

WHITE PAPER

Navigating an Era of Supply Chain Uncertainty

The forces reshaping supplier resilience across America



www.achilles.com

 **Achilles**
Global Risk Management

Contents

Section One

Executive Summary

Section Two

Introduction: The Rules of
Supply Chains Are Changing

Section Three

Supply Chains in a More
Fragmented World

Section Four

The Financial Health
of America's Suppliers

Section Five

Workforce Pressures are
Becoming a Supplier Risk

Section Six

The New Front
Line of Cyber Risk

Section Seven

What Resilient
Organizations Do Differently

Section Eight

Five Questions Every
Supply Chain Leader Should
Be Able to Answer

Section Nine

Resilience is Now a
Business Strategy

Appendix

Sources and Methodology

Executive Summary

For decades, supply chains have been optimized around a relatively simple equation: lower cost, greater scale and faster delivery. Global sourcing, supplier consolidation and lean operating models have delivered enormous economic value. That model is now being tested.

Tariffs and changing trade relationships are altering sourcing economics. Geopolitical tensions are increasing exposure to disruption. Labor and skills shortages are constraining

capacity. Cyber threats increasingly enter through third parties. At the same time, supplier financial distress, insurance exposure and regulatory expectations are making supplier risk harder to manage through periodic reviews alone.

The result is not the end of globalization, but it is the evolution of supply chain management from a primarily efficiency-focused discipline into a broader business resilience capability.

Several signals point in the same direction:

1. Trade policy is changing sourcing economics

Tariffs, trade restrictions and geopolitical relationships are reshaping the cost and viability of established supply arrangements.

2. Supplier pressure is becoming operational pressure

Financial distress, higher input costs and labor constraints can affect capacity before a supplier formally fails.

3. Critical dependencies often sit below the visible supplier relationship

Several apparently independent suppliers may depend on the same country, material, manufacturer, technology provider or logistics route.

4. Digital and contractor ecosystems are extending organizational exposure

Cyber risk, skills availability, insurance and compliance can enter through third parties over which the organization has limited direct control.

5. Resilience depends on recognizing change early

Periodic reviews remain useful but provide limited insight into changing dynamics and what has changed between assessments.

The supply chain challenge facing US organizations is therefore changing. What used to be a simple question of “**Does a supplier meet our onboarding criteria?**”, is increasingly “**Has anything changed that could make this supplier a risk and will we know early enough to do something about it?**”

The numbers behind the shift

- 82% of surveyed companies affected by new tariffs
- 31% experiencing supplier failure or distress
- 1.9 million potential unfilled US manufacturing jobs
- 48% supply chain-related share of analyzed breaches
- 24,737 US business bankruptcy filings
- 30–50% of annual EBITDA potentially lost in a prolonged shock



The Rules of Supply Chains Are Changing

For much of the past three decades, supply-chain management was a story of optimization. Companies searched globally for lower-cost inputs, consolidated supplier bases to increase purchasing leverage, reduced inventory and built faster, more interconnected logistics networks.

The logic was compelling. Lower costs, greater scale and faster movement of goods helped businesses compete more effectively. But highly optimized supply chains perform best when the conditions on which they were built remain relatively stable. Those conditions are changing.

Trade relationships are being reassessed. Tariffs are altering the economics of established sourcing arrangements. Governments are paying closer attention to critical materials and strategic industries. Geopolitical tensions are disrupting transportation routes, energy markets and access to key inputs. Labor shortages are constraining specialist capacity, while cyber threats increasingly move through interconnected supplier and technology ecosystems.

None of these pressures is entirely new. What has changed is their combination, their reach and the speed at which they can now affect established supply arrangements.

The supply chain is no longer simply the mechanism through which a company acquires goods and services. It is an interconnected operating system through which financial, operational, technological, regulatory and geopolitical risks can enter the business.

A supplier that was financially healthy six months ago may now be under pressure from higher input costs, weaker demand or more expensive financing. A sourcing decision that once made sense on landed cost may look very different after a tariff or trade restriction. A contractor that passed an annual compliance review may subsequently lose key certifications, insurance coverage or skilled personnel. A relatively low-spend supplier may provide a digital connection, specialist component or operational capability whose loss would

have consequences far beyond the value of the contract.

The challenge is therefore not simply whether individual suppliers meet criteria at onboarding or even if they are performing today. It is whether organizations understand the dependencies behind those relationships and how external change could affect them.

This shouldn't mean abandoning globalization, reshoring production, carrying more inventory or maintaining multiple suppliers for everything a business buys. Efficiency remains essential, and global supply chains continue to deliver significant economic value. Resilience requires a more deliberate balance.

Organizations need to understand which suppliers, materials and capabilities are genuinely critical, and which relationships would be difficult, expensive or time-consuming to replace. They also need to recognize that supplier risk is not fixed and be able to track the signals that suggest that things are changing. Financial health, ownership, workforce capacity, insurance, cyber exposure, trade conditions and regulatory status can all change after an initial assessment has been completed.

These issues have traditionally sat across different functions. Tariffs may be managed by trade and procurement teams. Financial distress may be considered by finance. Labor availability may sit with operations and human resources. Cybersecurity may be owned by IT and security. Insurance may sit with risk management. But suppliers connect them.

