Enterprise Resilience

Transform.

The Resilient Economy: Integrating Competitiveness and Security

Compete.

Council on Competitiveness

The Resilient Economy: Integrating Competitiveness and Security

This publication may not be reproduced, in whole or in part, in any form beyond copying permitted by sections 107 and 108 of the U.S. copyright law and excerpts by reviewers for the public press, without written permission from the publishers.

ISBN 1-889866-33-4

THE COUNCIL ON COMPETITIVENESS is a nonprofit, 501(c) (3) organization as recognized by the U.S. Internal Revenue Service. The Council's activities are funded by contributions from its members, foundations, and project contributions. To learn more about the Council on Competitiveness, visit our home page at www.compete.org.

COPYRIGHT © 2007 Council on Competitiveness

DESIGN Soulellis Studio

Printed in the United States of America

Enterprise Resilience

Transform.

The Resilient Economy: Integrating Competitiveness and Security

Debra van Opstal
Council on Competitiveness

Debra van Opstal is Senior Vice President, Programs and Policy for the Council on Competitiveness.
This paper was developed as part of the Council's work to improve the productivity and resilience of American enterprises.

The Resilient Economy: Integrating Competitiveness and Security

Table of Contents

Letter from the President	4
Acknowledgments	5
In a Nutshell	6
The Competitiveness and Security Conundrum	8
Seeking the Upside of Security: Learning from Five Sectors	15
Warning: Turbulence Ahead	23
Ratcheting Up Resilience: Best Practices Among the Leaders	30
Policy Priorities	39
Appendices	45

Letter from the President

On behalf of the Council on Competitiveness, I am pleased to release *Transform. The Resilient Economy: Integrating Competitiveness and Security.*

The Council relies on the power of ideas, and the power of America's business, academic and labor leaders, to promote the ideas that propel our nation's future productivity, standard of living and security. We believe that Enterprise Resilience is one of these powerful ideas, and one of three cornerstones of economic competitiveness and new value creation: innovation, enterprise resilience and sustainability.

One of the most transformational ideas has been our insight immediately after the tragedy of 9/11 that there must be a business case for security and that, done right, security could become a productivity-driver, not just a sunk cost. Twenty years ago, the Council was at the forefront of a similar business revolution that transformed quality from a "nice to have" into a core business practice—one that became an integral part of productivity growth. We hope to launch a new and transformational dialogue on the value of risk management as a driver of competitiveness, for companies and countries alike.

The Council pioneered this breakthrough approach to risk, competitiveness, and homeland security under the great leadership of project co-chairs Chad Holliday, chairman of the Council and chairman and CEO of DuPont, and Jerry Cohon, Council Executive Committee member and president of Carnegie Mellon University. This work would not have been possible without their executive insights and true enterprisewide vision. We also are very grateful to Governor Thomas Ridge, a Council Distinguished Fellow for the project, who brought his unique perspective as a public sector leader and first secretary of homeland security. Finally, the dedication, expertise and hard work of the advisory committee—ably led by Catherine Allen, former CEO of BITS, and Robert Moore, director of corporate security at Merck—was instrumental in creating the on-the-ground insights that enabled us to identify the business benefits of security and risk management.

We also would like to thank the U.S. Department of Energy and the Defense Threat Reduction Agency for providing the seed funding for our work on competitiveness and security, during a time in which imagining security as anything other than a sunk cost was difficult. We also thank the U.S. Department of Commerce, Technology Administration and Under Secretary Robert Cresanti for recognizing the competitiveness benefits of resilience and for their support as we continue to move the resilience paradigm forward.

The NASDAQ was an invaluable partner in helping us to convene a fertile day-long discussion on "Why Wall Street Should Value Resilience" in October 2006. Our special thanks to Anna Ewing, Joan Conley and Ed Knight. Deloitte partnered with the Council to bring this challenge to the forefront in the business community with a special FORTUNE supplement, *Weathering Any Storm,* in March of 2007. Jim Quigley, the CEO of Deloitte provided the leadership vision for that issue. Jim Porter from DuPont and Tim McNulty from Carnegie Mellon

provided continuing guidance and support throughout the project. Within the Council, Debra van Opstal and Mary Marchal were our thought leaders on the initiative.

