



Supply chain resilience, *redefined*

Why there is “no playbook”—and how CSCOs build fit-for-purpose resilience that performs in any crisis

Why does it feel like there is “no playbook” every time?

When disruption hits, many supply chain organizations replay the same first 72 hours: stand up a war room, accelerate supplier calls, expedite freight, triage customer allocations, and rebuild schedules—while executives ask for answers that are hard to produce quickly: What will stop? For how long? What’s the best alternative? What will it cost?

COVID-19 made this scramble visible across industries, but it wasn’t unique. The same questions surface in factory fires, cyber incidents, sanctions, port disruptions, extreme weather, supplier distress, labour actions, tariffs and geopolitical conflicts. Disruption is not rare; it is persistent—and increasingly systemic.

That is why a core resilience paradox keeps showing up: organizations can have deep expertise in crisis response, yet still feel like they have “no playbook.” What’s missing is rarely effort. It’s a codified operating model and a set of pre-built options that turn uncertainty into repeatable decisions.

Resilience is not a crisis playbook for the last disruption. It is an operating capability designed to perform across disruptions—especially the ones you have not yet experienced.

“Resilience is not a crisis playbook for the last disruption. It is an operating capability designed to perform across disruptions—especially the ones you have not yet experienced.”

Executive call to action

For CSCOs, the implication is straightforward: resilience must become a repeatable operating capability, not an episodic crisis response.

For CEOs, CFOs, and boards, the implication is equally clear: resilience requires deliberate trade-offs—often a “resilience premium”—that may look like cost when disruption is absent but becomes enterprise value protection when disruption occurs. The cost avoidance achieved during a disruption offsets the incremental transactional expense in aggregate.



Deloitte research shows the post-disruption rebalancing is real: 86.2% of manufacturers reported de-risking their supply chains in the past two years, and 97% of companies surveyed in a global trade study reported reconfiguring supply chains in some way.^[1]

Yet the hardest work remains—deep-tier visibility, governance cadence, and the capabilities that prevent the next disruption from becoming a crisis.

This article cuts through the complexity of operational resilience, giving leaders a practical way to identify risks, strengthen capabilities, and respond with confidence. It offers:

1. A clear framework for assessing supply chain risk
2. A capability model for building resilience across the enterprise
3. A repeatable playbook for managing disruption across its full lifecycle
4. Examples of how leading organizations have translated resilience into business value



Executive panel:

10 questions a resilient CSCO can answer quickly

1. Which products and customers are our 'crown jewels'—and what service levels must not fail?
2. Which components, suppliers, sites, lanes, and systems could stop flow within days?
3. Where are our true single points of failure (including Tier 2/3 and critical suppliers)?
4. What is our time buffer for each crown-jewel product family—and what is the fastest recovery path?
5. Which alternates are already qualified (suppliers, materials, lanes, plants)?
6. What triggers a plan switch—and who has decision rights to execute it?
7. What are our pre-agreed customer allocation rules under scarcity?
8. What is our resilience premium today—and what failure cost does it protect?
9. What are the top emerging risks that could outpace our current playbooks (e.g., cyber, critical minerals, trade actions)?
10. When was the last time we rehearsed a disruption scenario end-to-end (tabletop or simulation)?

Why the “no playbook” feeling persists

In practice, the “no playbook” feeling is typically the result of three gaps:

1. **A codified operating model:** repeatable routines that convert risk awareness into decisions and actions—before, during, and after disruption.
2. **Company-specific calibration:** resilience must be engineered to what the organization must protect and to where its true single points of failure sit.
3. **A sustained governance cadence:** many organizations invest in resilience after a shock and then let attention fade, reverting to the lowest unit cost optimization. The boom-bust cycle leaves the enterprise exposed—especially when the next disruption is different.

A fourth gap increasingly shows up in executive conversations: insufficient senior-leader cadence on supply chain risk and trade-offs. Supply chain risk is still too often treated as episodic reporting rather than a standing agenda item tied to risk appetite and investment decisions.



The cost of not being prepared: disruption is expensive—and increasingly systemic

For operators, disruption shows up as missed schedules, missed shipments, plant downtime, premium freight, and quality and compliance holds. For CEOs and CFOs, it shows up as earnings volatility, working-capital shocks, and customer trust and satisfaction erosion. For boards, it is enterprise value at risk.

The scale can be staggering. In the past 25 years alone, individual events have generated economic losses measured in the hundreds of billions of dollars—such as the Great East Japan Earthquake (Cabinet Office estimate ~US\$210B) and major weather events like Hurricane Katrina (~US\$125B) and Texas Winter Storm Uri (estimates up to ~US\$295B).^{[2][3][4][14][15]}

Geopolitical instability and conflict are having significant impacts on global supply chain. For example, rerouting Asia–Europe cargo around the Cape of Good Hope due to Red Sea attacks adds 10–14 days per voyage and \$1–2M (USD) in fuel per ship, with container rates rising 200–400% on affected routes.