The organizations best positioned for the next decade will not necessarily be those that eliminate every source of uncertainty, but they are more likely to be the ones that understand where the business is exposed, recognize material change early and retain enough flexibility to respond.

That is the emerging resilience challenge: not to make supply chains less global or less efficient, but to become more intentional about where the business depends on others and proactively managing the risk.

Supply Chains in a More Fragmented World

For years, geography could often be treated primarily as a question of cost, logistics and market access. Increasingly, organizations may also need to consider trade policy, geopolitical relationships, critical materials, sanctions, transportation routes and the resilience of the countries in which important suppliers operate. That doesn't necessarily mean abandoning global sourcing, but for many it does increasingly make **geographic exposure another variable in supplier strategy**.

Trade relationships are evolving

For decades, many supply chains were designed around the assumption that goods, components and materials could move relatively freely between major trading economies. Although trade restrictions, tariffs, sanctions and political tensions have always existed, what appears to be changing is the degree to which trade policy is becoming an active consideration in supply chain planning.

McKinsey's 2025 Supply Chain Risk Pulse found that **82% of surveyed companies said their supply chains had been affected by new tariffs**, while 20–40% of supply chain activity was affected in some way among those companies. Thirty-nine percent reported higher supplier and material costs.

The significance extends beyond the immediate cost of a tariff. A change in trade policy can alter the relative economics of suppliers in different countries. It can affect landed costs, lead times, inventory decisions and the attractiveness of established sourcing arrangements. That may encourage organizations to reconsider geographic exposure even where an existing supplier continues to perform well.

Supply chains may become more regional

There are signs that some organizations are reconsidering the geographic shape of their supply chains. Nearshoring, reshoring and regional sourcing have received increasing attention as businesses consider how to balance cost against resilience, lead time and exposure to trade disruption, however, the picture is unlikely to be uniform. Global supply chains remain economically important, and moving production closer to end markets can introduce its own costs, capacity constraints and supplier dependencies.

For many organizations, the practical response may therefore be selective diversification rather than wholesale regionalization. A company might retain global sourcing where the economics remain compelling while looking for alternative sources for particularly critical components, materials or capabilities. The question becomes less about whether a supply chain is global or regional and more about **where geographic concentration creates an exposure the organization may not be comfortable carrying**.

Critical materials are increasingly strategic

The issue becomes more significant where there are limited sources of supply. Governments and businesses are paying

increasing attention to materials and components that are important to strategic industries but are concentrated in a relatively small number of countries or producers. McKinsey's Global Materials Perspective 2025 highlights increasing use of export restrictions, resource nationalization, stockpiling and other measures by governments seeking greater control over strategically important supply chains.

For procurement teams, this introduces a different dimension of supplier risk. A supplier may be commercially attractive and operationally reliable but still sit within a supply chain that depends heavily on a particular country, material or processing capability. In such circumstances, the exposure may not be visible by looking at the direct supplier alone.

Organizations are rethinking supplier concentration

Global supply chains have become increasingly vulnerable to disruption driven by geopolitical tensions, trade policy changes, economic instability, and climate-related events. In this environment, concentration risk matters more than ever. Organizations that depend heavily on a small number of suppliers, regions, or critical sources of supply may face greater exposure should disruption occurs, making diversification and contingency planning increasingly important.

Why geographic exposure matters

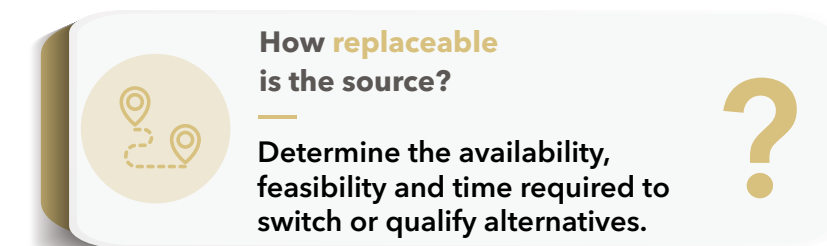
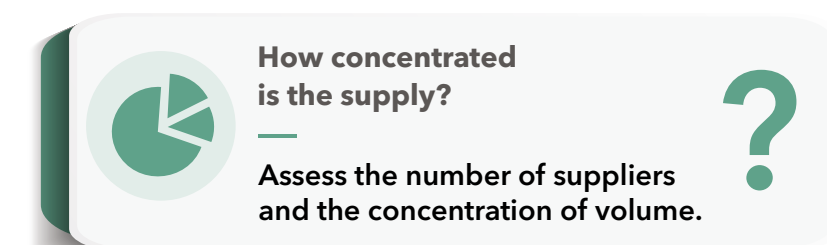
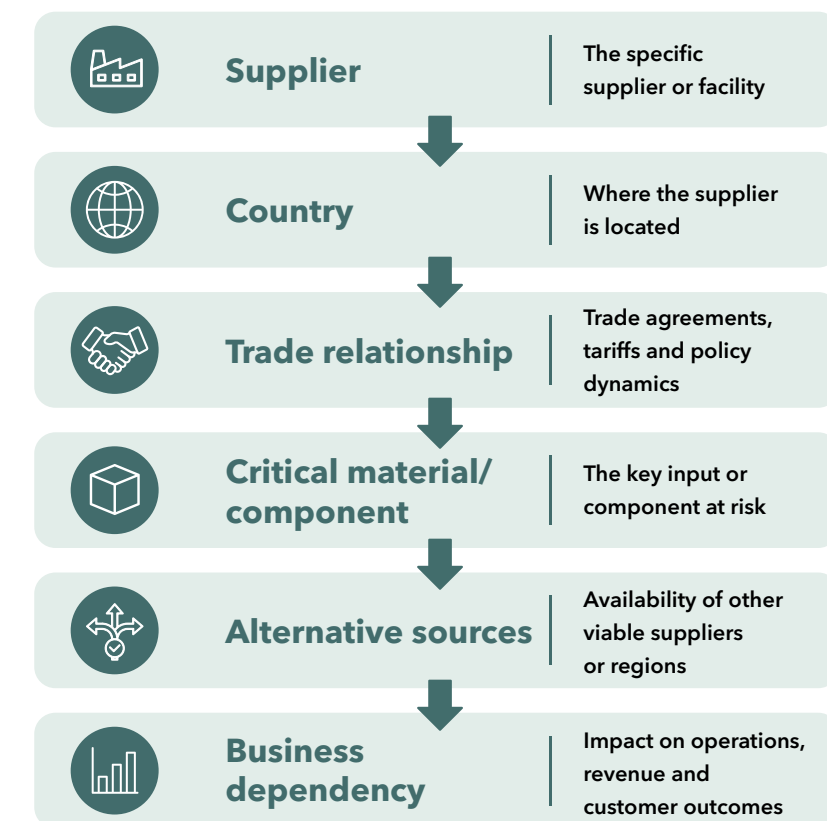
Geography has always influenced supply chains. What may be changing is the range of questions that geography raises:

