McKinsey & Company

Operations Practice

A practical approach to supply-chain risk management

In supply-chain risk management, organizations often don't know where to start. We offer a practical approach.

by Tucker Bailey, Edward Barriball, Arnav Dey, and Ali Sankur

© Phil Leo/Michael Denora/Getty Images

March 2019

In the last decade, a number of organizations have been rocked by unforeseen supply-chain vulnerabilities and disruptions, leading to recalls costing hundreds of millions of dollars in industries ranging from pharmaceuticals and consumer goods to electronics and automotive. And multiple government organizations and private businesses have struggled with cybersecurity breaches, losing critical intellectual property due to failures in the supplier ecosystem.

At the heart of these crises is a common theme—the lack of robust processes to identify and successfully manage growing supply-chain risks as the world becomes more interconnected. New threats, such as cyber-ransom attacks, are emerging alongside more traditional and longer-acknowledged supplier risks, such as supplier bankruptcy.

The challenge of supply-chain risk management has been exacerbated by globalization, where even sensitive products like defense systems use raw materials, circuit boards, and related components that may have originated in countries where the system manufacturer did not even know it had a supply chain. This increased complexity has brought with it more potential failure points and higher levels of risk.

Yet progress in addressing these risks has been slow. In our 2010 survey of 639 executives covering a range of regions and industries, 71 percent said their companies were more at risk from supply-chain disruption than previously, and 72 percent expected those risks to continue to rise (from “The challenges ahead for supply chains: McKinsey Global Survey Results,” Nov 2010, McKinsey.com). In 2018, the United States government stood up multiple agencies and task forces to better address supply-chain risk (including the Critical Infrastructure Security and Cybersecurity Agency in the Department of Homeland Security and the Protecting Critical Technology Task Force at the Department of Defense), and the private sector continues to seek a uniform and proven methodology for assessing and monitoring risks in a way that truly minimizes business disruption.

We believe public- and private-sector organizations have struggled to progress significantly on this topic for several reasons:

1. **Supply-base transparency is hard (or impossible) to achieve.** In modern multi-tier supply chains, hundreds or thousands of suppliers may contribute to a single product. Even identifying the full set of suppliers from the raw-material sources to a final assembled system can require a significant time investment.

2. **The scope and scale of risks is intimidating.** The probability and severity of many risks is difficult to ascertain (How likely are certain weather patterns? How often will a supplier’s employee be careless in cybersecurity practices?), and therefore difficult to address, quantify, and mitigate.

3. **Proprietary data restrictions impede progress.** In complex products, Tier 1 or 2 suppliers may consider their supply chains to be proprietary, limiting visibility at the purchaser or integrating-manufacturer level.

Rather than admiring the problem and these difficulties, we suggest organizations begin to tackle issues in a structured way, cataloging and addressing known risks while improving the organization’s resilience for the inevitable unknown risk that becomes a problem in the future.

A structured approach to supply-chain risk management

We recommend that organizations start by thinking of their risks in terms of known and unknown risks.

Known risks can be identified and are possible to measure and manage over time. For instance, a supplier bankruptcy leading to a disruption in supply would be a known risk. Its likelihood can be estimated based on the supplier’s financial

The challenge of supply-chain risk management has been exacerbated by globalization.

history, and its impact on your organization can be quantified through consideration of the products and markets the supplier would disrupt. Newer risks such as cybersecurity vulnerabilities in the supply chain are also now quantifiable through systems that use outside-in analysis of a company's IT systems to quantify cybersecurity risks.

Organizations should invest time with a cross-functional team to catalog a full scope of risks they face, building a risk-management framework that determines which metrics are appropriate for measuring risks, "what good looks like" for each metric, and how to rigorously track and monitor these metrics. This team can also identify gray areas where risks are hard to understand or define (e.g., tiers of the supply chain where no visibility exists). This analysis can dimensionalize the scale and scope of unknown risks.

Unknown risks are those that are impossible or very difficult to foresee. Consider the sudden eruption of a long dormant volcano that disrupts a supplier you didn't know was in your supply chain, or the exploitation of a cybersecurity vulnerability buried deep the firmware of a critical electronic component. Predicting scenarios like these is likely impossible for even the most risk-conscious managers.

