Risk Intelligence and the Resilient Company

Applying a more sophisticated approach to risk management can help leaders continue to generate value through disruption and uncertainty.

By Ananya Sheth and Joseph V. Sinfield

BUILDING THE RESILIENCE OF LARGE, COMplex enterprises is critical in today's uncertain and interconnected world. At a time when a container ship grounded in the Suez Canal can bottle up 12% of the world's trade, or a virus can disrupt the global flow of commodities, components, and talent, a corporation's ability to quickly adapt in the face of unfolding events is essential to its survival and prosperity.

Business resilience is a dynamic property that is retrospectively measured by the stability and longevity of corporate value across changing contexts. In real time, it manifests in an enterprise's timely adaptation to both immediate and gradual changes in the business environment.

Our work, which employs a complex adaptive systems view of businesses, shows that resilience derives from three fundamental adaptive capacities: sensing and monitoring, to recognize emerging changes in the business environment; business model portfolio development, to build and test capabilities across operating contexts; and fundamental capability development, to drive growth with longevity and avoid corporate stall.[1] Moreover, each of these capacities hinges on the development of a capability for *risk intelligence*.

We define risk intelligence as the honed ability to rigorously interpret risks and the consequences or opportunities they pose

Simon Prades

for a company.[2] It allows leaders to see through environmental complexity and systematically identify, categorize, and group risks. This enables them to look beyond known risk factors and intentionally explore yet-to-be-known risks, thereby embracing rather than avoiding uncertainty. Importantly, it brings recognition that individual risks or the forms in which they manifest matter far less than the often-shared consequences they have on a company's value exchange system — that is, the manner in which it manages, identifies, creates, conveys, delivers, captures, protects, and sustains value.[3] And finally, it provides leaders with a network view of risks that enables more effective allocation of risk mitigation resources by illuminating not just the direct consequences of risks but the manner in which they could cascade across the company's value exchange system. In this article, we break down risk intelligence into actionable elements that leaders can pursue to help harden their organizations for the long term.

THE RESEARCH

- The authors undertook a holistic study of enterprise resilience that began with the extraction of corporate risk factors from two decades of 10-Ks filed by S&P 500 companies, investment analyst reports, and academic databases.
- They organized the risks into a value-centric framework composed of eight functions and 99 major risk categories; they then cross-linked the categories and functions with input from risk experts and leaders in 10 economic sectors and 26 industries to create a quantitative risk network.
- They also analyzed cybersecurity risk acknowledgement in S&P 500 10-Ks for five sectors.
- Their research was supported by the National Science Foundation under grant no. 2049782.[i]

Identify, Categorize, and Interpret Risk Events

Leaders cannot accurately predict specific risk events, nor can they prepare their companies for all risks. They can, however, identify, categorize, and interpret risk events in a systematic manner that reveals how seemingly different events could have similar consequences.

The first step is to work through each business value function and identify plausible risk events that may have implications for its effectiveness. To aid in this process, we constructed an industry-agnostic inventory organizing three tiers of 99 major risk categories identified in our study in relation to individual value exchange system components. (See "A Value Function Risk Inventory.") While inevitably not exhaustive, this resource serves as a robust starting point to identify potential risks faced by any enterprise.

Next, leaders should characterize and group risk events by their scope of impact, the *permanence* of the changes they induce, and the frequency of event occurrence. (See "Characterizing Risks.") Leaders can then interpret the linkages between each group of risk events and the components of the company's value exchange system.

Risk categorization begins with understanding a risk event's scope, which conveys an absolute sense of how widely a risk's effects will be felt across the range of affected stakeholders. The wide scope of the COVID-19 pandemic created supply- and demand-side effects across entire value networks, whereas narrow-scope events, such as a labor strike at an individual manufacturing facility, tend to have more bounded effects. When multiple stakeholders experience simultaneous or sequential disruptions, the increased complexity of the impact prevents the system from self-organizing to normalcy. Such circumstances also may invite interventions from sovereign states or international organizations, which can aid recovery or act as new disruptive forces.