Critical chokepoints can delay global trade at a pace of billions per day, as seen in the Suez Canal “Ever Given” blockage (~US\$9.6B/day of trade halted).^{[5][16]}

Financial shocks can cascade into supplier distress and trade disruption at a global scale (for example, world merchandise trade volumes fell 12.2% in 2009).^[6]

And digital disruption now produces physical disruption: outages and cyber events can generate multi-billion-dollar impacts across sectors (for example, Parametrix estimated ~US\$5.4B in direct losses for Fortune 500 companies from the July 19, 2024 CrowdStrike outage).^[7]

“Resilience is operational insurance—designed to protect flow, protect earnings, and protect trust.”

A definitive risk taxonomy: board-complete and operator-usable

Most organizations have some form of “risk taxonomy.” The problem is that many are either too abstract to drive operational decisions or too narrow to satisfy executive oversight. A board needs a complete view of enterprise exposure; a CSCO needs a practical view of what will break flow. A dual-view taxonomy closes that gap by pairing a board-complete risk universe with an operator-usable lens on how disruptions show up in execution.^[1]

View 1: The Four-Plane risk universe (origin +controllability)

The Four-Plane view organizes supply chain risk by where it originates and how controllable it is. This makes it well suited to CEO/CFO/board conversations about risk appetite, concentration, and where resilience investment should be designed into the system versus treated as an external contingency.

- Plane 0 — Internal operations risk (fully controllable):** Disruptions originating inside the enterprise: facilities, people, processes, and systems. Examples include equipment reliability failures, quality events, labor availability, internal IT/OT outages, and cyber incidents that stop production or fulfillment.
- Plane 1 — External event risk (uncontrollable—prepare and respond):** Macro disruptions outside the enterprise's control: natural disasters, extreme weather, pandemics, geopolitical conflict, trade actions, infrastructure chokepoints, and macroeconomic shocks. The strategic question is not whether these will occur, but whether the network can absorb and recover.
- Plane 2 — Supplier-intrinsic risk (partially controllable via selection and monitoring):** Risks resident within suppliers and third parties: financial distress, ownership/control issues, cyber posture, regulatory exposure, and sustainability non-compliance. These risks can be reduced through segmentation, qualification standards, contracting, monitoring, and supplier switching/exit options.
- Plane 3 — Structural and design risk (controllable through redesign):** Risks created by the architecture of the supply chain itself: concentration in a single supplier/site/region, single logistics lanes, lack of Tier 2/3 visibility, product designs that prevent substitution, and dependence on a single technology platform or service provider. These are often the hidden amplifiers that turn an event into an enterprise-level crisis.

Why this matters to boards: Plane 3 risks are frequently self-inflicted, created by years of optimization decisions. When a Plane 1 event hits, those design choices determine whether the organization experiences a brief constraint or a full shutdown.^[8]

View 2: The “flow-stopper” lens (what breaks supply chains in the real world)

For operators, resilience is ultimately about protecting flow. The flow-stopper lens translates risk categories into four execution realities that can be triaged quickly and linked to predefined actions:

- **No supply exists:** Absolute shortage or capacity collapse (e.g., upstream production outage, allocation, embargo, catastrophic supplier failure).
- **Supply exists but cannot be accessed:** Logistics or compliance prevents access (e.g., port congestion, border restrictions, sanctions/export bans, lane disruption, carrier failure).
- **Supply arrives but cannot be used:** Quality, spec, or compliance blocks use (e.g., contamination, non-conformance, regulatory holds, counterfeit risk).
- **The network cannot process or fulfill:** Internal constraints stop conversion or fulfillment (e.g., plant/DC outage, labor disruption, systems outage, OT cyber incident).

Economic viability overlay (the constraint CSCOs face even when flow can be maintained): In some disruptions, supply can keep moving—but only through options that are economically unsustainable (for example, premium freight, spot buys, emergency outsourcing, or absorbing tariff shocks without alternates). In these cases, the question is not just whether flow

can be restored, but whether flow can be sustained within margin, cash, and customer-trust guardrails.