- Where is the supplier based?
- Where does it manufacture?
- Where do its critical inputs come from?
- Which trade relationships does it depend on?
- How exposed is it to tariffs or export restrictions?
- Are alternative sources available?
- How easily could production be moved?

And what happens if the relevant country, region or trade route becomes disrupted?

These questions do not necessarily lead to a single answer. For some suppliers, geographic concentration may be an acceptable commercial trade-off. For others, particularly where substitution is difficult, it may represent a material source of vulnerability. The important consideration may therefore be less about **avoiding geographic risk altogether** and more about understanding where geographic exposure matters most.

Geography is changing the economics of supply: From supplier location to supply-chain exposure



The Financial Health of America's Suppliers

Supplier distress is becoming harder to ignore

Supplier financial health has always mattered. What is changing is the range of external pressures that can affect a supplier's ability to deliver, often before visible signs of distress emerge. For example, tariffs do not affect only the price paid by the buyer. They may also change supplier margins, working-capital requirements and competitiveness. Some suppliers may absorb part of the increase, pass some through and struggle to recover the remainder. Financial pressure can therefore build behind apparently stable commercial performance.

US business bankruptcy filings increased 7.1% in the twelve months ending December 2025, rising from 23,107 to 24,737. While still well below historical peaks, business filings have been increasing since their post-pandemic low.

That does not mean that a rise in bankruptcies translates directly into widespread supplier failure. Most businesses

experiencing financial pressure will not necessarily become insolvent, and a supplier can experience significant deterioration without entering bankruptcy at all.

The more useful question is probably not whether a supplier is about to fail, but whether its financial position is changing in ways that could affect its ability to deliver. Higher input costs, weaker demand, tighter financing conditions, rising labor costs or the loss of a major customer can all put pressure on a supplier before the effects become visible through a formal insolvency process.

Achilles' 2025 Risk & Sustainability Survey provides another indication of the issue: 31% of respondents reported experiencing supplier financial failure or distress affecting their supply chain during the previous 12 months.

Financial monitoring should be proportionate to dependency. Suppliers whose failure would materially affect operations require closer attention than those that are readily replaceable.

Which industries face the greatest pressure?

Financial pressure is not distributed evenly across the US economy. Sectors such as manufacturing, construction, transportation, energy and healthcare each face different combinations of cost, labor, demand, capital and regulatory pressures. The nature of the exposure also varies considerably within each sector.

Manufacturing, for example, is navigating changing input costs and trade conditions alongside continued investment and demand for skilled labor.

In its second-quarter 2026 survey, the National Association of Manufacturers found that 83.1% of manufacturers identified rising raw-material costs as a top business challenge, up sharply from 57.5% in the first quarter.

Construction faces a different combination of pressures, including labor availability, financing conditions and the cost of materials. Transportation businesses can be particularly sensitive to fuel, equipment, labor and demand conditions, while healthcare suppliers operate within an environment of significant labor and cost pressures. This makes a simple ranking of "the most financially stressed industries" difficult to establish from any single measure.

For procurement teams, the more useful approach may be to consider **financial pressure in the context of dependency**.

A small supplier operating in a financially pressured sector may represent little risk if alternatives are readily available. Conversely, a relatively healthy supplier can represent a significant exposure if it provides a highly specialized component, service or capability that would be difficult to replace.

What happens when a critical supplier fails?

The immediate assumption is often that supplier failure means finding another supplier. In practice, the consequences can be more complicated. A replacement may not be immediately available. Qualification or certification may take time. Existing suppliers may not have spare capacity. Tooling, intellectual property, technical knowledge or specialist skills may make substitution difficult. The resulting impact can extend beyond the purchasing relationship into production schedules, project delivery, customer commitments, working capital and revenue.