To fully categorize risk events, leaders must also consider the permanence of their consequences. Both the pandemic and the 2021 Suez Canal blockage caused supply-side disruptions, but the permanence of the changes each event induced varied significantly. While supply chain shocks such as the canal blockage often follow a self-organizing correction mechanism in which price increases lower demand and normalize the lagging supply, the same formula cannot be applied to counter a protracted situation like the pandemic.[4] It is important to understand permanence before planning and implementing a response strategy. For example, the business interruption created by the pandemic had a scope that was broader and consequences that were of greater permanence, affecting a significantly larger set of value system functions in comparison to the more limited impact of the canal blockage.

How often a risk event occurs is important too, because the enterprise mechanisms needed to handle frequent events can be different from those employed for singular events.[5] Although companies learn from all events, their responses to those that occur repeatedly are typically converted into standard operating procedures.[6] For example, the adoption of barcodes and scanners to

track and manage inventory in real time has largely eliminated stock-keeping record errors and delays resulting from mismatching data.

Our scope, permanence, and frequency (SPF) framework provides a structured view that shows how a risk event itself is less important than its consequences. The framework is especially useful when multiple risk events occur at the same time, because it gives managers a common, logical approach for considering them and quickly gaining information and understanding. By then connecting those events to the company's value exchange system, managers can more easily see when diverse risks are nonetheless leading to similar consequences for its value functions.[7]

Consider a manufacturer dealing with both an overseas supplier whose products are suddenly subject to much higher tariffs due to a trade war, and the bankruptcy of a value chain partner. These risk events share SPF characteristics (the scope of both is interfirm, their permanence is reversible, and their frequency is low), and, as important, both events also affect the same value functions. The bankruptcy and the trade war are both likely to slow inputs and raise costs on the supply side and make it more difficult to meet customer demand. Both also would require the manufacturer to secure new supply sources and stabilize operational cash flow. By characterizing these potential risk events according to the SPF framework and linking them to value functions, managers can then view them more simply as groups of risks that have shared consequences for a company's specific value functions and deserve similar preparedness and response.

