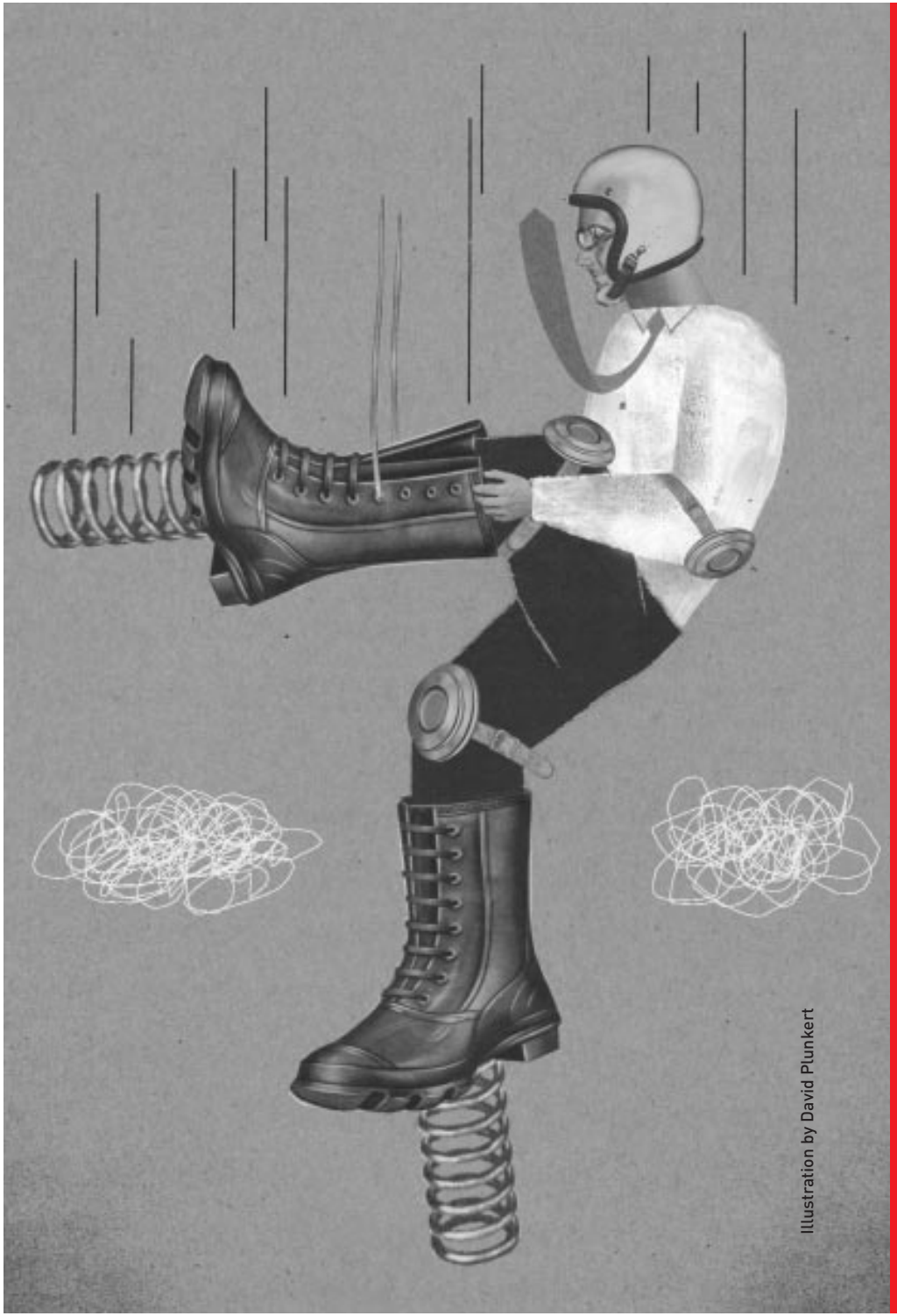


Illustration by David Plunkert

Enterprise Resilience: Managing Risk in the Networked Economy

Enterprise Resilience: Managing Risk in the Networked Economy

by Randy Starr, Jim Newfrock, and Michael Delurey

Two companies; same crisis; vastly different responses and outcomes.

A Nordic telecommunications company and its primary competitor, another European telecom manufacturer, both depended on the same Koninklijke Philips Electronics NV semiconductor plant in New Mexico for chips to power their mobile phones. But when a fire broke out at the factory in March 2000, the supply chain was disrupted.