This is why supplier failure is better understood as an **operational event with financial consequences**, rather than simply a finance issue. The potential exposure is also greater where several parts of the supply chain depend on the same underlying supplier, facility, geography or specialist capability. That makes supplier financial health particularly relevant when considered alongside concentration and dependency.

Leading indicators procurement teams should monitor

Financial statements and credit ratings remain useful, but they are not necessarily the only signals available to organizations assessing supplier resilience.

Depending on the supplier and the level of criticality, procurement teams may consider indicators such as:

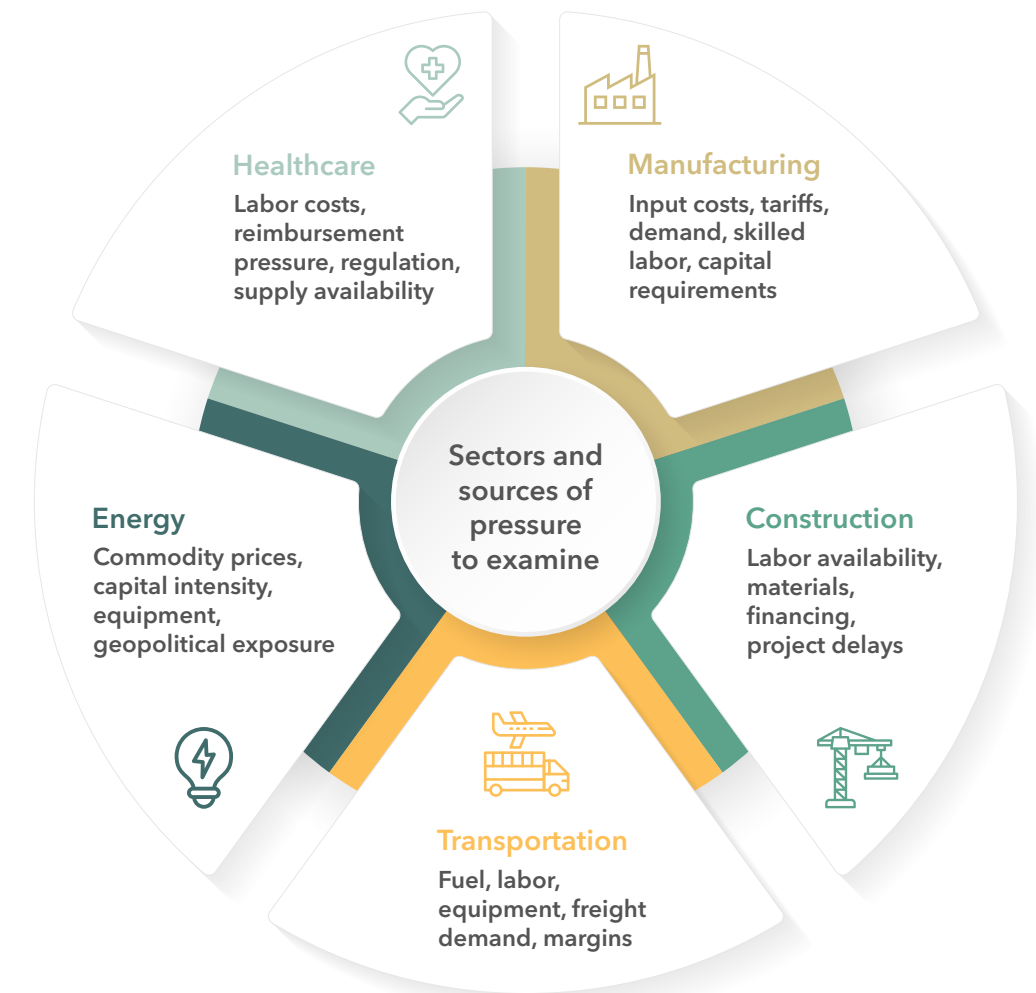
- Deteriorating financial performance
- Increasing debt or financing pressure
- Late payments or changes in payment behavior
- Significant changes in ownership or management
- Rapid changes in pricing

- Significant workforce reductions
- Legal judgments, liens or insolvency proceedings
- Changes in insurance coverage
- Adverse media or reputational events

No individual indicator necessarily means that a supplier is in difficulty. The value comes from **looking for changes and combinations of signals**, particularly among suppliers where failure could have a material operational consequence.

Financial pressure does not necessarily indicate supplier failure. The significance depends on the supplier's role, substitutability and potential impact on the business.

Where supplier pressure can build



Workforce Pressures are Becoming a Supplier Risk

Financial stability and geography remain useful measures of supplier resilience, but are only part of the picture. The conditions that determine whether a supplier can continue to perform are broader and some of them can change well before they are reflected in financial results. Workforce capacity is one such factor that is emerging as an important indicator.

While US labor markets have cooled from post-pandemic highs, access to specialist skills remains constrained across many industries. Deloitte and the Manufacturing Institute estimate that manufacturing could require 3.8 million additional employees between 2024 and 2033, with as many as 1.9 million positions potentially remaining unfilled. In the fourth quarter of 2025, 72.1% of manufacturers reported a need for skilled production workers, including technicians, welders and machinists.