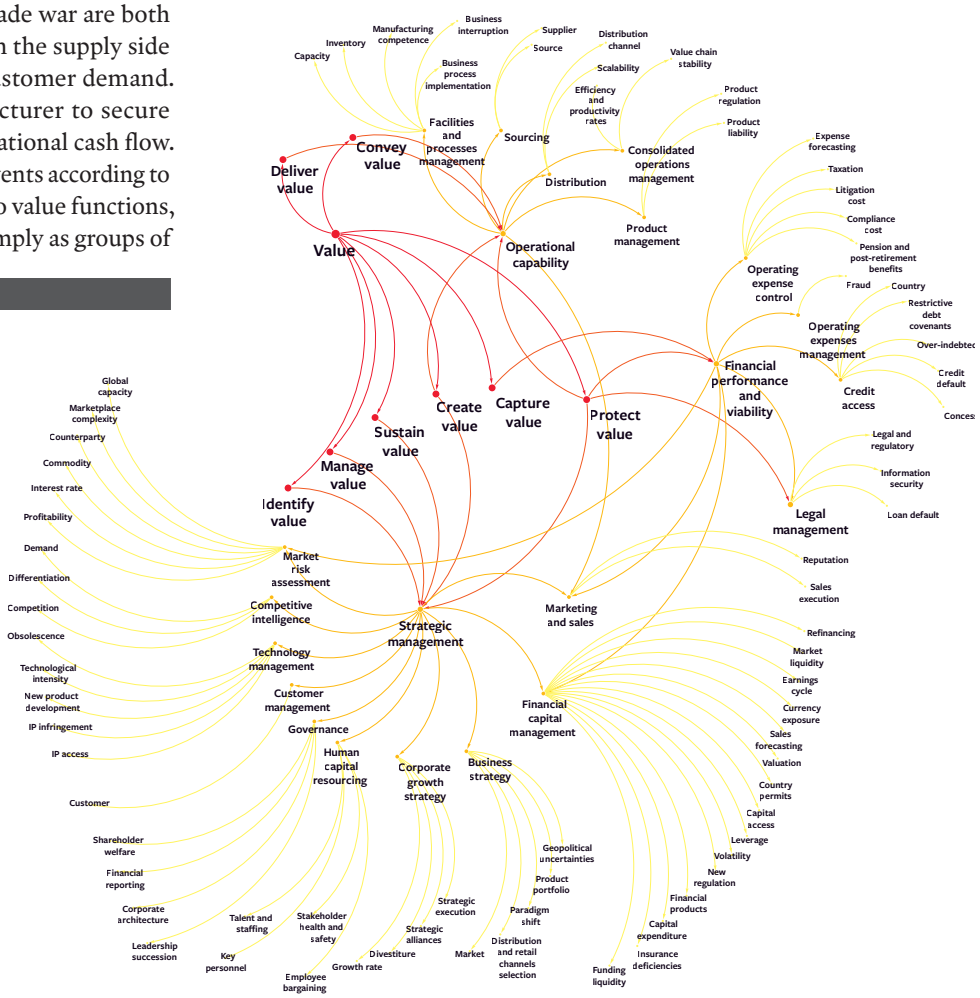
Compartmentalize and Reduce Uncertainty

Uncertainty about the consequences of a risk event is unavoidable, but it can be managed based on where the level of uncertainty falls on a spectrum between complete knowledge and complete ignorance (both of which are extreme and unlikely).[8] Leaders should then seek to convert risks with higher levels of impact uncertainty to lower levels. (See "Managing Levels of Impact Uncertainty.")

Risk events causing level 1 uncertainty usually entail a very limited number of future scenarios with clear intrafirm effects, where causal linkages between risk events and the enterprise's value exchange system can be accurately known. Examples of such events include routine variation in production, expected sales losses,

A Value Function Risk Inventory

This risk inventory derived from 20 years of S&P 500 data shows how the functions of a company's value exchange system (red nodes) link to business functions and their respective risk categories.



and human errors in performing manual tasks. When specific types of level 1 events occur frequently, they are indicative of errors in process or oversight that can be rectified permanently if diagnosed correctly. For instance, cargo thefts — a recurrent problem at logjammed transport hubs — can be prevented using optical character recognition scanners that track container freight and maintain real-time records. Importantly, at level 1, the overall uncertainty of the impact on firm value is within an expected, acceptable range.

Risk events causing level 2 uncertainty involve a larger number of alternate future scenarios and have interfirm consequences; however, even though they are more challenging, the probability that they will occur and their effects can be estimated. Businesses' formal scenario-planning exercises often involve level 2 events in which previously acquired knowledge regarding the impact of risk factors leads to improved accuracy and an effective exercise overall. The six-day Suez Canal blockage was predictable because a multiship pileup had closed the canal for two days in 2018. As a result, the Pentagon had already worked a longer blockage into its normal operational preparedness.[9]

Risk events causing level 3 uncertainty involve a bounded set of scenarios where certain known risk events may affect the company in unknown ways. There is limited knowledge about how a chain reaction of consequences from a risk event might manifest at this level. Typically, these risks include less frequently occurring events with intra-industry scope and multi-stakeholder implications, which should be considered worst-case scenarios.

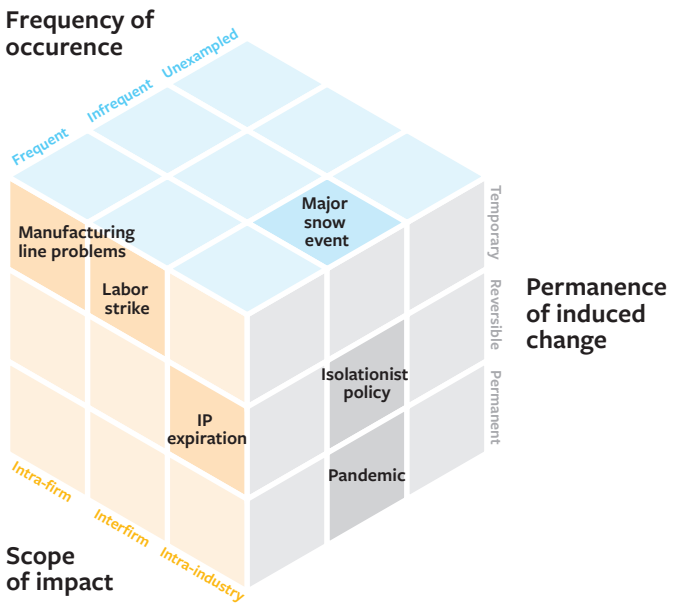
Port Revel, a training facility situated on a lake in the French Alps, reduces level 3 uncertainty by helping ocean shipping companies simulate worst cases and identify the previously unknown consequences of operating increasingly large container ships through shipping infrastructure largely designed for smaller vessels. It closely replicates conditions at the trickiest spots in maritime transport, allowing trainee pilots to navigate scaled giant container ships through strong gusts of wind across a mini-Suez, steer and dock cruise ships in a crowded mini-San Francisco Bay, and maneuver oil tankers through an imitation Port Arthur. These exercises draw out unanticipated ship performance and pilot behaviors, helping to identify and address previously unknown event consequences.

