
  2. Collaboration among stakeholders
  3. Lack of integration to broader enterprise risk or GRC tools and processes already in use

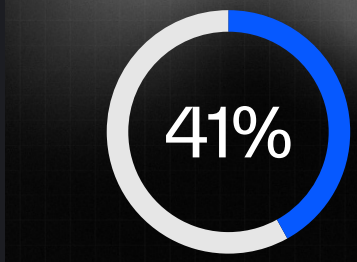
The manufacturing sector maintains a large and complex supply chain system. With an average of 3.8 supply chain breaches per organization this year, disruptions can cascade worldwide. A large attack surface and persistent threats across its interconnected networks means that TPRM is directly supporting operational continuity.

Compared to 2024's top priority of understanding how to penalize suppliers when they don't remediate an issue, this year respondents cited a lack of integration across tools and platforms. Compared to other industries, manufacturing organizations marked multiple solutions that they use frequently, telling us that TPRM is a high priority. Unfortunately, if these solutions aren't seamlessly integrated they could be missing out on the full picture of risk.

Despite these investments, the industry shared that 58% of its TPRM programs are considered early and developing. As the second lowest rate of maturity, this is surprising given that board and executive mandates reportedly drive TPRM programs. This could signal a disconnect between leadership strategy and program execution.

Finally, the sector's approach to risk tiering based on level of access to critical data reflects concerns around protecting intellectual property, securing operational technology, and the potential for supply chain attacks to compromise sensitive manufacturing processes or product designs.

41% of organizations outsource analysis of data and results from monitoring



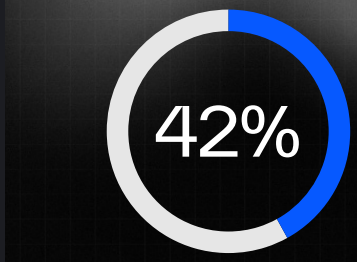
This can drive internal resources to focus on higher value work.

3.8 average breaches negatively affect supply chains

3.8

Manufacturing is no stranger to advanced, persistent threats.

42% of respondents described their TPRM program as established and optimized



The second lowest rate among industries.

Defense

At a Glance

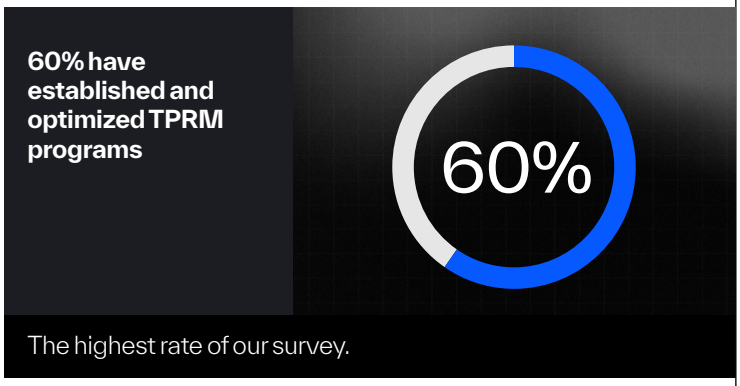
- **Most used tools:** Breach reporting services (39%); TPRM module as part of a GRC platform (37%); External security ratings (37%)
- **Risk tiering most commonly based on:** Yearly contract value
- **Department most likely to own third-party cyber risk:** Cyber or information security
- **Top 3 challenges and pain points:**
  1. Internal resistance to change
  2. Lack of integration to broader enterprise risk or GRC tools and processes already in use
  3. Collaboration across internal stakeholders

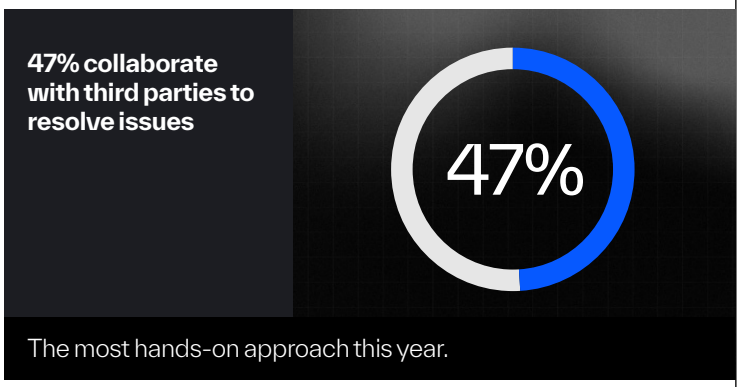
The defense sector maintains its status as the most mature and strategically focused industry.

Defense organizations lead all sectors with the highest rate of established and optimized TPRM programs at 60%, nearly double that of financial services and manufacturing. Years of continued investment, regulatory pressure, and awareness of supply chain vulnerabilities have proven effective.

Defense leads the way in executive engagement, with 30% of respondents briefing senior leadership on security monthly or more. Defense also takes a collaborative approach to vendor management, with 47% of respondents working with their third parties every step of the way, including 25% doing so directly until the issue is resolved.

Despite consistently strong programs, the industry still saw an average of 3.5 data breaches within its supply chain, a sign of just how sophisticated the threats have become. As with other sectors, defense respondents listed a lack of integration of broad enterprise risk and GRC tools as its top pain point. Even the most mature programs have their integration challenges.