It is undeniable that the world has gotten more risky. Businesses now function in a global economy characterized by increasing uncertainty, complexity, connectivity and speed. Managing this rapidly changing risk landscape is an emerging competitiveness challenge—a challenge that demands resilience: the capability to survive, adapt, evolve and grow in the face of change.

The Council on Competitiveness is proud to offer this report, which promotes a strategy of resilience for both the public and private sectors a strategy with clear benefits for our companies' competitiveness and our nation's homeland security.

Sincerely,

President

Council on Competitiveness

Acknowledgments

This work stands on the contributions of intellect, insight, time and funding from so many.

It would not have been possible without the first investor support of the U.S. Department of Energy, which believed in our vision. We would like to thank the Office of Electricity Delivery and Energy Reliability, especially Director Kevin Kolevar, as well as Alex de Alvarez, Hank Kenchington, Ken Friedman, and Rob Gross. Mike Evenson and Chris Walecka at the Defense Threat Reduction Agency reminded us that risk and resilience are embedded in military strategy. At the Department of Commerce Technology Administration, Connie Chang and Brian Tsou helped us link our message of security and resilience to the broader competitiveness goals of the country.

The members of the steering and advisory committees provided an on-the-ground reality check for the sector studies and helped to forge the conceptual transformation from competitiveness and security to risk and resilience.

New insights were developed through the five sectors studies by expert sector study leaders: Martin Wilhelm for the energy industries; Cheryl Charles for the financial services industry; John Glover for the pharmaceutical industries; and Mildred Hastbacka and Robert Weber for the chemical sector. Their original studies are posted on www.compete.org/enterprise resilience. With years of experience in public-private partnerships, Denise Swink offered invaluable and ongoing guidance on policy recommendations.

Other key partners have proved indispensable in promoting a true paradigm shift toward enterprise resilience. Mark Layton and Rick Funston from Deloitte shared their insights on enterprisewide risk management, and helped frame the Council's efforts to engage the public sector in promoting risk management strategies. Our NASDAQ colleagues gave us a window on Wall Street. Debra Ballen from the American Insurance Association helped us to reach out to experts in the insurance industry in order to understand the opportunities and constraints of the industry in this arena.

The leadership and colleagues at the Council are always generous with ideas, advice and support.

Paul Soulellis and the Soulellis Studio team envisioned and created the remarkable design for *Transform.*

In a Nutshell

Key Observations

- **Globalization, technological complexity, interdependence, terrorism, climate and energy volatility, and pandemic potential are increasing the level of risk that societies and organizations now face. Risks also are increasingly interrelated; disruptions in one area can cascade in multiple directions.**
- **The ability to manage emerging risks, anticipate the interactions between different types of risk, and bounce back from disruption will be a competitive differentiator for companies and countries alike in the 21st century.**

What Policymakers Should Know

The national objective is not just homeland protection, but economic resilience: the ability to mitigate and recover quickly from disruption.

Businesses must root the case for investment in resilience strategies to manage a spectrum of risks, not just catastrophic ones.

Making a business case for investment in defenses against low-probability events (even those with high impact) is difficult. However, making a business case for investments that assure business continuity and shareholder value is not a heavy lift.

There are an infinite number of disruption scenarios, but only a finite number of outcomes. Leading organizations do not manage specific scenarios, rather they create the agility and flexibility to cope with turbulent situations.

The investments and contingency plans these leading companies make to manage a spectrum of risk create a capability to respond to high-impact disasters as well.

Government regulations tend to stovepipe different types of risk, which impedes companies' abilities to manage risk in an integrated way. Policies to strengthen risk management capabilities would serve both security and competitiveness goals.

What CEOs and Boards Should Know

Operational risks are growing rapidly and outpacing many companies' abilities to manage them.

Corporate leadership has historically viewed operational risk management as a back office control function. But managing operational risks increasingly affects real-time financial performance.

- The 835 companies that announced a supply chain disruption between 1989 and 2000 experienced 33 percent to 40 percent lower stock returns than their industry peers.
- Twenty-five percent of companies that experienced an IT outage of two to six days went bankrupt immediately. Ninety-three percent of companies that lost their data center for 10 days or more filed for bankruptcy within a year.

A preponderance of board members report that boards are under-informed about operational risk.

Lack of collaboration between risk specialties, and lack of consistent and "leading" metrics to anticipate emerging or interacting risks, are important gaps in the risk management process.