Level 4 uncertainty encompasses events with unknown risk factors that could have a variety of negative consequences, the repercussions of which can't be estimated. These unknown unknowns are usually expressed in 10-Ks through statements such as "Other unknown risks may impact our business operations and projected performance." It is challenging to develop scenario models in the presence of unknown unknowns. The models are incomplete representations of the world that could entail risks unimagined while developing them.

Once leaders order the uncertainty of impact into levels, they can focus on converting higher-level impact uncertainty into lower levels by discovering unknowns through data, simulation modeling, and logical analyses. For instance, the three-year gap between the U.K.'s Brexit referendum in 2016 and its departure from the European Union in 2019 offered leaders an opportunity to convert the imagined event into likely scenarios and capture its vast trade implications. By focusing on the most vulnerable aspects of their value chains, such as those with the highest number of cross-border transactions, leaders could have recognized the imminent redistribution of goods passing through congested ports and modeled rerouting scenarios. For example, Felixstowe was known to be handling 48% of the U.K.'s container trade, which could have been sent instead to multiple smaller and less busy ports. Evidence of impending port

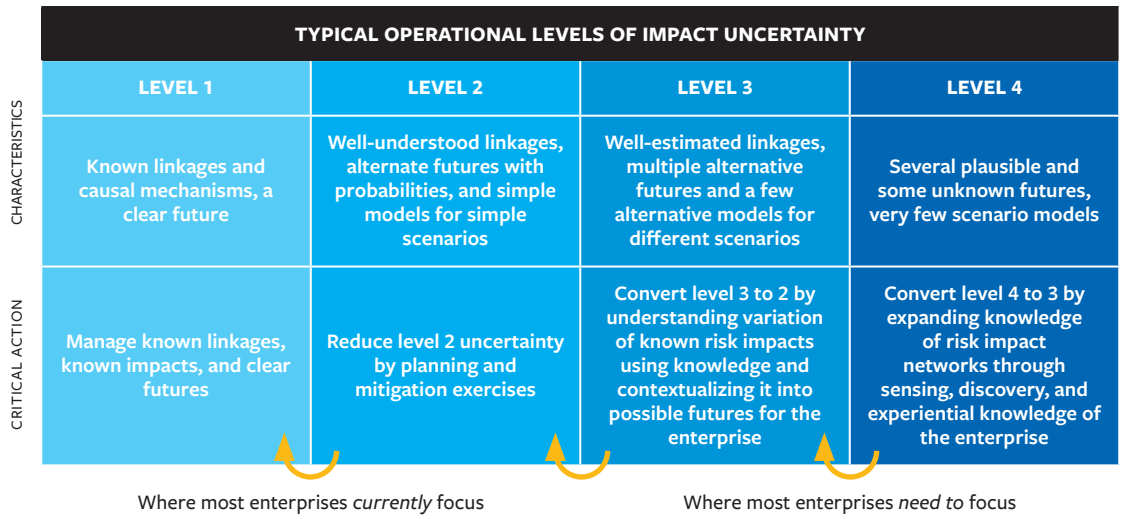
Characterizing Risks

Every risk can be characterized according to how widely its impact may be felt, how long the changes it causes may last, and how often it occurs. For example, a major snow event has intra-industry scope, induces temporary changes, and occurs infrequently.



