interos

Resilience 2022

The Interos Annual Global Supply Chain Report
Focus: IT & Technology Sector

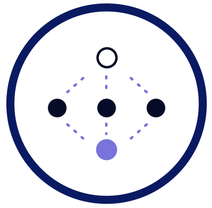
Commentary Report • May 2022 • www.interos.ai

Contents

Executive Summary

- Interos surveyed 300 global decision makers in the tech industry about the impact of continued supply chain disruption.
- Most tech institutions plan to make “wholesale changes” to their supply chain footprints amid continued supply chain shocks and rising geopolitical tensions. Companies plan to **reshore or nearshore an average of 49%** of existing contracts.
- Organizations were impacted by **three** significant supply chain disruptions during the past year costing on average **$199 million** in lost revenue
- Disruption in the tech industry occurred **in all risk categories including financial, operational, cyber, ESG and geopolitical.** Most companies were impacted by sub-tier supplier issues, where they have limited visibility.
- Slightly **over half of a tech organization’s suppliers** are typically evaluated during risk analysis exercises. Less than 20% say they monitor supplier risks on a continuous basis.
- Technology solutions are seen as delivering significant benefits. While **most organizations currently lack advanced supply chain visibility solutions**, virtually all plan to implement them in the next 12 months.
- Supply chain risk management and operational resilience **demand collective responsibility, collaboration and information sharing** with both internal functions and external suppliers and strategic partners. Most executives acknowledge **they need to do a better job on all fronts.**

Key Findings

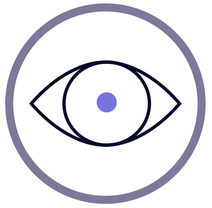


69%

say they plan to make wholesale changes to their supply chain footprint

$199M

is the average annual cost of supply chain disruptions to each organization

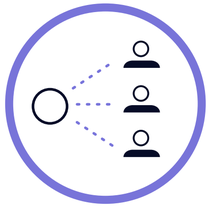


19%

of organizations currently monitor supplier risks on a continuous basis

76%

plan to implement or introduce technology to gain visibility within the next 12 months



87%

agree that collective responsibility is required to protect against supply chain disruptions

1

Reconfiguring Global Supply Chains in Response to Disruptive Events

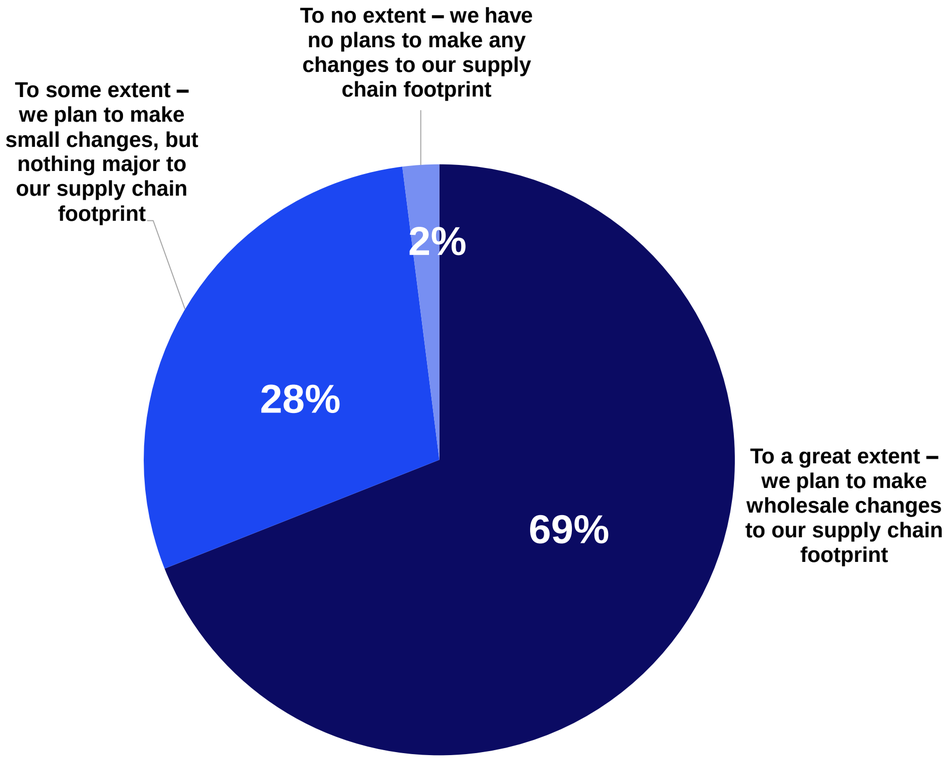
More than half of organizations plan to make ‘wholesale changes’ to their supply chain footprints

Major supply chain disruptions can no longer be considered rare events. Global shocks such as the US-China trade war, the COVID-19 pandemic and, most recently, Russia’s invasion of Ukraine, continue to ripple across the world’s supply networks. Organizations must adapt to these new realities – and many already are.

Enthusiasm for globalization – built on a plentiful supply of cheap labor – has waned in many parts of the world. It should be no surprise that almost three-quarters (69%) of respondents say their organizations plan to make “wholesale changes” to their supply chain footprints. Another 28% expect to make “small changes”.

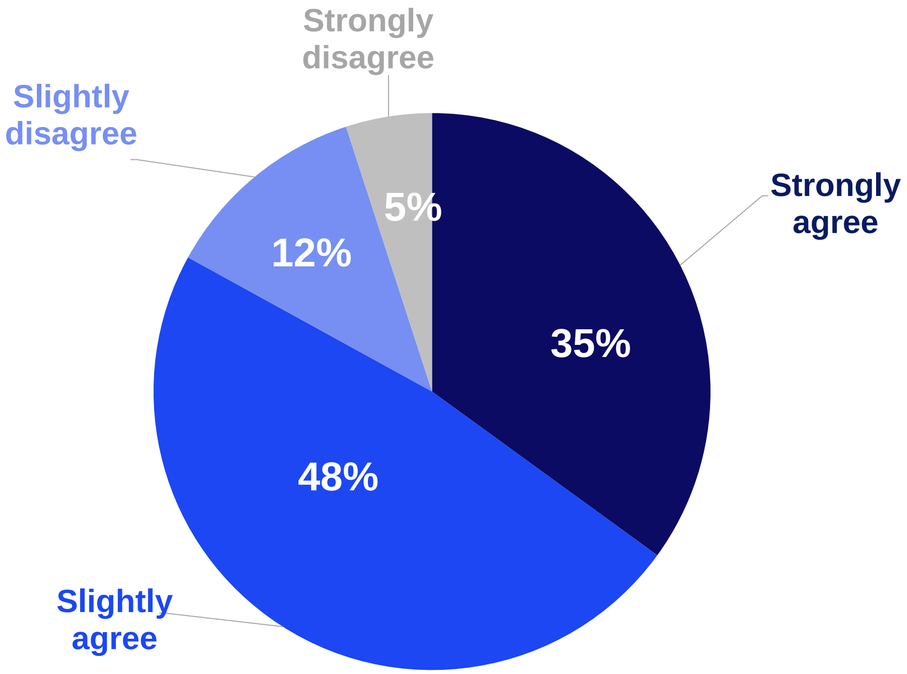
The drivers for these changes will vary, depending on where customers are located, the company’s growth strategy, what it buys from suppliers or the services it delivers.