Construction faces similar challenges. In 2025, the Associated General Contractors of America found that 83% of firms employing craft workers had open

positions, with shortages particularly acute among electricians, mechanics, ironworkers and heavy-equipment operators.

These pressures can affect supplier performance before they become visible in financial results. A supplier may remain profitable and maintain a healthy balance sheet while facing growing constraints in its ability to recruit, retain and deploy the specialist skills required to deliver.

For buying organizations, changes in workforce capacity can therefore provide an early indication of pressures that may ultimately affect supplier performance.

Capability and capacity can be measured

Many workforce-related risks can be observed directly through supplier and contractor data. Indicators such as workforce turnover, vacancy levels, reliance on temporary labor, training completion rates, professional certifications, license

compliance and safety performance can provide insight into a supplier's ability to maintain service levels and meet future demand.

The value lies less in any individual measure than in how these indicators change over time and alongside other supplier information. Rising turnover, persistent vacancies or declining certification compliance may point to emerging capacity constraints even where financial indicators remain strong.

This is particularly relevant in contractor-intensive industries, where workforce capability, supervision and operational controls can have significant consequences. In 2024, the United States recorded 5,070 fatal occupational injuries, including 1,034 in construction and 865 in transportation and warehousing. Fatal injury rates reached 9.2 per 100,000 workers in construction and 12.2 per 100,000 workers in transportation and warehousing.

These figures do not suggest that contractors are inherently higher risk. Rather, they highlight the importance of having the right skills, experience and controls in place to deliver safely and reliably.

For organizations that rely on specialist suppliers, contractors and service providers, workforce capability is therefore a useful complement to financial stability and other supplier risk indicators. The earliest sign of pressure may not be financial distress, but a growing difficulty in accessing and deploying the skills needed to deliver.

In an increasingly uncertain supply environment, identifying these changes early can provide valuable insight into where supplier resilience may be coming under pressure.

The New Front Line of Cyber Risk

Cybersecurity is often discussed as a question of protecting an organization’s own systems and networks. However, increasingly part of that challenge may sit outside the organization’s direct control.

Modern businesses depend on increasingly connected networks of suppliers, contractors, technology providers, logistics companies and other third parties. These relationships can provide efficiency and specialist capability, but they can also create additional points of connection between an organization and the wider digital environment.

The scale of that exposure is becoming harder to ignore. Verizon’s 2026 Data Breach Investigations Report found that third-party involvement in breaches had increased by **60%**, with supply chain-related breaches accounting for **48% of breaches** analyzed in the report.

The finding does not mean that suppliers are inherently insecure, nor that every third-party connection represents a significant cyber risk. It does suggest, however, that an organization’s cyber exposure may extend beyond the systems it owns and operates.

Vendor ecosystems as attack paths

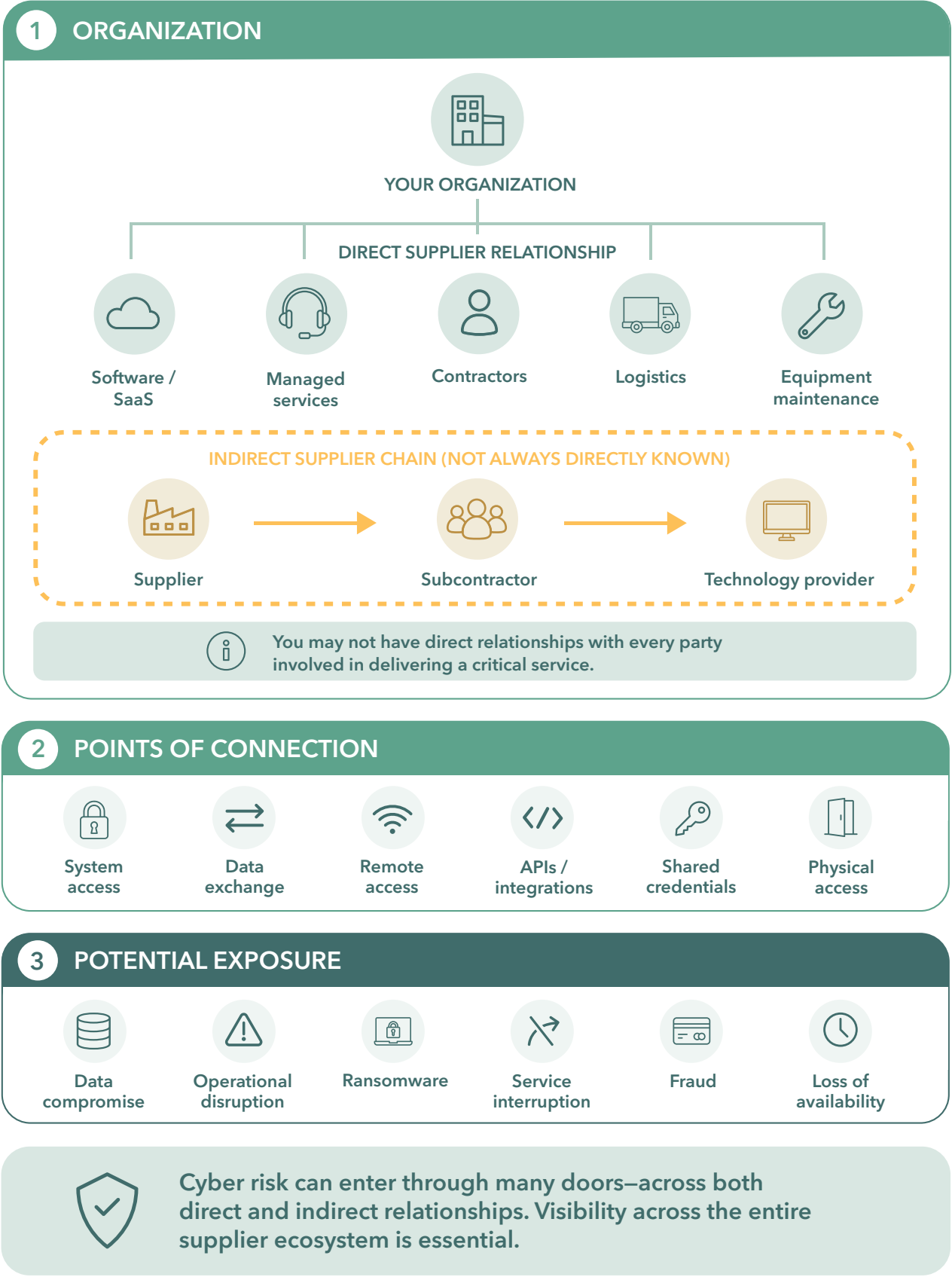
The traditional boundary around cybersecurity is becoming less straightforward. A supplier may have access to internal systems. A software provider may connect directly to corporate infrastructure. A contractor may require privileged credentials to maintain equipment. A logistics provider may exchange sensitive operational information. A cloud or technology provider may sit between an organization and hundreds of its own customers.