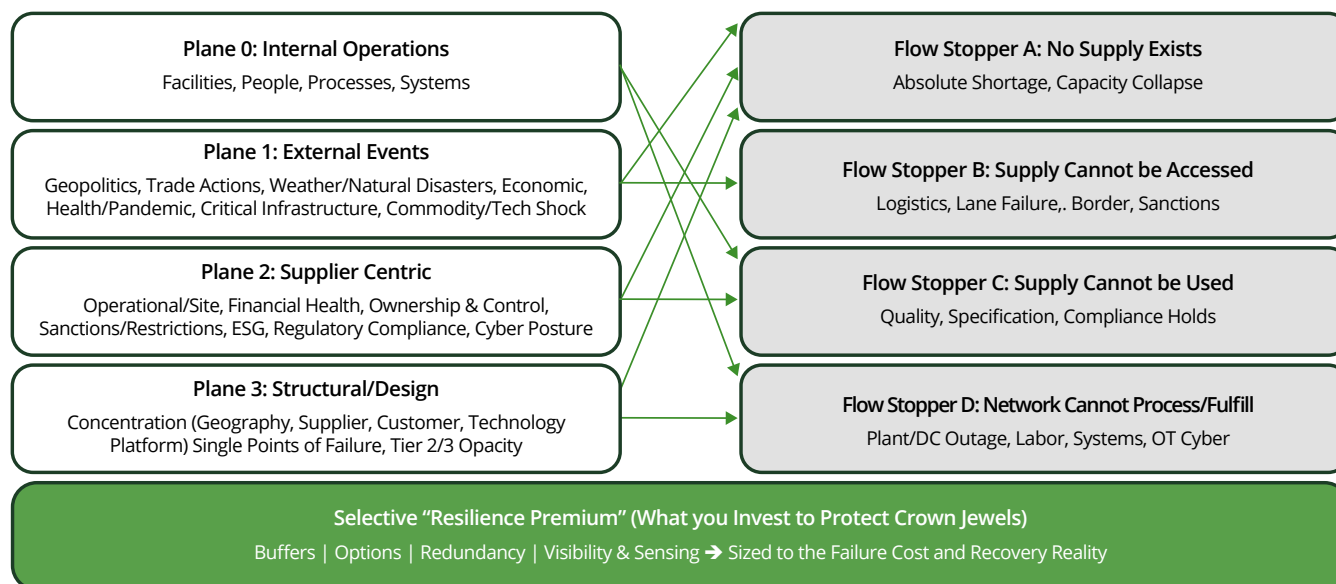
- **Cost-to-serve impact:** What is the incremental landed cost versus baseline, and what margin/working-capital exposure does it create?
- **Duration:** For how long would we need to operate in “expensive mode” (days, weeks, quarters) if the constraint persists?
- **Commercial levers:** Can we reprice, reallocate, substitute, adjust service promises, or redesign the network so the response is economically sustainable?

The power of the dual view is the bridge between enterprise risk and operational response. External events (Plane 1) often manifest as “no supply” or “no access.” Supplier-intrinsic risks (Plane 2) frequently show up as “no supply” or “can’t use.” Internal risks (Plane 0) most often appear as “can’t process.” Structural/design risks (Plane 3) amplify every flow-stopper—because concentration, lack of alternates, and poor visibility reduce the options available when time is short.^[8]

Used together, these views create a shared language across CSCO, CEO, CFO, and board discussions:

1. Identify where exposure sits (Planes);
2. Understand how it will break execution (Flow-stoppers), and;
3. Decide what selective resilience premium is justified to protect crown jewels (buffers, options, redundancy, visibility).^[1]

Figure 1. Dual-view resilience mapping: risk origin flow impact selective premium



Resilience Capability Model

Resilience is not synonymous with stockpiling inventory, adding capacity, relocating every supplier, or buying a new risk monitoring tool. It is a set of capabilities that reduce the performance impact of disruption and accelerate recovery.

- **Visibility:** Multi-tier supplier network mapping, shipment tracking, and demand sensing that illuminate exposure early.
- **Diversification:** Reduced single-vendor dependence, multi-geography sourcing, and multi-mode logistics.
- **Strategic reserves:** Targeted buffers for critical and sole-source items—sized by recovery realities.
- **Flexibility & agility:** Substitution-ready design, flexible production, and pre-qualified alternates that enable rapid reconfiguration.
- **Financial resilience:** Supplier and ecosystem financial monitoring, liquidity planning, and risk transfer where appropriate.

AI is increasingly becoming a resilience accelerator, not a stand-alone strategy. When built on a strong data foundation, AI can fuse signals across events, suppliers, logistics, and operations—enabling earlier detection, faster prioritization, and more consistent decision execution. As one example, Deloitte’s Supply Chain Resilience Operate capability (including SupplyHorizon) is designed to bring together monitoring, intelligence, and advanced analytics so teams can cut through the noise and focus on mitigation execution.^[13]

- **Signal fusion:** Combine external event signals with supplier, shipment, and shop-floor data to detect emerging disruptions earlier.
- **Decision acceleration:** Automate triage by flow-stopper type and recommend response actions (e.g., secure supply, reroute shipments, contain quality, restore processing).
- **Execution assurance:** Track mitigation actions and exceptions across the network so leaders can intervene before small delays become systemic misses.