Priorities for Universities

Learning to Change

- Create cutting-edge, cross-disciplinary resilience curricula and research centers

Priorities for Policymakers

Lead by Incentive

- Include resilience criteria in procurement and research and development processes

Reinforce Market Mechanisms

- Explore expanded U.S. Securities and Exchange Commission (SEC) disclosure requirements on non-financial material risks

Reduce Risk and Cost for Resilience Solutions

- Leverage computational capabilities of universities and national laboratories to strengthen modeling and simulation of operational risks
- Catalyze regional networks for crisis management and information exchange
- Expand technology test beds to demonstrate the cost-effectiveness of resilience solutions

Invest in Training and Education to Change the Culture

- Create a Resilience Curriculum Fund to embed resilience in undergraduate and professional education
- Stimulate cross-disciplinary research centers on resilience

Priorities for Business

Walk the Talk at the Top

- Inspire cultural transformation

Link Operational Risk to Revenues

- Organize risk management processes as a continuum

Take a Systems Approach

- Identify critical vulnerabilities across business assets and operations

Manage with Metrics

- Benchmark risk management performance on the operational side

Harness New Technologies

- Apply technology solutions, that create early warning and tracking capabilities, as well as coordination across the organization

Create Adaptive Capacity

- Develop capabilities to mitigate a variety of outcomes from disruptions

The Competitiveness and Security Conundrum

Key Findings

After the shock of 9/11, the Council on Competitiveness introduced the concept that America's security is also a national competitiveness challenge.

Our economy—the engine of jobs and prosperity—could be brought to its knees by a well-placed terrorist attack. And, for the first time in our nation's history, its economic assets and infrastructure were on the front lines of a battlefield: key targets and even pathways for attack. By the same token, however, the economy could suffer an equally damaging blow from excessive security measures that stifled productivity and slowed commerce.

The Council and Carnegie Mellon University, in conjunction with The Business Roundtable, the National Academies, the National Association of Manufacturers and the National Governors Association, convened the first-ever National Symposium on Competitiveness and Security. Its goal: to bring together America's public—and private—sector leaders to "Create Opportunity Out of Adversity." Two hundred and fifty national leaders—CEOs from some of America's largest companies, as well as executives from government, labor and academia—gathered in Pittsburgh to share their experiences and insights on the right balance between competitiveness and security.

Armed with a powerful and compelling framework, Chad Holliday, the CEO of DuPont, and Jerry Cohon, the president of Carnegie Mellon, convened a CEO-level steering committee to bring unique leadership perspectives on the risk-benefit calculations of security investment, and a platform for peer-to-peer advocacy dialogue with senior administration officials and congressional leaders.

> **"Creating the right balance between economic competitiveness and homeland security remains a critical national challenge. This challenge calls for private sector leadership and action."[1]**
>
> **Chad Holliday and Jerry Cohon: co-chairs, Council on Competitiveness Steering Committee on Competitiveness and Security**

An expert advisory committee co-chaired by Robert Moore, director of global security for Merck, and Catherine Allen, then CEO of BITs, managed a complex sector study process that investigated best practices in five industries: chemical, electric and gas utilities, financial services, petroleum, and pharmaceutical.

What we learned is that the challenge is not security: it is resilience.

What Policymakers Should Know

It's a Whole New Ball Game for Risk (Irrespective of Terrorism)

Globalization, technological complexity, interdependence, and speed are fundamentally changing the kind of risks and competitive challenges that companies—and countries—face. Failure, whether by attack or accident, can spread quickly and cascade across networks, borders and societies. Increasingly, disruptions can come from unforeseen directions with unanticipated effects. Global information and transportation networks create interdependencies that magnify the impact of individual incidents. These new types of risk demand new methods of risk management. (See "Test Your Risk IQ" at right.)

Resilience Trumps Protection

Homeland security is often seen as a protective, even defensive, posture. But Maginot lines are inherently flawed. Fences and firewalls can always be breached. Rather, the national focus should be on risk management and resilience, not security and protection. Resilience—the capability to anticipate risk, limit impact and bounce back rapidly—is the ultimate objective of both economic security and corporate competitiveness.

The Business Case Begins with Business Risks

The business case for investment in resilience has to be rooted in meeting a spectrum of business risks. It cannot be based solely on the possibility of disaster. In fact, most of the investments that lead-

Test Your Risk IQ

Which of these poses the greatest risk?