But the common message is clear: “business as usual” is no longer an option.



Q: To what extent does your organization have plans to redesign your supply chain footprint? (Not showing all answer options) n=300

Over 4 in 5 tech executives agree their supply bases are too concentrated in certain geographic locations



Q: To what extent do you agree with the following statement? "My organization has too many suppliers concentrated in one area of the world and this is of concern to us"; n=300

As the tech community reshapes its global footprint to regain control of supply chains and remove vulnerabilities, one of the main areas targeted is concentration risk.

Russia's invasion of Ukraine highlighted the dependence of the US, Europe, and other nations on these two countries for critical commodities such as oil and gas, coal, nickel, palladium, wheat, corn and fertilizer. Elsewhere, semiconductor manufacturing is heavily concentrated in Taiwan, while China controls an outsized share of rare earth minerals used to make products such as batteries for electric vehicles.

Disruptions in concentrated supply chains can devastate and destabilize economies a world away. Diversifying supply bases is an urgent priority for companies and governments looking to protect themselves.

DATA DIVE

83% agree their organization currently has too many suppliers concentrated in one area of the world

Companies are retreating from global supply chains – half of suppliers are set to be reshored or nearshored

Concentration risks, shortages, and growing lead times have strengthened the case for local sourcing and manufacturing among technology executives.

Supply chain operating models of the last 30 years dictated that products be manufactured where costs are lower and labor is plentiful. But as wage gaps have closed and cybersecurity concerns over foreign actors have mounted, calls to “reshore” production to home countries such as the US, or “nearshore” it in adjacent ones such as Mexico, have grown.

While this trend is still emerging, the Interos survey indicates a clear appetite for increased reshoring. Funding and executing these plans will be high on the list of challenges.

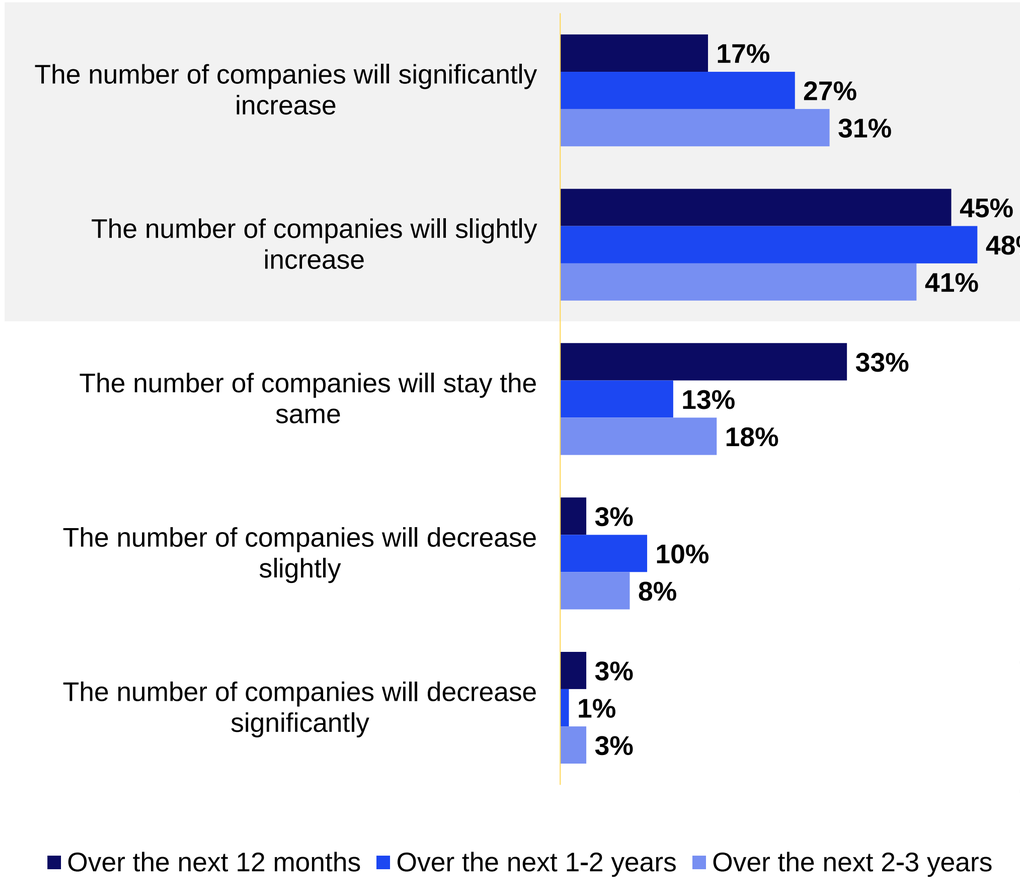
"What we have to address is a shortage of raw materials, changes in demand patterns and problems with lead times.”

– Procurement Executive, IT & Technology, France

49% **of suppliers are expected to be reshored or nearshored on average in the next three years**

Q: What percentage of your organization’s suppliers do you expect to reshore/nearshore in the next three years?; n=300

More than 6 in 10 tech companies plan to increase the number of companies in their supply chains



62% next 12 months

76% next 1-2 years

71% next 2-3 years

‘Significant’ or ‘slight’ increase in numbers

Irrespective of specific reshoring/nearshoring opportunities, there is a need to diversify supply bases to address concentration risk and reduce dependence on the single sources (by design) or sole sources (no alternative options) that characterize many industries.

A clear majority of tech executives plan to increase the number of firms in their supply chains steadily over the next three years – compared with 3% that plan to significantly reduce them. It’s worth noting that for the technology sector, that percentage is far lower than global average of 14%.

This may be due to increased pressure on the industry to divest from sources in countries like China. Balancing the pressure to reduce sole sources while also reducing foreign dependence is sure to present a challenge.

Q: To what extent will the number of companies in your organization’s supply chain change over the following timeframes? Over the next 12 months; Over the next 1-2 years; Over the next 2-3 years” n=300.