Making the trade-offs explicit: the resilience premium

A concise resilience premium menu helps make trade-offs tangible: A practical way to size the resilience premium is to quantify two realities for each crown-jewel product family:

1. How long the network can continue operating if replenishment is disrupted - **“Time to Survive”** (TTS).
2. How long it takes to recover supply - **“Time to Recover”** (TTR).

Leaders should also agree the maximum “expensive mode” duration (and acceptable margin erosion) they will tolerate before shifting to repricing, allocation, substitution, or network redesign. The gap between the two makes the trade-off explicit—revealing where buffers, alternates, or recovery support are justified, and where they are not.

- **Buffers:** Targeted inventory and time buffers for crown-jewel products and single points of failure.
- **Options:** Pre-qualified alternates (suppliers, materials, lanes) and flexible capacity that can be activated quickly.
- **Redundancy:** Deliberate duplication where needed to avoid catastrophic single-point failure.
- **Visibility & sensing:** Early detection, quantified impact, and coordinated response across the extended enterprise.

From firefighting to strategic advantage: the resilience maturity ladder

Progressing from one level to the next is not a simple step. It typically requires changes in data, governance, operating routines, and talent.

- **Level 1** — Reactive (Crisis response): Ad hoc response. Limited visibility beyond Tier 1. Success depends on heroics and premium freight.
- **Level 2** — Aware (Structured monitoring): Basic monitoring and continuity plans for critical nodes. Response is faster but still reactive.
- **Level 3** — Proactive (Multi-tier visibility): Multi-tier mapping for crown jewels. Defined options (alternates, buffers) and tested response routines. Resilience becomes repeatable.
- **Level 4** — Resilient (Anticipatory): Concentration guardrails embedded in design and sourcing. Regular simulations. Cyber and technology resilience drills. Early warning drives action.
- **Level 5** — Strategic advantage: Resilience is a competitive moat: it is measured, governed, and continuously improved; it enables share gain during disruption.

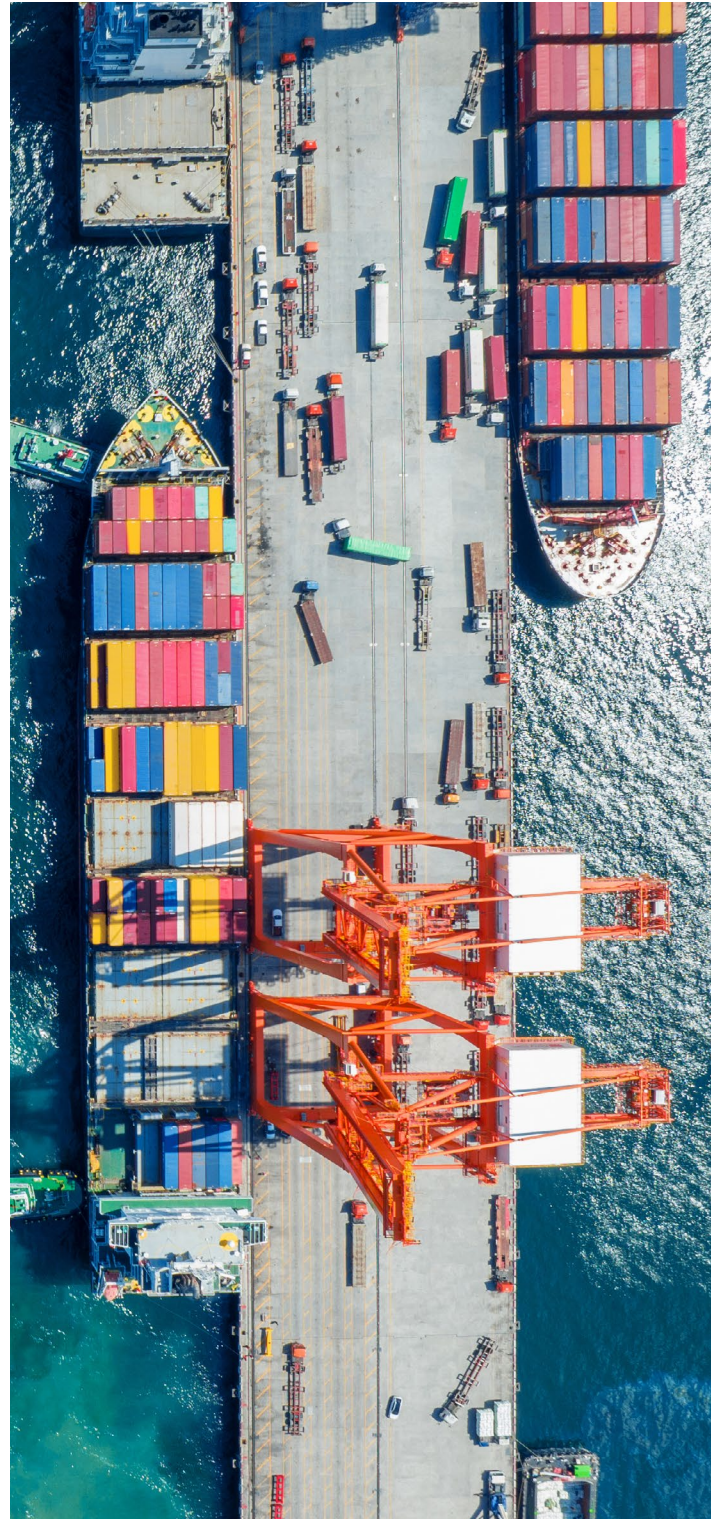
The hard transitions (what changes to move up a level)

