interos

Resilience 2022

The Interos Annual Global Supply Chain Report
Focus: Chief Information Security Officers (CISOs)

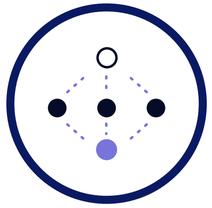
Commentary Report • May 2022 • www.interos.ai

Contents

Executive Summary

- Interos surveyed 750 Chief Information Security Officers (CISOs) and IT security decision makers across multiple industries about the impact of continued supply chain disruption.
- Organizations 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 50%** of existing supplier contracts.
- Organizations were impacted by **three** significant supply chain disruptions during the past year costing, on average, a combined **$160 million in lost revenue**.
- Disruption causes were **split evenly between financial, operational, cyber, ESG and other risk categories.** Most companies were impacted by sub-tier supplier issues where they have limited visibility.
- Slightly **over half of an organization’s suppliers** are typically evaluated during risk analysis exercises. Only one-tenth of CISOs, IT and IT security executives say they continuously monitor supplier risks.
- Technology is seen by IT and IT security leaders as delivering significant benefits. While **most organizations currently lack advanced supply chain visibility solutions**, they 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 CISOs and IT executives acknowledge **they need to do a better job on all fronts.**

Key Findings

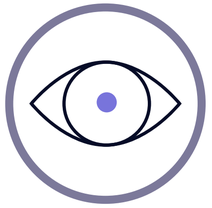


68%

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

$160M

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

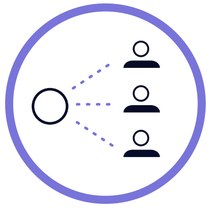


11%

of organizations currently monitor supplier risks on a continuous basis

80%

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



81%

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

1

Reconfiguring Global Supply Chains in Response to Disruptive Events

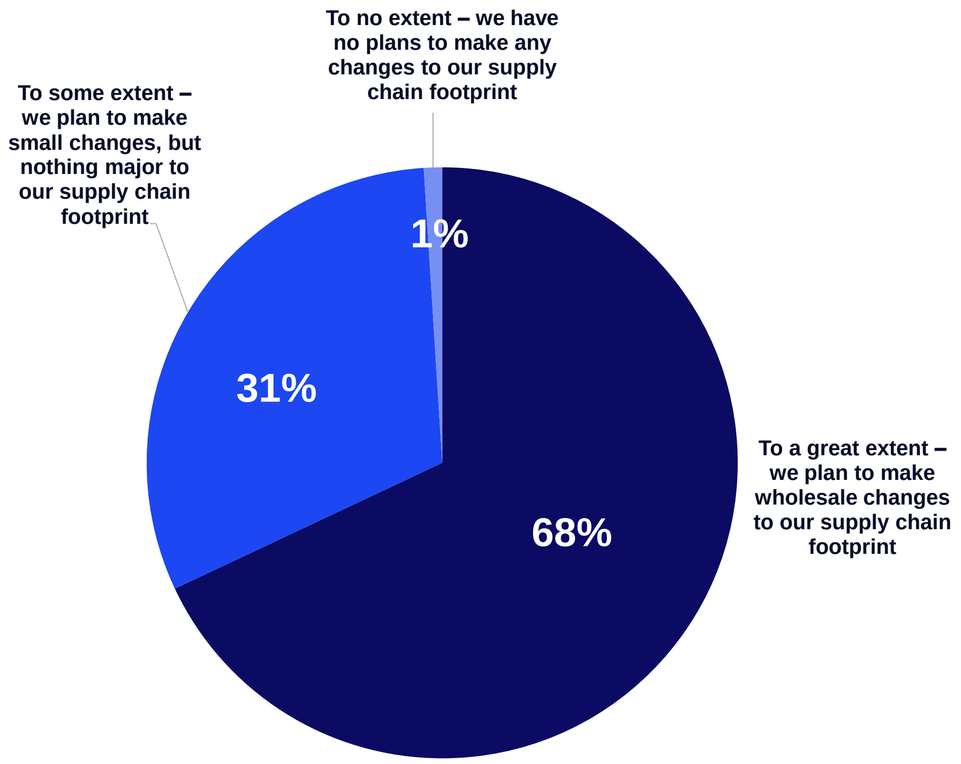
Two-thirds of IT and IT security leaders say their organizations plan to make ‘wholesale changes’ to supply chain footprints

Major supply chain disruptions can no longer be considered rare events. Global shocks such as the US-China trade war, COVID-19 and 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, technology and low-cost shipping – has waned in many parts of the world. Almost 7 in 10 CISOs/IT security leaders say their organizations plan to make “wholesale changes” to their supply chain footprints. Nearly one-third (31%) expect to make “small changes”.