2

Supply Chain Disruptions are Frequent, Expensive and Often Hidden From View

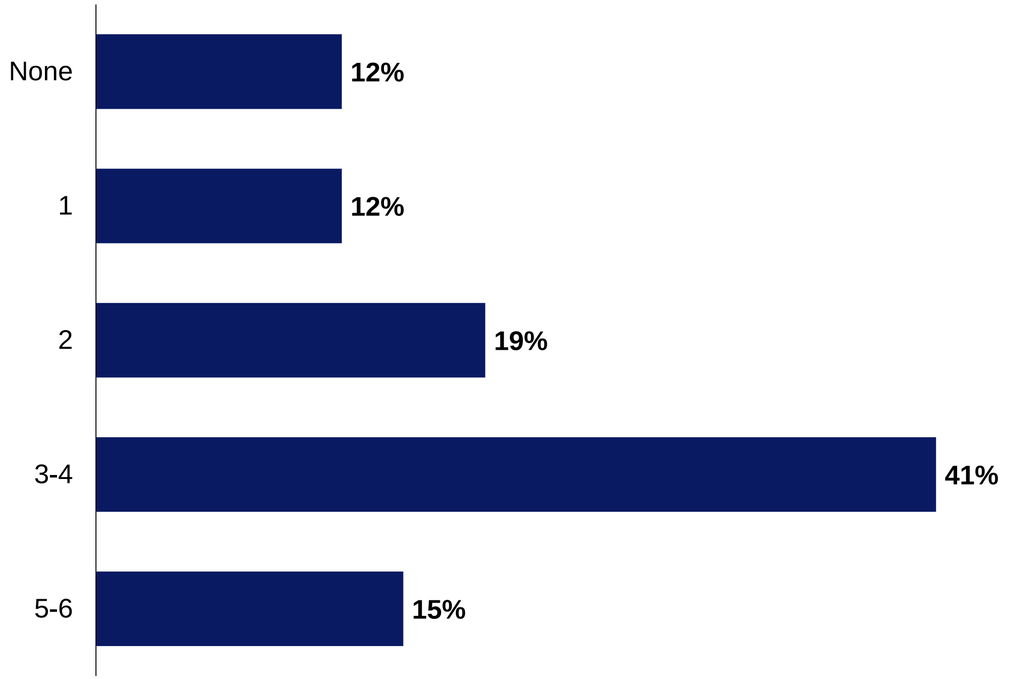
Disruptive, high-impact supply chain events are now a regular occurrence

Supply chain disruptions have become a regular item in mainstream news media during the past few years. COVID-19 and Russia's war on Ukraine have dominated the headlines, but other important stories have included numerous cyber events including the ubiquitous Log4j vulnerability as well as shortages of microchips.

Unsurprisingly, our findings show that the number of major shocks supply chain teams must contend with has increased as well. On average, tech executives said their organizations were impacted by three significant risk events, including cyber-attacks and political instability, during the past 12 months, while 15% said it was more than four.

This demonstrates the importance not only of having resources and processes in place to respond to such disruptions, but also proactive risk planning, assessment, mitigation and monitoring strategies.

Number of significant supply chain events impacting organizations in the last 12 months



Q: How many significant supply chain events (e.g. cyber-attack, political instability, etc.) has your organization been impacted by within the last 12 months? (Not showing all answer options); n=300

DATA DIVE

3 The average number of significant supply chain events that organizations have experienced in the past 12 months

Frequent supply chain disruptions cost tech organizations tens of millions of dollars a year

$199M

The average annual cost of supply chain disruptions

Q: In your estimation, what is the annual cost in revenue to your organization as a result of supply chain disruption? n=300

Major supply chain disruptions can reduce supply availability and cause delays. But they are also costly from a financial perspective, since they may involve increased costs to remedy damages and recover from cyber breaches, possibly repair and update software or even lose business and contracts if in violation of evolving regulations. Reputational damage could also cause persistent losses.

On average, our survey suggests that the annual cost of supply chain disruptions to tech organizations is $199 million, or 1.72% of their annual revenue. This figure varies somewhat by geography. The greatest loss as a percentage of annual revenue was reported in France ($389M) while the lowest was reported in Canada ($99M).

Interestingly, this was the opposite of results for the A&D sector, where Canada faced the costliest disruptions ($189M) and France ($107M) saw the least expensive.

Despite these variations, the total costs remain significant and, in many cases, can be avoided or reduced through a more proactive approach to supply chain risk management and operational resilience.

Tech organizations cannot afford to ignore any of the six major categories of supply chain risk

A forward-thinking approach to effective supply chain risk management must consider all potential sources of disruption, whether frequent and relatively predictable or rare and difficult to foresee. This is because the financial impact to tech organizations of risk events is spread evenly across the six categories shown in the chart opposite.

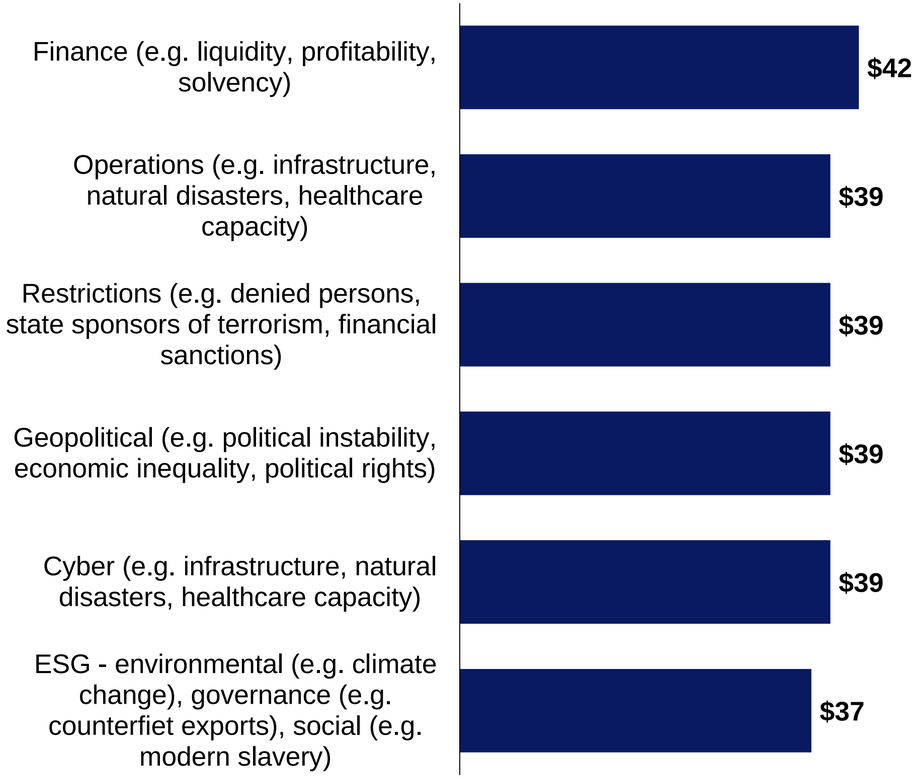
The average annual disruption cost ranges from a high of $42 million in the case of financial issues – a key supplier going bankrupt, for instance – to $37 million for environmental, social and governance (ESG) risks – for example, fines for breaching human rights laws at a factory or service location.