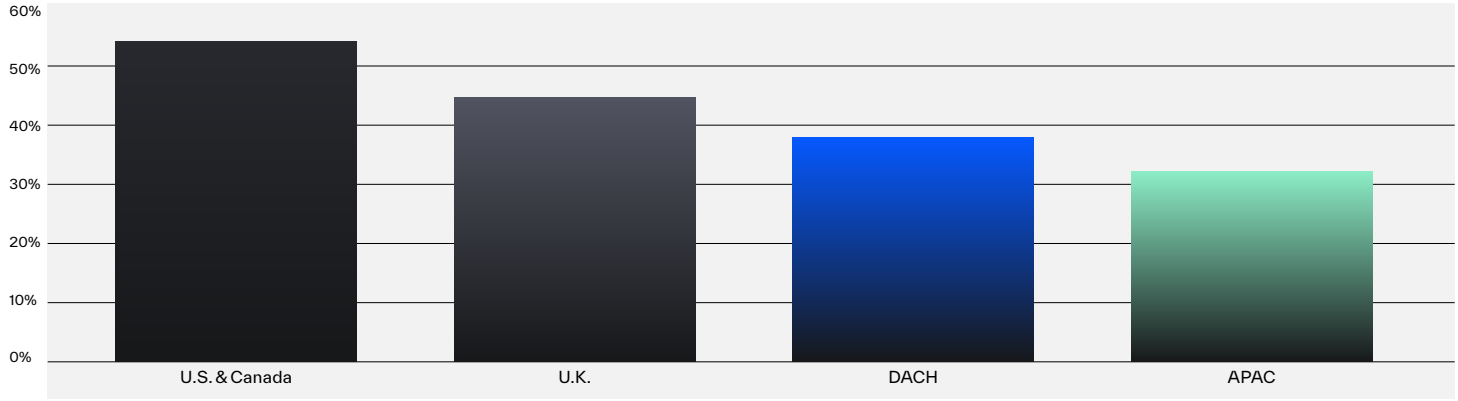




Region-Specific Analysis

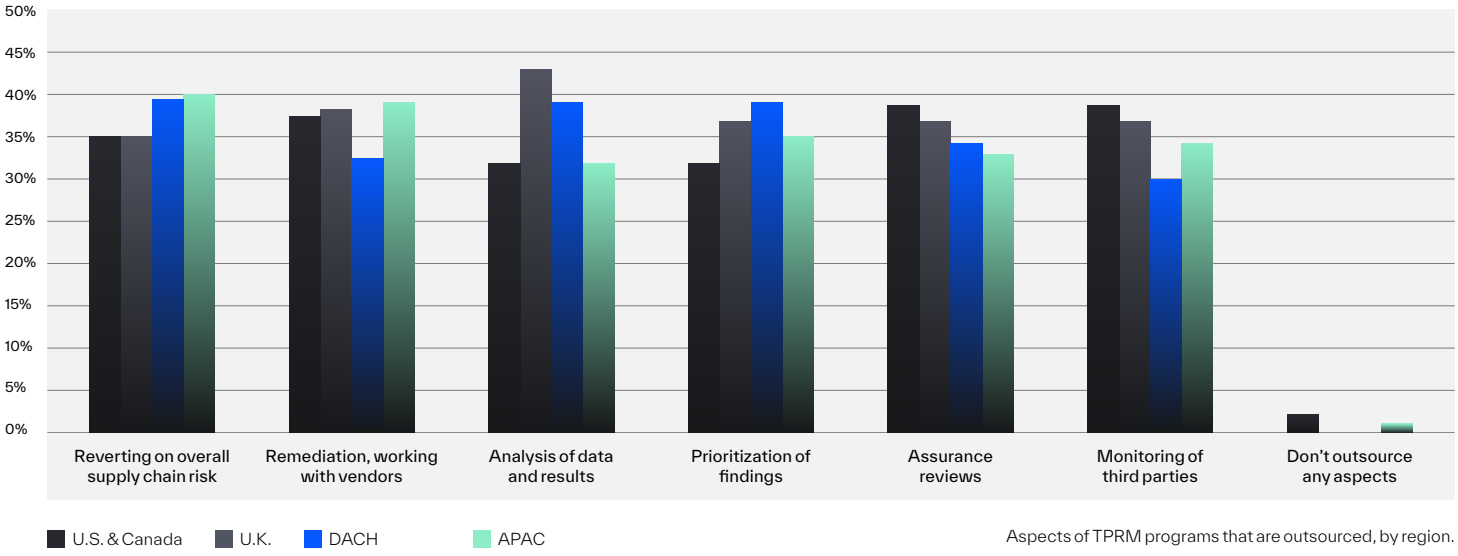
Global insights: Program maturity

Established and Optimized TPRM Programs



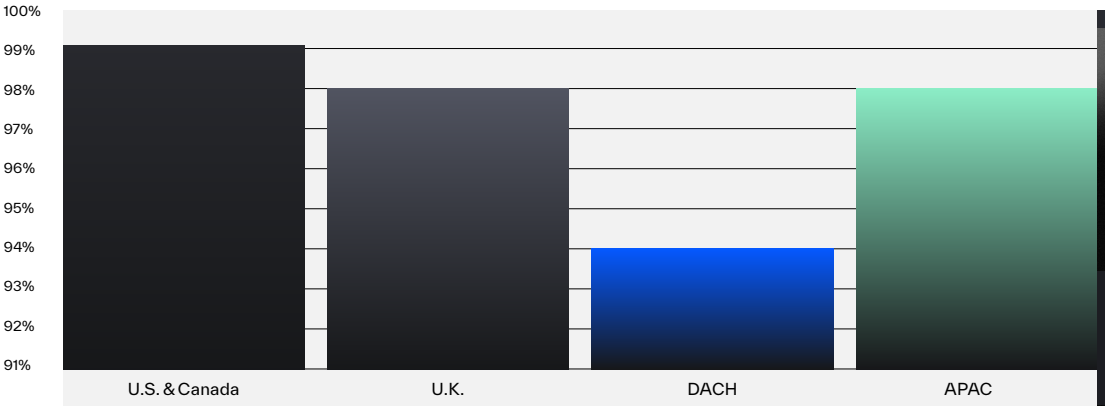
Percentage of programs considered established and optimized by region.

Outsourced Aspects of TPRM Programs



Aspects of TPRM programs that are outsourced, by region.