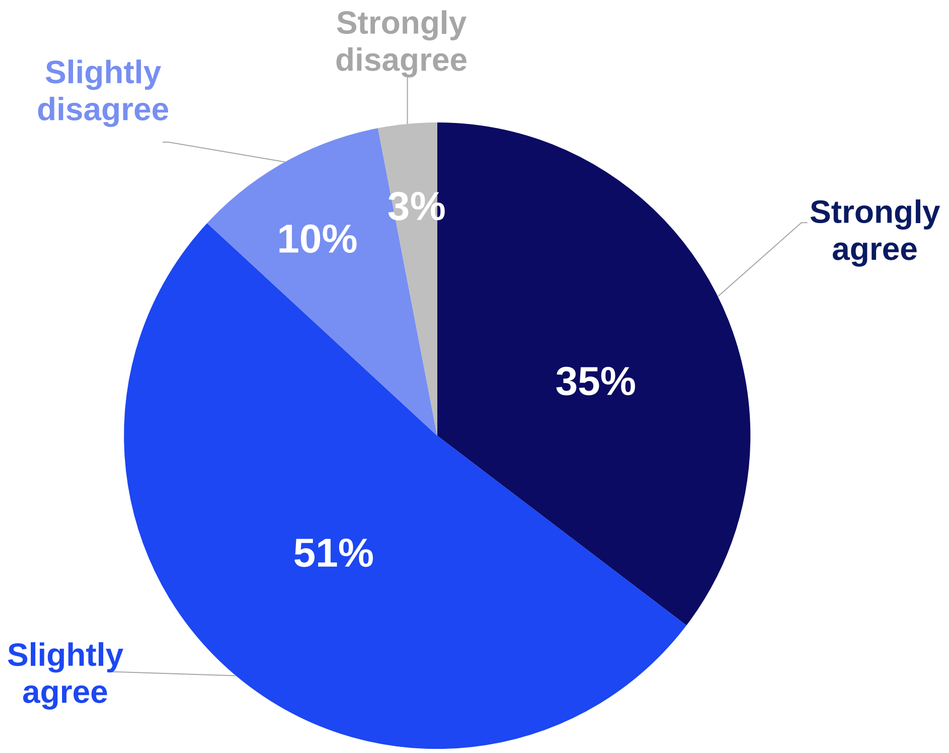
The drivers for these changes vary depending on customer location, company growth strategies, supplier sourcing needs, and the products and services the company delivers.

But the common message from CISOs 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=750

More than 8 in 10 CISOs/IT security leaders 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=750

Concentration risk is a key area of focus as organizations reimagine their supply chains for growth and resilience.

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 IT security and procurement leaders in companies and governments that are looking to protect themselves.

DATA DIVE

86% 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, supply shortages and growing lead times have strengthened the case for local sourcing and manufacturing across multiple industries.

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 logistics problems have mounted, calls to “reshore” production to home countries such as the U.S., 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.

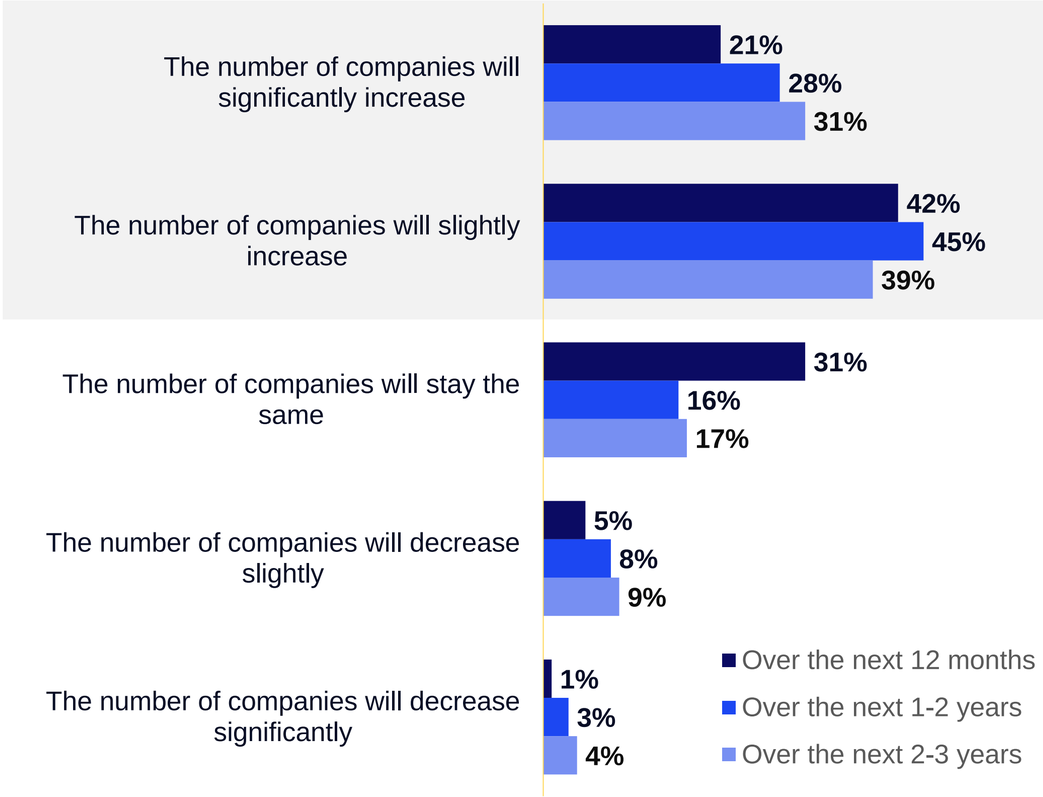
“We have a system of multiple redundancies in all aspects of our supply chain structure to greatly help alleviate bottlenecks at any one point in any chain.”

– IT/Security Executive, IT & Technology, Canada

50% **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=750

More than 6 in 10 organizations expect to increase the number of companies in their supply chains



63% next 12 months

73% next 1-2 years

70% next 2-3 years

‘Significant’ or ‘slight’ increase in numbers

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=750

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 IT and IT security leaders say they plan to increase the number of firms in their supply chains steadily over the next three years – compared with 13% or less that plan to reduce them.

When considered with our other findings, it becomes clear that organizations are serious about managing supply chain risk more effectively and increasing operational resilience.

2

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

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

While COVID-19 lockdowns have dominated global headlines, supply chain turmoil can come in many forms: see the Suez Canal blockage, auto factory shutdowns due to a shortage of microchips, and spiking energy and food prices caused by Russia's war on Ukraine.