Managing Levels of Impact Uncertainty

Once managers have mapped risks to the appropriate level, they should take the critical action recommended to convert higher-order risks to lower-order risks.



congestion also could have implied the high likelihood of delays and the need to hold more inventory in the U.K. to guarantee on-time deliveries.

Systemwide changes that are likely to have permanent effects are typically caused by noticeable megatrends, such as technological breakthroughs, changes in consumer demand patterns, global events, or regulatory body interventions. Once these trends are on a company's radar, they can be tracked and rapidly interpreted (if the necessary observation and modeling capabilities are in place). For instance, the European Union's carbon border tax, which was enacted in December 2022 after years of debate, won't be fully implemented until 2026, offering companies several years to reduce the uncertainty arising from it.

Further, for potential events that may be infrequent yet high impact, businesses can examine other industries where the consequences of similar events might be better recognized; then they can interpret the implications for their own value exchange system. For example, Brexit strategists could have studied cross-border trade between the U.S. and Canada and the U.S. and Mexico in the automobile and white goods sectors to help them navigate looming free-trade agreements and border regulations.

The active identification of plausible risk events and their potential consequences are the kinds of actions that contribute to building true risk intelligence. However, our research indicates that companies place little emphasis on discovering unknown and plausible risk events and their outcomes and instead focus attention on managing known risks.

We also find that companies do not have a similarly complete knowledge of risks, even when those risks are publicly disclosed by direct competitors. Our study of 10-Ks revealed significant variation in the acknowledgement of risk factors, even among companies in the same industry. For instance, there was a lag of as much as eight years in acknowledging cyber risks after the first public data breach within a group of 18 comparable companies in the financial sector. This pattern was consistent in four additional sectors — including retail, telecom, technology, and health care.

Moreover, our analyses revealed only marginal levels of acknowledgement of causal relationships between risk factors, which are how risks impact companies in the real world. It is only logical that a known or unknown risk factor, when manifested, would likely influence other linked known and unknown risk factors, thereby creating a cascade of consequences. This ultimately would affect a company in potentially known but unexpected (or, worse, misunderstood) ways.

While most companies think they are preparing for risk events, they tend to focus only on level 1 and 2 uncertainty and therefore develop highly specific but narrow mitigation plans. Take Maersk, for example, which in 2017 fell victim to a ransomware cyberattack that brought down its entire network for days and halted

its operations at 76 port terminals globally at a cost of roughly $300 million.[10] Yet the shipping company did not publicly acknowledge the risk of a cyberattack until its 2013 annual report, despite the risk of hacking and other cyberthreats having been well known since the late 1990s (although perhaps not seriously regarded as a primary risk for shippers). Thus, few risks are entirely unknown, and industry-specific unknowns may not be unknowns in other sectors.

Construct and Contextualize an Enterprise Risk Network

To gain clearer insight into level 3 and 4 uncertainty, it is important to understand the linkages among enterprise risks. Developing quantified risk networks (QRNs) can help. A QRN is a weighted map that links all identified potential risks to a company's value exchange system functions and helps decision makers interpret related impacts. Moreover, QRNs can reveal counterintuitive insights, such as a function's indirect exposure to risks typically associated with a different but connected function. For example, the risk of inaccurately forecasting shipping demand in a freight company directly affects its operating expense management function and indirectly affects facility capacity, operational capability, and customer concessions, as well as the company's reputation.

Companies should build their own risk networks for three reasons. First, each company has its own unique value exchange system that is best understood by its leaders. Second, resilient companies need to build in redundancies, which is challenging to do in resource-constrained environments. Custom QRNs highlight the most connected — and most vulnerable — value functions, creating an order of priority for allocating resources to bolster the enterprise. Third, custom QRNs provide a shared picture of risk for company leaders, who may or may not agree on critical vulnerabilities. The QRN-building activity focuses managerial attention on the often disregarded but potentially crucial functions and related risk categories to ultimately help leaders anticipate and prepare for the future.