The Nordic company's officials noticed the problem even before being told that a plant had gone down. Its chief supply troubleshooter immediately put together a team of 30 supply chain experts to fan out across Europe, Asia, and the U.S. to patch together a solution. They redesigned chips, accelerated a project to boost production, and used the company's clout to obtain more chips from other suppliers. The other company, with fewer fail-safe and troubleshooting systems built into its supply network, came up millions of chips short of the supply needed to launch a critical new product.

The result, according to the *Wall Street Journal*: The Nordic company's market share grew by 3 percent; the competitor's dropped by the same amount. Before long, the other company withdrew from the handset market.

This stark tale of gain and loss underscores a new operating reality confronting companies everywhere: Drivers of earnings, definitions of risk, underlying risk interdependencies, and ways to manage them have changed. Firms generally have thought of risk as the downside hazard to their financial portfolios and have concentrated their risk management efforts on hedging their portfolios against loss. But the Nordic company's success in weathering a potentially debilitating disruption to its supply chain, and ultimately gaining competitive advantage from its efforts, shows that companies can profit by adopting a broader understanding of and more comprehensive processes for managing risk across the extended enterprise in an increasingly complex global economy. In doing so, they establish greater enterprise resilience (ER).

In this article, we detail the differences between conventional enterprise risk management and enterprise resilience, and explain why a keen understanding of the distinction is essential today, when the boundaries of every major corporation have expanded, increasing a company's vulnerabilities and its potential for competitive advantage. We also identify how senior executives can assess their organization's resilience profile and risk management approach. And we explain how corporate managers can align risk mitigation strategies with the most significant earnings-driver risks, and close dangerous gaps in their company's resilience profile.

The Adaptation Imperative

Enterprise resilience is the ability and capacity to withstand systemic discontinuities and adapt to new risk environments. A resilient organization effectively aligns its strategy, operations, management systems, governance structure, and decision-support capabilities so that it can uncover and adjust to continually changing risks, endure disruptions to its primary earnings drivers, and create advantages over less adaptive competitors.

A resilient organization establishes transparency and puts in place controls for CEOs and boards to address risks across the extended enterprise. It can withstand improper or fraudulent employee behavior, IT infrastructure failures, disruptions of interdependent supply chains or customer channels, intellectual property theft, adverse economic conditions across markets, and the myriad other discontinuities companies face today.

Establishing greater resilience is especially necessary in the current economic and security environment, which poses a new set of challenges to executives and boards. The openness and complexity of today's extended enterprise increases the firm's dependence on a global financial, operational, and trade infrastructure. Although that provides for greater efficiency and effectiveness, it also exposes most companies to risks that were unfamiliar during the era of national markets and the vertically integrated enterprise — and compounds the effect of conventional business risks.

What's more, the legal and regulatory landscape has undergone significant change since the September 11, 2001, terrorist attacks and the accounting and governance scandals in the United States, raising the level of diligence stakeholders expect from senior executives, boards of directors, and board audit committees in ensuring the safety and continuity of the enterprise. The July 2002 United States' National Strategy for Homeland Security recommends that industry sectors and corresponding government agencies responsible for critical infrastructure protection develop national infra-

structure assurance plans that bridge the public and private sectors. The Sarbanes-Oxley Act of 2002 has tightened boards of directors' audit committee responsibilities, imposed new CEO and CFO certification requirements, and raised the "standard of care" obligations on management dramatically. The Basel II Accord commits financial-services institutions to set aside larger capital reserves against possible future operational disruptions.

Guided by these and other requirements, underwriters of risk, such as insurance, equity, and debt markets, will more aggressively distinguish between those businesses that are resilient and those that are not. To maintain earnings consistency and preserve and grow shareholder value, chief executives and board members need the capacity to sense and respond effectively to increasingly complicated levels of risk — risks that cannot necessarily be transferred through conventional means, such as insurance.

Interdependence Risk

Our emphasis on the importance of earnings consistency matches that of the capital markets. A company's fate is determined by its ability to generate a reliable pattern of earnings growth. Companies that reduce earnings volatility and lower the probability of large losses are rewarded by financial markets with less expensive and better access to capital. What's more, markets place "consistency premiums" on the stock valuations of companies that both promise and produce a steady pattern of increasing profits.