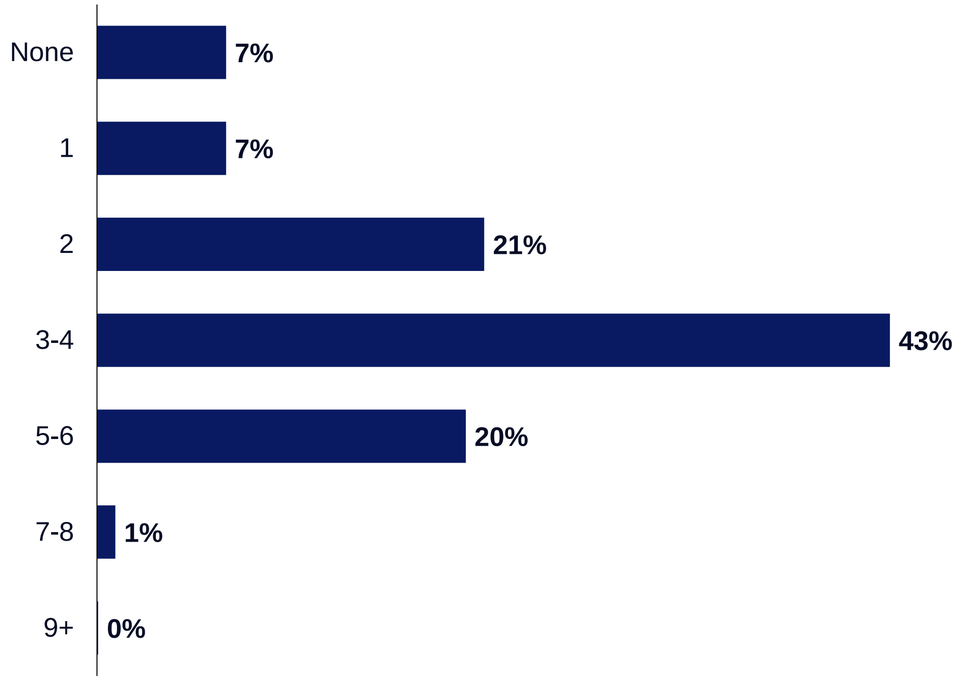
Unsurprisingly, our findings show that the number of major shocks that IT security teams must contend with has increased as well. On average, CISOs and IT leaders said their organizations were impacted by three significant risk events, including cyber-attacks and political instability, during the past 12 months, while 21% said it was more than five.

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

DATA DIVE

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

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=750

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

$160M

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=750

Major supply chain disruptions can reduce supply availability, extend lead times, and delay order fulfillment. 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 pay penalties if in violation of increasing restrictions. Reputational damage could also cause persistent losses.

According to IT and IT security leaders, the annual cost to their organizations of supply chain disruptions is $160 million, or 1.87% of their annual revenue. This figure varies quite a bit by geography and by sector. The highest costs were reported in Canada ($187 million) and in government ($200 million), while the lowest were in the UK and Ireland ($113 million) and in IT and technology ($135 million).

Despite these variations, the total costs are significant and can be avoided or reduced through proactive supply chain risk management and operational resilience.

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

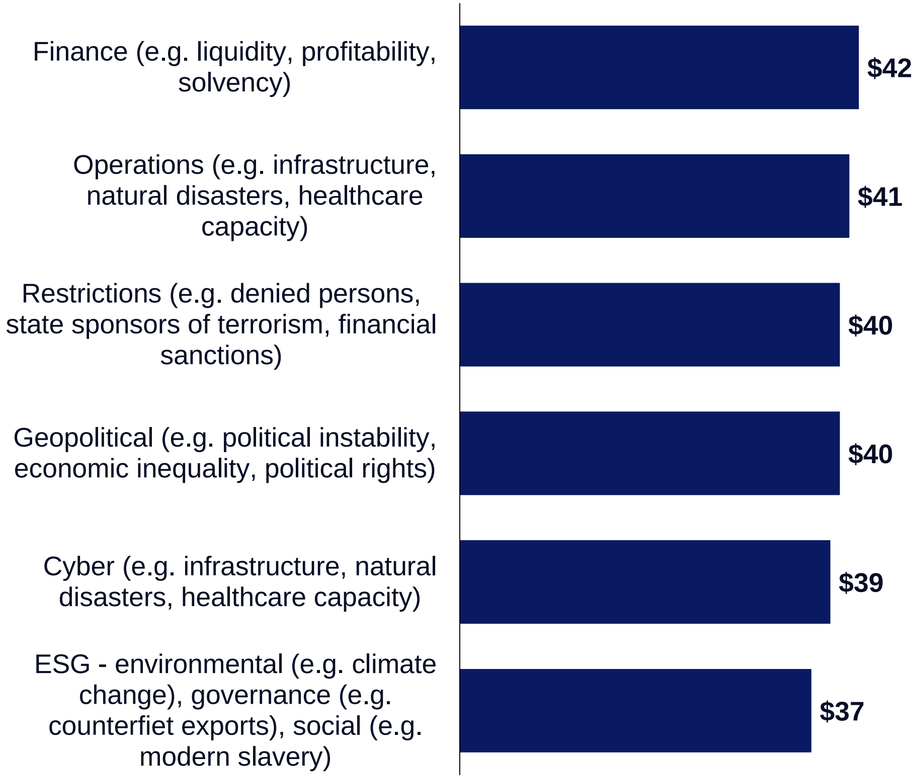
A forward-thinking approach to effective supply chain risk management must consider all potential sources of disruption, whether frequent and relatively predictable or rare and difficult to foresee. This is because the financial impact to organizations of risk events is evenly spread across the six categories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

The average annual disruption cost, according to IT and IT security respondents, ranges from $42 million for financial issues – such as a key supplier going bankrupt – 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 CISOs, IT leaders and their organizations must take each of these risk factors seriously and refrain from focusing on just one or two categories in isolation.