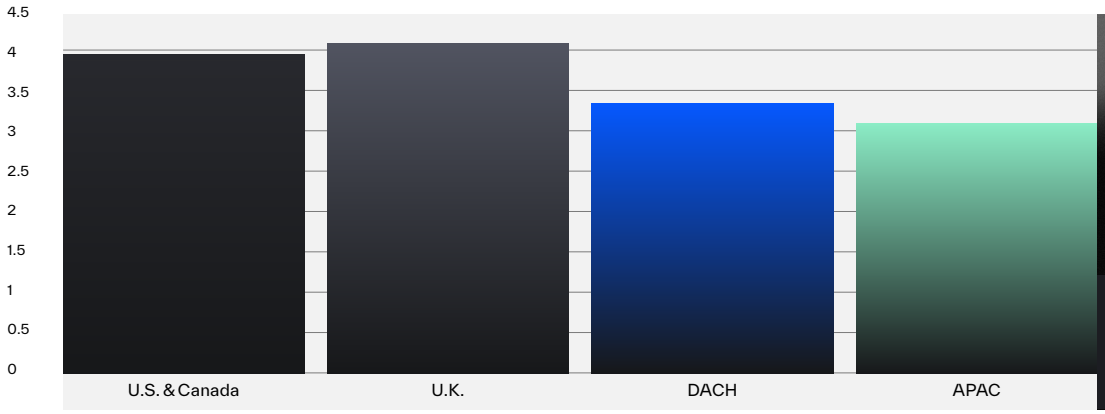
Organizations Negatively Impacted by a Supply Chain Breach



97%
Globally

An average of 97% of global respondents say they were negatively impacted by a supply chain breach.

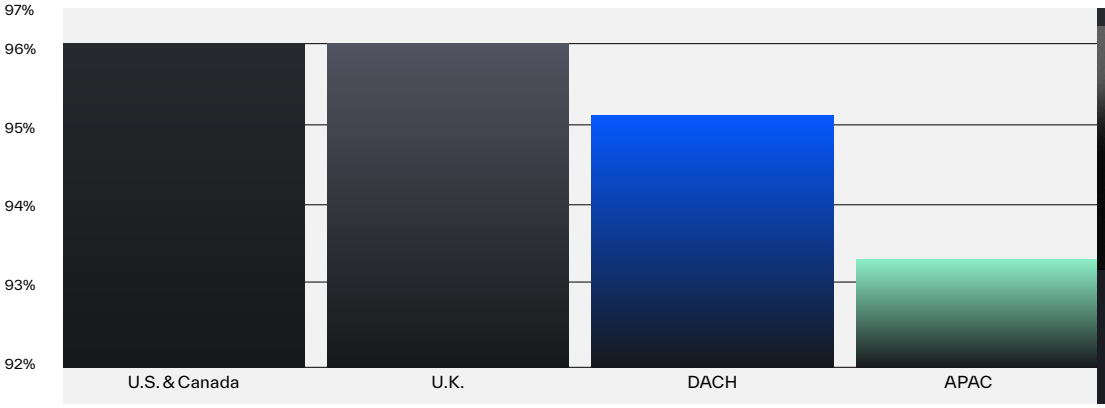
Mean Number of Supply Chain Cyber Breaches



3.7
Globally

The mean number of breaches reported from all global respondents was 3.7.

TPRM Budget Increases



95%
Globally

An average of 95% of global respondents estimate that their spending increased in the past year.

U.S. and Canada

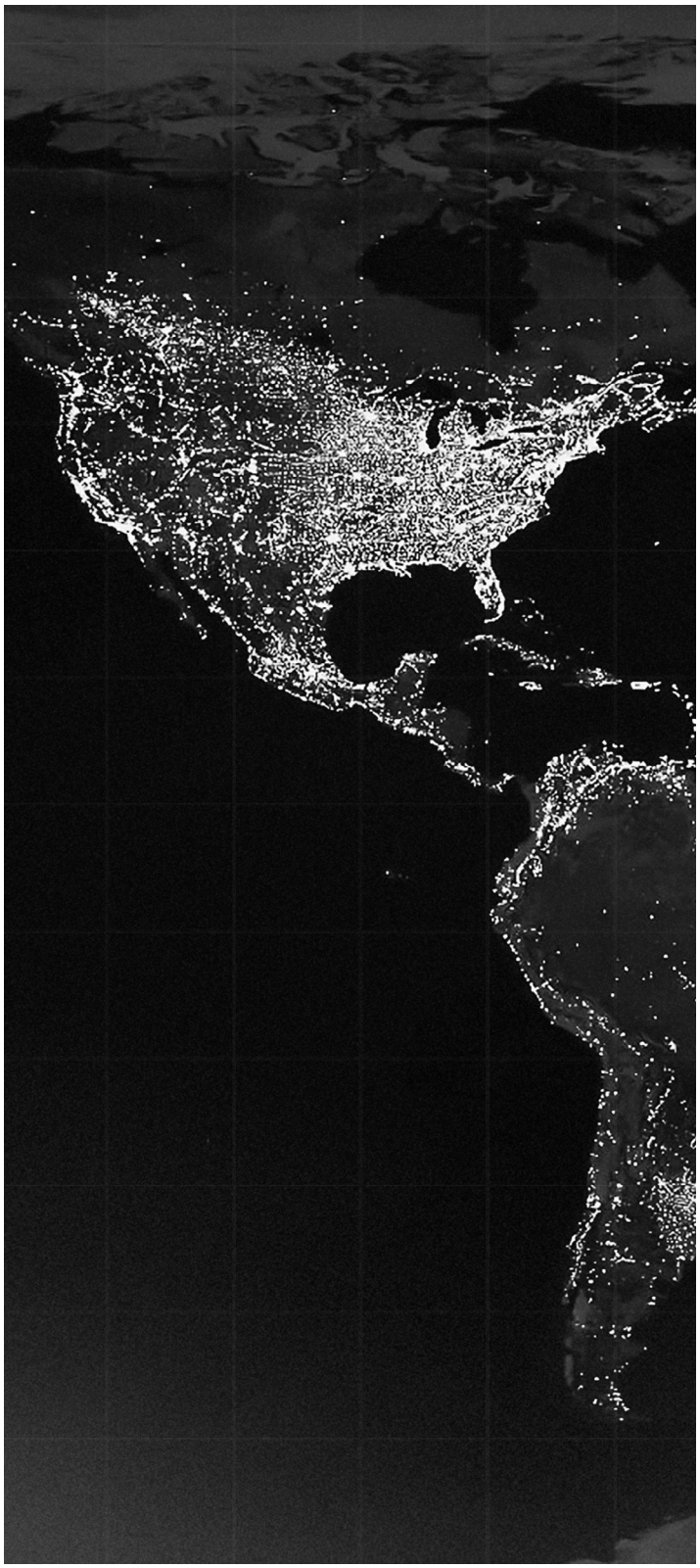
The U.S. and Canada region leads globally in TPRM program maturity, with 54% of organizations reporting an established and optimized program. The U.S. also demonstrates the strongest executive involvement, with 34% of companies briefing senior management on a monthly or more basis. Compared with just 18% in 2024, this 16% increase is a big step in the right direction.

