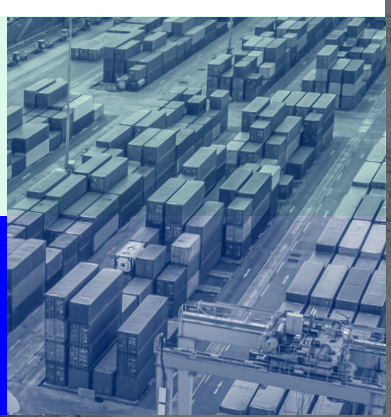
Spirity
TOMORROW:TODAY

Report

The State of Supply Chain Defense

Annual Global Insights Report 2022



BlueVoyant

Foreword

Welcome to BlueVoyant's third annual global insights report. Our 2021 survey, Managing Cyber Risk Across the Extended Vendor Ecosystem, explored the scope of the supply chain defense challenge but also the quantity and severity of breaches due to weaknesses in supply chains. While we will detail comparable findings in this year's report, we'll focus attention on how organizations are moving past problem identification and mitigating cyber risk challenges within supply chain vendors. We'll also explore the challenges identified by this year's respondents in establishing internal and third-party sourced functions and technologies for supply chain risk mitigation.

While organizations are generally making supply chain defense a priority, the news isn't all good. Our survey found that 40% of organizations still rely on their suppliers to ensure adequate security. Because risk is distributed throughout vendor ecosystems, relying on vendors to mitigate without any oversight will leave organizations vulnerable. This is reflected by the fact that 98% of respondents have been negatively impacted by a cybersecurity breach that occurred in their supply chain, versus 97% in 2021.

With traditional solutions, vulnerability and security issue identification has been the expected outcome — with a significant amount of false positives — but the holy grail has become risk reduction. How does an organization successfully mitigate risk within its supply chain once it's identified?

Not surprisingly, working with third-party suppliers to improve their posture continues to be one of the primary pain points in managing supply chain cyber risk. Another persistent challenge is the lack of internal understanding across the business that suppliers are part of the organization's security posture.

Here are the top three pain points listed by respondents:

- Internal understanding across the business that third-party suppliers are part of their cybersecurity posture.
- Meeting regulatory requirements and ensuring third-party cybersecurity compliance.
- Working with third-party suppliers to improve their posture.

The data shows that cyber risk hasn't decreased and, in fact, more organizations than ever have reported being negatively impacted by a cybersecurity breach that occurred in their supply chain. Further evidence of this shows that from 2021 to 2022 every vertical saw an increase in the number of breaches that negatively impacted them within the previous 12 months, with almost every vertical suffering from an average of one breach more than the previous year. We believe it's never been more evident that organizations' risk is distributed across their supply chains and therefore must be identified and mitigated.

Methodology

BlueVoyant commissioned its third annual survey undertaken by independent research organization, Opinion Matters, in September 2022.

Twenty-one 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 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, Europe (DACH, France, and the Netherlands), the U.K., APAC (Australia and the Philippines), and Singapore.

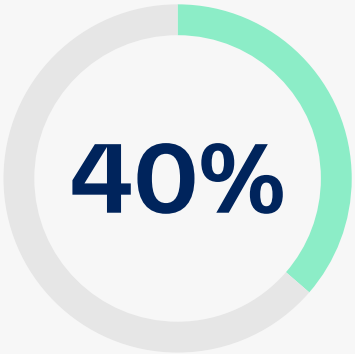
Table of Contents

At A Glance

↑

98%

of respondents have been negatively impacted by a cybersecurity breach that occurred in their supply chain, versus 97% in 2021.



of respondents rely on the third-party vendor or supplier to ensure adequate security.

Key Findings

Staying informed of risk

While a greater percentage of companies (29% in 2021 to 38% in 2022) said that supply chain cyber risk was not on their radar, we are nevertheless seeing an increased use of technology by organizations so they can better understand and be more informed of risk. While questionnaire use has been consistent, at just below 30% from 2020 through 2022, the increase in the use of security ratings services is up from 36% to 39%. This indicates that organizations progressively value continuous monitoring versus more static data analysis, while maintaining their questionnaire process to meet compliance requirements.

Continuing on a trend from the past two years, the number of companies reporting a supply chain size of more than 1,000 companies has increased. In 2020, only 14% of all companies surveyed reported having more than 1,000 companies in their supply chains; in 2021 that number more than doubled to 38%, and in 2022 we saw another substantial increase to 50%. As we stated in the 2021 report, more companies are becoming aware of the full extent of their supply chains.

Improving vendor risk visibility

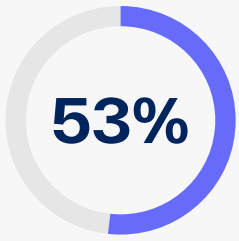
In 2021, 53% of companies audited or reported on supplier security more than twice per year; that number in 2022 has improved to 67%. While this is a positive trend, organizations that do not frequently examine supplier security remain vulnerable to emerging — including zero-day — attacks that often occur immediately after these vulnerabilities are disclosed. Without continuous monitoring and an accurate way to determine which suppliers are using a particular technology accompanied by rapid mitigation, damage from these threats can be devastating.

In one month alone in 2022, the Zyxel Critical Authentication Bypass, VMware Remote Code Execution, and the compromise impacting Okta users all emerged. Continuous monitoring, the capability to assess which suppliers are affected, and a process to work with suppliers to mitigate exploits are all required for organizations to defend against supply chain cybersecurity threats.

BlueVoyant Viewpoint

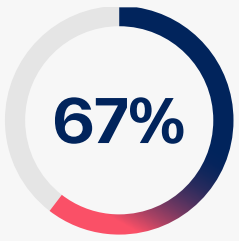
While it is jarring to see a higher percentage of companies that say supply chain cyber risk is not on their radar, we're seeing more technology adoption and a greater organizational awareness of supply chain size among this years' respondents. This observation, coupled with a consistent number of companies indicating that working with suppliers to improve their performance is one of their key pain points, provides evidence of an increasing need for automated technology that can continuously monitor large supply chains while helping suppliers directly mitigate cyber risk.