- **Level 1 > 2:** Move from heroics to basic routines—documented roles, monitoring, and repeatable response activation.
- **Level 2 > 3** (often the hardest): Move from Tier-1 awareness to Tier-2/3 visibility for crown jewels plus real, pre-qualified options (alternates, buffers, lanes).
- **Level 3 > 4:** Encode resilience into design rules (concentration guardrails) and rehearse cross-enterprise execution through simulations and drills.
- **Level 4 > 5:** Shift from resilience as a cost to resilience as advantage—measured, governed, continuously improved, and used to win share during disruption.

What makes maturity progression hard (and how to make it real)

Building resilience capability will take time and investment. Most organizations can progress to level 2 relatively quickly. Progressing beyond that will require real organizational commitment.

- **You can't 'buy' maturity:** tools help, but maturity is governance + data + routines + talent.
- **Moving from Level 2 > 3 is usually the hardest step:** it requires multi-tier visibility for crown jewels and pre-built options, not just monitoring. This is where survey-based approaches to understanding your extended supplier base breakdown and digital supply network illumination capability and risk sensing are required.
- **Moving from Level 3 > 4** requires encoding resilience into design rules (concentration guardrails) and rehearsing cross-enterprise execution.
- **Level 5** is earned when resilience shifts from cost to advantage: leaders can quantify the premium and show how it protects value and enables faster offense.



Mini caselets: resilience in action

Toyota: institutional learning that compounds over time

Resilience lesson: design rules and supplier expectations built before the crisis determine performance during the crisis.

Toyota is one of the most publicly documented examples of resilience built through institutional learning. Its story reinforces a core principle: fortunes in crisis depend more on choices made before the disruption than on actions taken during the disruption.^[27]

After major disruption experiences in the 2000s and 2011, Toyota strengthened continuity requirements across its supply network and embedded resilience into supplier expectations and design rules. The payoff became visible years later when global supply shocks re-emerged and Toyota's preparedness helped it sustain operations longer and recover faster than many peers.^[12]



What they did

- Treated disruption as a learning loop: formalized post event reviews and converted lessons into standard design and sourcing rules.
- Deepened visibility into sub tier dependencies for critical components—so exposures were known before the next shock.
- Built targeted reserves for specific sole source/critical items where recovery times are long.



What leaders can copy

- Institutionalize learning: make post event redesign mandatory, not optional.
- Translate resilience into a few non negotiable design rules (for example, concentration guardrails and pre qualified alternates for crown jewel components).
- Use targeted buffers selectively—where the cost of failure is outsized and recovery is slow.

Ford: financial resilience that protected operational freedom

Resilience lesson: disruption is as much a cash shock as a material shock—financial flexibility can be a supply chain advantage.

Supply chain resilience is often discussed in physical terms—suppliers, inventory, and logistics. But the ability to sustain operations through disruption is also financial. The Global Financial Crisis demonstrated that demand shocks, supplier distress, and trade finance constraints can disrupt supply chains even when factories are intact.

A widely cited example is Ford's decision to secure additional liquidity ahead of the crisis, creating financial flexibility when many competitors were constrained. The broader lesson is that resilience investments include not only physical options, but also financial options that preserve decision freedom when disruption compresses both supply and cash.



What they did

- Built financial 'reserves' ahead of the crisis to maintain operating flexibility under uncertainty.
- Enabled quicker, more decisive actions during downturn conditions when access to capital is constrained.
- Demonstrated that 'reserves' can be financial as well as physical—supporting suppliers and continuity when ecosystems are stressed.