These similarities in cost impact highlight the fact that tech organizations must take each of these risk factors seriously and should refrain from focusing all their efforts on just one or two categories in isolation.

COMPARISON

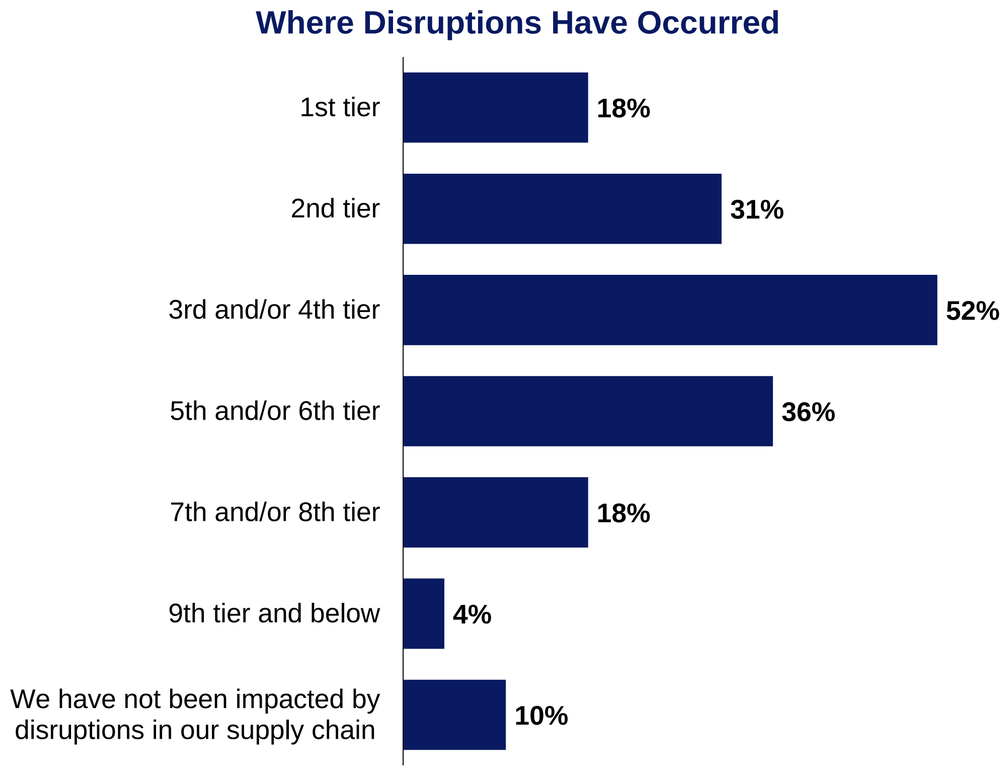
2021

In 2021, Tech executives rated Cyber risk as the most-impactful risk, while damages estimates in 2022 show all risk factors to be nearly equally damaging.



Q: In your estimation, what is the annual cost in revenue to your organization as a result of supply chain disruption per category? n=300

Most tech organizations have experienced supply chain disruptions beyond their Tier 1 suppliers



Q: Disruptions in which of the following tiers of your organization's supply chain have impacted your business operations? (Not showing all answer options); n=300

Tech organizations need to focus beyond Tier 1 suppliers given that the overwhelming majority of executives reported supply chain disruptions occurring outside their direct supply base, with the highest proportion occurring in Tiers 3/4.

This is a common gap for several reasons: First, because tech organizations lack visibility into their sub-tiers, severely limiting their ability to stay ahead of disruption. Second, because Tier 1 partners themselves either lack information about potential disruptions further upstream or don't share this data in a transparent and timely way.

Many risk events are therefore hidden from view. Supply chain managers may discover the issues only when products or components stop arriving.

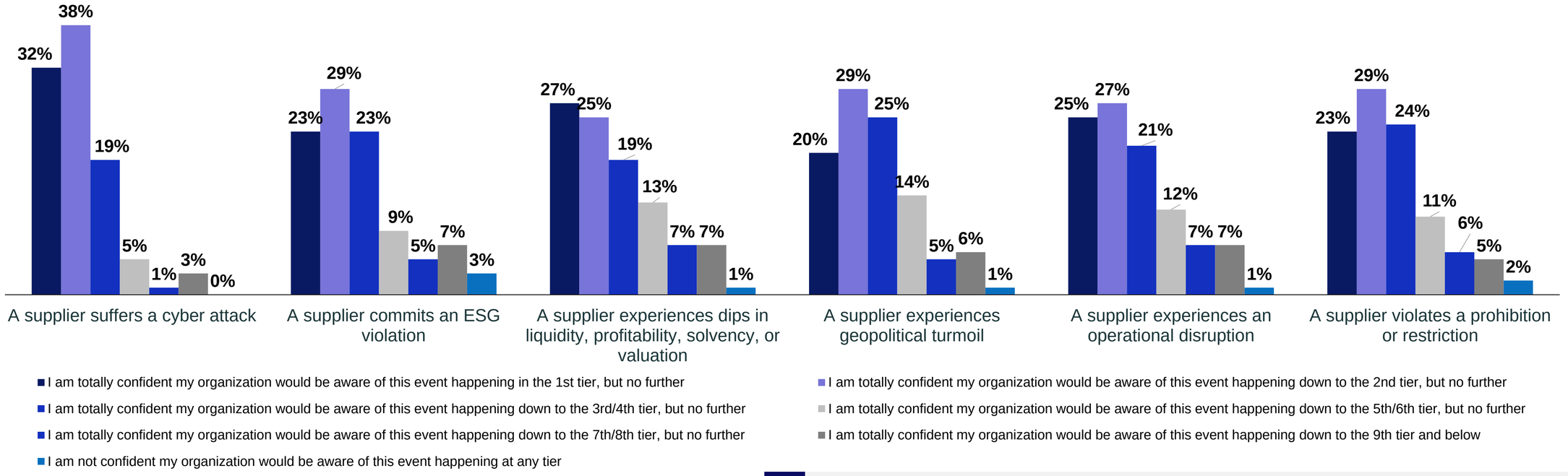
DATA DIVE

52% of organizations have experienced disruptions beyond Tiers 1 and 2 of their supply chain

Note: This report uses the term "Tiers," as opposed to "parties". For the purposes of this report, a Tier 1 supplier is the same as a 3rd party, a Tier 2 supplier is a 4th party, etc.

The majority of tech executives are confident they would know about disruptive events at Tiers 1 and 2 only

The danger of being taken by surprise when disruptions happen – leaving little time to respond in a cost-efficient way – is underlined by the fact that most survey participants in the tech sector are confident they would only be aware of the six risk events shown below if they originated in the first two tiers of their supply bases. More than a fifth (20-32%) depending on the event type) say they only have confidence at the Tier 1 supplier level. This leaves many organizations at the mercy of invisible supply chain shocks.



