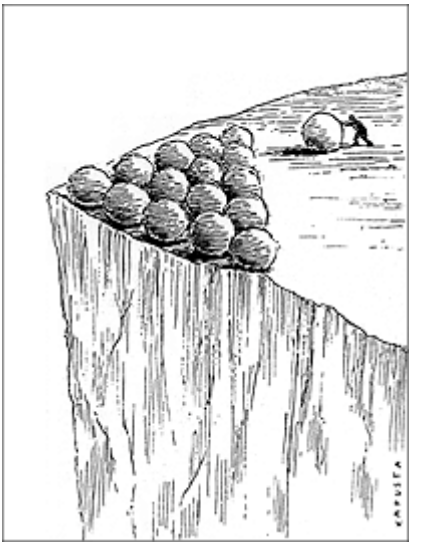
MMC Views



Operating Risk Goes Systemic

by L. Ware Preston III

L. Ware Preston III is a vice president of J&H Marsh & McLennan. He is based in New York.

Technological advances and innovative business models are driving an across-the-board transformation in the way companies operate. From the tangible benefits of such strategies as just-in-time inventory management, outsourcing and consolidation of manufacturing capacity, to the exciting potential offered by the growth of electronic commerce, these developments are helping firms reduce costs, increase productivity, improve quality and speed product to market. They are enhancing established capabilities and adding important new ones. The resulting strategies go beyond improving the bottom line: many help minimize common risks that imperil health and safety, destroy property or even simply create personal inconvenience.

These developments are also shaping a more interdependent economy—one that is more reliant on systems and information flow. More interdependence can improve efficiency, but in some cases it translates into less business diversity. As a result, when something goes wrong in one sector, the repercussions are more likely to be widespread, affecting a large number of entities. The same innovative developments that are growing the economy can end up compounding errors exponentially for an individual company.

Creating and sustaining shareholder value will depend increasingly on a company's ability to take more systemic operating risk *and* manage it better than the competition. Managing this particular brand of risk will likely become one of the defining business challenges as we move into the next century.

Systemic Operating Events

Systemic events are hardly new; history is rife with calamities ranging from wars to epidemics to economic collapses to natural disasters. The difference today is that in addition to the long established systemic events, new events whose causes are more closely related to how companies and consumers behave are occurring more frequently.

A common pattern has emerged: Competitive pressure to add value, and to gain competitive advantage through new business models and technology, is intensifying. The rewards, which are often immediate and sizable, mask the increase in systemic operating risk. When something goes wrong, the resulting damage can be surprisingly widespread and long-lasting.

Consider the following examples:

- Antibiotics have saved millions of lives, but their over-prescription has spurred the evolution of drug-resistant bacteria, such as *Staphylococcus Aureus,* posing a worldwide health risk.

- Toll-free numbers have been a hugely successful means of enhancing services to customers. The value of information flowing through telecommunication systems that serve 800 numbers at peak times is enormous. But even with redundancies and alternative routing, service interruptions occur and wreak widespread havoc, if only for a short time.

- Feeding waste animal protein to cattle was viewed as an economical way to increase growth rates and lower the cost of beef. But the discovery that it can transmit the agent that causes so-called "Mad Cow" disease to healthy cattle (and, in a modified form, to people) nearly destroyed the market for British beef and has placed beef under consumer suspicion and regulatory scrutiny worldwide.

- Saving precious memory space in early computers by providing only two-digit fields for the year in dates saved hundreds of millions of dollars. The result today is the "Year 2000" bug. Billions of dollars are being spent to fix the problem. Nonetheless, because many computer networks link companies with suppliers and customers in long value-added chains, failures may cause widespread disruption. Of greater concern is the possibility that a universal misunderstanding of the problem yields a series of flawed solutions.