The business activities that enable the firm to gain a competitive advantage and sustain growth vary across both industries and companies. For some, manufacturing facilities represent the core earnings driver; for others, IT networks, customer support operations, supply chains, intellectual property, or a combination thereof power earnings. Traditionally, risks have not been perceived in the context of key earnings drivers, but rather in broad categories, each of which was managed in a functionally isolated way. Thus, financial risk became the province of the CFO, operations risk the responsibility of the COO, and network security the task of the CIO. Rarely do they or their business continuity or security programs link together in support of strategic objectives.

Senior executives have understandably renewed their attention to conventional risk mitigation programs. Seventy-five percent of Fortune 1000 CEOs surveyed by RoperASW on behalf of Booz Allen Hamilton in late 2001 expressed increased concern about such day-to-day activities as mail processing, travel, protection of employees, and protection of infrastructure. But by defining risk and security narrowly as the protection of personnel, plant, data, and financial position, CEOs and boards overlook the more prevalent perils they face conducting business in a networked global economy.

Diagnose Your Enterprise Resilience: Eight Fundamental Questions

Are the complexity of the extended enterprise and major earnings drivers across it transparent?

Are interdependencies understood and interdependence risks identified?

What programs are in place to ensure the viability of earnings drivers?

Are these programs fully aligned with corporate strategy and objectives, and do we understand the trade-offs within these programs?

Do we know what we spend on resilience?

How good is our situational awareness — that is, do we have enough business intelligence, internal and external, and is it directed to the appropriate parties?

Do we distill such intelligence properly and in a timely enough fashion to react to it?

Who is accountable for resilience, and how do we make decisions and measure progress?

Networks are one of the great advances in industrial organization. Over the course of the last half century, the vertically integrated company has given way to the networked enterprise, an organizational structure characterized by greater agility and adaptability. Successful firms today must deal with intertwined layers of information, raw materials, analytical data, customer communication and service, and network infrastructure — at unprecedented speed — while maintaining countless secure relationships with third-party organizations, such as suppliers, technology outsourcers, and government regulators. "The diversity of networks in business and the economy is mind-boggling," writes Albert-László Barabási, the physicist and author of *Linked: The New Science of Networks* (Perseus Publishing, 2002). "There are policy networks, ownership networks, collaboration networks, organizational networks, network marketing — you name it."

Yet while the organizational and economic impact of networks is well known, their vulnerabilities remain largely unexplored by businesses. The reliance on open borders, transnational alliances, and global markets for capital, goods, and services has generated a "just in time" economy, which, although remarkably cost-efficient, leaves companies open to a range of discontinuities that can affect operations, reputation,

customer habits, legal standing, regulatory compliance, earnings performance, and ultimately shareholder value. We call these new vulnerabilities, collectively, interdependence risk, and define it as unanticipated risk exposure across the extended enterprise that is beyond an individual organization's direct control. Examples of interdependence risk include supply chain disruption, government intervention, and public infrastructure destruction.

The scale and impact of a disruptive event is a function of the relative importance of the dislocated entity and the degree of its integration into a broader extended enterprise. A problem that appears localized could ripple across an extended enterprise, an industry sector, or even a national or multinational economy. The capacity to withstand such disruptions is a function of a firm's systemic resilience — its ability to understand its interdependencies, and to foresee and plan around discontinuities that can occur within them.

Interdependencies have grown not only within the private sector. Governments and industries are increasingly dependent on each other at a level of intricacy not seen — in the United States, at least — since World War II. The National Strategy for Homeland Security calls for the development of protection plans in 14 "critical infrastructure sectors" (such as energy, telecommunications, defense industrial base, and banking and finance); although private industry overwhelmingly owns and operates these sectors, government and business must collaborate to develop and implement the assurance plans. One current public–private sector partnership model is the National Security Telecommunications Advisory Committee (NSTAC), which supports the Office of the President in addressing telecommunications issues vital to U.S. national security and emergency preparedness needs. The stakes in such collaboration can be enormous. A war game, cosponsored by Booz Allen with the Council for Excellence in Government in December 2001, and designed to model the effects of an intentional release of pneumonic plague in multiple metropolitan locations, found that casualties would be dramatically reduced by cross-sector knowledge-sharing mechanisms. (For more on the war game, see "Bioterrorism: Improving Preparedness and Response," page 135.)