Each relationship can be legitimate and necessary, but each also creates a connection that may need to be understood. This is particularly relevant because supplier ecosystems are rarely static. New suppliers are added, existing relationships change, systems are integrated, subcontractors are introduced and access privileges evolve.

The challenge for organizations may therefore be less about determining whether a supplier is “secure” in absolute terms and more about understanding **where connectivity exists, what access it provides, and what could happen if that relationship were compromised.**

How cyber risk enters through supplier ecosystems

The supplier ecosystem can create multiple routes into the business



Section Six

Increasing regulatory expectations

Regulatory expectations are also placing greater emphasis on understanding third-party risk. The direction of travel is not uniform across industries or jurisdictions, and specific requirements vary considerably. However, financial services, critical infrastructure, healthcare and other highly regulated sectors are generally seeing greater scrutiny of third-party relationships and supply chain resilience.

For organizations operating in these environments, supplier oversight is therefore increasingly connected with wider requirements around cybersecurity, operational resilience, incident response and governance.

This creates an important overlap between procurement, risk management and cybersecurity.

Why supplier and cyber risk increasingly overlap

Procurement often has the clearest view of who the organization buys from.

Cybersecurity may have a clearer view of where digital exposure exists. Neither perspective necessarily provides the complete picture on its own.

A supplier may be commercially important without having significant digital access. Another may have a relatively small contract but provide a highly connected technology service. A third may have no direct system access but provide a service whose interruption could materially affect operations.

This suggests that supplier cyber risk is not simply a technology question. It can sit at the intersection of supplier criticality, connectivity, access and consequence. For some organizations, that may mean greater coordination between procurement and cybersecurity when assessing third parties, particularly where suppliers have privileged access, handle sensitive information or provide services that are difficult to replace.

Rather than “**Is this supplier cyber secure?**” It may be more useful to ask “**What does our relationship with this supplier allow it to affect?**”



What Resilient Organizations Do Differently

There is no single model for supply chain resilience. The right approach will depend on the organization, its sector and the consequences of disruption.

What is becoming harder to sustain, however, is treating supplier risk as something that can be assessed periodically and then left unchanged. In a more uncertain environment, resilience depends on maintaining a current view of where the business is exposed and how those exposures are changing.

Four practical areas provide a useful framework.

1. Prioritize dependency alongside spend

Not every supplier presents the same level of business exposure. Identify the suppliers, materials, services and capabilities whose loss or disruption could have a material consequence for the organization.

This may include high-spend suppliers, but it can also include smaller specialist

suppliers that are difficult to replace or support a critical part of the operation.

A more useful measure of importance is the consequence of losing access to a supplier: what would happen if the organization could no longer rely on them?

2. Monitor material change

A supplier assessment provides a snapshot. Resilience requires some consideration of what happens afterwards.

Define the changes that could warrant attention. For example, deterioration in financial health, changes in ownership, loss of insurance coverage, cyber incidents, sanctions exposure, significant workforce changes or changes in operating conditions.

The aim is to focus attention on changes that could alter the risk of relying on a particular supplier, and establish what should happen when they occur.

3. Connect risk signals to business consequence

Individual risk indicators rarely tell the whole story.

A supplier facing financial pressure may present limited exposure if alternatives are readily available. The same level of financial pressure could be much more significant where the supplier is highly concentrated, difficult to replace or provides a critical capability.

Risk signals should be considered alongside **dependency, substitutability, concentration and potential business impact**.

This shifts supplier risk assessment away from simply identifying problems towards understanding which problems actually matter.