Vendor Risk 2021



audited or reported on supplier security more than twice per year

Vendor Risk 2022



audited or reported on supplier security no more than twice per year

Budget for supply chain risk continues to rise

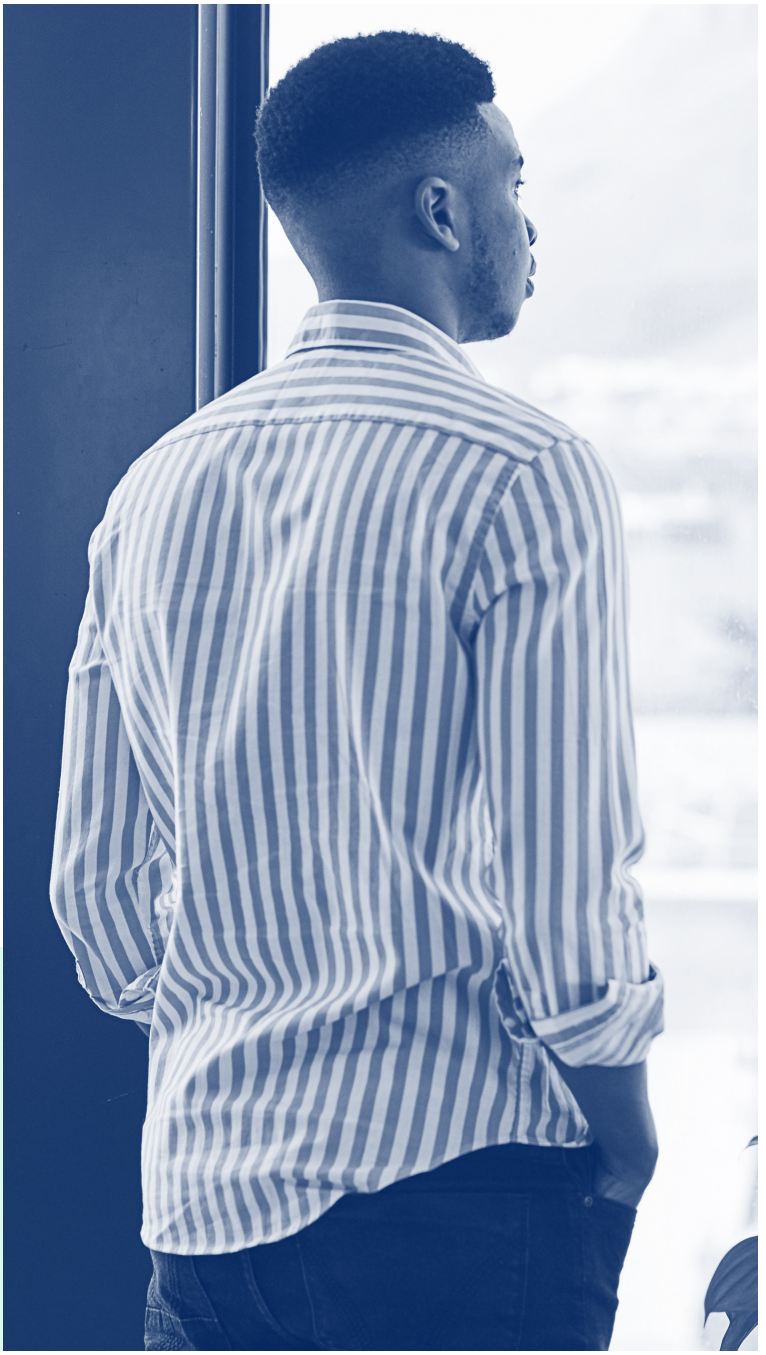
In terms of budget increases, 25% of respondents reported budget increases of 26-50%; 37% revealed increases of 51-100%; and 20% signaled an increase of more than 100%. Only 11% indicated there was no increase, and just 4% said they had a decrease.

It will be interesting to see how these budget increases will be invested, and if they will mirror the top three pain points, which include:

- A lack of internal understanding across the business that third-party vendors and suppliers are part of their cybersecurity posture (26%).
- The challenge of meeting regulatory requirements and ensuring third-party cybersecurity compliance (24%).
- The challenge of working with third-party suppliers to improve their performance (21%).

Unfortunately, despite the reported increases in budgets, many organizations continue to be blind to cyber risk and unable to determine if an issue is remediated.

That said, 40% of respondents said they had no way of knowing when or if an issue arises with a supplier. And 42% reported that if they do discover an issue in their supply chain ecosystem and inform their supplier, they cannot verify that the matter was resolved. They can only hope the supplier fixed it.



BlueVoyant Viewpoint

Managing distributed risk associated with hundreds and even thousands of suppliers has become a defining cybersecurity challenge in today's increasingly complex business environment. As organizations have increased the number and variety of suppliers they work with, they have simultaneously exposed their enterprises to the vulnerabilities of those suppliers. Organizations increasingly need to identify, validate, prioritize, and confirm that mitigations have taken place through direct relationships with suppliers.

Recommendations

Work with your suppliers to improve their security postures

Going into 2023 and beyond, working with suppliers and equipping them to address cyber risk should be a top priority. Assuming that your vendors are aware of their security posture and taking proactive steps, such as patching vulnerabilities, relying on trust alone is a risky path.

Traditional approaches to monitoring supply chain risk, such as security ratings services, only alert organizations to vulnerabilities in their supply chain. It is left to the supplier to act on alerts, and mitigate vulnerabilities and risky behaviors. With a holistic approach that includes proactive outreach to the supply chain to work with individual suppliers, organizations gain broad visibility into their extended ecosystem. By that extension, they move beyond continuous monitoring to include risk reduction through direct contact with suppliers. While use of security ratings services has increased from 36% in 2020 to 39% in 2022, that upturn has not resulted in fewer organizations being negatively impacted by breaches that occurred in their supply chain.

Educate your internal team around the importance of addressing supply chain risk

Your attack surface is as far-reaching as your smallest vendor. Their vulnerabilities are your own, and it's critical that the entire security organization, executive team, and board of directors is aware of this. One of the primary challenges in the creation of a comprehensive supply chain cyber risk program is organizational buy-in and budget allocation. Senior leadership, even those not involved with cybersecurity, must be able to understand that supply chain cyber risk is a critical aspect of business hazard that can represent major financial, reputational, and continuity damage. Educating your senior leadership team can come in the form of monthly or quarterly briefings that share your current risk posture and any issues to be aware of.

Integrate continuous supply chain monitoring and report to the board and senior leadership team early and often

Point-in-time assessments, such as surveys, only reveal risk at that moment and are not sufficient. Using continuous monitoring in your supply chain defense strategy provides a dual advantage. First, organizations can maintain an adaptive understanding of the risk within their supply chain to ensure they are addressing the vulnerabilities that could compromise their own security posture. Second, frequent contact and visibility into supply chain environments helps eliminate blind spots where sensitive information might be unknowingly stored.

Of our survey respondents, the highest percentage (27%) brief their management team on supply chain cyber risk quarterly. By regularly updating senior leadership and the board and continuously monitoring your suppliers, the organization can get ahead of security issues in its supply chain before they are exploited by bad actors.

Vertical Market Analysis

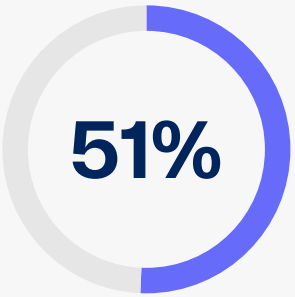
Financial Services

As one of the most targeted vertical markets, the financial services sector is one whose customers expect an extremely fast response after a data breach. With the majority of financial services organizations surveyed (41%) working with between 1,001-10,000 suppliers, these businesses have a wide attack surface with many opportunities for a breach.