Interdependence risk — within the private sector or across the public and private spheres — underlies many recent reports of operating loss. Consider what happened in September 2002 when a labor dispute shut down West Coast ports for several weeks. As critical supply chains stopped functioning normally, severely constraining manufacturing and product replenishment, U.S. companies lost an estimated $1 billion per day. The events highlighted the interdependencies among shipping companies, supply chain–intensive industries, contract logistics providers, and government agencies.

War-Gaming and Resilience Planning

Frequently conducted in conjunction with an enterprise resilience audit, war-gaming is an effective tool for understanding a company's or an industry's resilience posture. These strategic simulations use mock crises to gauge how well executives and staff are prepared to face serious business discontinuities.

The most effective war games occur over two days and involve a series of crisis simulations in which critical components of a company's or an industry's resilience are tested with players from different, yet related, stakeholder groups. Through a real-time simulation — with one group making a move, and others responding, action by action — vulnerabilities can be exposed and mitigation strategies developed.

For example, Booz Allen Hamilton and the Conference Board sponsored a port security war game in October 2002, just after West Coast ports in the U.S. were shut by a labor action. (See "Port Security War Game: Implications for U.S. Supply Chains," page 143.) Participants included representatives from government agencies, supply chain–intensive industries, and contract logistics providers. The war game simulated an unanticipated closure of shipping ports after several "dirty bombs" were found in containers shipped to U.S. ports. The exercise found that companies reliant on the ports would likely have to sacrifice just-in-time efficiency to some degree, and replace it with a more robust "just-in-case" supply pipeline.

With such insights, companies can attempt to find the necessary balance between just-in-time production and just-in-case resilience, and to answer crucial questions: What would be the effect on earnings if we stockpiled three weeks of supply? Are there innovative ways to create these reserves besides paying for them outright? What loss would insurance cover? What are the projected costs of alternative shipping versus stockpiling? How well do we understand whom to call and what to do during such an event? How prepared are we to communicate mediation steps?

War-gaming's greatest value is that it exposes ideas that participants don't realize they have and uncovers solutions that are not apparent. Additionally, war-gaming forces organizations to think differently, to examine the validity of their assumptions about systemic risks. For example, the port security war game uncovered the critical fact that companies must consider security a strategic and necessary element of global trade resilience. Another insight was that local and national public–private partnerships are essential to finding an effective global port security solution. When war games include participants from interdependent companies or involve a mix of private-sector and public-sector players, consensus can be forged on the need for collective action, and the action plan itself can take shape.

— R.S., J.N., and M.D.

ER vs. ERM

Risk management models have not kept pace with the shift from centralized to networked organizations. In military terminology, most enterprise risk management (ERM) programs rely on "point solutions," which attempt to moderate risks by "hardening" potentially vulnerable spots against attacks, a futile exercise in a networked enterprise. An organization cannot simultaneously harden all the nodes within its network; threats will just migrate from a hardened node to more vulnerable points. Military strategy has long since adapted to this new understanding. In the early 1990s, when the U.S. Department of Defense recognized that its war-fighting doctrine of "information superiority" increased its dependence on networked communications systems, it transitioned from the traditional risk management technique of hardening

every node to a "defense in depth" model, which uses a layered approach to security.

Directors and senior managers, many of whom are faced with analogous challenges, have not followed suit. In a recent survey of Fortune 1000 CFOs, treasurers, and risk managers by the National Association of Corporate Treasurers and other organizations, three-quarters of respondents agreed that a major disruption to their top earnings driver would either cause sustained damage to their company's earnings or threaten business continuity. Yet fewer than one-quarter of respondents said their current risk management efforts sufficiently anticipate a wide variety of potential large-loss events. (See Exhibit 1.)

Exhibit 1: **Enterprises Are Not Prepared to Recover from Major Disruptions**

- More than 75% of respondents say a major disruption to their top earnings driver would either cause sustained damage to their firm's earnings to threaten its continuity of operations.
- Less than 25% or respondents believe their current risk management efforts sufficiently address key areas of contingency planning.
- More than one-third of respondents say their company's senior management lacks a thorough understanding of the impact a major disruption would have on their company and the firm's level of preparation for a major disruption.
- Many senior executives still fail to recognize risk management as a priority.
- Improved communication among key stakeholders about risks and contingency planning is needed.