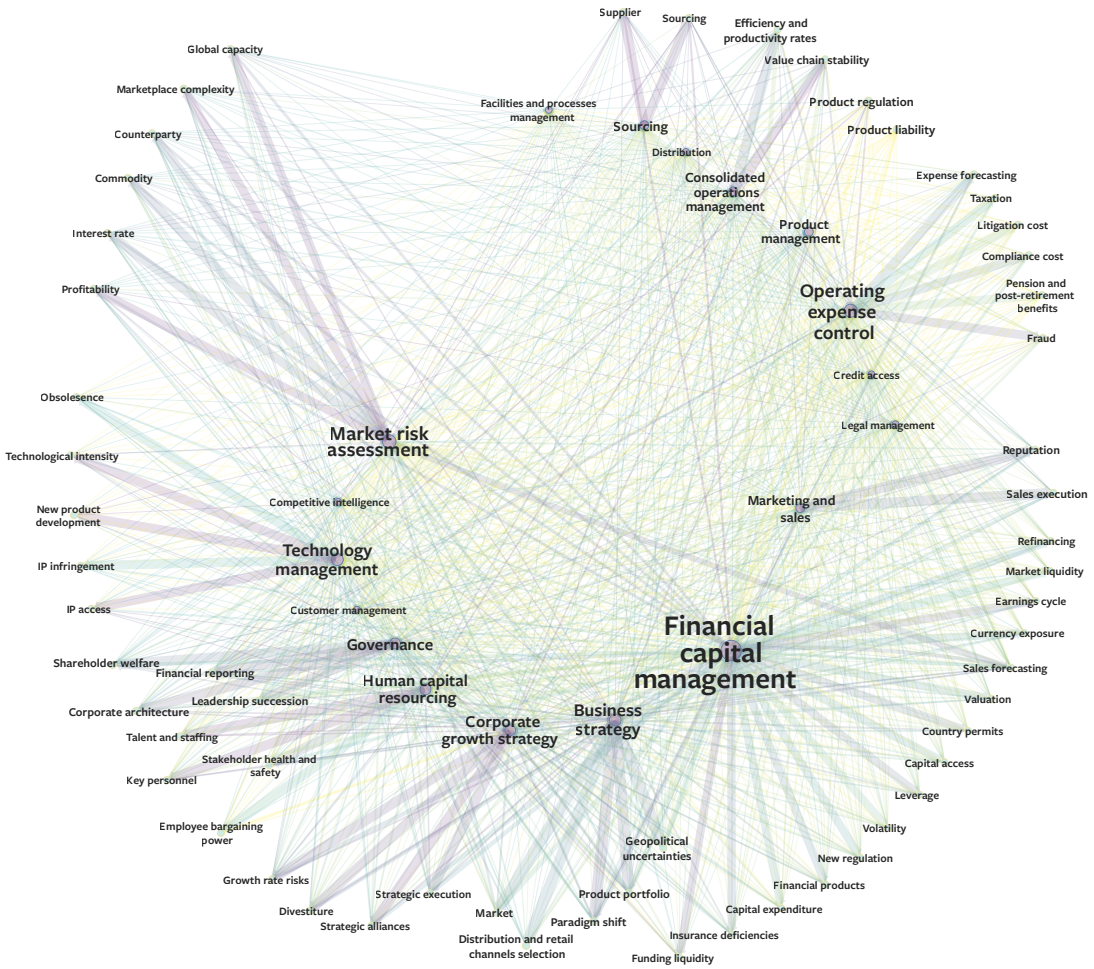
To gain clearer insight into level 3 and 4 uncertainty, it's important that leaders understand the linkages among enterprise risks.

To begin constructing your company's risk network, identify the risk events that are particularly relevant to your business by working from critical value functions upon which it relies (the orange and red nodes in "A Value Function Risk Inventory") and from the risk categories captured in the inventory (the yellow nodes). Identify plausible risk events in each category from data sources such as company memos, public risk disclosures, investment analyst reports, and historical knowledge. For example, leaders managing the operations function can use inventory risk categories, such as facilities and process management, sourcing, and distribution, to build a list of plausible risk factors or events (such as an unexpected storm, an equipment malfunction, input shortages, drained emergency supplies, worker health emergencies, communications interruptions, or labor strikes) that could affect business continuity. Note that these lists will likely contain several risk factors under each risk category.