Of all the sectors in our survey, financial services respondents represented the highest percentage that outsource data analysis and results from monitoring at 51%. By outsourcing that work to a vendor, these teams likely gain leverage for analysis and action. And speaking of outsourcing, this sector had one of the highest percentages of major budget increases of 51-100%, with 40% of organizations reporting this level. Though this is a 10% decrease for financial services compared to 2021, it still represents a positive shift in internal culture toward making supply chain defense a priority.

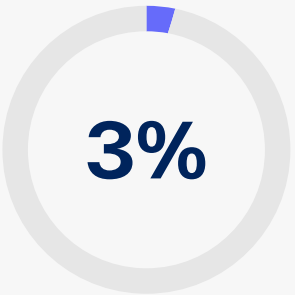
The top challenge for this sector is an internal understanding across the business that suppliers are part of the organization's cybersecurity posture (27%). This job may fall to the CIO, who 30% of our respondents in this sector said was responsible for cyber risk. Other pain points include:

- Meeting regulatory requirements and ensuring third-party cybersecurity compliance (23%).
- Onboarding new third-party suppliers with the speed and rigor required (21%).



outsource data analysis and results from monitoring.

Financial services had the highest percentage of respondents that outsource data analysis and results from monitoring (51% vs. 45% overall).



of respondents monitor their supply chain daily.

And only 1% of financial services respondents monitor in real time.

Healthcare and Pharmaceutical

The healthcare and pharmaceutical sector has much to contend with when it comes to cybersecurity, including the protection of sensitive health data and various regulatory standards to maintain. Third-party and supply chain risk continue to challenge this vertical as well, as more and more healthcare organizations are becoming interconnected and reliant on suppliers.

In general, healthcare and pharmaceutical companies are aware of supply chain cyber risk, with 61% of companies claiming that the issue is on their radar, and 39% saying it is a key priority. This is in part due to the disruptions that have affected the sector, with healthcare and pharmaceutical companies suffering from the most negative disruptions across the sectors. This is particularly notable when considering that healthcare and pharmaceutical is the vertical that has the most companies surveyed (20%) with less than 500 vendors or suppliers. In short, healthcare companies tend to have smaller vendor ecosystems but also tend to suffer more frequently from vendor cyber disruptions.

As a result, the adoption of vendor risk management programs and security ratings services has increased since last year. Healthcare companies maintain the highest rate of organizations across any vertical that fully monitors all third-party suppliers and partners, with a rate of 23%. Nevertheless, there has been a slight drop-off since the previous year in budgeting average for third-party cyber risk (55% in 2021 vs. 53% in 2022).

As of 2022, the CIO is the most likely role in a healthcare or pharmaceutical company to own third-party cyber risk (29%). The industry's top challenges for managing supply chain cyber risk are:

- Working with third-party suppliers to improve their security performance.
- Prioritizing which risks are urgent and which are not.
- Lack of in-house resources to manage the program.

42% have increased board scrutiny on supply chain cyber risk.
The sector also indicated the lowest likelihood (7%) to increase budget for resources to bolster supply chain cybersecurity.

46% rely on simply informing suppliers about problems and hoping they fix it.
This sector is also the least likely of any vertical (34%) to have no way of knowing if an issue arises with a third party's environment.

Utilities and Energy

The utilities and energy sector is one of the leading verticals in tackling supply chain cyber risk. Rising to the challenge of supply chain defense is an important one for the energy sector, as it remains one of the most frequently attacked verticals across all industries. Ninety-nine percent of energy companies have been negatively impacted by at least one supply chain breach in the last 12 months, the highest rate of any observed vertical.

The energy sector currently maintains the highest rate of any vertical to increase its yearly budget for supply chain cyber risk by more than 50%, with a mean of a 60% increase. Forty-nine percent[1] of energy companies in 2022 are also monitoring supply chain cyber risk on at least a monthly basis or more frequently, the highest frequency rate of any industry vertical, with an average of 29 reassessments per year. Forty-four percent are updating senior leadership on supply chain cybersecurity monthly or more often, which is also the highest rate of any vertical, maintaining an average of 35 briefings per year.

As of this year, CISOs are the most likely to bear responsibility for supply chain cyber risk at 27% (in line with other verticals), but unlike any other vertical, CPOs are the second-most likely position to own third-party cyber risk (23%). The industry's top challenges for managing supply chain cybersecurity risk are:

- Internal understanding across the business that third-party suppliers are part of their cybersecurity posture (27%).
- Meeting regulatory requirements and ensuring third-party cybersecurity compliance (23%).
- Working with third-party suppliers to improve their security performance (20%).

[1] **Including those monitoring in real time**

↑99%

of energy companies have been negatively impacted by at least one supply chain breach in the past year.
This represents the highest rate of overall impact in any industry surveyed.

49% are monitoring third-party cyber risk regularly.
And 44% are updating senior leadership on supply chain cybersecurity monthly or more frequently, which is also the highest rate of any vertical.

↑60%

Energy companies are increasing their budget for supply chain cyber risk by an average of 60% over 12 months.
Energy and utilities companies maintain the highest rate of budget increases of any vertical for supply chain cyber risk.

65% of companies are aware of supply chain risk.
However, this vertical has the highest rate (17%) to also claim it is not a priority.

There has been an 11% increase in regular risk reassessments.
Additionally, since 2021 monthly-or-better reporting to leadership has risen from 30% to 38%.

Business Services

The business services sector is largely diverse and complex, making it challenging to track trends across the different companies that compose it. In fact, many trends seem paradoxical but speak to the varied nature of the industry. In general, despite widespread awareness, third-party cyber risk is not considered a top priority for the industry, and the challenges have not been as embraced as compared to other verticals. While rates of third-party monitoring are reported to be in line with many other verticals, business services is the sector that most deprioritized third-party cyber risk and has oscillating rates of budgeting for it. Business services companies maintain among the lowest rates of monthly-or-better supply chain cyber risk reassessments, and also most infrequently brief senior management.

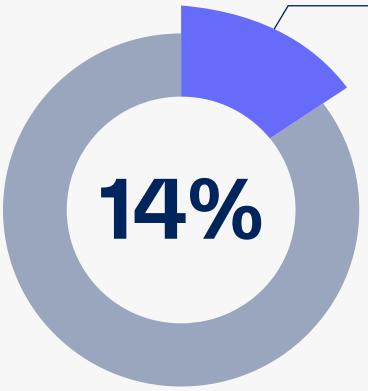
However, despite falling short of other verticals in these metrics, it's worth noting that there has been an across-the-board improvement in reassessment rates and reporting as compared to the previous year. Since 2021, monthly-or-more-frequent reassessment of supply chain cyber risk has increased from 29% to 40%[1]. Annual reporting to the senior management team on supply chain cyber risk has dropped from 27% to 10%, while monthly-or-more-frequent reporting has risen from 30% to 38%.