What leaders can copy

- Partner CSCO and CFO: treat cash and working capital as part of the resilience system, not separate from it.
- Monitor supplier solvency risk and design commercial terms that reduce cascading failures.
- Ensure the enterprise has the liquidity and governance to act quickly when disruption creates both a supply shock and a cash shock.



The resilience playbook: Prepare > Sense > Analyze > Respond > Recover > Adapt

A playbook becomes valuable when it is universal in structure but configurable in application. The following lifecycle is consistent across disruption types, yet it can be calibrated to each company's supply chain architecture, regulatory constraints, and service promises.

PREPARE	SENSE	ANALYZE	RESPOND	RECOVER	ADAPT
<i>(design resilience in)</i>	<i>(detect early and quantify impact)</i>	<i>(prioritize and determine trade-offs)</i>	<i>(crisis execution mode)</i>	<i>(return to stability)</i>	<i>(learn and redesign)</i>
- Define crown-jewel products, minimum service commitments, and what the enterprise must protect. - Map critical dependencies end-to-end, including sub-tier exposure for the most critical products and processes. - Set concentration guardrails (supplier/ site/route/ platform) and create options where risk is unacceptable. - Establish governance cadence and accountability so resilience does not fade after the last disruption.	- Build early warning across supplier health, lead-time volatility, logistics congestion, quality signals, cyber alerts, and compliance holds. - Create a single source of truth for decisions—visibility that spans supply, logistics, factories, and customer fulfillment. - Maintain accountabilities at the leadership level for risk detection and reporting	- Standardize impact assessment so leaders can quickly see what is affected and for how long, - Develop what options exist and quantify the cost/benefit of mitigations. - Prepare specific set of actions and expected outcomes to execute.	- Activate an empowered cross-functional war room with clear decision rights and escalation pathways. - Triage using the flow-stopper lens to trigger predefined actions: secure supply, reroute access, contain quality/ compliance, restore processing capability. - Protect customer trust through transparent allocation principles and credible recovery communication.	- Shift from central command to central orchestration as operations restart and resynchronize across internal functions and external partners. - Manage cash and working capital as tightly as physical supply—rebuilding inventory intelligently while avoiding a second shock. - Monitor rebound signals and recalibrate as constraints lift unevenly across regions and tiers.	- Run post-event reviews within 30–60 days: what failed in visibility, where options were missing, and which decisions reduced impact. - Redesign products, networks, and policies to reduce repeat exposure—substitution, portfolio simplification, alternate sources and lanes, cyber and data resilience. - Institutionalize learning: update governance, metrics, and training so resilience becomes cumulative advantage

What's next: persistent risks continue, and unfamiliar risks widen the playbook gap

The most compelling resilience argument is not that historical disruptions may recur—they already are. The argument is that the next major disruption is likely to combine familiar risk categories with conditions many organizations have not yet experienced at scale.

Many companies do not have crisis-specific playbooks for risks such as critical minerals restrictions, systemic cyber disruption, or rapid AI-driven demand volatility. But they do not need a unique playbook for each scenario if they build strong, generalizable capabilities. Visibility, diversification, strategic reserves, flexibility, and financial resilience are designed to perform across disruption types. However, based on current trajectory, the following risk categories are most likely to drive the next major supply chain disruption event and companies should embed these into their risk registries today.

- **Critical mineral dependency.**

China's export restrictions on rare earth elements signal a replication of the semiconductor shortage dynamic across battery materials, catalysts, and electronics. Western supply chain independence for critical minerals is a decade-long project.^[18]

- **Climate change and extreme weather.** The WEF projects weather-induced supply chain disruptions will increase materially over the next 15 years. The 2024 Hurricane Helene impact on the Spruce Pine, NC quartz mine—the world's primary source of ultra-pure quartz for semiconductor fabs—illustrated how climate risk now intersects directly with technology supply chains.^{[19][20][21]}

- **Taiwan / semiconductor geopolitical risk.** Taiwan accounts for ~60% of global foundry output and over 90% of advanced chip production; TSMC holds >55% of the global foundry market. A military or political crisis in the Taiwan Strait would make the 2020–2023 chip shortage look minor by comparison. Government CHIPS Acts are responses to this risk but are multi-year solutions to a potentially immediate threat.^{[22][23]}

- **AI-driven demand volatility.** Explosive AI infrastructure buildout is creating unprecedented demand for HBM memory, advanced packaging, and power infrastructure components—with lead times measured in years. Demand forecasting in AI-adjacent supply chains is structurally unreliable.^{[24][25]}

- **Systemic cyber supply chain attack.** The 2024 CrowdStrike event was non-malicious. A targeted, coordinated cyberattack against major logistics systems, port operations, or ERP platforms could create physical supply disruptions orders of magnitude larger.^[26]

In practice, this means shifting the resilience conversation from predicting the next event to ensuring the organization can sustain flow, recover quickly, and adapt—no matter what event occurs.

