Taking the risk and managing the risk.

Taming the beast: managing supply chain risk

August 14, 2025

Most supply chain risks are easy to diagnose in hindsight. The real value lies in anticipating risks and preparing for them before the crisis hits.

This is where many companies fail. Even when awareness is high, the approach can be siloed, under-resourced, and be reactive rather than proactive. People don't take risk management seriously when it's hard to put a value on events that haven't occurred yet, and it is hard to put a value on the effort to prevent events that haven't occurred.

Certain types of risks, like workforce injury rates at industrial sites, can be quantified when the frequency of incidence allows for statistical analysis. By contrast, procurement deals with many different types of materials and services, many different supplier relationships, many different transportation modes and carriers. Root causes are hard to predict and patterns can be challenging to find.

Further, supply-related risks usually have a commercial or production impact, which doesn't attract—or deserve—the same attention as loss of life and limb, or environmental disasters. But while commercial risks have a lower profile, their cumulative impact can be huge and existential.

Supply chain risk deserves attention: The financial and intangible impact of the supply chain disruption that occurred under your watch may show up on any page and in any footnote of next year's annual report, or as the top feed of today's Wall Street Journal.

At a high level, here's what supply chain risk management looks like when done well — and why it's worth doing.

Who should own supply chain risk?

Risk management is an enterprise concern. Supply risk should be managed in the context of an enterprise level risk management program.

Companies should start by creating a **corporate risk register**, owned at the CEO level and visible to the board. This register includes operational, financial, reputational, and strategic risks. If done right, supply chain risks will show up in the register.

The risk register serves many purposes:

- To size up the potential cost to the enterprise if those risks remain unmanaged, or if the response is inappropriate
- To categorize the root causes as well as the scope of impact of diverse risks
- To help prioritize—or, we will say, "triage"—risks that require attention
- To provide motivation and a directional business case for a risk management program.

Once senior leadership understands the potential impact and profile of the risk portfolio, it can develop a governance structure to manage it. By governance, we mean reporting/monitoring, oversight, coordination, mobilization of resources, escalation paths, and defined roles and responsibilities.

Governance includes the assignment of an enterprise-level team for the program overall, and function-specific owners. The Chief Procurement Officer may be a function-specific owner (for procurement), as would be the COO (for operations), and the CMO or head of Public Relations (for reputational risk). These owners would lead the effort to identify potential risks, mitigations, and responses in their areas, and coordinate with other owners to ensure that interface risks are also identified, and that all risks have an owner.

A core feature of good governance is measurement (KPIs) and tracking. While "risk" is difficult to measure directly, occurrences of adverse incidents can be a lagging indicator of gaps in risk management. For example, in industrial settings, safety KPIs such as incident rates serve as a (lagging) indicator of the health of the governing risk management framework. Compliance to safety procedures can serve as leading indicators. Industrial risk management is a very complex but because it is a well-developed field, it can provide ways of thinking about managing supplier and supply chain risk management. Changes in rates of incidence, such as changes in DIFOT rates, provide an indication of changes in risk (and possible changes in risk management effectiveness). Compliance measurement (e.g., supplier conformance to reporting requirements) is another source for KPIs. The risk register is essential to developing and setting targets for KPIs, to the extent that KPIs can be tied either to the root causes of risks, or to the business impact of risk incidents.

Know the risk

Risks show up differently by industry. In an industrial setting, risks are more likely to be related to frontline worker health and safety, or community and environmental impact. In a retail setting, these risks are more likely to be related to revenues or branding. In manufacturing, these risks may be related to lost margins resulting from downtime on the production line. In highly regulated industries, risks may be existential: oversight agencies can revoke the company's permission to operate. In the public's eye, any company can lose what is effectively a social license to operate. Consider the brand damage to companies whose suppliers were discovered to be sweat shops using child labor.

I have worked with companies ranging in diversity from defense contractors to financial institutions whose operations were shut down for long durations as a result of having breached regulatory requirements of one kind or another. In these cases, the shutdown nearly drove the respective companies out of business.

Disruptions in supplier performance and in the supply chain can often be the root cause of enterprise-level risk. The news frequently features examples such as tainted products from food manufacturers; accidents of commercial aircraft; environmental disasters at industrial sites. Any of these adverse events could have been supply chain-related: contaminated ingredients; out-of-compliance OEM parts; contracted inspectors not doing their jobs.

Triage the risk

We recommend developing a risk register as a first step to understanding the scope and depth of a company's exposure to risk. It should be developed as a joint effort of diverse stakeholders representing the scope of a company's operations. It should become a living document that is reviewed and updated on an ongoing basis.

In its simplest form, a risk register is a table of risks, with columns corresponding to estimates of likely frequency of occurrence ("once in 10 years") and likely impact ("2m production stoppage"). For many risks, it is feasible and reasonable to attach a corresponding dollar value of the impact on EBITDA, estimated to an order of magnitude ("$20m"). The product of frequency and EBITDA (1/10 x $20m = $2m) provides an estimate of expected impact. While this "estimate" is really just an educated guess, as a quantified value, to an order of magnitude, it is useful in triaging.

At the enterprise level (and then at the functional level), the business or function needs to identify the short list of risks are likely to have the biggest impact. By expressing these risks in terms of potential EBITDA impact, the register creates a business case for the risk management initiative. If more data is required to build the business case, Covid era examples provide many documented cases of business impact that can be compiled to build a financial case for risk management.

Profile your suppliers

In addition to the risk register, procurement should build a supplemental supplier portfolio risk assessment. This list is a table of might spend and/or strategic suppliers and records key information such as: rated strategic importance; what makes it strategic; a description of how the business would be affected if there were supply or service disruptions from this supplier; assessment of business health and market position; a summary of how potential risks should be managed. The analysis may include Tier 2 (supplier's supplier) and Tier 3 supplier dependencies.