Q: Down to which tier in your organization's supply chain are you totally confident you would be aware of, should one of the following events happen? (Not showing all answer options); n=300

COMPARISON

50% of tech leaders in our 2021 survey reported no ability to monitor beyond Tier 2.

3

Supply Chain Risk Practices Require Further Improvement

Organizations are not evaluating supplier risk in a significant majority of relationships

Identifying and assessing different types of supplier risk and understanding other factors such as the true value at risk in a given scenario, or the availability of alternative sources, is critical to operational resilience.

Risk prioritization via segmenting suppliers by their value to the organization is a pragmatic approach. However, it is concerning that just over half of suppliers (57%) are typically evaluated during the risk analysis process.

While a deeper level of analysis may be required for the most strategic and critical partners, it is necessary to assess a broader set of suppliers for financial, cyber and other risks, both for compliance and operational resilience reasons. Without this, firms leave themselves exposed.

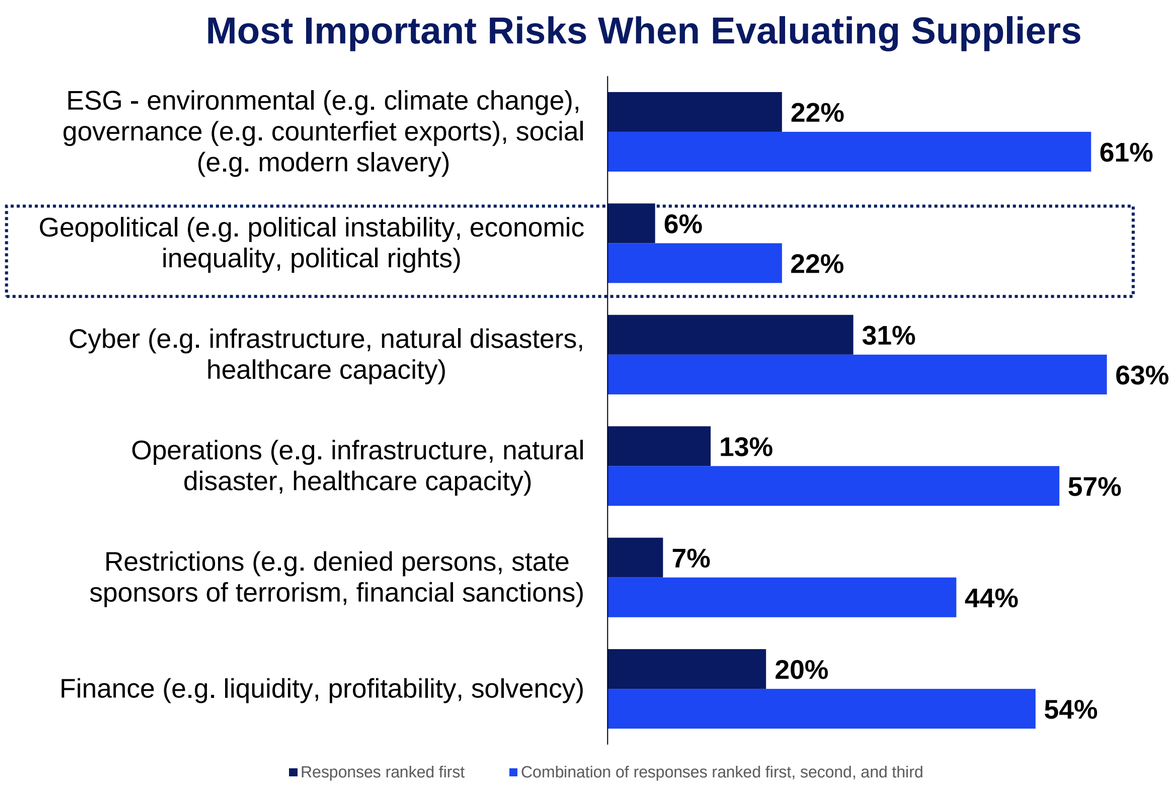
"[To build collective resilience] we have increased communication with our close suppliers and partners to find out the possibilities of disruptions happening and getting a head start… when they happen."

– IT/IT Security Executive, IT & Technology, UK

57% **of suppliers, on average, are evaluated as part of an organization's risk analysis**

Q: What percentage of your organization's suppliers are evaluated for risk as part of your organization's risk analysis?; n=300

Primary risk factors for tech are cyber and ESG but other factors are influential



Q: Which of the following factors are most important to your organization when evaluating strategic partners/suppliers?; n=300

While tech respondents ranked financial and ESG risks as the most-important factors when evaluating suppliers, risk factors are not always easily bucketed and must be evaluated collectively. For example, while geopolitical risk was rated lowest, geopolitical issues such as military conflict could emerge as issues in the cyber domain.

The war in Ukraine demonstrates how quickly conflict can disrupt fragile interconnected global supply chains, The ongoing US-China trade war and the threat of a Chinese invasion of Taiwan – the dominant player in semiconductor manufacturing – are other examples of major geopolitical issues that must be factored into supply chain risk management efforts.

Organizations that fail to take sufficient account of geopolitical risks, as part of a comprehensive supplier risk assessment, could be left scrambling to respond to sudden supply shortages, increased cyber risk, and government restrictions.

Only 19% of tech organizations say they monitor supplier risks on a continuous basis

The frequency with which organizations monitor risk across their supply chains is also critical. Less than 2 in 10 respondents said they “continuously” monitor supplier risks, with over three-quarters doing this on a weekly, monthly or quarterly basis.

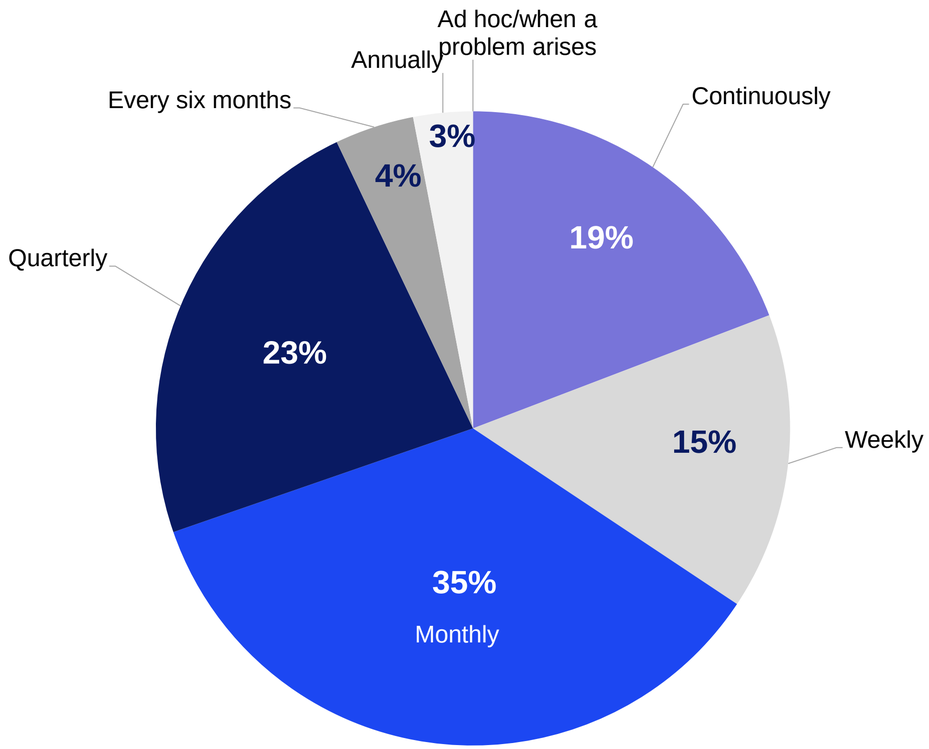
With so many potential sources of disruption across an extended global supply network, there can be significant benefits to those with real-time, near-real-time or at least daily warnings of risk events.