Source: Protecting Value Study, 2002. A survey of 199 financial executives and risk managers at Fortune 1000 firms in a variety of industries, sponsored by FM Global, the National Association of Corporate Treasurers, and Sherbrooke Partners. www.protectingvalue.com

In pursuing strategic objectives, boards and CEOs must factor into their decision making the trade-offs involved in selecting one risk alternative over another. Conventional ERM programs certainly help focus executives and directors on the nature of specific vulnerabilities, and they can provide partial frameworks to help firms protect potentially weak links from low-probability catastrophic risks. But they do not fully prepare companies for the discontinuities that can jeopardize earnings drivers. Conventional enterprise risk management fails to account for interdependencies across vertical and horizontal corporate operations and thus tends to underestimate the range and severity of risks faced by the firm. Such network discontinuities can accumulate exponentially and often spiral out of control, subjecting a company to levels of loss without modern precedent. So Barings Bank learned when the actions of a single trader in Singapore destroyed the centuries-old institution.

In sharp contrast to traditional ERM, enterprise resilience planning advances a company's speed and flexibility by crafting an integrated first line of defense and an offensive strategy to guard the entire extended enterprise against new, unavoidable risks that are the by-products of interdependent operations. ER results from a planned series of safeguards against discontinuities — encompassing everything from logistics, inventory control, and distribution channels to relations with government agencies, customers, and suppliers. Unlike enterprise risk management programs, which tend to focus only on how major categories of corporate risk interact at a tactical level, ER planning better aligns risk management activity and spending with the most fundamental components of corporate strategy and performance: corporate growth and profit drivers, earnings consistency, and shareholder value. Resilient organizations are sensing, agile, networked, and prepared. They think ahead to even the most outrageous possibilities, training themselves, as the *Harvard Business Review* put it, "how to survive before the fact." (See "Diagnose Your Enterprise Resilience: Eight Fundamental Questions," page 61.)

ER planning begins with the identification of the greatest risks across the enterprise, including interdependencies, and then generates a targeted program, integrated with overall corporate strategy, for mitigating these risks. ER is a continuous process that creates the ability to adjust readily to new risks and opportunities, based on the strategic priorities and operational tempo of the business. It enables executives and managers to make educated trade-off decisions when they develop a risk mitigation strategy, balancing the costs and benefits to meet overall risk management targets and improve earnings consistency.

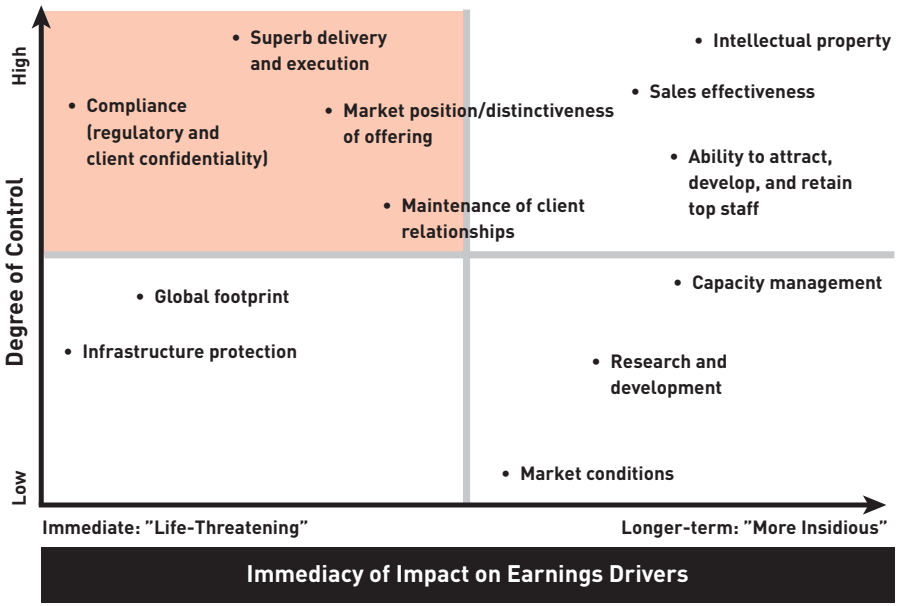
There are three essential steps to becoming a resilient enterprise:

Diagnose enterprise-wide risk and interdependencies. A company must first define its extended enterprise and determine its earnings drivers. Once this is achieved, a transparent and consolidated view of risks across the extended enterprise can be developed, helping executives to understand the company's network interdependencies. After the enterprise is mapped, a baseline view of risk mitigation plans and spending can be developed to identify gaps and prioritize risk mitigation objectives. The resilience diagnostic should yield quick-hit opportunities associated with critical risks that management must address in the near term.