I can provide two examples of supplier portfolio assessments. In one instance, I worked with an engine manufacturer that was failing and running out of cash. It had limited funds each month to pay its suppliers. I developed a summary of the top 100 or so suppliers and ranked them in terms of strength of the current relationship (specifically, their tolerance to late payments), how essential they were to keep production lines going, and what strategic recourse was available, if this supplier refused to continue doing business with us. We were able to project a viability horizon to estimate how much time the company had to generate sales to pay its suppliers before the supply base would crater.

In another instance, I worked with a new CFO who assessed the portfolio of high spend suppliers in terms of opportunities to capture rebates and early pay discounts, vs. the option to manage cash tightly with late payments. The accounts payable practices of this company had devolved into paying suppliers at 60+ days after receipt. With these late payments, the company was forfeiting both early pay discounts as well as supplier goodwill. The CFO developed a business case for the owners to infuse cash to shorten the AP cycle and capture early pay discounts and rebates where these were available, and to bring remittances to all suppliers into contract compliance.

While these are narrow examples, they illustrate how a portfolio-level view can inform decision making.

Get ahead of the risk

WhIle root causes of risks related to supply chain failures are highly diverse, there are certain classes of impact that can be anticipated and mitigated. The most obvious supply risk is, of course, to continuity of supply. Obvious mitigations include having backup suppliers, inventory stockpiles, pre-approved substitutes, and commercial terms (long term commitments, take-or-pay agreements, allocations).

Another class of risks in supply relates to defects, non-compliance to specifications, and quality problems. Mitigations include supplier-side quality reporting, performance and outcome criteria with appropriate remedies, fast feedback loops, and backup sources.

These techniques are second nature to any procurement professional. The reason for outlining them here is to point out that pro-active mitigation is only half of the story. The other half is being prepared to respond to incidents after the fact, when mitigations have not been successful.

Be proactive—create options now and prepare for the worst

Part of the governance required for risk management is having ongoing risk monitoring in place, and a crisis response team that can be activated as soon as a risk event has occurred.

The crisis response team has resources at its disposal, such as a dedicated war room, document repository, and communications solutions. The members of the team have designated replacements to step into their day-to-day roles when they are reassigned to the crisis response. While this sounds like a lot of "machinery" to put in place, in practice, it's relatively simple. A handful of individuals are preselected to mobilize when needed, and this same group has responsibility on an ongoing basis to monitor risks, update plans, and prepare.

Major risk events typically involve compound failures with unrelated root causes. While difficult to plan for, organizations can pre-organize a coordinated response. This has several features:

- Engagement with major stakeholder groups to communicate out what has happened, request input and support, and to gain alignment on action.
- Creative and lateral thinking. In the moment, intertwined risks can't be solved linearly, in isolation, or with conventional solutions. Timely, event-triggered responses may be completely different from the routine course corrections of normal business operations.
- Systems and big picture thinking. Compound failures involve interdependent systems and processes, rife with blind spots.

The crisis response team must be cross-functional, be able to think creatively, and bring a big-picture perspective. They must act cohesively and respond to leadership. This is a tough ask.

Risks involve compound failures.

It is important to note that there are differences in risk profiles across industries. Industries that are highly regulated or are subject to a high level of public scrutiny—e.g., public utilities, defense contractors, pharmaceuticals, brand-driven consumer products — are subject to an additional dimension of influence from external parties such as regulators, investors, media, and the public. Coordinating with these external stakeholders can play a big role in magnifying or mitigating their impact on the business.

For example, since procurement among defense contractors or nuclear utilities is tightly regulated for certain kinds of materials, a company may choose to be proactive in working with the respective agencies or legislative bodies to modify requirements to reduce costs or provide more flexibility in procurement.

In the nuclear industry, the restricted availability of safety-related parts due to the obsolescence of old plants and discontinued OEM production lines forces companies to look for alternative sources. In anticipation of the risk of obsolescence, a supply manager would proactively seek alternative sources and work with regulatory bodies to get approval for them.

The business case for risk management

Mitigations and preparations sound costly and distracting. Are they? You will only know once you've performed an initial assessment. The cost of the diagnostic is trivial compared to the cost of the risks. If you're on the battlefield, you need to open your eyes before you can look for cover or take aim.

Authorship

Peter Benda is a general management consultant specializing in strategic sourcing and supply chain management, front line productivity improvement, governance, and diagnostics. He has worked with clients in mining, utilities, manufacturing, financial services, transportation, defense, state agencies, and technology startups. Peter has authored articles on investment risk related to the supply chain. He is on the Board of Advisors to Axtom, a SAAS solution that uses AI to automate tendering, negotiation, and contracting. Axtom's goal is to free up purchasing professionals to focus on higher-value problems like strategy and risk management. This article was generated with the help of ChatGPT.

Hashtags

#SupplyChainRisk #RiskManagement #OperationalResilience
#EnterpriseRisk #ProcurementStrategy #CrisisResponse
#SupplyChainLeadership #EBITDAImpact #AIinProcurement #Axtom

Key words

supply chain risk; risk management; supply chain disruption; procurement risk; logistics risk; operational resilience; business continuity, supply continuity; enterprise risk; corporate governance; EBITDA; financial exposure; cost of risk; AI in supply chain; Axtom

Header

Do you know which risks are hidden in your supply chain? The next crisis won't wait for you to figure it out.

Images

- https://www.istockphoto.com/photo/hand-pull-out-wood-block-from-tower-growth-risk-strategy-in-business-gm919415502-252803219
- https://www.istockphoto.com/photo/close-up-of-a-damaged-green-net-gm2213950179-630795613?searchscope=image%2Cfilm