Futuristic Scenarios

These occurrences may, in fact, be harbingers of far more problematic challenges. As technology becomes more sophisticated and as business models become more radical, the resulting developments should bring unprecedented benefits. But the potential for damage will likewise be unprecedented. The following examples might have sounded somewhat far-fetched a few years ago, but today they must be taken seriously:

- Data mining. Imagine a future in which all data is digital, all databases are correlated and updated in real time and search engines equipped with powerful decryption capabilities are (covertly or openly) continuously at work. Getting the right information to the right place at the right time is of immense value. The more data being transferred, the greater the risk of breach of privacy. Digitized data magnifies the power of information—and thus the potential for abuse.

- Genetic engineering. In the future, various plants and animals may be engineered to possess a number of highly desirable traits. But there are hidden dangers: Suppose that a cloned plant or animal carries a seemingly inconsequential trait that in fact renders its future generation clones indefensible against some previously unknown pathogen. Narrowing biodiversity may have many such unintended consequences.

- Smart transportation. Planes, trains and ships may someday be guided by computerized instructions instead of by people. This will likely mean less congestion, greater speed, better use of space and reduced opportunities for human error. Decisions will be made by sophisticated sensors, elaborate communication systems, satellite positioning, fuzzy logic, networked computers and complex software. But significant risks could stem from sabotage, design errors or even a simple malfunction in a minor component. The results are unpredictable, but it is safe to say that chaos could easily ensue, with results ranging from general schedule disruption to serious injuries.

- Entertainment. As communication systems become more sophisticated, all forms of audiovisual entertainment may be routinely rented

through use of a micro-payment system over the Internet. The benefits are revolutionary; choice becomes unlimited and consumers get what they want when they want it. The frictional cost of delivering or obtaining content of this type drops dramatically because physical movement is not necessary. Ideally, what is transported is merely a digital representation of the content. Personal ownership of physical copies becomes obsolete because payment for use is cheaper and more convenient than ownership. But when the micro-payment system malfunctions, or the source of digital representations of content is unresponsive, or the Internet connection is interrupted, unlimited choice quickly changes to no choice. Not being able to download one's favorite music is not life-threatening—but a small malfunction can potentially wreak havoc across a broad range of electronic commerce.

Managing Systemic Operating Risk

The potential for damage from systemic operating events has not gone unnoticed by business. Enterprises are beginning to recognize that risk is increasing and that this risk cuts across organizational boundaries and business processes. Managers are seeing that systemic operating risk at once creates value and threatens survival. Some are reaching the conclusion that effective management of systemic operating risk in fact requires a more systemic approach to risk management—one involving all elements of the enterprise acting jointly to harness the power of different perspectives through alignment with a common sense of purpose.

Taking a more systemic approach to risk management calls for a number of changes in strategic, organizational, operational and financial responses to risk. Above all, it calls for greater coordination of these responses.

Strategic

Building shareholder value—and attracting the requisite financial and intellectual capital to build it—requires companies to be at or near the forefront of innovation. This places companies in increasingly complex strategic webs (both internal and external) defined by business relationships, networked systems, value chains and information flow. When detrimental events occur, large portions of these webs will probably be affected, with serious consequences for individual companies and those with whom they conduct business.

For example, decisions about dealing with various customers and suppliers—in particular, which operating strategies to adopt with each—should be supported by analysis across the entire company that measures the relationship between earnings potential and systemic operating risk. It is important to recognize the point at which further strategic investments in new means of operating are actually outweighed by the accompanying potential for systemic operating risk.

Risk and reward analysis may point to a need to diversify systemic operating risk through multiple operating strategies and additional customer/supplier relationships. Close analysis will reveal that what appears on the surface to be a few massively complex operating webs are actually a large number of smaller webs, some independent of each other and some highly correlated (both positively and negatively). Companies performing this sort of analysis will have the opportunity to manage exposure to systemic operating risk strategically, by searching out positions on a portfolio of operating webs.

In addition, business continuity planning and crisis management, usually thought of as operational responses to risk, will need to assume a more strategic role. Taking systemic operating risk creates franchise value but a systemic operating event may destroy it; hence, the likelihood of recovery from a systemic operating event should become a critical factor in the strategic decision-making process.