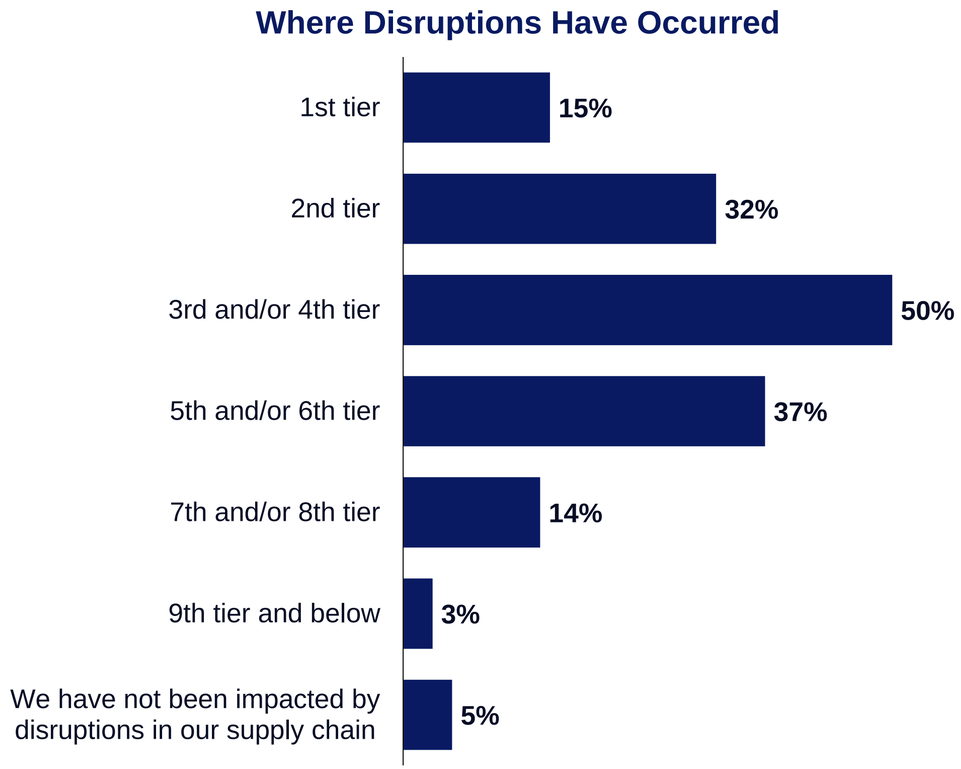
DATA DIVE

.55% The average annual percentage of revenue lost due to a category-specific supply chain disruption



Q: In your estimation, what is the annual cost in revenue to your organization as a result of supply chain disruption per category? n=750

Most 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=750

Organizations need to focus beyond Tier 1 suppliers given that the overwhelming majority (87%) of IT and IT security executives reported supply chain disruptions occurring outside their direct supply base. More than two-thirds (67%) reported being been impacted by risk events below Tier 2 (their supplier's suppliers).

This is a common gap for several reasons: First, because 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. IT and IT security managers may discover the issues only when their networks are attacked or product orders stop arriving on time.

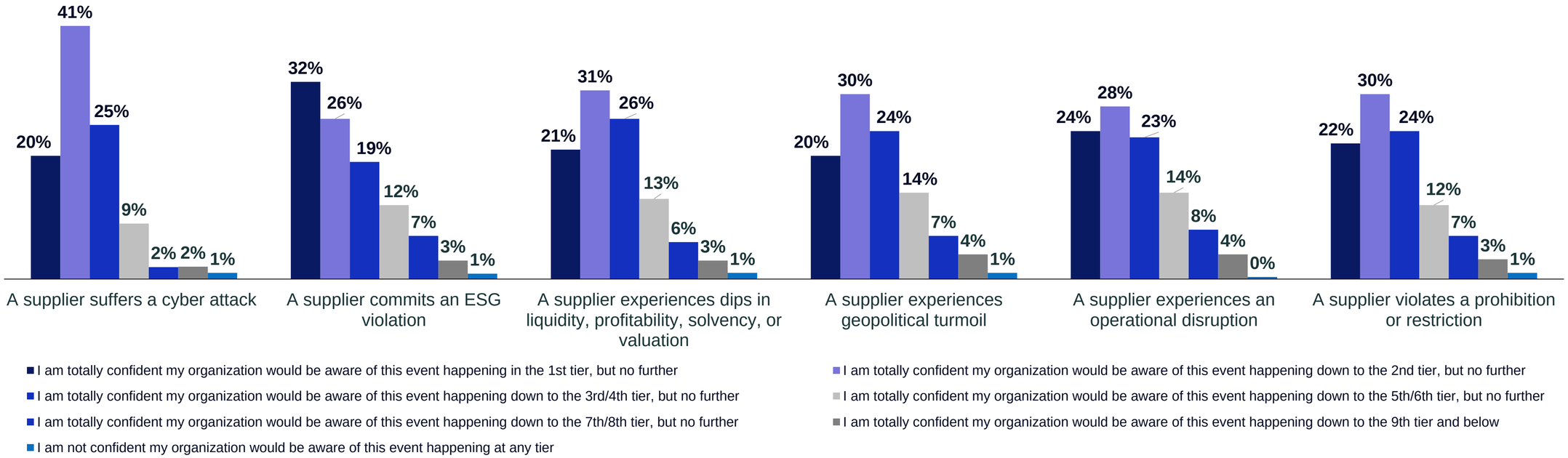
DATA DIVE

67% 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 IT and IT security 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 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. Between one-fifth and one-third of IT and IT security leaders, 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=750

3

Supply Chain Risk Practices Require Further Improvement

Organizations are not evaluating supplier risk in a significant minority 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 IT and IT security leaders say that only just over half of suppliers (56%) are typically evaluated during their 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.