Despite more mature programs, the region is not immune to sophisticated threats. Ninety-nine percent of organizations were negatively affected by supply chain breaches over the past year, averaging 3.9 incidents per organization. Compared to 89% in 2024, this is a 10% increase. This could be due to an increase in attacks, or simply better detection.

When comparing the two countries, Canada reports the highest average breach rate of any country surveyed at 4.4 incidents per year. While the U.S. may have stronger program control, organizations there expect ecosystem growth of just 8% on average.

Both countries listed cyber insurance requirements as their primary program driver, and the top challenge was the lack of integration with broader enterprise risk and GRC tools, cited by 17% of respondents.

Signs point toward strong financial commitment, with 96% of respondents estimating that spending increased. Organizations will need to get their houses in order to be fully effective, focusing on strategic alignment and tool integration.



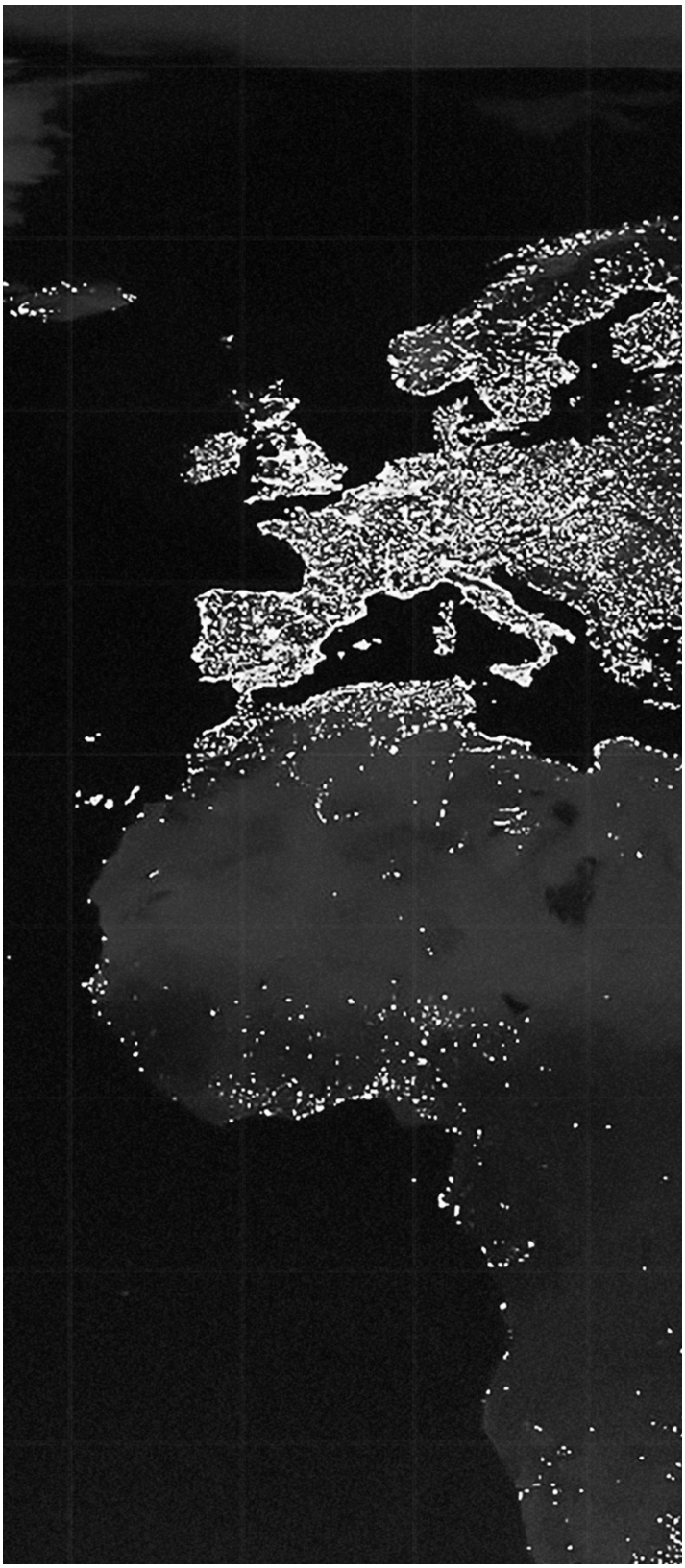
U.K.

The U.K. shows an interesting disconnect between investment and positive outcomes. Though 45% of organizations reported established and optimized programs (about midway between the U.S. and Canada, and DACH), the region still experienced the highest average breach rate at 4.1 incidents per organization. Ninety-eight percent of organizations reported negative impacts from supply chain breaches, a nearly 4% increase over 2024 (95%).

The U.K. leads all regions in outsourcing data analysis at 43%, which is the second-highest rate globally. This tells us that while organizations are collecting substantial data, they may not be translating it into actionable results that help reduce risk.