In certain other aspects of supply chain cyber risk, the business services sector has taken positive steps forward. There has been a consistent increase in the variety of supply chain cyber risk methods and technologies used by business services companies since the previous year, including the adoption of vendor risk management programs, security ratings services, and network scanning and penetration tests.

Among business services companies, a CISO is the most likely role to own third-party cyber risk (25%), followed by a COO (22%). The industry's top challenges for managing supply chain cyber risk are:

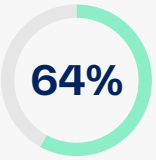
- Internal understanding across the business that third-party suppliers are part of their cybersecurity posture (32%).
- Meeting regulatory requirements and ensuring third-party cybersecurity compliance (25%).
- Working with third-party suppliers to improve their security performance (21%).

[1] **Including those monitoring in real time**

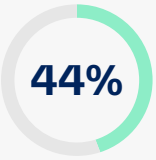


10,000+ suppliers

Manufacturing companies manage the largest supply chains of any industry, with 14% responsible for more than 10,000 suppliers.
And another 38% manage between 1,001 and 10,000 suppliers.



of respondents say that supply chain cyber risk is on their radar.
This is the same proportion as in 2021.



of manufacturing respondents have established an integrated enterprise risk management program.
This number is the highest of any industry surveyed in 2022.

Manufacturing

As the manufacturing sector continued to battle unpredictable supply chain disruptions this year, the industry made dramatic strides in managing third-party cyber risk. Certainly, industry-wide identification of the problem is a start: 64% of respondents stated that supply chain cyber risk was on their radar this year. But more important, this awareness has translated into action: 44% of manufacturing respondents have established an integrated enterprise risk management program, the highest of any industry surveyed in 2022.

Manufacturers reported higher than cross-industry average use of security ratings services, network scanning and penetration testing, as well as exchanges and marketplaces. Use of technical solutions increased within the industry as well, with 3% more use of exchanges and marketplaces (36% vs. 33% in 2021), and 4% more use of network scans, penetration tests, and security ratings services since 2021 (41% vs. 37% in 2021 for both).

With this progress, there are still several insights into the challenges and opportunities that lie ahead for this critical sector. The urgency and severity of supply chain-related cyber breaches in manufacturing makes it the most likely industry to receive budget increases for external resources this year – a trend that has continued from 2021. And while manufacturing companies are outsourcing activities across the entire supply chain defense spectrum, they had the highest reported use of risk prioritization services for any findings, removal of false positives (47% versus an industry average of 44%) and remediation services for mitigation plans and ensuring mitigation takes place (48% versus an industry average of 44%) – a signal that technical solutions alone cannot close the gaps in their supply chain cyber defense. Among these potential technical challenges were a host of other operational and process-related pain points:

- Meeting regulatory requirements and ensuring third-party cybersecurity compliance (25%).
- Internal understanding across the business that third-party suppliers are part of the cybersecurity posture (29%).
- Working with third-party suppliers to improve their security performance (23%).

Defense

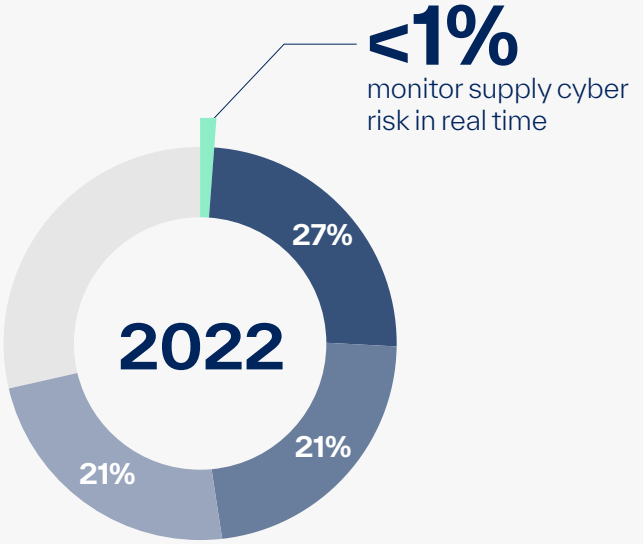
The defense sector was at the epicenter of supply chain cyber risk in 2022 as the world turned toward the Russian invasion of Ukraine. The uncertainty in this high-risk environment likely led to strengthened cyber defenses, and most important, increased attention to supply chain-related threats. The prioritization of supply chain risk grew in 2022, with 14% more respondents listing it as a "key priority" instead of "somewhat of a priority" (51% vs. 37%, respectively).

This year's survey also signaled a steady continuation of trends in the defense vertical's operational approach. Like previous years, defense continues to rank among the top-performing industries with both integrated enterprise risk management (43% compared to 41% across sectors) and vendor risk management programs (42% compared to 41% across sectors) in place. While the highest percentage continued to brief senior leadership quarterly (25%) within the sector, the number of respondents reporting updates daily to leadership (5%) and weekly (12%) grew by 2% and 1%, respectively.

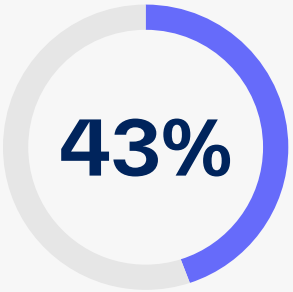
Despite strong internal processes and operations, defense respondents reported below-average use of technical solutions to manage supply chain cyber risk. Only 34% are using security rating services and 35% conducting network scans and penetration tests, compared to industry averages of 39% and 38%, respectively. The industry's higher preference toward on-site audits (31% compared to 28% last year) and external consultants (37% compared to 26% last year) has likely created challenges as they aspire to monitor more and more suppliers.

Last year, 26% stated that they monitored all of their suppliers for cyber risk, while this year that percentage has actually decreased to 21%. Even so, defense companies state that their top pain points in supply chain defense stem from internal processes. Other sector pain points include:

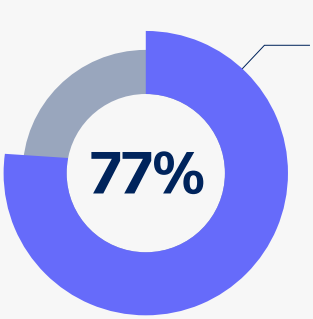
- Internal understanding across the business that third-party suppliers are part of the cybersecurity posture (26%).
- Meeting regulatory requirements and ensuring third-party cybersecurity compliance (24%).
- Enforcing SLAs with all our third parties/suppliers and getting them to comply (22%).