The questions leaders should align on

Resilience becomes an enterprise discipline when leadership aligns on three questions:

1. **What are we protecting?** Define crown jewels, minimum service commitments, and the value at stake if flow is interrupted.
2. **Where are our true single points of failure?** Identify structural concentration and sub-tier visibility gaps that can turn a disruption into a shutdown.
3. **Do we rely on muscle memory or heroics?** Assess whether sensing, decision rights, response activation, and orchestrated recovery are repeatable and rehearsed.

Conclusion

Firefighting is not a strategy. In an era where disruption is persistent, supply chain resilience becomes a defining enterprise capability—one that protects earnings, service, trust, and competitive position. To keep the approach tight, close the loop from exposure to action. Use the Four-Plane taxonomy to ensure you are board-complete, translate priority exposures through the flow-stopper lens to clarify what will actually break, and apply a selective resilience premium—buffers where recovery is slow, options where switching is feasible, redundancy where single points of failure are unacceptable, and visibility and sensing so decisions are early and coordinated.



Authors



Jim Kilpatrick

jimkilpatrick@deloitte.ca

Partner, Supply Chain & Network
Operations Leader, Canada
Deloitte



Ryan Ernst

ernst@deloitte.ca

Partner, Global Supply
Chain & Distribution
Deloitte



References

1. Deloitte Insights (Deloitte Research Center for Energy & Industrials), "Restructuring the supply base: Prioritizing a resilient, yet efficient supply chain" (May 23, 2024): <https://www.deloitte.com/us/en/insights/industry/manufacturing-industrial-products/global-supply-chain-resilience-amid-disruptions.html>
2. World Bank, "The Great East Japan Earthquake: Economic Impacts" (Knowledge Note 6-3), Cabinet Office estimate ¥16.9 trillion (~\$210B): <https://documents1.worldbank.org/curated/en/175611468044671950/pdf/793950BRI0drn000Box377374B00Public0.pdf>
3. Guinness World Records, "Costliest tropical cyclone" (Hurricane Katrina damage ~US\$125B): <https://www.guinnessworldrecords.com/world-records/415776-costliest-tropical-cyclone>
4. CBS News MoneyWatch, "Texas winter storm costs could top \$200 billion" (Perryman Group estimate up to \$295B) (Feb 25, 2021): <https://www.cbsnews.com/news/texas-winter-storm-uri-costs/>
5. Al Jazeera (Bloomberg citing Lloyd's List), "Suez Canal blockage halts \$9.6bn a day of ship traffic" (Mar 25, 2021): <https://www.aljazeera.com/economy/2021/3/25/suez-blockage-seen-halting-9-6-billion-a-day-of-ship-traffic>
6. Reuters via Investing.com, "World trade fell 12.2 pct in 2009 -- WTO" (Mar 26, 2010): <https://www.investing.com/news/forex-news/world-trade-fell-12-2-pct-in-2009---wto-127639>
7. Parametrix, "CrowdStrike to Cost Fortune 500 \$5.4b" (Jul 24, 2024): <https://www.parametrixinsurance.com/in-the-news/crowdstrike-to-cost-fortune-500-5-4-billion-insured-loss-range-of-540-million-to-1-08-billion>
8. MIT Sloan Management Review (Sheffi & Rice), "A Supply Chain View of the Resilient Enterprise" (Oct 15, 2005): <https://sloanreview.mit.edu/article/a-supply-chain-view-of-the-resilient-enterprise/>
9. MIT (CIO reprint), "How Wal-Mart Beat Feds to New Orleans" (Nov 1, 2005): https://web.mit.edu/sheffi/www/documents/cio_wal-mart.pdf
10. The Independent Review (Steven Horwitz), "Wal-Mart to the Rescue: Private Enterprise's Response to Hurricane Katrina" (Spring 2009): https://www.independent.org/pdf/tir/tir_13_04_3_horwitz.pdf
11. CNBC, "How Ford Avoided the Meltdown that Hit GM, Chrysler" (Apr 9, 2009) (\$23.6B loans): <https://www.cnbc.com/2009/04/09/how-ford-avoided-the-meltdown-that-hit-gm-chrysler.html>
12. Toyota, "Impact of the Disasters and Recovery Efforts" (Toyota Annual Report 2012, p.30–31) (supply chain visualization incl. tertiary/4th-tier suppliers; decentralizing sources; generalized designs): https://www.toyota-global.com/pages/contents/investors/ir_library/annual/pdf/2012/p30_31.pdf
13. Deloitte, "Supply Chain Resilience" (Operate / managed services): <https://www.deloitte.com/us/en/services/consulting/services/supply-chain-resilience-operate.html>