For organizations seeking to improve their ability to protect themselves against vulnerabilities in their supply chains, moving from a periodic to a continuous monitoring strategy should be high on the priority list.

“We have put in place the latest technology to ensure real time notifications are always preserved and met, this ensures everybody knows what they are doing and nobody is left in the dark.”

– IT/IT Security Executive, IT & Technology, UK

How Often Supplier Risk is Monitored



Q: How frequently is your organization monitoring supplier risk as part of your organization’s risk analysis?; n=299 [Shown to respondents said their organization evaluates suppliers as part of their risk analysis]

4

The Role of Technology in Managing Risk Proactively

Technology enables organizations to mitigate supply chain risk and gain a competitive advantage

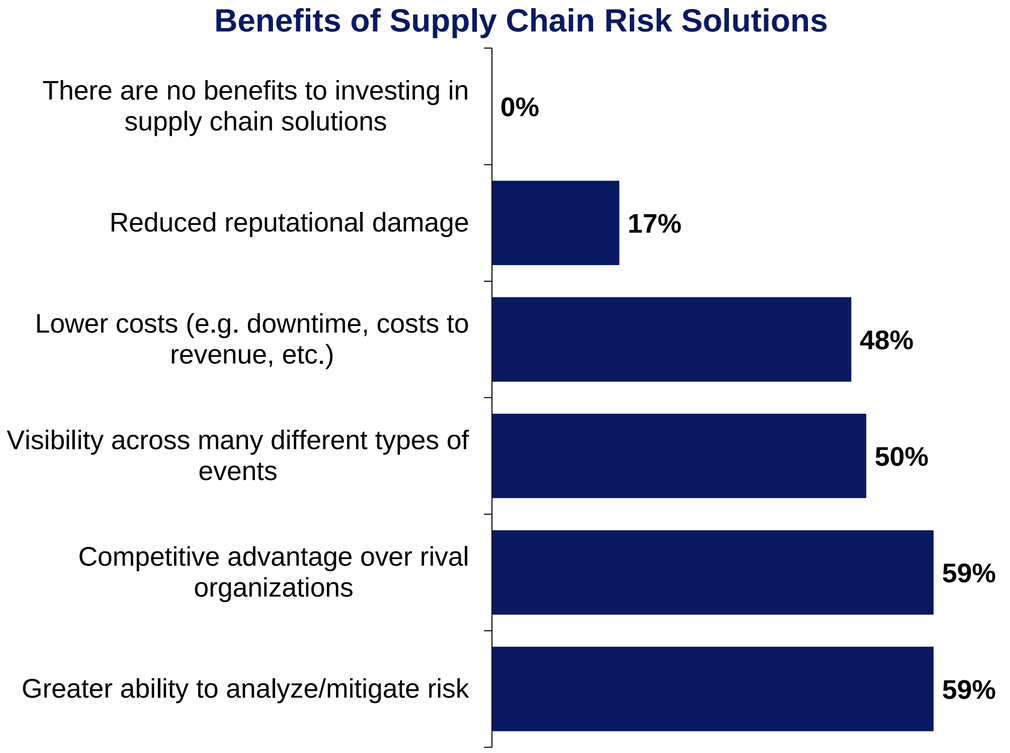
All of our tech industry respondents felt there were clear benefits to be gained by investing in software solutions for supply chain risk management.

Chief among these benefits is the ability to analyze and mitigate risk through enhanced access to data and information. Almost half of the sample also saw opportunities to gain competitive advantage over rivals through the proactive application of risk technology, rather than simply limiting the negative impact from supply chain disruptions.

Reducing extra costs associated with such disruptions and reduced chance of reputational damage via continuous monitoring were also identified as benefits by a substantial minority of executives.

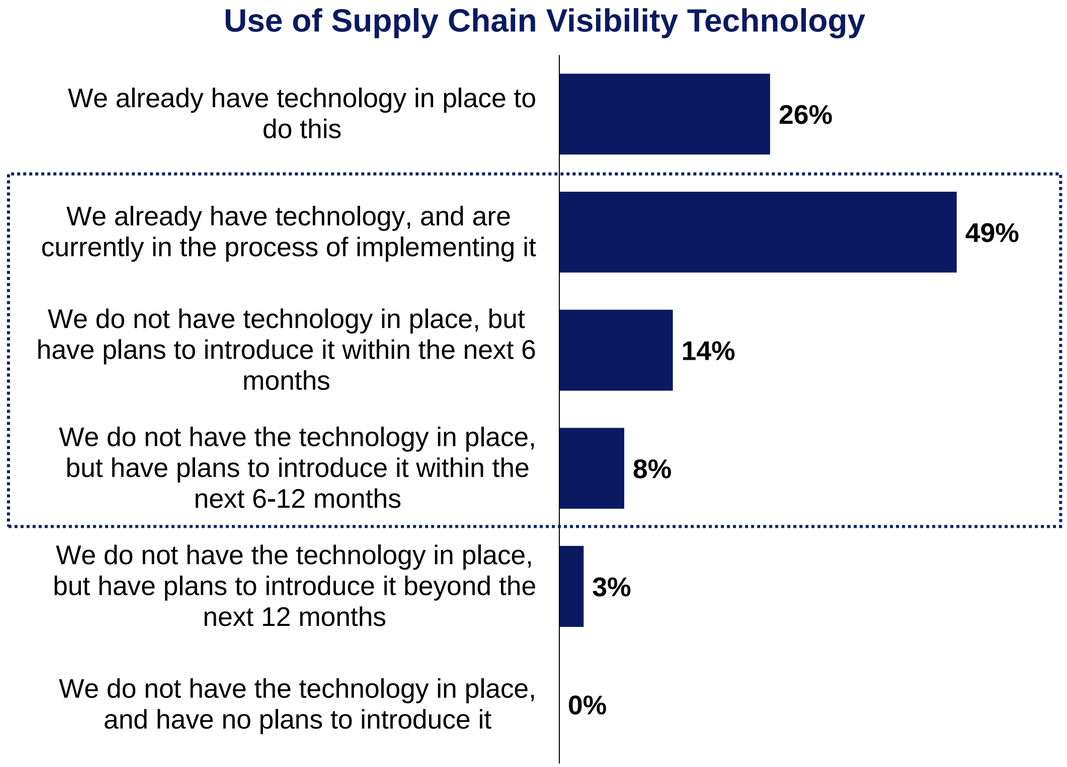
"We have ensured we have all the data and all the information we need for disaster recovery to make sure we get every scenario covered in regards to an emergency or needing to find resource."