44% of manufacturing respondents have established an integrated enterprise risk management program.
This number is the highest of any industry surveyed in 2022.



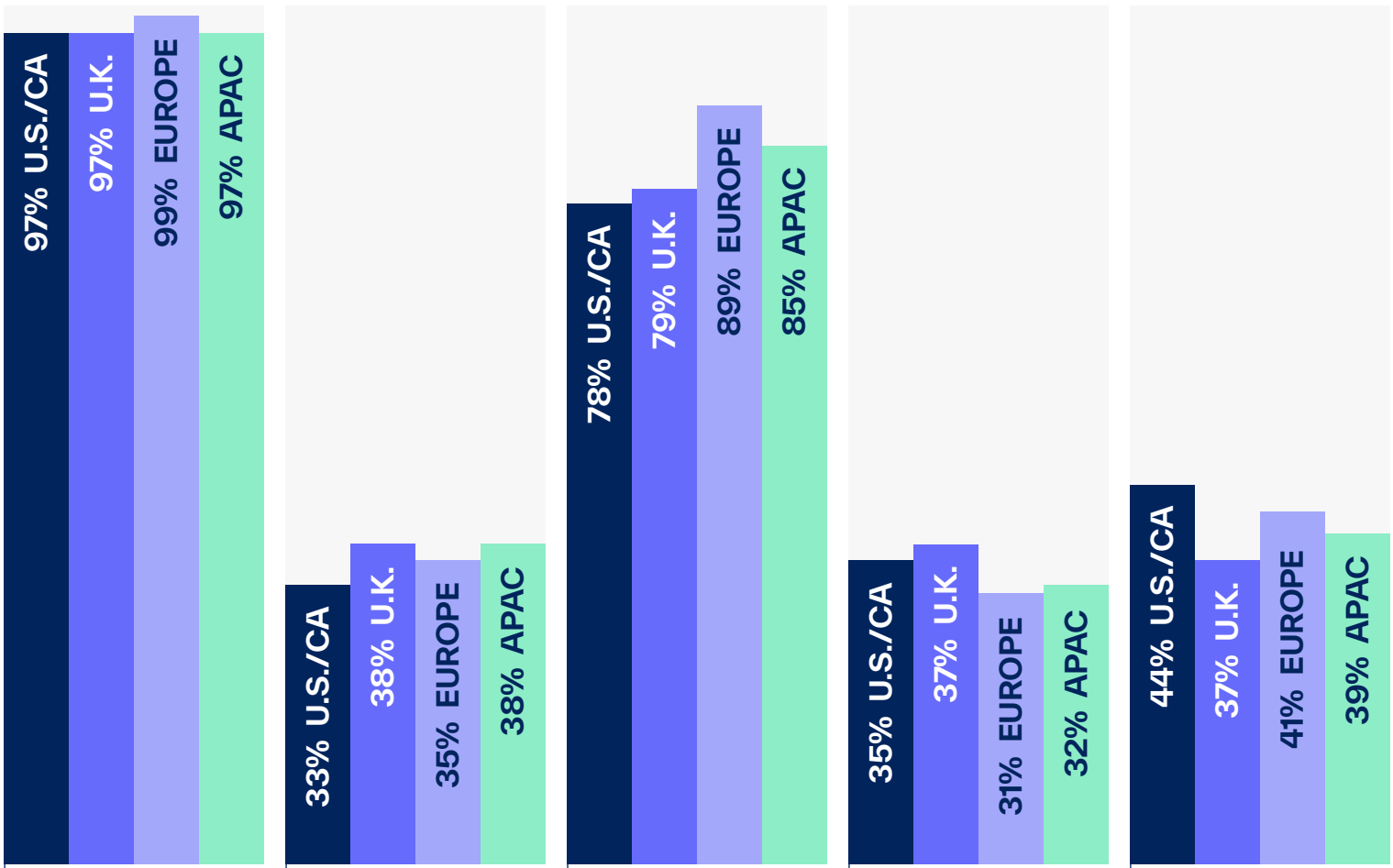
of respondents have no way of knowing if there's a cyber vulnerability impacting their supply chain.
And if they do discover an issue in their supplier ecosystem and inform their supplier, they cannot verify that the matter was resolved.



77% reported budget increases of 26% or more.
But 16% reported no changes at all – the highest of any industry sector in 2022.

Region-Specific Analysis

Global insights: Supply Chain Cyber Risk Key Country Comparisons



98%
Globally
Who say they've been negatively impacted by cybersecurity breaches in their supply chain

36%
Globally
Supply chain risk is a key priority

84%
Globally
Budget has increased in the past 12 months

33%
Globally
Only re-assess six-monthly or less frequently

40%
Globally
Wouldn't know if a risk emerged in a supplier

U.S. and Canada

After data analysis, the U.S. and Canada do not stack up well against other regions in a couple of key areas. For example, while globally 38% of respondents state that cybersecurity risk is not on their radar, that number is 41% in the U.S. and Canada. Similarly, a lower percentage (33% vs. 36% globally) state that supply chain risk is a key priority, the lowest of any region and down significantly from the 43% in 2021 who said it was a key priority.

Likely because of this, the U.S. and Canada were least likely to report a budget increase for supply chain defense. This year, just 78% reported a budget increase, down from 89% last year.

The good news is that in the U.S. and Canada enterprises are more likely to be working with their suppliers identifying the problem and helping them find a solution — 50% compared to 42% globally. It is likely why U.S. and Canadian respondents were more likely to report working with suppliers to improve their security performance as a supply chain defense pain point (25% compared to 21% of global respondents). Additonal good news is that U.S. and Canadian enterprises are more likely to outsource supply chain security, which may be why they were slightly less likely to report a negative impact from a cybersecurity breach in their supply chain — 97% compared to 98% globally — with respondents reporting less breaches than other regions. Thirty-eight percent of U.S. and Canadian respondents said they experienced a negative impact from only one cybersecurity breach.

Overall, the analysis found that respondents are:

- More likely to say cybersecurity risk is not on radar — 41% in the U.S. and Canada compared to 38% globally.
- Less likely to state that their supply chain is a key priority — 33% in the U.S. and Canada compared to 36% globally. This is down from 43% of respondents in the U.S. and Canada in 2021.
- More likely to see their budget for supply chain security decreased. The most common answer was that their budget increased 51-100% (32% of respondents) but 9% had their budget decrease, more than double the global rate (4%).
- Slightly less likely to be negatively impacted by a supply chain breach — 97% compared 98% globally.
- More likely to say they had no way of knowing if a problem arises with supply chain vendors (44% in the U.S. and Canada compared to 40% globally). Also, they are more likely to rely on the supplier to ensure adequate security (47% U.S. and Canada compared to 40% globally). But there are some bright spots. Half (50%) reported they are working with their suppliers to identify the issues and find a solution compared to only 42% of global companies.
- Recent breaches were more likely to increase budgets for external resources to help protect against supply chain cybersecurity issues in the U.S. and Canada (46% compared to 40% globally).