Adapt corporate strategy and operating model. The enterprise should use cost-benefit analysis that links cross-functional risk mitigation planning to corporate strategy. Equally important, the CEO and board must adopt a common risk management and resiliency vocabulary that is comprehensible and intuitive to all, enabling executives and directors to understand a company's risk exposure and to make trade-off decisions in implementing risk mitigation strategies while pursuing strategic objectives.

Endure increased risk and complexity. This step involves developing an organizational structure that oversees and integrates business intelligence and risk monitoring for the extended enterprise; has the analytical tools and support capabilities to improve decision making and responses to risk as it changes; can measure risk mitigation with clearly defined benchmarks; can monitor the organization's resilience pro-

Exhibit 2: **Prioritizing Earnings Drivers—Service Company Example**



file; and can implement best-practice risk mitigation solutions. The resilient organization, through an enhanced sensing capability, integrates business intelligence to improve situational awareness.

The ER Audit

As an initial step to building enterprise resilience, companies can apply a comprehensive, three-phase ER audit procedure that can aid senior management teams in developing integrated risk mitigation programs grounded in a company's real needs and built around its actual earnings drivers.

Step One: Enterprise Topology and Earnings-Driver Classification. In the diagnostic's first stage, the firm should identify its key earnings drivers and their associated risks. (See Exhibit 2.)

This should be done by mapping the extended enterprise and drawing a consolidated and transparent picture of how the company organizes systems, processes, and relationships inside and outside its walls to generate revenue and profits. The company must distinguish the earnings drivers themselves; the business processes, capabilities, and technologies that support them; and their vulnerabilities. To accomplish this, interviews are held with corporate decision makers and key management staff in all functional domains. Relationships among customers, partners, and suppliers are explored; IT network safeguards inventoried; and assets charted.

Step Two: Resilience Profiling and Baselining. After plotting the earnings drivers, the firm should use modeling tools and best practices in enterprise design to produce initial snapshots of an enterprise's "resilience profile" for each essential aspect of a company: financial, operations, technology, personnel, and security. Then the company's existing profile should be compared with an optimal level of resilience — a "to be" state — in each of these operations.

The firm's current risk mitigation plans, procedures, and costs, including business continuity and security programs, are examined in this phase. The intent is to determine how the current programs and the spending on them align with the earnings drivers identified in phase one. Both explicit and implicit risk mitigation spending must be baselined. Such spending includes costs associated with known security, business continuity, and disaster recovery programs, as well as costs associated with security, continuity, and recovery that are buried in budgets for departments or functions, such as IT or marketing. War-gaming is a particularly useful exercise in doing such advanced resilience profiling. (See "War-Gaming and Resilience Planning," page 63.)

A vital part of this phase is the development of an "interdependency map" to identify interdependence risks across the extended enterprise — hazards to earnings drivers that may result from unanticipated regulatory action, changes in supplier relationships, problems at clients, or other externalities. The baselining exercise also seeks to understand how market trends and corporate strategies will influence earnings drivers in the future. For example, a consumer goods manufacturer might discover that the business unit managing logistics between the factory and retailers for the company's flagship Product A is unaware of a new distribution chain developed by the team overseeing up-and-coming Product B. These redundant distribution channels could leave the manufacturer vulnerable because the delivery of two critical products would be interrupted simultaneously if the supply chain network sustained a disruption.

Such profiling and baselining helps identify gaps between existing risk mitigation programs and identifiable needs, allowing management to visualize at a glance weaknesses and strengths in the firm's current risk exposure and resilience posture. This impact analysis can identify areas for new investment and disinvestment. For example, a major retailer with state-of-the-art just-in-time inventory systems that require continual data inflows to determine how to stock shelves could be financially crippled if a disruption were to temporarily shut down its network grid.