For unknown risks, reducing their probability and increasing the speed of response when they do occur is critical to sustaining competitive advantage. Building strong layers of defense combined with a risk-aware culture can give an organization this advantage.

Managing known risks

Organizations can use a combination of structured problem solving and digital tools to effectively manage their known-risk portfolio through four steps:

Step 1: Identify and document risks

A typical approach for risk identification is to map out and assess the value chains of all major products. Each node of the supply chain—suppliers, plants, warehouses, and transport routes—is then assessed in detail (Exhibit 1). Risks are entered on a risk register and tracked rigorously on an ongoing basis. In this step, parts of the supply chain where no data exist and further investigation is required should also be recorded.

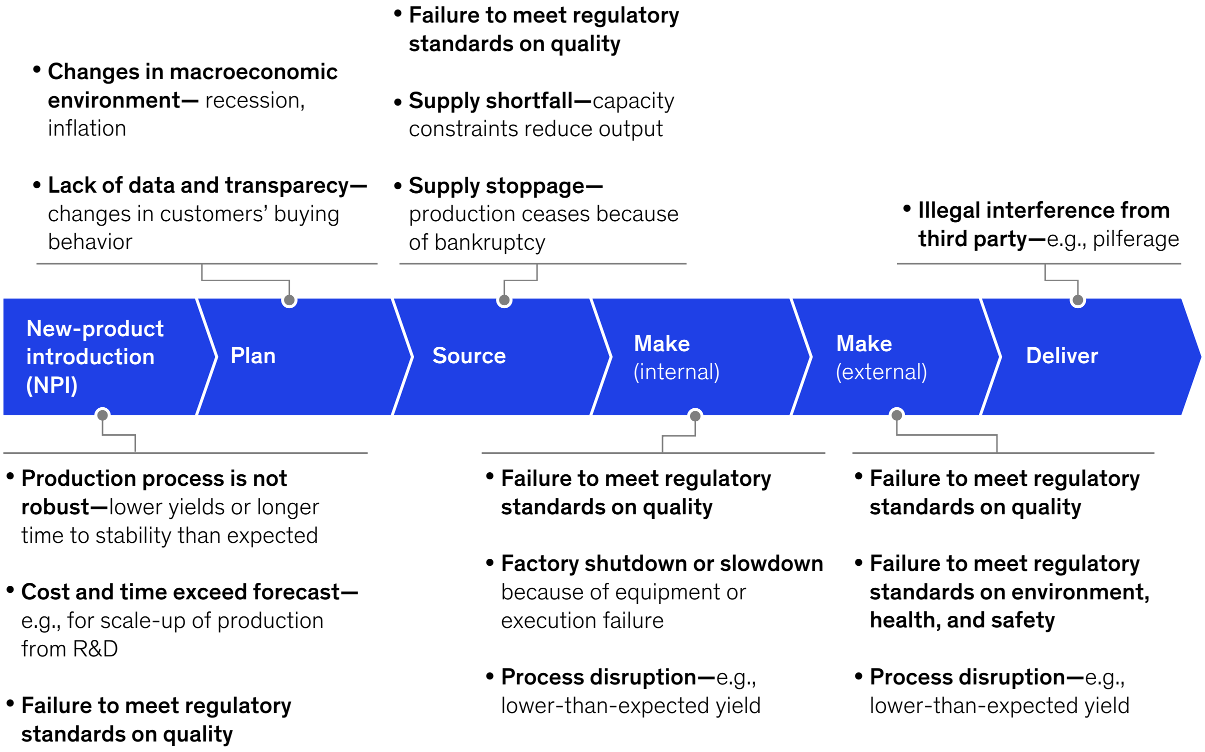
Step 2: Build a supply-chain risk-management framework

Every risk in the register should be scored based on three dimensions to build an integrated risk-management framework: impact on the organization if the risk materializes, the likelihood of the risk materializing, and the organization's preparedness to deal with that specific risk. Tolerance thresholds are applied on the risk scores reflecting the organization's risk appetite.