One area of concern — only 16% of organizations in the U.K. reported briefing their leadership team monthly or more, the lowest rate across the globe. Without executive input and organizational support, programs will struggle to be strategic. Compared to 24% in 2024, this area has decreased.

Organizations reported the highest expected ecosystem growth at 11% and say their tier vendors are primarily based on contract value. As their attack surface widens with the addition of new vendors, these organizations may struggle if they don't consider risk factors like data access or operational criticality.



DACH (Germany, Austria, and Switzerland)

The results out of DACH revealed a combination of trust-based management and potential strategic misalignment. With only 39% of organizations reporting established and optimized (the second lowest across the globe), the region actually showed the lowest breach impact of any region at 94%. However, compared to 88% in 2024, this is still a concerning increase.

The region reported that 23% of organizations rely solely on vendor attestation from risk questionnaires in TPRM, the highest rate globally. Switzerland specifically leads this approach at 29%, while at the same time reporting the highest adoption of dedicated TPRM platforms at 40%.

We also found that executive engagement across the region was low. Twenty-six percent of DACH organizations brief leadership annually or less, the lowest rate globally. Germany and Switzerland lead this point, with around 30% of their organizations providing updates yearly or less. Only 21% of DACH organizations brief leadership monthly or better, which can create a vacuum.

One extreme case is Austria, which saw 100% of organizations reporting supply chain breaches and 42% either relying on third parties to self-remediate issues or having no way of knowing if an issue even arises. These rates are the lowest in these categories.

Fortunately, it's not all bad news. Organizations also seem to be doing more with less, outsourcing 39% of reporting functions. Ninety-five percent of organizations estimated spending increased in the past year. More investment is helpful, but the region will need to focus on executive engagement to remain strategic.

APAC (including Australia, Philippines, Malaysia), Japan, and Singapore

This year, we surveyed organizations across Australia, the Philippines, Malaysia, Japan, and Singapore. The results were some of the most diverse, which isn't surprising given the range of economic and cultural nuances across this region.

APAC reported the lowest program maturity (for established and optimized programs) among countries surveyed at 32% (nearly half the rate of the U.S. and Canada), yet they averaged just 3.1 supply chain breaches per organization, lower than the global average.

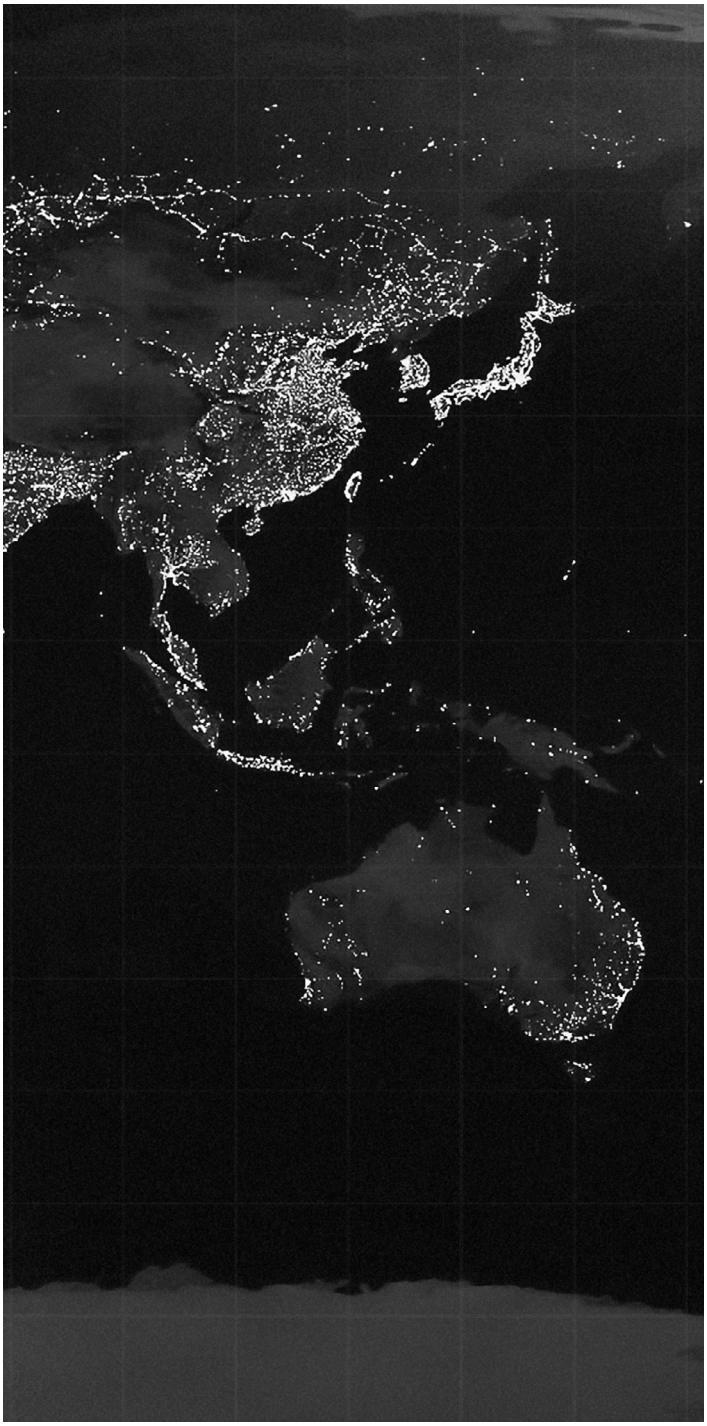
APAC also demonstrates the highest rate of working directly with third parties to resolve issues at 47%, compared to 42% in other regions (the U.S. and Canada, and DACH). This could suggest a relationship-based strategy that potentially offsets process or technology limitations. However, as these vendor ecosystems grow, relying on collaboration alone can lead to critical blind spots.