- ❑ **Leaking water**
- ❑ **Overgrown trees**
- ❑ **Falling Debris**
- ❑ **Viruses**
- ❑ **All of the Above**

If you answered all of the above, you would be right. Water leaking into a chemical containment vessel created a cloud of toxic gas that led to the chemical disaster in Bhopal India in 1984. Thought to be the world's worst industrial disaster, the accident killed 3,000 people and injured 200,000 people. Overgrown branches was the proximate cause of a power blackout in August of 2003 that left 50 million people in the United States and Canada without power for several days and resulted in at least $6 billion in economic damage. Debris on a rail track, according to the National Transportation Safety Board, was a possible cause of the CSX train derailment in the Howard Street Tunnel in 2001. The accident created a five-day-long fire, released toxic chemicals and severed fiber optic cables, which then caused a slowdown in Internet service. The love bug computer virus in 2000 attacked 45 million computers and caused between $6–$10 billion in economic losses. Risk cannot be eliminated; mitigation and recovery are essential parts of the risks mangagement structure.

Wal-Mart's Supply Chain Resilience

It happens every spring: The snow starts melting, people trade in their winter parkas for swimsuits, barbecue grills are dusted off, and lawn mowers are started up. When this happens, customers expect their local Wal-Mart and Sam's Club to be ready for them as they buy the sunscreen, hamburgers, and lawn equipment for that first warm weekend.

Unfortunately, this shift occurs at a different time all across the country, and there is no way to peg it to a date on a calendar as one can with a holiday. That means that Wal-Mart's merchandisers and transportation, logistics, and operations teams need to be ready to transition quickly, and in a manner that enables stores in Minnesota to continue stocking snow shovels while the Alabama stores start to stock flip-flops.

The same data management systems that allow Wal-Mart to meet changing customer needs during seasonal transitions, also allow them to react quickly to a disaster anywhere in the country, by flowing essential merchandise to the affected communities. This structure enables the right merchandise mixture as well: water, cleaning supplies and propane to communities in the strike zone; extra food, diapers and toiletries to towns with a sudden influx of evacuees.

This capability was most evident during Hurricane Katrina, when Wal-Mart was able to bring 66 percent of its stores in the affected region back into operation with 48 hours, and 93 percent within seven days. The company used its proprietary systems to start planning alternative routes and emergency staging areas—even while Katrina was still a tropical depression in the Atlantic Ocean. An automated inventory management system created visibility into the location of needed resources. And, since every truck is equipped with on-board computer technologies, shipments could be redirected at any time.

This kind of supply chain sophistication could not have been justified solely on disaster preparedness grounds. Disaster management is a key side-benefit of supply chain resilience, and the nation a key beneficiary. But its investment is rooted in enhanced productivity, inventory visibility, and supply chain continuity and flexibility, all of which are core to competitive advantage.

ing organizations are making—investments that can run in the hundreds of millions of dollars—are aimed at managing the risks they face on a day-to-day basis. For example, the supply chain flexibility that Wal-Mart pioneered—a capability that enabled the company to operate despite the devastation wrought by Hurricane Katrina—was not specifically created to cope with catastrophe. Rather, Wal-Mart's significant investments in RFID tags, software, and staging centers were intended to meet the day-to-day complexities of customer demand. But in the process, Wal-Mart's supply chain resilience also created extraordinary disaster management capabilities. (see "Wal-Mart's Supply Chain Resilience" above)

Regulatory Solutions Often Reinforce Risk Silos

For companies, there are an infinite number of disruption scenarios, but only a finite number of outcomes. In the end, it does not matter whether power failures, floods, strikes or terrorist attacks cause the down time. Causes count less than creating the agility and flexibility to mitigate risks and manage outcomes.

Government, however, tends to see different categories of risk—terrorism and natural disaster, climate change, worker safety, governance—as different problems requiring separate sets of regulatory solutions. In today's risk environment, that creates three potential problems:

- First, it often results in a "check the box" response that is at odds with the need to create value by managing risk on an enterprisewide basis.
- Second, because risks cascade across networks and private enterprises in complex ways, risk silos may actually increase risk exposure.
- Third, it sets up the potential for inconsistent and often overlapping sets of regulatory requirements, which raise cost and complexity without actually improving outcomes.