It is critical to design and use a consistent scoring methodology to assess all risks. This allows for prioritizing and aggregating threats to identify the highest-risk products and value-chain nodes with the greatest failure potential.

Exhibit 1

Assess value-chain nodes to identify key risks.



- **Changes in macroeconomic environment—** recession, inflation
- **Lack of data and transparecy—** changes in customers' buying behavior

- **Failure to meet regulatory standards on quality**
- **Supply shortfall—**capacity constraints reduce output
- **Supply stoppage—** production ceases because of bankruptcy

- **Illegal interference from third party—**e.g., pilferage

New-product introduction (NPI) | **Plan** | **Source** | **Make** (internal) | **Make** (external) | **Deliver**

- **Production process is not robust—**lower yields or longer time to stability than expected
- **Cost and time exceed forecast—** e.g., for scale-up of production from R&D
- **Failure to meet regulatory standards on quality**

- **Failure to meet regulatory standards on quality**
- **Factory shutdown or slowdown** because of equipment or execution failure
- **Process disruption—**e.g., lower-than-expected yield

- **Failure to meet regulatory standards on quality**
- **Failure to meet regulatory standards on environment, health, and safety**
- **Process disruption—**e.g., lower-than-expected yield

Step 3: Monitor risk

Once a risk-management framework is established, persistent monitoring is one of the critical success factors in identifying risks that may damage an organization. The recent emergence of digital tools has made this possible for even the most complex supply chains, by identifying and tracking the leading indicators of risk. For example, a large organization operating in a regulated industry identified 25 leading indicators of quality issues at its plants and contract manufacturers, ranging from structural drivers including geographical location and number of years in operation to operational performance metrics, such as “right first time” and deviation cycle times. These 25 indicators were carefully weighted to develop a quality risk-exposure score, and then tracked on a regular cadence.

Successful monitoring systems are customized to an organization’s needs, incorporating impact, likelihood, and preparedness perspectives. Hence, while one organization may track deviations on manufacturing lines to predict quality issues, another may follow real-time Caribbean weather reports to monitor hurricane risk at its plants in Puerto Rico. Regardless, it is critical to have an early warning system to track top risks to maximize the chances of mitigating, or at the very least limiting, the impact from their occurrence.

Step 4: Institute governance and regular review

The final critical step is to set up a robust governance mechanism to periodically review supply chain risks and define mitigating actions, improving the resilience and agility of the supply chain.

An effective supply-chain risk-management governance mechanism is a cross-functional risk board with participants representing every node of the value chain. It typically includes line managers who double-hat as risk owners for their function, giving them ownership of risk identification and mitigation. In most cases, the risk board receives additional support from a central risk-management function, staffed with experts to provide additional guidance on identifying and mitigating risks.

An effective board will meet periodically to review the top risks in the supply chain and define the mitigation actions. The participants will then own the execution of mitigation actions for their respective functional nodes. For example, if the board decides to qualify and onboard a new supplier for a critical component, the procurement representative on the board will own the action and ensure its execution.

Additionally, in many organizations the risk board will also make recommendations to improve the agility and resilience of the supply chain, ranging from reconfiguring the supply network, finding new ways of reducing lead times, or working with suppliers to help optimize their own operations. Increasing supply-chain agility can be a highly effective mitigation strategy for organizations to improve their preparedness for a wide range of risks.

Managing unknown risks

Unknown risks are, by their nature, difficult or impossible to predict, quantify, or incorporate into the risk-management framework discussed above for known risks. In our experience, mitigating unknown risks is best achieved through creating strong defenses combined with building a risk-aware culture.

Building strong defenses

Strong defenses, from request-for-proposal (RFP) language to worker training, all contribute to an organization identifying and stopping unknown risks before they affect operations. Exhibit 2 outlines typical layers of defense organizations employ to defend against unknown risks.

Building a risk-aware culture

A risk-aware culture helps an organization both establish and maintain strong defensive layers against unknown risks, as well as respond more quickly when an unknown risk surfaces and threatens operations.