14. NOAA/National Hurricane Center, Tropical Cyclone Report: Hurricane Katrina (updated Jan 4, 2023): https://www.nhc.noaa.gov/data/tcr/AL122005_Katrina.pdf
15. Texas Comptroller of Public Accounts, "Winter Storm Uri 2021: The Economic Impact of the Storm" (Oct 2021): <https://comptroller.texas.gov/economy/fiscal-notes/archive/2021/oct/winter-storm-impact.php>
16. Lloyd's List, "Suez Canal remains blocked despite efforts to refloat grounded Ever Given" (Mar 24, 2021): <https://www.lloydslist.com/LL1136229/Suez-Canal-remains-blocked-despite-efforts-to-refloat-grounded-Ever-Given>
17. MIT Sloan Management Review reprint PDF (Sheffi & Rice), "A Supply Chain View of the Resilient Enterprise" (Fall 2005): https://web.mit.edu/scresponse/repository/Sheffi_Rice_SC_View_of_the_Resilient_Enterprise_Fall_2005.pdf
18. CSIS, "What China's Ban on Rare Earths Processing Technology Exports Means" (Jan 8, 2024): <https://www.csis.org/analysis/what-chinas-ban-rare-earths-processing-technology-exports-means>
19. World Economic Forum, "How climate hazards are reshaping business realities and responses" (Mar 26, 2025) (Business on the Edge study): <https://www.weforum.org/stories/2025/03/how-climate-hazards-are-reshaping-business-realities-and-responses/>
20. Smithsonian Magazine, "Hurricane Helene Shatters 'Critical' Quartz Mines..." (Oct 3, 2024): <https://www.smithsonianmag.com/smart-news/hurricane-helene-shatters-critical-quartz-mines-that-power-the-worlds-electronics-solar-panels-and-ai-180985187/>
21. Carolina Journal, "WNC quartz mining operations halted, risking global semiconductor supply" (Oct 1, 2024): <https://www.carolinajournal.com/western-nc-quartz-mine-at-center-of-trillion-dollar-chip-industry-temporarily-shutdown-amid-helene-havoc/>
22. Taipei Representative Office in Singapore, "Taiwan and the Global Semiconductor Supply Chain" (Feb 2024 issue) (market share table): <https://www.taiwanembassy.org/uploads/sites/86/2024/02/240202-February-Issue.pdf>
23. IEKTechMap, "Taiwan Semiconductor Landscape" (accessed 2026): <https://ieknet-eng.iek.org.tw/IndustryMap/IndustryMap.html>
24. Epoch AI, "Advanced packaging and HBM... were the bottlenecks on AI chip production in 2025" (Mar 12, 2026): <https://epoch.ai/data-insights/ai-chip-supply-chain-constraints>
25. TrendForce, "Memory Wall Bottleneck: AI Compute Sparks Memory Supercycle" (Jan 16, 2026): <https://www.trendforce.com/insights/memory-wall>
26. CSIS, "Maritime Port Digitization and Systemic Cyber Risk" (Feb 5, 2026): <https://www.csis.org/blogs/strategic-technologies-blog/maritime-port-digitization-and-systemic-cyber-risk>
27. MIT Sloan Management Review, Toshihiro Nishiguchi and Alexandre Beaudet, "The Toyota Group and the Aisin Fire" (Oct 15, 1998): <https://sloanreview.mit.edu/article/the-toyota-group-and-the-aisin-fire/>



This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte Canada

At Deloitte, our Purpose is to make an impact that matters. We exist to inspire and help our people, organizations, communities, and countries to thrive. Our work underpins a prosperous society where people can find meaning and opportunity. It builds consumer and business confidence, empowers organizations to find imaginative ways of deploying capital, enables fair, trusted, and functioning social and economic institutions, and allows our friends, families, and communities to enjoy the quality of life that comes with a sustainable future. And as the largest Canadian-owned and operated professional services firm in our country, we are proud to work alongside our clients to make a positive impact for all Canadians.

Deloitte provides industry-leading consulting, audit and assurance, tax, advisory and managed services to nearly 90% of the Fortune Global 500® and thousands of private companies. We bring together world-class capabilities, insights, and services to address clients' most complex business challenges.

Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited. Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

To learn more about Deloitte Canada, please connect with us on [LinkedIn](#), [X](#), [Instagram](#), or [Facebook](#).