What CEOs and Boards Should Know

Enterprise Risk Management is a Competitive Advantage

Businesses make money by taking risks, but lose money by failing to manage them. A study by Deloitte Research indicated that many of the largest losses in value among the world's largest global companies were a result of a failure to manage risk effectively and systematically. The study found that most firms were exposed to more than one type of risk—whether strategic, operational, market or financial—and failed to manage the relationships among these different types of risk. Actions taken to address one type of risk had the potential to increase exposure to other types of risk.

The failure to manage risk on an enterprise basis takes a huge toll. The study found that almost half of the 1000 largest global companies suffered declines in share prices of more than 20 percent in a one-month period between 1994 and 2003, relative to the Morgan Stanley Capital International (MSCI) World Index. And the value losses were often long-standing. By the end of 2003, share prices for one-quarter of the companies had not recovered to their original levels.[3]

Managing Operational Risks is Key

The business equivalent to homeland security and critical infrastructure protection is operational risk management—a domain that many executives see as the most important emerging area of risk for their firms. (See Chart 1, following page)

Increasingly, failure to plan for operational resilience can have "bet the firm" results.

- Research on supply chain resilience demonstrated that the 835 companies that announced a supply chain disruption between 1989 and 2000 experienced 33 percent to 40 percent lower stock returns than their industry peers, regardless of

What is resilience?

Resilience is the capacity for complex systems to survive, adapt, evolve and grow in the face of turbulent change. The Resilient Enterprise is risk intelligent, flexible and agile.[2]

1. Operational Risk Identified as Most Important Risk Facing Executives Today

Source: Tillinghast. "A Changing Risk Landscape." New York: Towers Perrin, November 2006.

industry, cause of disruption or time period. Such firms experienced 7 percent lower sales growth and 11 percent higher costs. Changes in operating income, sales, total costs and inventories remained negative in the two years after the problems were disclosed.[4]

- 25 percent of companies that experienced an IT outage of two to six days went bankrupt immediately. Ninety-three percent of companies that lost their data center for 10 days or more filed for bankruptcy within a year.[5]

Operational Risks Remain Stovepiped and Undermeasured

Different aspects of operational risk—physical and employee security, environmental health and safety, IT security, business continuity, disaster management, supply chain security, energy supply and quality—are frequently separated from one another within the organization, and sometimes delinked from overall corporate risk management.

On the financial side, there are increasingly sophisticated systems that measure market and credit risk—often using sophisticated algorithms and supercomputers to model risk exposure. By contrast, although operational risks are arguably at least as complex, operational risk exposure tends to be measured by checklists, which are often based on experience and instinct. In fact, as Chart 2 on page 13 indicates, boards are not as comfortable with their non-financial as their financial risk management.

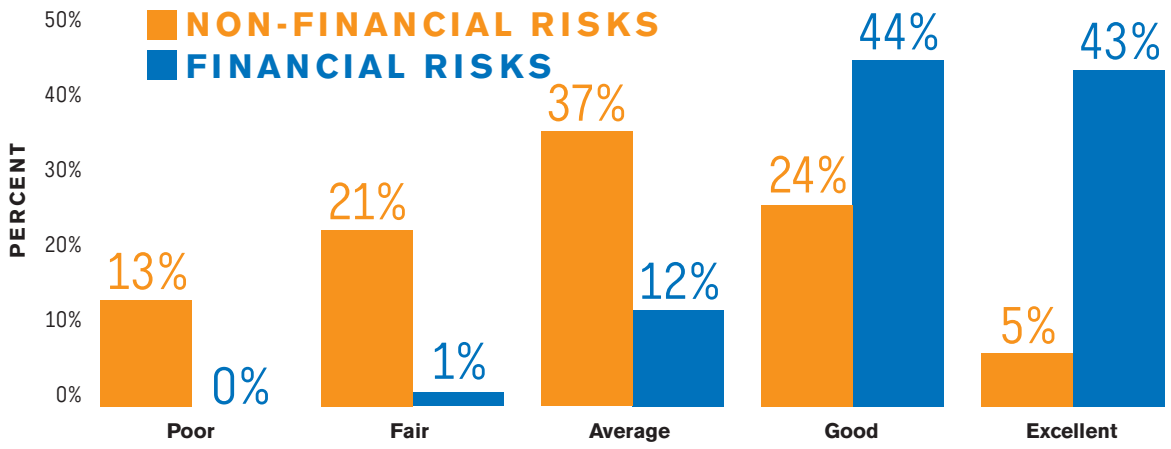
Industry Continues to Face a Risk of Reactive Regulation

Given that six years have passed since 9/11, it is tempting to believe that the danger of a major attack

2. Boards Are Less Confident in Non-financial Risk Management

Source: Deloitte. "In the Dark II." Deloitte, 2007.