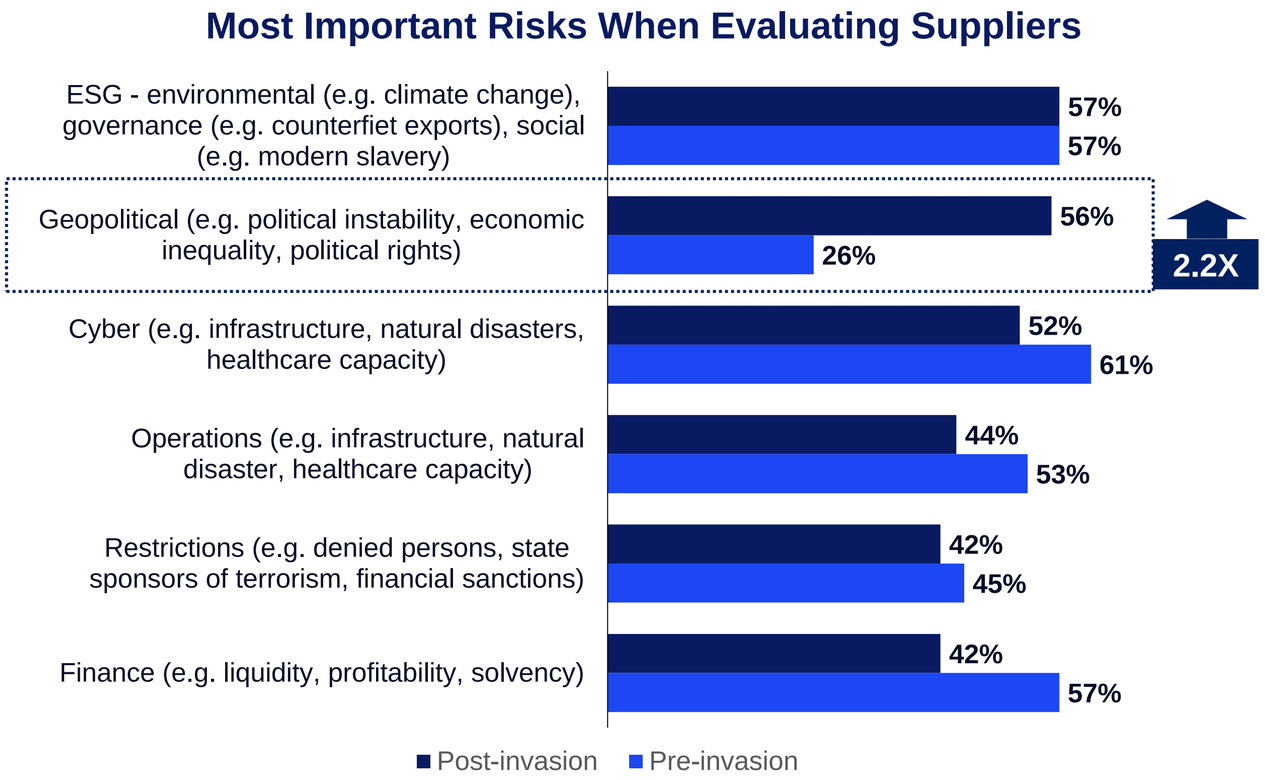
"Being able to make faster and more informed decisions allows us to reduce supplier risk."

– IT/Security Executive, Aerospace & Defense, France

56% **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=750

Geopolitical risk factors have more than doubled in importance since Russia invaded Ukraine



Q: Which of the following factors are most important to your organization when evaluating strategic partners/suppliers? (Combination of responses ranked first, second and third, not showing all answer options); Before n=750, After n=84

Geopolitical issues such as military conflict, social unrest, and terrorist attacks are often downplayed in supply chain risk analysis. Just prior to Russia's invasion of Ukraine, for example, our survey found that a quarter of IT and IT security leaders (26%) prioritized such considerations in their supplier evaluations. Asked the same question a few weeks into the war, however, and that figure had more than doubled to over half of the sample (56%).

The war in Ukraine demonstrates how quickly conflict can disrupt fragile global supply chains, especially those that are heavily dependent on another country. The ongoing U.S.-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 among suppliers ahead of time are left scrambling to respond to sudden supply shortages, logistical problems, cost increases and government restrictions.

Only 11% of organizations say they monitor supplier risks on a continuous basis

The frequency with which organizations monitor risk across their supply chains is also critical. Only slightly more than 1 in 10 IT and IT security respondents said they “continuously” monitor supplier risks, with almost three-quarters doing this on a weekly, monthly or quarterly basis.

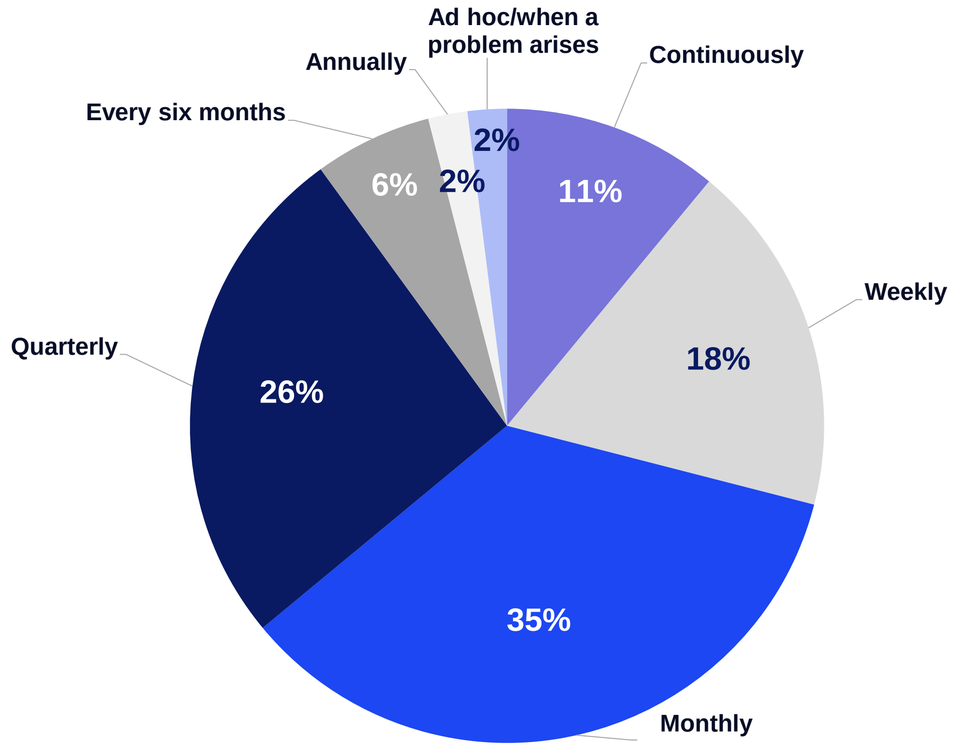
With so many potential sources of disruption across an extended global supply network, there can be significant benefits to those with real-time, near-real-time or at least daily warnings of supplier risk events.