U.K.

The U.K. is a bit more nuanced than the U.S. and Canada. For example, while the percentage of respondents who state supply chain cyber risk is not on their radar is relatively high at 43%, a bigger percentage than the global average, indicating that it's a key priority at 38%. This is significantly higher than last year, when only 27% of U.K. firms considered supply chain security a key priority. It is an issue that they're behind the global average in monitoring frequency, with the most common response given being every six months (27%). Even with recent high-profile breaches, like Solar Winds, U.K. respondents were less likely to report budget increases. In the U.K. 97% of respondents reported a negative impact from a supply chain breach, compared to the slightly higher 98% of global respondents.

In the U.K., the numbers showed:

- They are more likely to say cybersecurity risk is not on the respondent's radar (38% globally, compared to 43% in the U.K.).
- They are more divided on whether supply chain security is a priority. Respondents were more likely to not be a priority (19% in the U.K. compared to 15% globally), but 38% say it's a key priority compared to 36% of global respondents.
- They are more likely to be monitoring key supply chain suppliers, but less likely than global enterprises to monitor all suppliers (14% of U.K. respondents say they monitor all suppliers vs. 17% of global enterprises).
- U.K. enterprises are less likely to outsource supply chain cyber defense, except for data analysis and results from monitoring when compared globally (48% compared to 45% globally).
- U.K. respondents are less likely to not know of an issue with a vendor (37% of U.K respondents compared to 40% globally). This is down slightly from 38% not knowing if a risk arose in their supply chain last year. The good news is they are less likely to rely on vendors for adequate security (35% U.K. compared to 40% globally), and are more likely to work with suppliers each step of the way until the issue is rectified (45% in the U.K. compared to 40% globally).
- U.K. respondents were less likely to report increased budgets despite recent attacks and more scrutiny. Only 79% of respondents said their budget increased in the last 12 months, compared to 92% in 2021.

Europe (DACH, France, and the Netherlands)

Europe generally scores higher marks than other regions. European companies are more likely to report monitoring of their entire supply chains. They are also more likely to monitor supply chains more frequently and brief senior management daily or weekly than other regions. When it comes to budgets, compared to other regions European respondents are more likely to report an increase and less likely a decrease for supply chain defense. Perhaps because of the increased monitoring, Europe respondents were slightly more likely to report negative impact from a supply chain breach — 99%, the highest of any region, compared to 98% globally.

Overall, here are the key findings:

- European enterprises are the most likely to monitor their entire supply chain (21% of European respondents compared to 17% globally).
- Like the U.S. and Canada, European respondents are more likely to use integrated and enterprise risk methods for supply chain or security ratings services compared to global enterprises (45% vs. 41%, respectively).
- European enterprises are more likely than the global average to be monitoring their supply chain on a weekly or monthly basis.
- They are also more likely to brief senior management daily or weekly.
- European executives are more likely to see their budget for supply chain defense increase and less likely to see it decrease.

APAC (Australia, Philippines, and Singapore)

APAC companies prioritize supply chain cybersecurity risk at a high rate, consistent with the U.K. Slightly better than the global average for organizations that state cybersecurity risk is not on the radar, APAC countries are showing signs of an improved focus on supply chain cyber risk.

In this region, the numbers showed that:

- APAC enterprises are in line with global respondents in saying supply chain cybersecurity risk is not on their radar (38% globally compared to 37% of respondents in APAC).
- They are most likely to brief senior management quarterly (31%).
- APAC enterprises say they have been negatively impacted by a supply chain breach at a rate of 97%, slightly lower than the global average.
- There is an even split between CIO and CISO (both 24%) owning supply chain cyber risk in APAC organizations.
- They are more likely to know if an issue arises with a supplier (39% of APAC respondents have no way, less than 40% of global respondents) and only 36% are relying on suppliers for adequate security (compared to 40% globally). However, they are less likely to work with suppliers to fix problems.
- APAC enterprises are less likely to experience more scrutiny and increased budgets due to recent breaches.

Singapore

While in 2021 Singapore outscored other regions, things have changed and not necessarily for the better in 2022. The country is now lagging behind global respondents in some key measures. Last year 93% of respondents reported being negatively impacted by a cybersecurity breach that occurred in their supply chain, but that number rose to 97% in the 2022 survey. And compared to the global percentage of 36%, just 33% state that supply chain security is a key priority. And 42%, as compared to the global average of 38%, say supply chain security isn't on their radar. On the positive side, more companies are reporting more than 100% budget increases than the norm and they are less likely to rely on suppliers for adequate security.

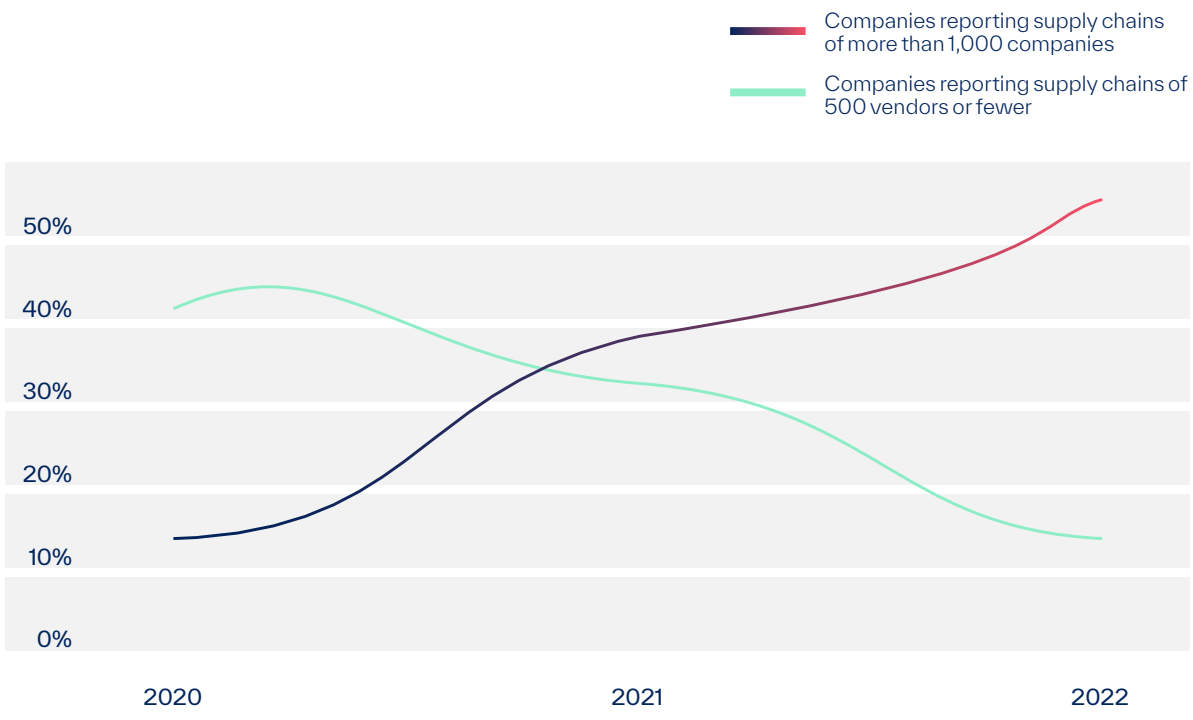
Overall, the survey found:

- Singapore enterprises were more likely to say supply chain security is not on their radar (42% of Singapore respondents compared to 38% globally).
- Respondents were more likely to say supply chain security isn't a priority —17% compared to 15% globally — and as a key priority 33% compared to 36% globally.
- Singapore respondents were slightly more likely to say their supply chain budget will decrease (5%), compared to global respondents (4%), but much more likely to report a more than 100% increase in budget.
- Like the U.S. and Canada, CIOs in Singapore are 30% more likely to own supply chain risk than CISOs.
- Respondents in Singapore were less likely to say they had no way of knowing if issues arise with a supplier — 35% compared to 40% globally. They are also less likely to rely on suppliers for adequate security, or 29% compared to 40% globally. Singapore enterprises were less likely to report increased scrutiny and breaches from recent large supply chain attacks.

Final Thoughts

The supply chain cyber defense problem has not gone away, and it appears to have somewhat worsened. Ninety-eight percent of respondents reported having been negatively impacted by a cybersecurity breach that occurred in their supply chain. At the same time, 50% reported supply chains of more than 1,000 companies, up from 38% in 2021 and 14% in 2020. Are these organizations simply more aware of their supply chains?

However, the pain points tell the story. CIOs, CISOs, and CPOs are still struggling to increase their businesses' understanding that suppliers are part of their cybersecurity posture. In addition, respondents listed the challenge of working with third-party suppliers to improve their posture as one of their top three pain points, almost universally.



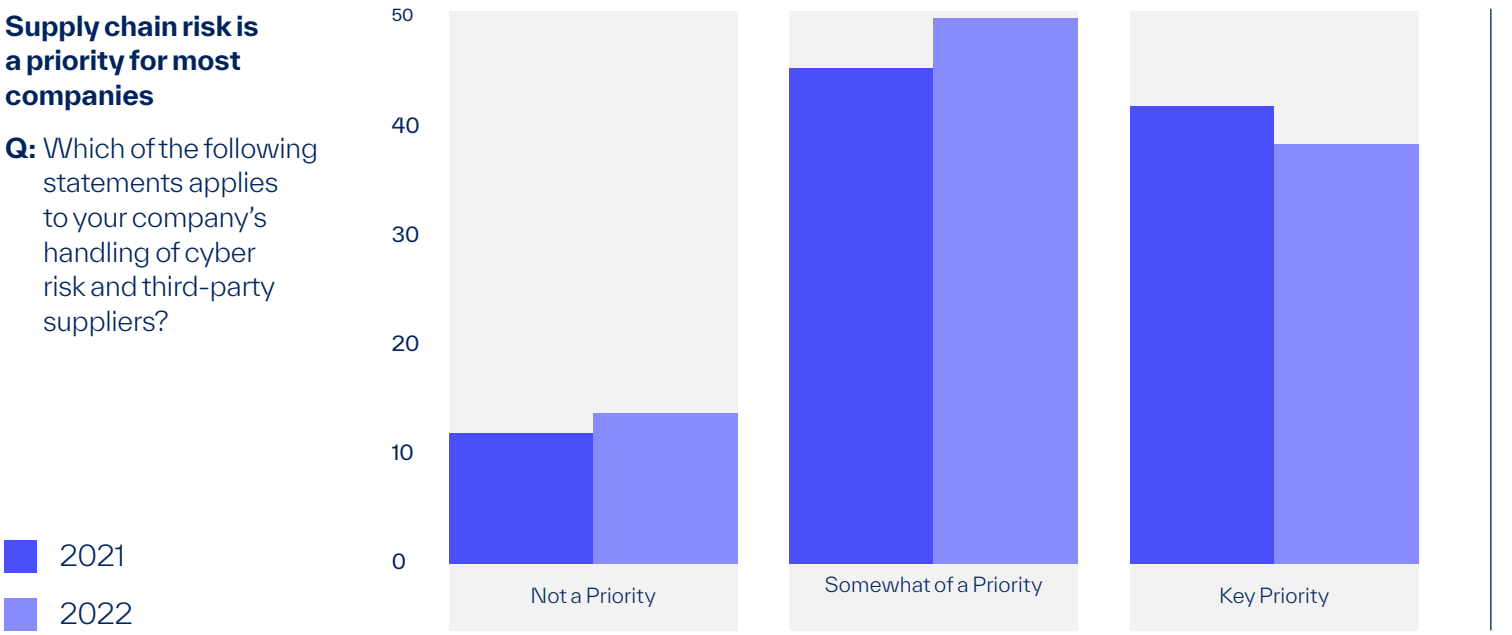
And while budgets continue to increase across most verticals, with only 11% of companies overall reporting no increase and 4% indicating a decrease, the adverse effects of inadequate supply chain defense are being felt more and more. Respondents are aware that there's a problem; the solution has been elusive.

Regardless of corporate ownership, the realization that risk is distributed across supply chains should drive different behaviors. Continuous monitoring has increased, and senior management is being briefed more often, all of which are positive signs. We can only hope that next year's survey shows fewer than 38% of respondents reporting that supply chain risk isn't on their radar, and increased realization of the need to work directly with suppliers. These factors will be what drives a dramatic decrease in the percentage of companies negatively impacted by a supply chain cybersecurity disruption.