– Security/IT Executive, IT & Technology, Canada



Q: In your opinion, what are/would be the greatest benefits to your organization investing in a supply chain solution that can analyze risk across multiple categories? (Not showing all answer options); n=300

One quarter use intelligent supply chain visibility solutions – but most plan to implement them soon



Q: Does your organization plan on leveraging automated/intelligent solutions to gain visibility into interdependencies into your supply chain? (Not showing all answer options); n=300

Understanding the interdependencies between an organization and its suppliers at different tiers is a necessary component of operational resilience because many supply chain disruptions originate among indirect suppliers further upstream.

Without this level of visibility, managers cannot make truly informed decisions about where and how to mitigate potential sources of risk.

Supply chain visibility is a big data problem that requires a big data solution.

While about a quarter of respondents already use intelligent and automated technology for this purpose, almost three-quarters say they are implementing it or plan to introduce it within 12 months.

COMPARISON

45% of tech executives in 2021 considered AI/intelligent visibility solutions to be the most beneficial method of supply chain monitoring out of 7 options, which was a higher percentage than any other option.

Most would happily partner with a solution provider that offers broad visibility of supply chain risks

"[We are] Ensuing that we have a system in place that checkmate and distribute information in real time to all staff at all levels and in all locations without any part being jeopardized by any outer level disruptions."

– Procurement Executive, IT & Technology, US

The importance of having multi-tier supply chain visibility and the need for advanced technologies to obtain it highlights the crucial role that risk solution providers play in helping organizations to improve their supply chain risk management practices and build greater resilience.

This fact explains why the vast majority of both procurement and IT/IT security executives across all geographic regions in our survey of financial service institutions agree that they would value a partnership with a vendor that can deliver visibility of supply chain risks to all relevant functions and stakeholders within their organizations.

DATA DIVE

97% Of tech leaders have implemented or plan to introduce technology to gain visibility of supply chain interdependencies in the next 12 months.

87% **would value a partnership with a vendor that gives supply chain risk visibility to all relevant departments**

Q: To what extent do you agree or disagree with the following statement? "My organization would value a partnership with a vendor who helps give us visibility over supply chain risks, to all relevant departments"; n=270 who "strongly agree" or "somewhat agree"

5

Operational Resilience is a Multiplayer Game

Collective responsibility is key to help organizations reduce their exposure to supply chain shocks

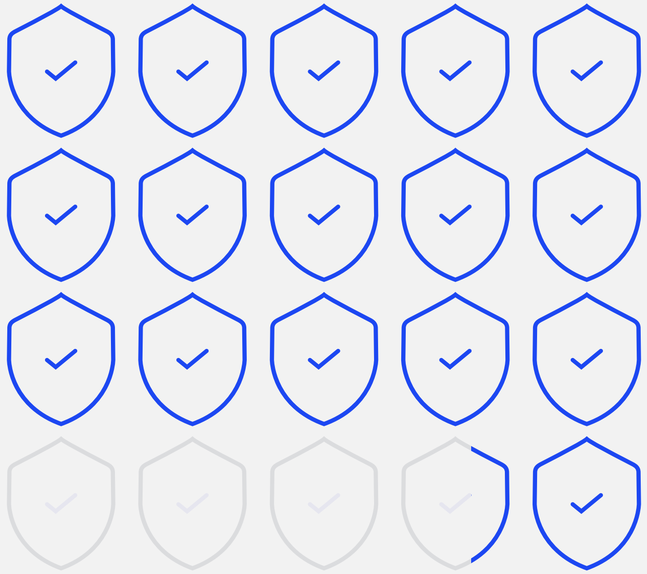
"[To build collective resilience we] have increased communication with our close suppliers and partners to find out the possibilities of disruptions happening and getting a head start…"

– Security/IT Executive, IT & Technology, UK

Interos defines operational resilience as "the ability to continue providing products or services in the face of adverse market or supply chain events. An operationally resilient organization manages risk in a strategic and proactive way to prevent, respond to and recover quickly from disruptions that could impact its customers, brand reputation or financial performance, and to seize new business opportunities."

Achieving operational resilience is not, however, something that one organization can do on its own; it requires collective responsibility and an ecosystem-wide approach. This is recognized in the finding that **almost 9 out of 10 tech** executives agree that working collaboratively across internal functions and with key suppliers and other external partners is critical if they are to equip their organizations to respond effectively in the face of constant and significant supply chain disruptions.

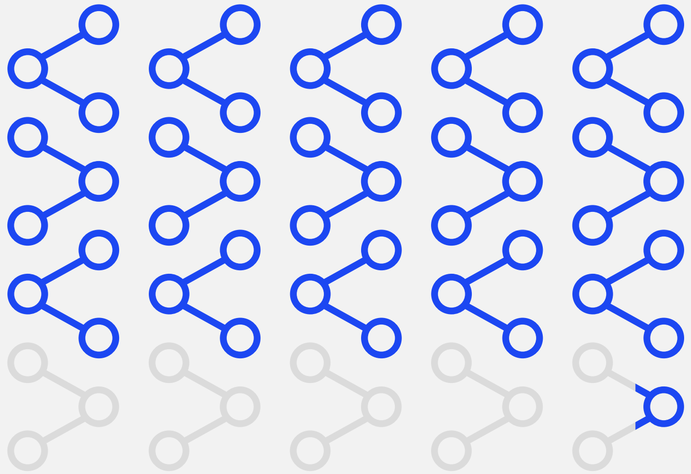
87% **say cooperation across internal departments and with suppliers is vital to protect against disruptions**



Q: To what extent do you agree or disagree with the following statement? "Collective responsibility (e.g. across departments/suppliers/partners) is critical to help ensure my organization is best protected against supply chain disruptions"; n=263 who "strongly agree" or "somewhat agree"

Better internal collaboration and information sharing is needed to manage supply chain risk effectively

80% **agree they need to improve how they collaborate and share information internally across departments**



Q: To what extent do you agree or disagree with the following statement? “My organization needs to improve how we collaborate/share information internally (e.g. across departments) when it comes to supply chain risk”; n=232 who “strongly agree” or “somewhat agree”

Collective responsibility for supply chain risk starts within the four walls of an organization. Without effective cross-functional information sharing and collaboration, it is difficult to align interests, develop processes and mitigate risks jointly with external suppliers and other partners.