— **Acknowledgement.** Management and employees need to feel empowered to pass on bad news and lessons from mistakes. This openness fosters an environment where it is okay to voice and deal with issues. Culturally, it is critical that the organization not get discouraged or point fingers when a risk event occurs, and instead works harmoniously towards a rapid resolution.

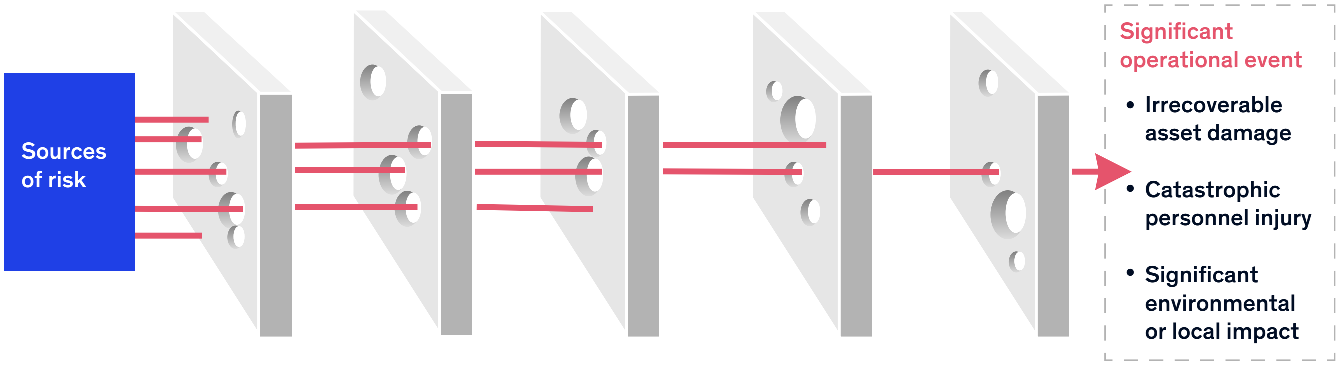
— **Transparency.** Leaders must clearly define and communicate an organization’s risk tolerance. Risk mitigation often has an associated incremental cost, and so it is important to align on which risks need to be mitigated and which can be borne by the organization. An organization’s culture should also allow for warning signs of both internal and external risks to be openly shared.

— **Responsiveness.** Employees need to be empowered to perceive and react rapidly to external change. This can be enabled by creating an ownership environment, where members feel responsible for outcome of actions and decisions.

— **Respect.** Employees’ risk appetites should be aligned with an organization, so that individuals or groups do not take risks or actions that benefit themselves but harm the broader organization.

Exhibit 2

Layers of defenses help organizations manage unknown risks.



Sources of risk

Significant operational event

- Irrecoverable asset damage
- Catastrophic personnel injury
- Significant environmental or local impact

Risk management barriers

Design quality, configuration control
- Preserving margins
- Protecting the design basis
- Strictly controlling configuration

Equipment health, performance
- Overseeing maintenance strategies
- Monitoring, intervening
- Running and maintaining capital assets

Oversight, assurance methods
- Developing oversight structure
- Strengthening independence and quality

Decision-making processes
- Emergent-issue responses
- Operational focus for resolution
- Risk-informed

Worker, operator fundamentals
- Frontline skills and behaviors
- Clearly defined standards of performance

Event, emergency preparedness
- Operator, organizational readiness
- Infrastructure, materials
- Response, mitigation equipment

◀ Risk processes, standards, competency, organization, and culture ▶

The road ahead

Global supply chains are irreversible, as are the supply-chain risks that globalization has brought with it. Our experience suggests that it is critical for organizations to build robust programs for managing both known and unknown supply-chain risks. Leaders should also recognize that risk management is not merely about setting up processes and governance models, but also entails shifts in culture and mind-sets. By employing these approaches, organizations increase their chances of minimizing supply-chain disruptions and crises, while capturing the full value of their supply-chain strategies.

Tucker Bailey and **Edward Barriball** are partners in McKinsey's Washington, DC office. **Arnav Dey** is an engagement manager in the Boston office, and **Ali Sankur** is a senior practice manager in Chicago.

Designed by Global Editorial Services