In some cases, competitor analysis will take account of

vulnerabilities to systemic operating risk and likely reaction to systemic events with an eye toward capitalizing on others' misfortunes.

Organizational

As most organizations have developed, the risk management function (driven by the benefits of specialization) has sorted itself into "silos" according to type of risk. In many cases, these silos have hardened, making it more likely that systemic operating risk (which may span several silos) is unidentified. The solution is an organizational structure for risk management that preserves the benefits of specialization where this is important, but that also transcends organizational boundaries.

Balancing these competing objectives should lead to reorganization of the risk management function. Radical reorganization may be in order for those companies particularly driven by innovation. For others, the reorganization may be subtle, leaving many silos intact but with more permeable walls. No matter what shape this reorganization of risk management takes, a number of common characteristics are likely to be evident.

The responsibility for assessment of systemic operating risk will reside at a senior position independent of business unit leaders. Objectivity is critical. From this position, both internal and external data related to systemic risk will be collected and analyzed on as close to a real-time basis as possible. The analysis will flow up as input to strategic decisions and down to business units in the form of directives to make tactical adjustments in exposure to systemic operating risk and in operational responses to risk.

Continuous analysis of systemic risk will flow to a centralized finance unit with responsibility for financing risk throughout the enterprise. This unit will factor analysis of systemic operating risk into decisions on capital structure, allocation of capital to business units and entering into transactions with counter-parties as a means of hedging systemic operating exposures. Many companies may find it necessary to form a different vehicle, such as a new generation of captive insurer, that is dedicated to financial intermediation of systemic operating risk.

Operational responses to risk, such as prevention, mitigation and recovery measures, will continue to require specific expertise and thus are likely to remain in silos (although they will communicate freely on best practices and lessons learned in a commonly understood language of risk). Aided by the development of a common risk language, management of systemic operating risk will become part of corporate culture.

Operational

Non-systemic operating events (e.g., fires, liability claims, customer complaints) occur frequently, allowing refinement of operational responses through trial and error. No such luxury exists for making adjustments to measures for preventing, mitigating or recovering from systemic operating events. Often there is no such thing as a second chance.

Consequently, scenarios must substitute for history in planning operational measures for managing systemic operating events. Because even the most complete scenarios may not reflect the reality of an actual event as it unfolds, plans must be flexible. Companies must exercise good judgment, not rote reaction. In some cases, simply letting the event run its course may be the most prudent response.

Given this perspective, in an attempt to prevent, mitigate and recover from systemic operating events, enterprises will need to:

- Commit significant resources to development of systemic

operating risk scenarios.

- Perform simulations as a means of testing plans and training those responsible for responding to systemic events.

- Analyze all systemic events for relevance to their operations.

- Identify all failure points that may lead to a systemic event and take preventive measures.

- Search for ways to isolate potential failures so that they do not lead to systemic events.

- Form pacts with other enterprises to coordinate efforts to reduce systemic damage.

- Capitalize on investments in management of systemic operating risk by communicating the value of these investments to customers, suppliers, employees and investors.

Financial

The financial response to non-systemic operating risk is typically a combination of self-insurance insurance and planned and/or ad hoc assumption of risk at the business unit or corporate level. With the exception of taking an ad hoc approach (which may not be prudent when dealing with particularly severe problems) these financial responses also apply to systemic operating risk. However, the primary financial response, and the point of reference for considering other financial responses, should be the enterprise's own capital structure.

As the level of systemic operating risk increases, companies will need to adjust their capital structures to support recovery from a systemic event while maintaining the capacity to continue making investments in value-enhancing opportunities. In many cases, this means that more capital and greater liquidity must come from investors whose risk and reward preferences include exposure to systemic operating risk. Moreover, for purposes of measuring performance, companies will need to allocate capital internally on the basis of exposure to systemic operating risk just as some do now for exposure to market and credit risk.