Next, characterize relevant risks using the SPF framework, identify plausible scenarios related to the company's value functions, and identify potential responses. This exercise gives managers the opportunity to pay extra attention to less appreciated risks and helps them reduce the overall level of uncertainty of the impact of risks on the company's value exchange system.

Since the archetypal company is organized by function, the consequences of potential risks on individual functions (such as a labor strike's effect on sourcing) and the interconnectivity between different value functions themselves should be estimated for each functional node in the QRN. For instance, once managers define the level of interconnectivity between the sourcing and operations functions in their company, they can deduce the direct consequences of a labor strike for sourcing and its indirect consequences for operations. Weighting impacts, even using relative terms such as high, medium, and low, provides a common language for managers to discuss significant risks and plausible scenarios and can help resolve debate on what is likely or what is important. Functions identified as particularly important or vulnerable should be analyzed by experts to develop a deeper understanding of the risks affecting them and their interconnectivity.

We created a generic QRN, beginning by asking leaders with sector and functional expertise to indicate interconnectivity between their function and other business functions on a 10-point scale. (See "A Quantitative Risk Network.") Then we asked the leaders to indicate the potential impact of specific risks to their functional area arising from these connections. For example, a sales and marketing expert who indicated significant



A Quantitative Risk Network

This visual representation of a generic QRN reveals the linkages between risk categories and enterprise functions. It illustrates how companies can isolate and identify key value functions that link several connected risks and are therefore particularly significant in building enterprise resilience. The more central the function, the larger its font size; the thick links in the QRN imply high-impact relationships between functions and risk categories.

interconnectivity with the business strategy function was asked whether sales forecasting risks, sales execution risks, and reputation risks would have a high, medium, or low impact on business strategy. Companies can follow this process to build a codified understanding by leveraging their internal leaders as well as external experts. Once coded, the data forms the basis for a network representation of risks and a company-specific QRN.

Such a QRN helps leaders better understand a company's vulnerability to risk events by illuminating those functions that are central to the value exchange system. A risk event affecting a central function would imply a strong cascade of negative effects across the company's value exchange system. For example, financial capital management connects directly to 15 financial risk categories and indirectly to 30 risk categories from other functions. Any event occurring in any one of the risk categories affecting financial capital management will have implications for all other connected functions; for instance, significant currency exposure will likely affect the company's sourcing decisions. Thus, protecting the financial capital management function is critical to resilience. In contrast, a negative effect on the marketing and

sales function is unlikely to cause a cascading impact in this company.[11]

Expert knowledge, industry insights, experience, and the simulations are all useful in building a network view of enterprise risks. QRNs are baseline resources that help a company isolate and objectively model for worst-case scenarios, estimate cause-effect patterns, and effectively reduce level 3 and 4 uncertainty.

A company with a well-honed QRN will be able to differentiate between the scope and consequences of a business interruption due to, say, a pandemic and a transport route blockage. It will also be able to pinpoint the parts of the business that will likely experience significant consequences from these events, such as value delivery, value creation, and value protection, and identify the precise business functions that should be guarded for each of these events. In the case of the pandemic, these functions would include financial capital management, market risk assessment, and technology management; for the lower-scope blockage, these would include operations management and operating expense control. Furthermore, the company could use the value function risk inventory and build scenario models for risk events identified within each of these functions.

Ultimately, pairing the knowledge of plausible risk events and their likely interactions with the company's value functions enables strategists to develop tailored mitigation plans and response strategies. Leaders who recognize the need to better understand a specific set of scenarios can invest in developing precise models to reduce the uncertainty of their impact on the company.

THE VALUE EXCHANGE SYSTEM THAT DRIVES any large, complex enterprise is continuously challenged as contexts vary in the dynamic business environment. This raises the stakes for anticipating change, exploring new variations of business models, and continuously pursuing the next wave of growth-enabling capabilities. Risk intelligence helps leaders in this work, enabling them to better focus on maintaining continuous value exchange and fostering the adaptability needed to achieve resilience.