The swing in program maturity is wide: Singapore leads globally with 60% program maturity and 32% monthly or more frequent briefings, second only to the U.S. But the Philippines reports just 23% maturity and 100% were impacted by breaches. Australia was behind in program maturity at 30%, despite actively engaging with their vendors (53%). Malaysia reported the lowest country-level breach rate at 2.9 incidents, while maintaining high external security ratings platform adoption at 40%. This percentage spread makes establishing a regional baseline nearly impossible.

Spending was one area of focus. APAC organizations reported the lowest rate of estimated spending increased in the past year at 93%, with 89% of Australian organizations estimating bigger spending. We saw that organizations are outsourcing strategic functions like reporting at 40% (tied for the highest globally) rather than operational tasks.

Singapore's TPRM program success should serve as a model for what's possible in the region. With maturity rates matching or exceeding those of the U.S. and Canada, strong executive engagement, and sophisticated tool adoption, Singapore proves that organizational support rather than silos is critical for program success.

Like every other surveyed region, APAC cited integration with enterprise risk and GRC tools as their top operational challenge. This could suggest that they're investing in tools before building a strong foundation.



Final Thoughts

After six years of research, the 2025 State of Supply Chain Defense reveals a critical turning point: organizations have built TPRM programs, but struggle to make them truly effective. With 46% of programs established and optimized — up from earlier years when basic awareness was the challenge — the question has shifted from "should we do this" to "why isn't this working?"

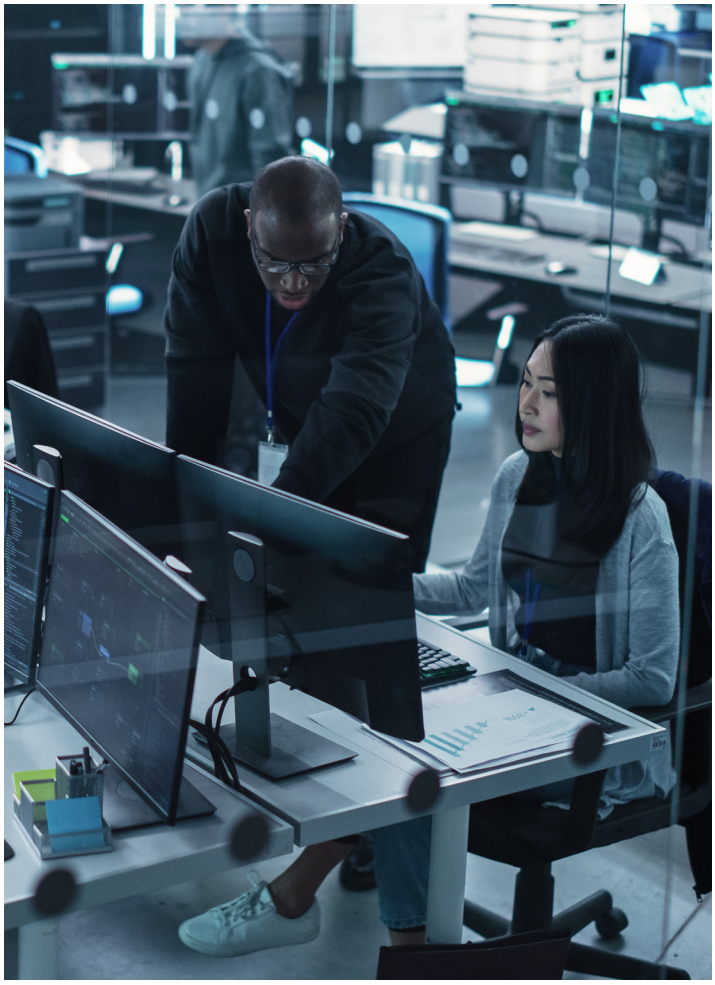
We can look to three persistent themes in this year's data:

- **Maturity without internal commitment** creates programs that function but lack organizational support. Only 24% of organizations brief executives monthly, while 60% cite internal resistance, lack of collaboration, and insufficient executive support as top barriers.
- **Compliance without risk reduction** means boxes are checked, but security outcomes become an afterthought. With only 16% of programs primarily driven by risk reduction (as opposed to cyber insurance or contractual obligations), organizations prioritize meeting requirements while 97% still experience breaches. With 64% of TPRM programs sitting outside security in finance, legal, or procurement, organizations may be prioritizing compliance over reducing risk exposure.
- **Investment without integration** leads to fragmented programs. Despite 95% of respondents expecting budget increases in the next year, the lack of integration with enterprise risk and GRC tools emerged as the top challenge across all regions. Deploying tools like sophisticated monitoring, continuous assessments, and security ratings platforms is helpful, but if they operate in silos, they can't provide actionable results.

Looking ahead, we predict several trends that will define the landscape:

- **Collaboration:** Vendor relationships require partnership, not just monitoring or a hands-off approach. As ecosystems grow and the attack surface widens, it's time to scale this collaborative approach.
- **Integration:** When organizations can connect their TPRM program into broader risk management strategies, they'll gain holistic visibility into their entire ecosystem.
- **Regional divergence:** Looking at results out of Singapore and the Philippines, or across Europe, tells us that organizational culture and economic context are critical to success — not just technology.