As enterprises begin to restructure and allocate capital in relation to systemic operating risk (thus gaining an appreciation of the cost of capital needed to support this risk), they will look externally for counter-parties with whom they can trade this risk. At times, these enterprises will find themselves in a position where exposure to systemic operating risk exceeds their ability to obtain additional capital. Also, they will undoubtedly find (as they do now for market and credit risk) that their perspective on systemic operating risk may change faster than their ability to make strategic, organizational or operational adjustments. Both of these situations will spur the demand for counter-parties to take on some of the risk—a demand met by firms that have a different perspective on systemic operating risk or that are better able to diversify a particular risk element.

Coordinating Responses

As important as it may be to make changes to strategic, organizational, operational and financial responses to risk, the changes alone are unlikely to be sufficient. Successfully managing systemic operating risk requires coordinating these responses. Coordination implies a need for a set of metrics for risk and a language for risk management understood throughout the enterprise. This is essential for managing risk that overlaps organizational boundaries (and thus becomes subject to numerous perspectives). Without a common understanding across the board, systemic operating risk management is only as

strong as the weakest response.

Opportunities

The emergence of systemic operating risk and the high value to be gained from managing it effectively present a number of opportunities for firms and professionals that help others manage risk. Conversely, it may threaten firms that miss out on the potential opportunities.

Probably the most challenging opportunity—itself a foundation for the other opportunities—is to provide information and analytical techniques that can help companies assess exposure to systemic operating risk. In many cases, the data exists but has not been put in a format that is easily usable. Designing and implementing systems to collect this data and turn it into useful information presents an enormous stand-alone opportunity.

As a further step, this information may then be used as input to elaborate models of how companies operate and relate to customers and suppliers. These models can be used to generate systemic risk scenarios as input to decisions on how to respond. Another important service can be to provide technical solutions that help prevent or mitigate the importance of a systemic operating event. Examples of these solutions include encryption, backup systems, Internet surveillance agents and early warning systems of an imminent systemic event.

In the area of financial intermediation, we can identify several major opportunities. One is to provide guaranteed access to capital needed to recover from a systemic operating event. A guarantee is important because systemic operating events tend to exert a negative influence on capital providers' perception of the affected company's performance. Another opportunity is to offer insurance, warranty or financial guarantee products that are responsive to the risk. This is possible because systemic operating risk, like windstorm and earthquake risk, can be diversified once understood. In some circumstances, the signal broadcast by the very existence of insurance or a guarantee may be its greatest value.

Still another opportunity is to facilitate trading of systemic operating risk by acting as a counter-party that assumes systemic operating risk through a variety of transactions, strips out the actual risk and parcels it for distribution to others better equipped to handle it. Yet another is to factor systemic operating risk analysis into asset management and investment advisory services. This is particularly important when assets are linked to obligations affected by systemic operating risk or when a systemic operating event is likely to influence, positively or negatively, each member of an asset class or a number of different asset classes.

Finally, there is an opportunity to provide management consulting that explicitly includes advice on strategic and organizational responses to systemic operating risk. In fact, this may be an imperative given the link between business strategy and systemic operating risk. Enterprises will need access to the body of knowledge possessed only by professional service firms that serve a diverse set of clients with exposure to a large variety of systemic operating risks.

A More Measured Approach

The growing importance of new business models and technological innovations constantly redefine how companies operate. These are important factors that can add considerable value to many segments of the economy. With the opportunities come challenges in the form of systemic operating risk. While systemic operating risk may occur less frequently than non-systemic risk (such as liability claims), they are often more severe. More important, because this risk stems in part from a growing interdependence among businesses, when something goes wrong the impact is transmitted to a large number of otherwise independent exposure units—simultaneously, by chain

reaction, or a combination of both.

Managing systemic operating risk requires a more measured approach to risk management involving coordination among strategic, organizational, operational and financial responses to risk. Systemic operating risk presents a major opportunity for firms and professionals in the risk management business—but they need to understand both the challenges and the complexity of the relevant issues.

Viewpoint, Winter 1998-99

Back to Top | MMC Views home page