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.

“To ensure our resilience, we have set up with our suppliers and partners alert modules which, over time, will allow real-time monitoring of political, climatic, economic, technological and social risks.”

– IT/Security Executive, Financial Services, France

How Often Supplier Risk is Monitored



Q: How frequently is your organization monitoring supplier risk as part of your organization’s risk analysis?; n=744 [Shown to respondents who 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 750 IT and IT security executive survey respondents felt there were clear benefits to be gained by investing in software solutions for supply chain risk management.

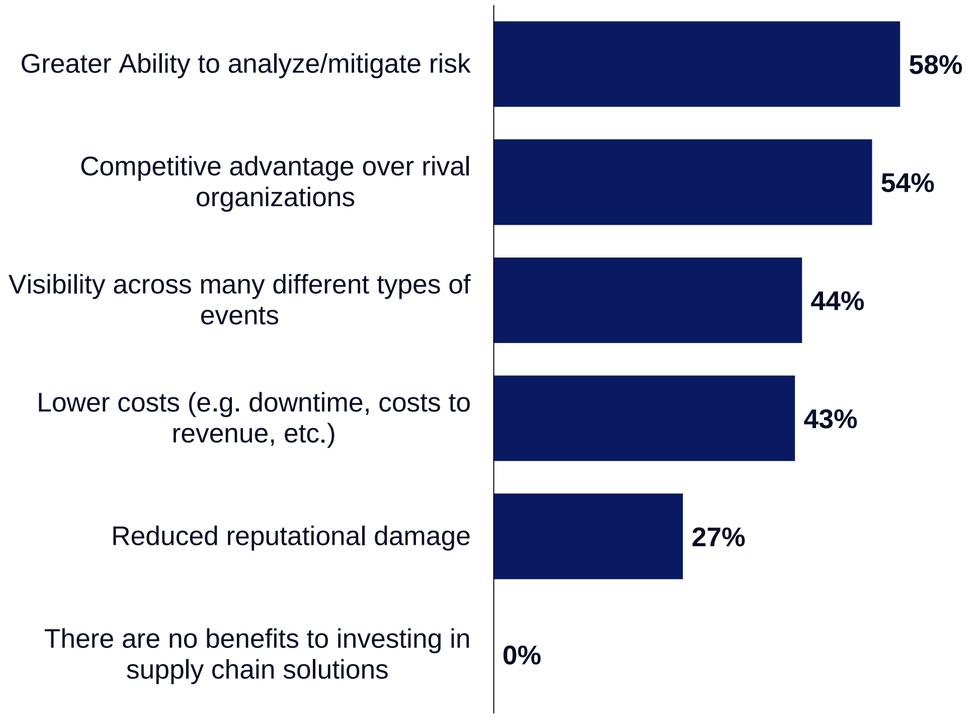
Chief among these benefits is the ability to analyze and mitigate risk through enhanced access to data and information. More than half of CISOs and IT leaders also saw opportunities to gain competitive advantage over rivals, in addition to limiting the negative impact from supply chain disruptions.

Reducing extra costs associated with such disruptions and improving visibility across different types of risk events via continuous monitoring were also identified as benefits by a substantial minority of IT and IT security leaders.

"Disruption is the new normal, so we have to move with it. We are implementing digital technologies to improve our supply chain planning."

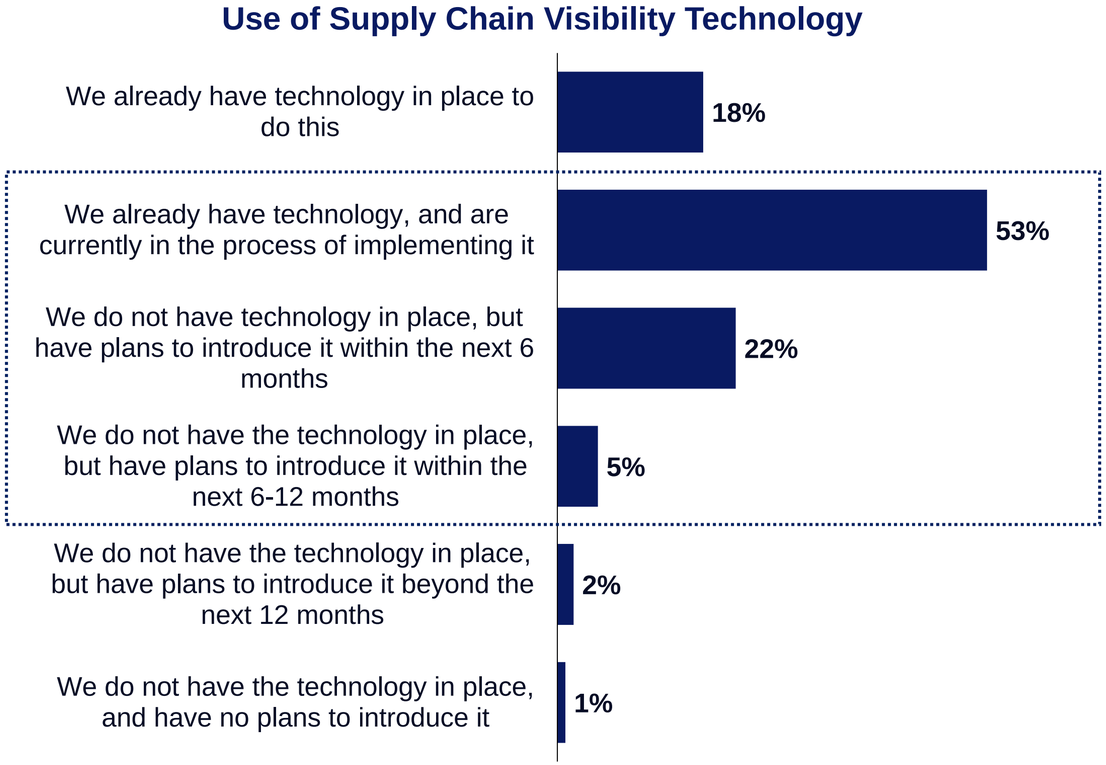
– IT/Security Executive, Aerospace & Defense, France