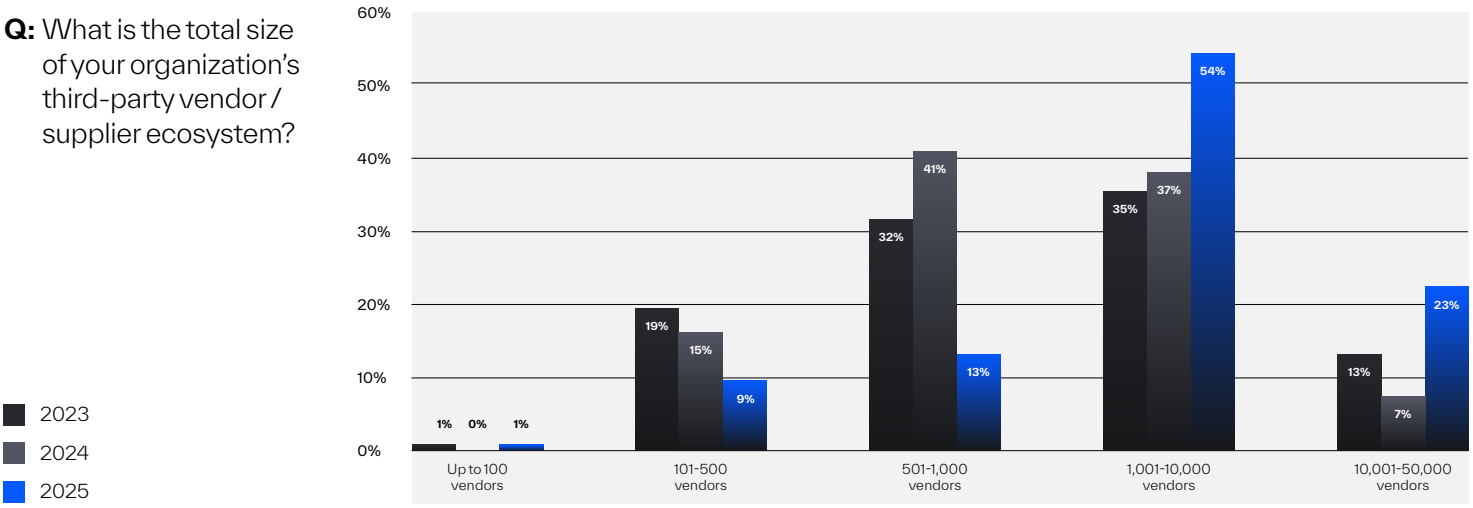
The main takeaway from 2025? Without organizational alignment, even the most sophisticated programs will fail to thrive. Integrated systems and genuine commitment to risk reduction over simply meeting compliance requirements will be the difference in delivering positive security outcomes and drowning in box checking.



Data Appendix

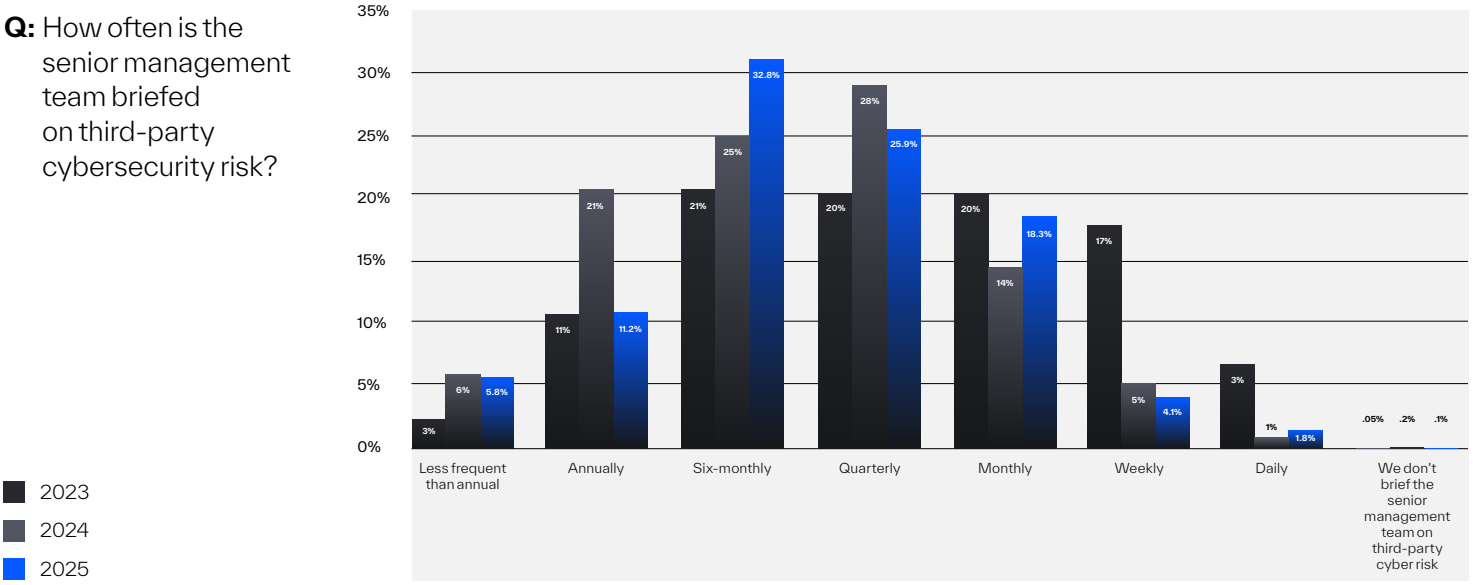
Supply chain ecosystem growth

Q: What is the total size of your organization's third-party vendor / supplier ecosystem?