How would you rate your organization's record of measuring and monitoring financial and non-financial aspects of performance?



on the United States has abated. Unfortunately, a successful and devastating attack on U.S. soil remains the gold standard for global terrorism. To date, efforts to regulate security have been incremental and sector-specific. But regulatory incrementalism could become a regulatory tsunami if a major attack occurs and industry has not taken the necessary steps to ensure its resilience.

Executive Priorities

Priorities for CEOs and Boards

Corporate executives need to transform current risk management practices with a vision and strategy to implement enterprisewide approaches, and build in the flexibility, agility and adaptability that are characteristic of resilient systems.

Walk the Talk at the Top Inspire cultural transformation by creating a vision for the enterprisewide resilience approach, connect the organizational silos, and engage the entire workforce in risk management.

Link Operational Risk to Revenues Organize risk management processes as a continuum—from prevention to profit—to enable consideration of financial trade-offs among different approaches.

Take a Systems Approach Identify critical vulnerabilities across business assets and operations, including competitive context, and analyze how disruptions might unfold.

Manage with Metrics Benchmark risk management performance on the operational side, identify leading rather than lagging indicators, and quantify the

effectiveness of alternative risk management strategies.

Harness New Technologies Apply technology solutions that create early warning and tracking capabilities, as well as coordination across the organization.

Create Adaptive Capacity Develop capabilities to mitigate a variety of outcomes from disruptions, regardless of cause, rather than planning for specific scenarios.

Priorities for Universities

Universities should position themselves to drive new research, knowledge creation and educational curricula that will build the theoretical and practical groundwork for a resilient economy.

- Create cutting-edge, cross-disciplinary resilience curricula that prepare students for a turbulent, interdependent work environment.
- Develop interdisciplinary research centers that help government and industry respond to the challenges of building resilience.
- Galvanize local and regional efforts to enhance infrastructure resilience and preparedness along with economic development.
- Communicate the importance of aligning security and competitiveness to policy-makers, business leaders, and the public.

Priorities for Public Policymakers

Public policy should strive to reduce uncertainty and inconsistency, lead by incentive where possible, use market mechanisms more creatively and public-private partnerships more effectively, and support education and training programs that change cultures.

Lead By Incentive

- Leverage the government's buying clout to embed resilience criteria in the procurement selection processes and supply chains.
- Leverage the government's investments in technology to embed resilience criteria in the evaluation and selection process for emerging technologies.

Leverage Market Incentives More Creatively

- Expand guidance on disclosure of non-financial material risks in SEC filings.
- Support policies that incentivize risk management through the market rather than through prescriptive regulation.

Effective Partnerships: Reduce Risk and Cost

- Fund additional research to develop sophisticated computational modeling of operational risk and quantitative measures of effectiveness in risk management processes.
- Create regional networks to exchange information on infrastructure or system risk management, crisis planning and preparedness, non-proprietary best practices, and intelligence-sharing between the public and private sectors.
- Expand the program of technology test beds, such as the U.S. Department of Energy National SCADA Test Bed, which helps companies test how their current operating systems would interface with innovative security solutions.

Education and Training: Change the Culture

- Establish a Resilience Curriculum Fund under which universities and other education/training providers could apply for competitively awarded grants to develop resilience curricula and training programs, either stand-alone or embedded in existing curricula.
- Stimulate cross-disciplinary synthesis of resilience and research at a system level.

Seeking the Upside of Security: Learning from Five Sectors

The Council's core insight immediately following the events of 9/11 was that the attacks not only had critical security repercussions, they also had major competitiveness implications. With so much of the economic infrastructure owned or operated by the private sector, any solution for addressing homeland security threats and scalable responses would have to come from within business, not imposed from the outside.

In response to this insight, the Council launched first-of-their-kind studies in five sectors to identify a business case for security. The approach was grounded in the parallels with integrated quality and safety that evolved in the 1980s and 1990s. Businesses traditionally viewed both quality and safety as cost drivers. But new management and organizational approaches transformed them into productivity-enablers.