Benefits of Supply Chain Risk Solutions



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=750

Less than a fifth 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=750

Understanding the interdependencies between an organization and its suppliers at different tiers is essential because many supply chain disruptions originate among indirect suppliers (those at Tier 2 and even further upstream).

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

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

While less than one-fifth of CISOs and IT executives say they already use intelligent and automated technology to gain visibility of supplier interdependencies, 80% say they are implementing it or plan to introduce it within 12 months.

"Through AI and big data, our whole supply chain will operate more efficiently and allow us to anticipate problems before they happen."

– IT/Security Executive, Aerospace & Defense, Canada

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

"We are employing AI to enhance our resilience. It improves visibility and the pace at which we can react."

– IT/Security Executive, Aerospace & Defense, U.S.

The importance of having multi-tier supply chain visibility and the need for advanced technologies to obtain it highlights the crucial role that 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 IT and IT security executives across all geographic regions and industry sectors covered in our survey 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

80% plan to introduce technology to gain visibility of supply chain interdependencies in the next 12 months

84% **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=629 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

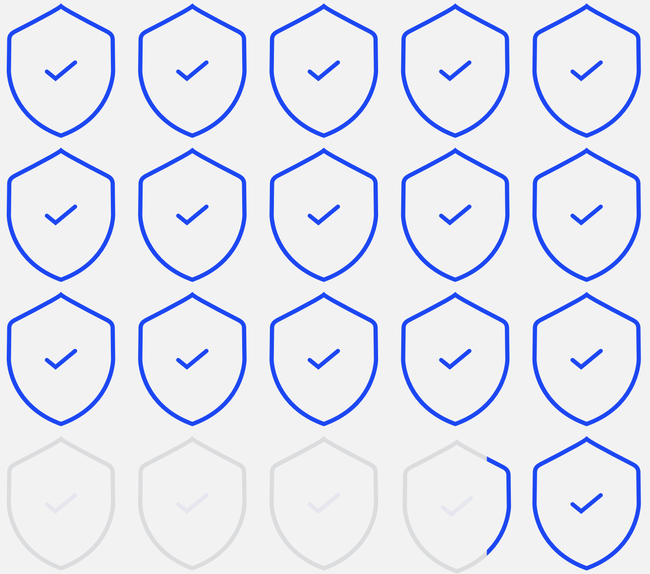
"We have increased communication with our close suppliers and partners to find out the possibilities of disruptions happening, and getting a head start when they do happen."

– IT/Security 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 over **8 out of 10** IT and IT security 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.

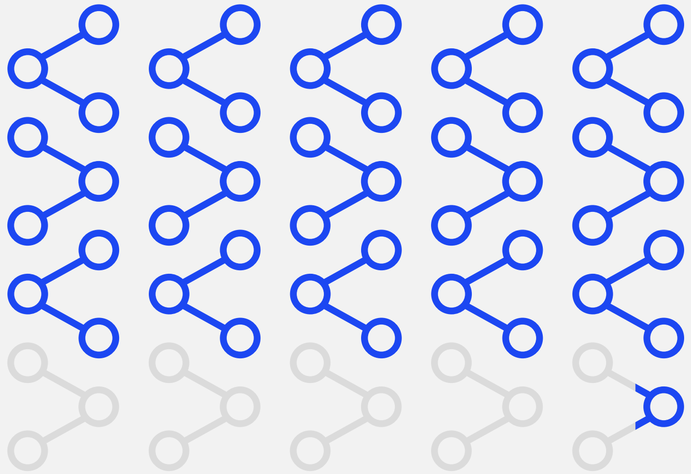
81% **say cooperation across internal departments and with suppliers is vital to protect against disruptions**



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=605 who "strongly agree" or "somewhat agree"

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

78% 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=582 who "strongly agree" or "somewhat agree"

To build and maintain resiliency in your business, you must minimize the downside while maintaining the ability to act on opportunities that may present themselves."

– IT/Security Executive, Pharmaceuticals, Ireland

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.

Almost four-fifths of IT and IT security 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 procurement, IT security and supply chain managers to identify and plug vulnerabilities at suppliers with access to their systems and networks.