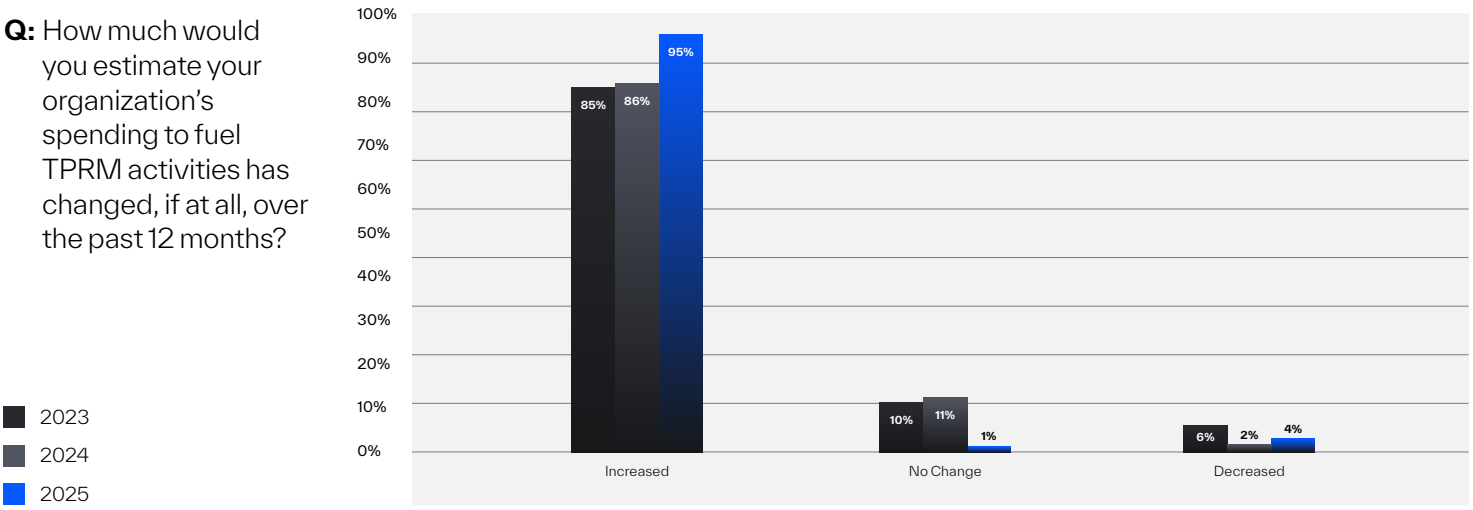
Senior management teams are regularly briefed on third-party cyber risk

Q: How often is the senior management team briefed on third-party cybersecurity risk?



Budgets continue to increase at a similar pace to previous years

Q: How much would you estimate your organization's spending to fuel TPRM activities has changed, if at all, over the past 12 months?



References & Opinion Matters Disclaimer

2025: The research was conducted by Opinion Matters among a sample of 1,800 respondents, CTOs/CSOs/COOs/CIOs/CISOs/CPOs responsible for supply chain and cyber risk management were surveyed from companies with 1,000-plus employees across a range of industries including: financial services, healthcare and pharmaceutical, manufacturing, utilities and energy, defense and retail. To gain a global perspective, the research was conducted in the following countries/regions: U.S., Canada, DACH (Germany, Austria, Switzerland), the U.K., APAC (including Australia, Malaysia, and the Philippines), Japan, and Singapore. The data was collected between September 16 and September 25, 2025.

2024: The research was conducted by Opinion Matters among a sample of 2,100 respondents, CTOs/CSOs/COOs/CIOs/CISOs/CPOs responsible for supply chain and cyber risk management were surveyed from companies with 1,000-plus employees across a range of industries including: business services, financial services, healthcare and pharmaceutical, manufacturing, utilities and energy, and defense. To gain a global perspective, the research was conducted in the following countries/regions: U.S., Canada, DACH (Germany, Austria, Switzerland), Denmark, the U.K., the Netherlands, APAC (including Australia and the Philippines), and Singapore. The data was collected between August 20 and August 29, 2024.

2023: The research was conducted by Opinion Matters among a sample of 2,100 respondents, CTOs/CSOs/COOs/CIOs/CISOs/CPOs responsible for supply chain and cyber risk management were surveyed from companies with 1,000-plus employees across a range of industries including: business service, financial services, healthcare and pharmaceutical, manufacturing, utilities and energy, and defense. To gain a global perspective, the research was conducted in the following countries/regions: U.S., Canada, DACH (Germany, Austria Switzerland), France, the U.K., the Netherlands, APAC (Australia and the Philippines), and Singapore. The data was collected between October 11 and October 20, 2023

2022: The research was conducted by Opinion Matters, among a sample of 300 respondents per territory (2,100 in total) CTOs/CSOs/COOs/CIOs/CISOs/CPOs (aged 18 and older) responsible for supply chain and cyber risk management working in companies employing 1,000-plus employees guaranteeing 50 respondents per industry sector per territory in the following: Financial services, Healthcare & pharmaceutical, Utilities & Energy (combined: equal split), Business services (i.e., professional services/legal and so forth), Manufacturing, and Defense: U.S. and Canada (natural fallout), DACH (Germany, Austria, Switzerland) (natural fallout), France, U.K., the Netherlands, APAC (Australia, Philippines) (natural fallout), and Singapore. The data was collected between September 23 and October 4, 2022.

2021: The research was conducted by Opinion Matters, among a sample of 1,200 respondents (aged 18 and older) CTOs/CSOs/COOs/CIOs/CISOs/CPOs responsible for supply chain and cyber risk management working in companies employing 1,000-plus employees guaranteeing at least 50 respondents per industry sector per country in the following: Financial services, Healthcare & pharmaceutical, Utilities & Energy (combined: equal split), Business services (i.e., professional services/legal and so forth), Manufacturing, and Defense. U.S., Canada, Germany, the Netherlands, U.K. and Singapore. The data was collected between June 22 and July 6, 2021.

2020: The research was conducted by Opinion Matters, among a sample of 1,505 respondents CIOs/CISOs/CPOs (aged 18 and older) responsible for supply chain and cyber risk management working in companies employing 1,000-plus employees in the U.S., U.K., Mexico, Singapore, and Switzerland. The data was collected between June 17 - 25, 2020.

Opinion Matters abides by and employs members of the Market Research Society and follows the MRS code of conduct and ESOMAR principles. Opinion Matters is also a member of the British Polling Council.

BlueVoyant

Cyber Defense

BlueVoyant delivers a comprehensive cloud-native security operations platform that provides real-time threat monitoring for networks, endpoints, and supply chains, extending to the clear, deep, and dark web. The platform integrates advanced AI technology with expert human insight to offer extensive protection and swift threat mitigation, ensuring enterprise cybersecurity. Trusted by more than 1,000 clients globally, and the 2024 Microsoft Worldwide Security Partner of the Year, BlueVoyant sets the standard for modern cyber defense solutions.

To learn more about BlueVoyant, please visit our website at **www.bluevoyant.com** or email us at **contact@bluevoyant.com**