4. Establish response options before disruption

Visibility alone does not create resilience. Where a material dependency is identified, organizations should consider what options would be available if conditions deteriorated or a supplier became unavailable.

Depending on the circumstances, these might include alternative suppliers, additional capacity, inventory or lead-time buffers, contractual protections, contingency arrangements, qualification of alternative materials or suppliers, or plans for transferring work.

Not every risk warrants additional investment or redundancy.

The objective is to understand the available options **before they are needed**, and to determine where the potential consequence justifies the cost or effort of preparing them.

From monitoring to preparedness

Taken together, these actions suggest a broader approach to supplier resilience.

- Understand where you depend.
- Understand what could change.
- Understand what those changes could mean.
- And, where the consequences warrant it, prepare for what you might do next.

The result is a more informed basis for deciding where dependency is acceptable, where exposure needs to change and where preparation is worth the investment.

Five Questions Every Supply Chain Leader Should Be Able to Answer

Building resilient supply chains requires continuous confidence in the organizations that build, maintain and support it. These five questions provide a simple test of supply chain resilience.

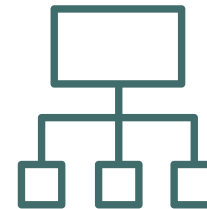
1



Where are our most consequential supplier dependencies?

Look beyond spend to the products, services, materials and capabilities that would be difficult to replace.

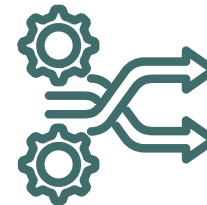
2



Where is exposure concentrated, and how much room is there to pivot?

Multiple suppliers can create the appearance of diversity while leaving an organization exposed to the same underlying market or geographic disruption.

3



What could external change allow those suppliers to affect?

Consider cost, capacity, operational continuity, digital access, customer commitments and regulatory exposure.

4



How quickly would we recognize a material change in supplier risk?

Annual reviews may not reveal financial deterioration, expired cover, new sanctions, cyber events or changing subcontractors when they occur.

5



What realistic alternatives do we have?

Resilience depends not only on identifying exposure, but on understanding the time, cost and feasibility of responding.

The most resilient organizations don't simply respond to disruption, they recognize changing risk profiles early enough to act before projects or operations are affected.

Resilience is Now a Business Strategy

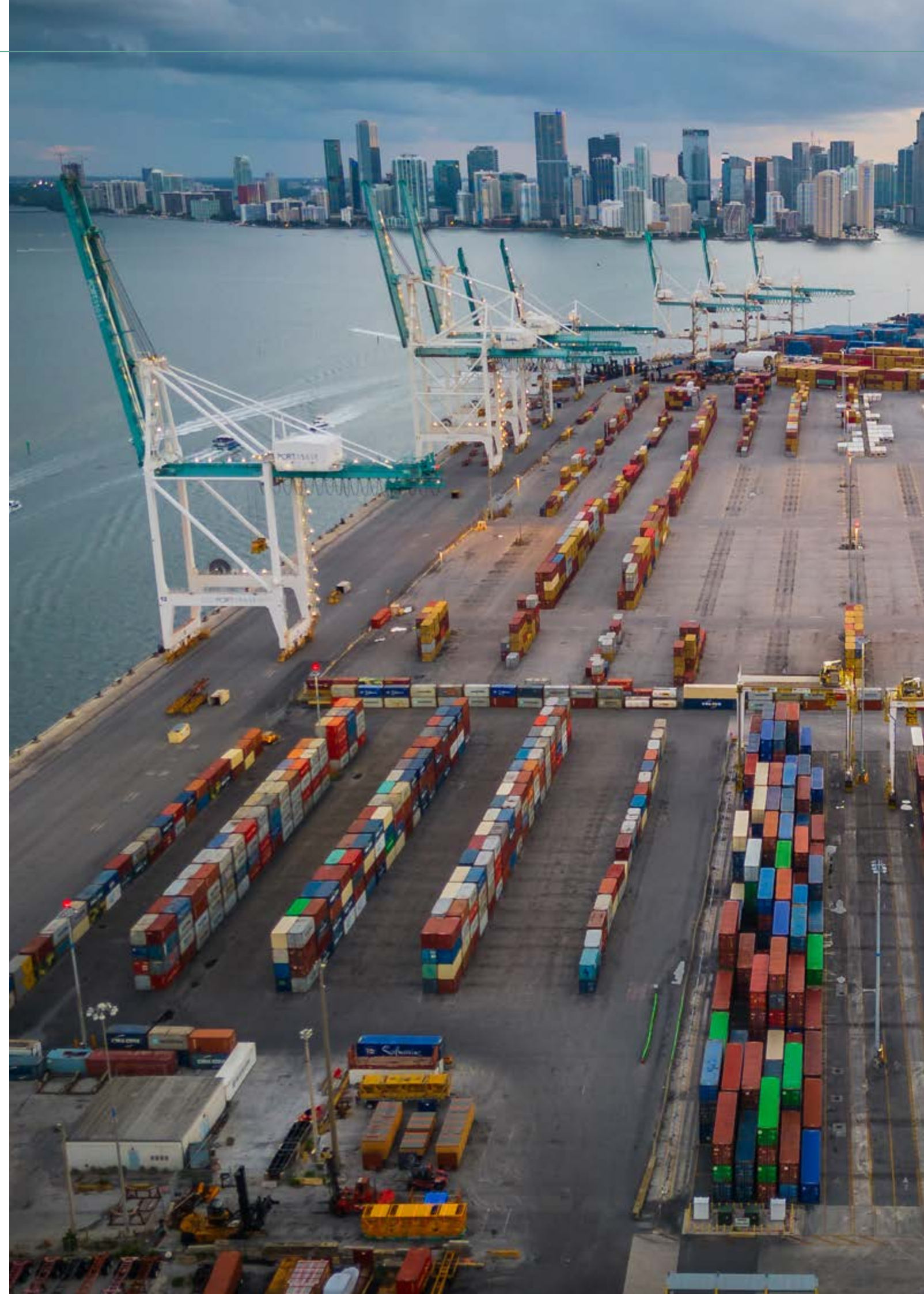
Every supply chain involves choices between cost, speed, control and resilience. While organizations are unlikely to eliminate uncertainty, they can develop a clearer understanding of where they are dependent on others, how those dependencies are changing and where they have the flexibility to respond.