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

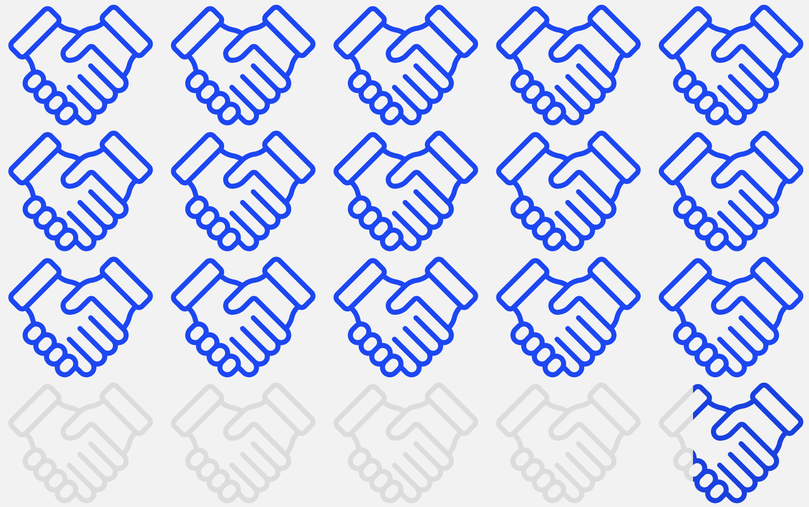
"Joint cooperation is vital. All parties in the supply chain should know what is expected from them. We can assist the lower tiers in providing knowledge, expertise and help them (part financially) to invest in the latest technology."

– IT/Security Executive, Aerospace & Defense, U.S.

Operational resilience is a multiplayer game; it requires the support and cooperation of suppliers and strategic partners throughout the supply chain. Again, an overwhelming majority of CISOs and IT leaders 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.

79% **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=595 who "strongly agree" or "somewhat agree"

Conclusions and Recommendations

Conclusions & Recommendations

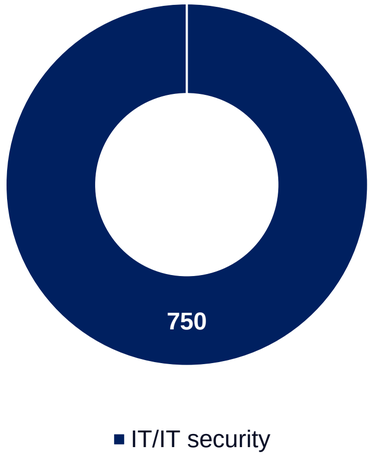
- To enhance supply chain security, CISOs/ IT security leaders should focus on mapping out the supply chain and continually monitoring suppliers. The CISO should look at multiple factors other than just cyber, to access the strength and resilience of a supplier. A financially healthy, well-run supplier will react quickly to address a breach and provide a solution.
- 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 you 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 cyber, financial, operational, geopolitical 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 internal cross-functional and external supplier collaboration.

Appendix

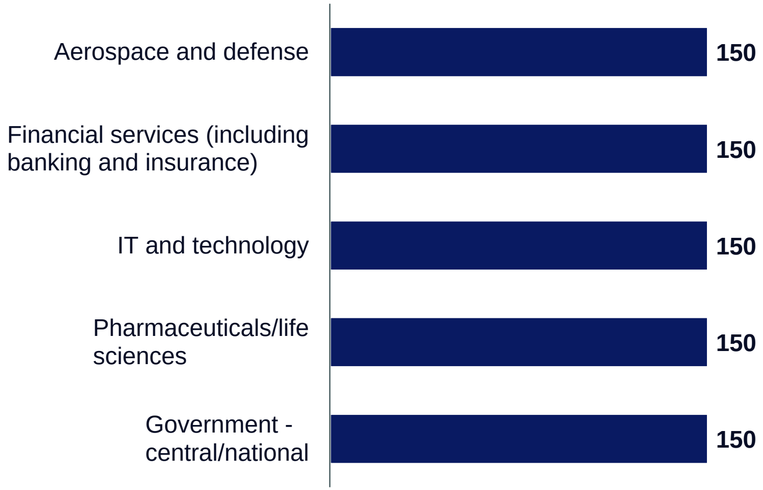
Survey Demographics

750 IT and IT security decision makers were interviewed in January, February and March 2022

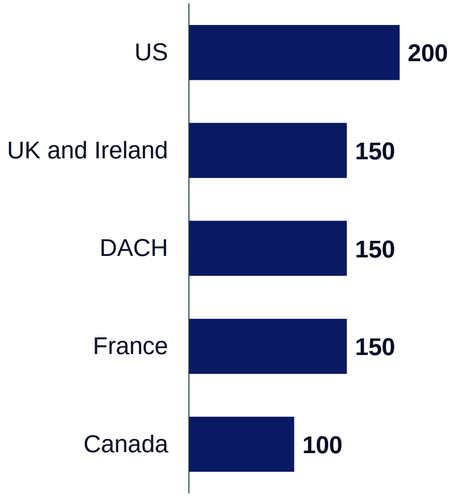
Role



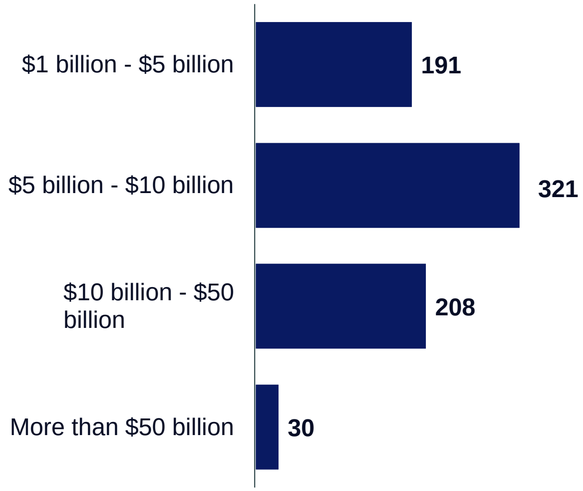
Industry Sector



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 • May 2022 • www.interos.ai