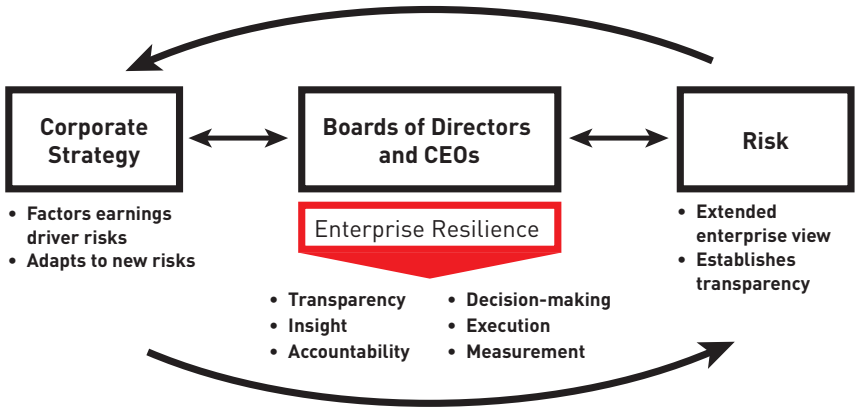
By contrast, even the largest advertising agency could get by without too much damage if it lost its computers for a day or longer. However, an ad agency must pro-

tect the safety of its key personnel because its human assets are its most significant earnings driver. Consequently, during the diagnostic's analysis stage, the to-be resilience state for the retailer would establish that the safeguarding of technology infrastructure is its highest target for investment, and personnel security is a lower investment target; the ad agency might have the opposite resilience profile. This rating does not imply that the retailer has a lower regard for personnel safety; it simply recognizes that the retailer's investments need to be focused on the technology infrastructure because that infrastructure is one of its primary earnings drivers.

Step Three: Resilience Strategy. The final phase of an enterprise resilience audit aims to develop a new resilience program based on the analyses of the firm's earnings-related risk mitigation needs. The most critical gaps between existing risk management programs and the to-be profile are isolated. After the financial commitment needed to close these gaps is determined, a cost-benefit analysis helps rationalize investment needs, finding the optimal balance among components of the risk mitigation effort.

The cost assessment examines business resilience from three perspectives: people, operations (process and technology), and interdependencies. As an example, an established meat products company might learn that, overall, it has well-protected supply and distribution networks, moderate operations risk thanks to mature crisis and disaster management plans, but weak personnel security because its hiring and management procedures at international subsidiaries are inadequate. On the basis of this evaluation, the company could decide to reduce resources earmarked for disaster management and network oversight and redirect them to improve its recruitment, training, and inspection practices. Otherwise, it increases the risk that a devastating incident will occur (e.g., poor inspection practices could allow tainted meat to reach consumers and cause them to become ill).

Exhibit 3: **Corporate Strategy and Risk Integration**



After setting the gap-closing priorities and developing the full risk mitigation strategy, the executive team should agree on a migration path and gain the board's agreement on a timetable for the institution of near-term and longer-term resilience goals. Over time, enhanced business intelligence and information sharing should be developed to promote greater situational awareness.

Risk Is Reality

We believe that companies need to adopt a more integrated approach to risk management — one that links business strategy to enterprise resilience and business continuity planning. Using diagnostic tools, war-gaming, and decision-support capabilities, companies can establish a more effective, continuous, and consistent methodology for protecting the enterprise from internal and external risks.

The establishment of enterprise resilience should involve not only those routinely responsible for risk management and security, such as the CFO, CIO, and chief security officer, but also the CEO, the business unit general managers, the board of directors, and the board's audit committee. With their collaboration, a new risk management approach can be developed to provide a steady stream of information to the organization's top decision makers about the vulnerability of earnings drivers. (See Exhibit 3.) Done this way, ER planning will improve corporate governance and enhance decision making within a company.

Businesses have always faced risks, but recent events have provided dramatic evidence that, in today's economy, risk is reality. Not all risks can be anticipated, but they can be managed, by senior executives, boards, and stakeholders working together to create a resilient enterprise. Stakeholder expectations are higher than ever, and enterprises that are more resilient will experience more rewards — from increased customer and partner loyalty to the realization of premiums for improved earnings consistency. +

Resources

Mark Gerencser and DeAnne Aguirre, "Security Grounds the CEO Agenda," *s+b*, Second Quarter 2002; www.strategy-business.com/press/article/?art=313296&pg=0

Ralph W. Shrader and Mike McConnell, "Security and Strategy in the Age of Discontinuity: A Management Framework for the Post-9/11 World," *s+b*, First Quarter 2002; www.strategy-business.com/press/article/?art=228408&pg=0

Diane L. Coutu, "How Resilience Works," *Harvard Business Review*, May 2002; www.hbsp.harvard.edu

Gary Fields, "An Ominous War Game," *Wall Street Journal*, December 4, 2002