Data Appendix

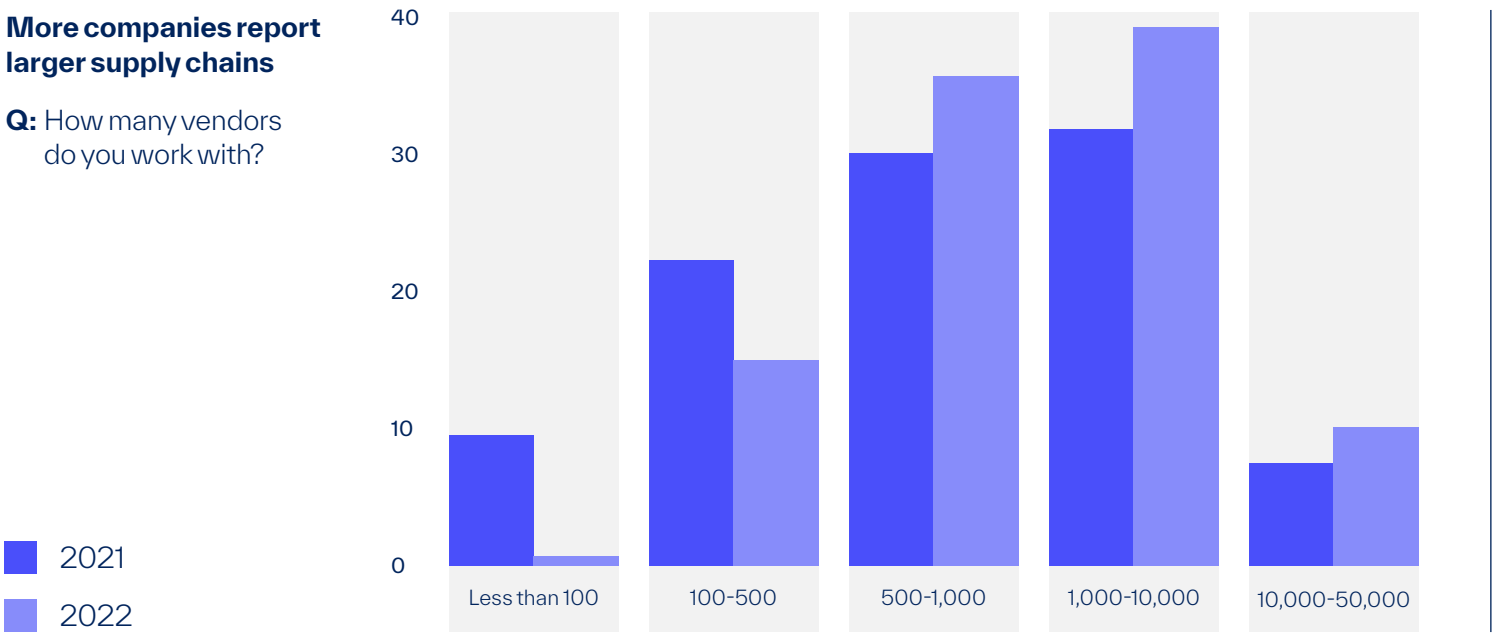
Supply chain risk is a priority for most companies

Q: Which of the following statements applies to your company's handling of cyber risk and third-party suppliers?



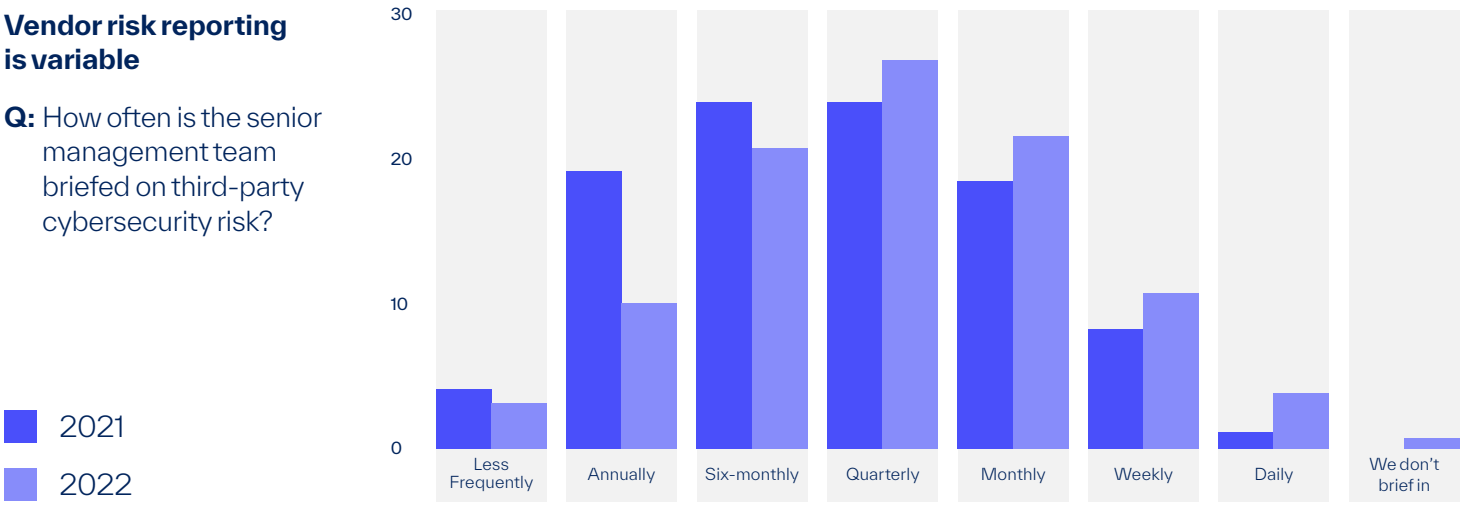
More companies report larger supply chains

Q: How many vendors do you work with?



Vendor risk reporting is variable

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



Budgets are increasing but at a slower rate

Q: Has your budget for supply chain/third-party cybersecurity risk management changed compared to the past 12 months, and if so, how?

	2021	2022
Yes, increased by up to 25%	3.3%	2.6% (- 0.7%)
Yes, increased by 26-50%	28.7%	25.4% (-3.3%)
Yes, increased by 51-100%	42%	37% (-5%)
Yes, increased by more than 100%	17%	19.5% (+2.5%)

↑84%

No, it has stayed the same	5.1%	11.1% (+6%)
Yes, decreased	3.8%	4.2% (-0.4%)

↓15%

References & Opinion Matters Disclaimer

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.

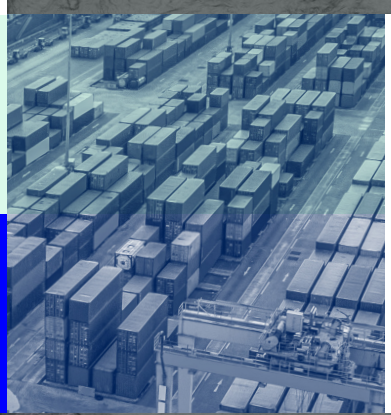
2021: The research was conducted by Opinion Matters, among a sample of 1,200 respondents (aged 18 and older) CTOs/CSOs/COOs/CIOs/CISOs/CPOs responsible for supply chain and cyber risk management working in companies employing 1,000-plus employees guaranteeing at least 50 respondents per industry sector 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, which is based on the ESOMAR principles.

Spirity
TOMORROW:TODAY

Rock-solid cyber defense you can trust



BlueVoyant

Contact **Spirity Enterprise** at

hello@spirity.hu

or visit

https://www.spirity.io/supply-chain-defense

to learn more.