Four-fifths of surveyed tech executives agree they need to improve how they collaborate and share information between departments. In the case of cyber threats that means organizations require close cooperation between IT security, supply chain and procurement managers to identify and plug vulnerabilities at suppliers with access to their systems and networks.

With increasingly complex and tighter regulation, close integration among professionals in the finance, sustainability, sourcing, legal and enterprise risk functions is critical.

An overwhelming majority accept their organizations must improve external collaboration with suppliers

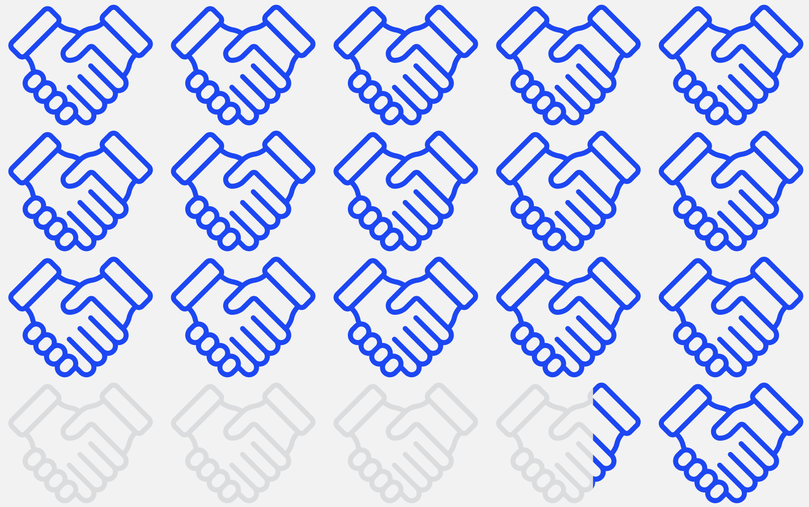
"Joint cooperation is vital. All parties in the supply chain should know what is expected from them. We can assist the lower tiers in providing knowledge, expertise and help them (part financially) to invest in the latest technology."

– IT/Security Executive, Germany

Operational resilience is a multi-player game; it requires the support and cooperation of suppliers and strategic partners throughout the supply chain. Again, an overwhelming majority of tech executives agreed that they need to do a better job of external engagement when it comes to building operational resilience.

Supplier collaboration in risk management is vital for several reasons. First, because trust-based relationships are essential if suppliers are to share sensitive data about their own supply chains and risks that may impact efficient operations. Second, because business continuity and contingency plans need to be understood and stress-tested between different organizations. And third, because effective risk mitigation strategies often require coordinated decision making, aligned processes, and joint investments, metrics and incentives.

78% **agree they need to improve how they collaborate and share information externally with suppliers/partners**



Q: To what extent do you agree or disagree with the following statement? "My organization needs to improve how we collaborate/share information externally (e.g. with partners and suppliers) when it comes to supply chain risk"; n=232 who "strongly agree" or "somewhat agree"

Conclusions and Recommendations

Conclusions & Recommendations

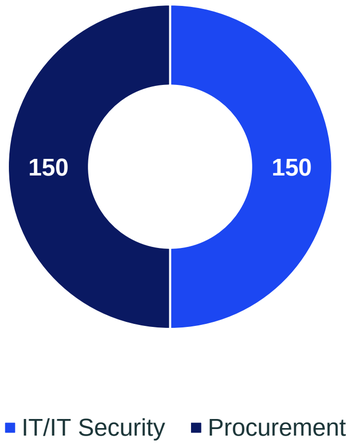
- When reconfiguring global supply chain footprints, focus on reducing concentration risk for products and services by diversifying the number of suppliers and their geographic locations to broaden your options during disruptive events.
- Operational resilience requires proactive risk planning, assessment, mitigation and monitoring capabilities, as well as the ability to react quickly and effectively when a major disruption happens. Make the case for additional resources to do this upfront work if required and ensure they pay attention not only to direct, Tier 1 suppliers, but also to key indirect suppliers at Tiers 2, 3, and beyond.
- Align the depth and rigor of supplier risk assessments according to their value and importance to the business, while broadening the number of suppliers that are evaluated for financial, operational, geopolitical, cyber and ESG risks.
- Move from a periodic approach to supplier risk monitoring to a strategy that puts a premium on real-time insights and speed of action.
- Invest in operational resilience solutions that map interdependencies across multiple tiers of the supply chain, provide visibility of relationships and major risk factors, and enable your organization to monitor supplier risks and potentially disruptive events on a continuous basis.
- Educate internal stakeholders about the need for proactive supply chain risk management and operational resilience. Build a collaborative culture of risk awareness and develop processes, governance mechanisms and incentives that drive information sharing and foster cross-functional collaboration.

Appendix

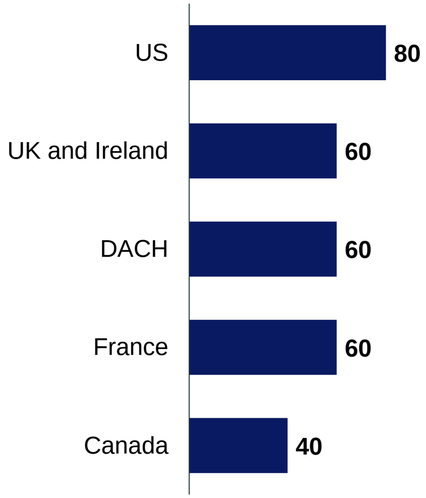
Survey Demographics

300 IT, IT security and procurement decision makers in the technology sector were interviewed in January, February and March 2022.

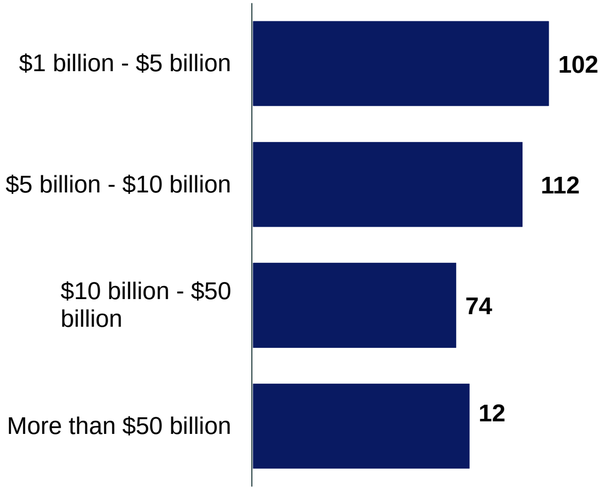
Role



Location



Revenue Size



Figures show the number of survey respondents in each category.

Interos commissioned independent technology market research specialist Vanson Bourne to undertake the quantitative research upon which this report is based. Interviews were conducted online using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.

About Vanson Bourne: *Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com.*

Commentary Report • March 2022 • www.interos.ai