To create and nurture risk intelligence, a company needs a central risk management function that is staffed with broad functional expertise and given the resources required to identify and categorize risks. It needs to embrace a mindset of risk uncertainty versus risk avoidance and reduce the levels of uncertainty. It needs a company-specific quantified risk network that is updated in a dynamic manner. And finally, it needs a culture of risk intelligence in which leaders across the organization share a common framework and language for interpreting risks and guiding resource allocation for risk mitigation efforts. Ultimately, honing a risk intelligence capability represents the key to building a resilient enterprise. ■

Ananya Sheth (*@ananyasheth*) *is a postdoctoral research fellow at the Stevens Institute of Technology's Stevens Business School.* **Joseph V. Sinfield** *is a professor of civil engineering and the director of the Institute for Innovation Science at Purdue University.*

REFERENCES

1. A.B. Sheth, "Pathways to Enterprise Resilience" (Ph.D. diss., Purdue University Graduate School and the Lyles School of Civil Engineering, 2021). We define "growth with longevity" as multi-decadal business growth founded on one or more fundamental capabilities that enable the pursuit of multiple new markets across contexts over time.
2. "Risk intelligence" has been defined in various ways. See F. Caldwell, "Risk Intelligence: Applying KM to Information Risk Management," Vine 38, no. 2 (June 2008): 163-166; D. Evans, "Risk Intelligence," in "Handbook of Risk Theory: Epistemology, Decision Theory, Ethics, and Social Implications of Risk," eds. S. Roeser, R. Hillerbrand, P. Sandin, et al. (Dordrecht, Netherlands: Springer, 2012), 603-620; S. Mashingaidze, "Risk Intelligence: How Lessons From Folktales/Fables Contribute to the Implementation of Risk Management in Banks," Risk Governance & Control: Financial Markets & Institutions 5, no. 4 (October 2015): 19-25; D. Wu and J. Birge, "Risk Intelligence in Big Data Era: A Review and Introduction to Special Issue," IEEE Transactions on Cybernetics 46, no. 8 (August 2016): 1718-1720; and A. Marshall, U. Ojiako, V. Wang, et al., "Forecasting Unknown-Unknowns by Boosting the Risk Radar Within the Risk Intelligent Organisation," International Journal of Forecasting 35, no. 2 (April-June, 2019): 644-658.
3. J. Liu, T. Tong, and J. Sinfield, "Toward a Resilient Complex Adaptive System View of Business Models," Long Range Planning 54, no. 3 (June 2021): article 102030.
4. Y. Sheffi, "What Everyone Gets Wrong About the Never-Ending COVID-19 Supply Chain Crises," MIT Sloan Management Review 63, no. 2 (winter 2022): 7-10.
5. A. Griffiths and M. Winn, "Slack and Sustainability" (presentation at the Academy of Management Annual Meeting, Honolulu, Hawaii, August 2005).
6. M.K. Linnenluecke, A. Griffiths, and M. Winn, "Extreme Weather Events and the Critical Importance of Anticipatory Adaptation and Organizational Resilience in Responding to Impacts," Business Strategy and the Environment 21, no. 1 (January 2012): 17-32.
7. A. Sheth and A. Kusiak, "Resiliency of Smart Manufacturing Enterprises via Information Integration," Journal of Industrial Information Integration 28 (July 2022): article 100370.
8. "Decision-Making Under Deep Uncertainty: From Theory to Practice," eds. V.A.W.J. Marchau, W.E. Walker, P.J.T.M. Bloemen, et al. (Cham, Switzerland: Springer, 2019); and H. Courtney, J. Kirkland, and P. Viguerie, "Strategy Under Uncertainty," Harvard Business Review 75, no. 6 (November-December 1997): 67-79.
9. M. Shelbourne, "Pentagon Said It Was Ready for Extended Suez Canal Blockage," USNI News, March 29, 2021, https://news.usni.org.
10. J. Leovy, "Cyberattack Cost Maersk as Much as $300 Million and Disrupted Operations for 2 Weeks," Los Angeles Times, Aug. 17, 2017, www.latimes.com.
11. To identify pairs that are important to the risk network, we chose pairs that experts deemed as having 40% or more risk impact. In practice, however, this value should be selected based on qualitative criteria, such as the risk positioning of the company and industry.
i. The opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

Reprint 64408. For ordering information, see page 4.