In a less predictable world, resilience comes from knowing where the business is exposed. And how readily it can pivot when conditions change.

Discover how Achilles helps organizations strengthen supply chain resilience

Achilles enables this approach by bringing together multiple sources of supplier intelligence, including financial health, insurance, compliance, contractor competence, ESG, cyber risk, adverse media and geopolitical exposure, providing a continuously updated view of supplier risk and helping organizations identify where action can strengthen supplier performance and resilience.

Learn more at
www.achilles.com



Sources and Methodology

This report draws on a combination of primary research, US government data, industry surveys and independent research to examine the forces shaping supplier resilience in the United States.

Achilles’ own research provides insight into how organizations are experiencing supply-chain disruption, supplier financial distress and current approaches to supplier oversight. These findings are considered alongside external data to provide broader economic, workforce, cybersecurity and geopolitical context.

The report does not attempt to produce a single measure of “supply-chain resilience.” Conditions vary significantly by industry, geography, business model and supplier relationship. Statistics are therefore used to illustrate the scale and direction of particular pressures rather than to suggest that all organizations face the same level of exposure.

Primary research

Achilles Risk & Sustainability Survey 2025

Achilles’ survey research provides data on supplier financial distress, supply-chain disruption and approaches to supplier information and risk

management. Findings cited in this report include the proportion of organizations experiencing supplier financial distress, disruption and reliance on manual or spreadsheet-based processes.

[Achilles industry research and insights](#)

US economic, workforce and safety data

US Bureau of Labor Statistics (BLS)

BLS data is used for measures including producer prices, job openings, employment conditions and occupational safety. The report draws particularly on the Producer Price Index, Job Openings and Labor Turnover Survey and Census of Fatal Occupational Injuries.

[BLS Producer Price Index](#)

[BLS Job Openings and Labor Turnover Survey](#)

[BLS Census of Fatal Occupational Injuries](#)

National Association of Manufacturers (NAM)

NAM’s Manufacturers’ Outlook Survey is used to provide industry-specific evidence on tariffs, input costs, workforce requirements and business conditions.

[NAM 2025 Fourth Quarter Manufacturers’ Outlook Survey](#)

Associated General Contractors of America (AGC)

AGC’s workforce research provides evidence on the availability of skilled construction workers and the difficulty contractors report in filling particular roles.

[AGC 2025 Workforce Survey Analysis](#)

Cybersecurity and third-party risk

Verizon – 2026 Data Breach Investigations Report

The Verizon DBIR provides independent analysis of real-world cybersecurity incidents. The report uses its findings on third-party involvement in breaches to illustrate how cyber exposure can extend across supplier and partner ecosystems.

[Verizon 2026 Data Breach Investigations Report](#)

National Institute of Standards and Technology (NIST)

NIST guidance is used as supporting context for cybersecurity supply-chain risk management and the management of risk across third-party relationships.

[NIST Cybersecurity Supply Chain Risk Management Practices](#)

Cybersecurity and Infrastructure Security Agency (CISA)

CISA guidance provides additional context on cybersecurity supply-chain risk, particularly for organizations operating within critical infrastructure and other high-consequence environments.

[CISA Cybersecurity Supply Chain Risk Management](#)

Trade, geopolitical and supply-chain strategy

McKinsey – Supply Chain Risk Pulse 2025

McKinsey’s annual survey of supply-chain leaders is used to illustrate the reported impact of tariffs on supply-chain activity, supplier and material costs and demand.

[McKinsey Supply Chain Risk Pulse 2025](#)

Deloitte – Enhancing Supply Chain Resilience in a New Era of Policy

Deloitte research provides context on tariffs, geopolitical uncertainty, reshoring, nearshoring and the changing balance between cost and resilience in US manufacturing.

[Deloitte: Enhancing Supply Chain Resilience in a New Era of Policy](#)

McKinsey – Global Materials Perspective 2025

This research is used to provide context on critical materials, supply concentration, export restrictions and the increasing strategic importance of certain resources.

[McKinsey Global Materials Perspective 2025](#)





Address

Achilles Information, LLC.,
5271 California Ave, Suite 290
Irvine, CA 92617



Email

enquiries@achilles.com



California

+1 949 899 6850



Texas

+1 281 809 4400



Web

www.achilles.com