In the same way, the business community historically viewed security as a sunk cost, not a strategic opportunity. But if integrated quality and safety management systems could become business drivers and pathways for productivity growth, why couldn't the same be true for integrated security management? (see "We've Been Here Before" at right)

Study leaders across the five sectors identified three generic approaches to security:

- *Security as the price of doing business (the "as little expense as possible" approach)*

We've Been Here Before

It is instructive to remember that 20 years ago, America's business leaders thought that quality was a luxury they couldn't afford until the Japanese demonstrated that building quality into processes and production, rather than inspecting out the rejects, was a better formula for success. In fact, the Council on Competitiveness was born as part of America's response to the total quality management challenge from Japan.

In the same way, the chemical industry created a new framework for integrated safety management after the disaster in Bhopal, India. Today, the industry calculates that the savings from its safety program are five times greater than the direct cost of injuries—which includes the avoided costs of lost production, process interruptions, equipment replacement, litigation and damage to employee confidence, customer relations and public image. The drive toward zero accidents was not just the right thing to do; it became a best business practice.

Views From the Industry Trenches

- "Future security practices really depend on what the government is going to do." *Chemical Industry Executive*
- "Environment, safety and security activities are well-integrated and coordinated with both corporate and operations, and work collaboratively with information security and supply chain security. The crisis management teams have been in place since the early 1980s and involve high-level executive teams, functional teams, area regional teams and site emergency teams." *Chemical Industry Executive*
- "Customers care most about reliability, not security. Security cannot come at a premium." *Power Industry Executive*
- "Wall Street would frown upon companies who invest money in security as a waste of capital. Money is invested in utilities because of the dividends. But when utilities spend more on infrastructure, money available for dividends will shrink." *Natural Gas Industry Executive*
- "Our corporate risk management focuses on market and credit risks. Security and other operational risks are managed on the operational level by the asset owners. A risk management committee, comprised of several senior members of the firm, meets regularly to discuss the risks the firm faces. But security risk is not viewed as a major risk management concern." *Power Industry Executive*
- "It took us a good long time to convince our CEO that the world has changed. In the past, the regulators looked at results. In the old days, (if the results were good), you could assume that we were managing the hell out of risk. Today, they say: 'Show me your risk management processes.' If you cannot document how your structure produced those results, they assume it could be luck, and you are not managing risk." *Financial Services Executive*
- "In the past, project managers viewed their function narrowly as getting oil out of the ground. Security was viewed as a necessary cost to allow them to do their job. In current projects, security is so tightly integrated with the management team that it does not even have a separate budget." *Oil Industry Executive*
- "Our operating system was never built for digital security. There have been specific cases in which hackers got all the way into the digital process controls. As we've moved into higher levels of digital integration, creating visibility through the value chain, our systems have become electronically linked. Automating oil field production increases the level of exposure as well. And cyber-vulnerabilities create physical security problems. Physical security is enabled by digital security—all physical security locking mechanisms are now IT controlled. Security has become a strategic issue." *Oil Industry Executive*
- "Security is mostly physical security. It involves the protection of people and facilities, but not products or intellectual property. The risk management group identifies and mitigates insurance risk." *Pharmaceutical Industry Executive*
- "In our company, security is involved in key business decisions from the ground floor. When new facilities are being planned, new products launched, new business relationships established or new acquisitions made, security input is required." *Pharmaceutical Industry Executive*

- *Security as a strategy (standardize across the operation to strengthen security but rationalize the cost)*
- *Security as a strategic opportunity (seize opportunities to gain multiple benefits from security investments)*

Security perceptions and practices vary widely from sector to sector; even companies within the same industry differ in their security approaches. In general, the financial services and oil industries tend to be ahead of the curve in seeing security as part of risk management and financial reward. For financial service companies, international agreements, like the Basel Accord, and domestic regulatory standards initially motivated the integration of security with risk management. The oil industry tends to integrate security into major business decisions because of its history of operating in unstable and often unpredictable regions. Leaders in the chemical and pharmaceutical industries led the way with voluntary safety standards in the 1990s—which expanded after 9/11 to include security. But the companies are far from uniform in the way they view security. Similarly, utility firms are at varying stages of sophistication in the way security is positioned within their companies. (see "Views from the Industry Trenches" on previous page)

But in each of the five sectors studied, there is anecdotal evidence of an upside to security that goes beyond mere loss avoidance.

In fact, leadership-class companies are transforming the way they think about—and manage—security and risk. Security is "baked into" every process and decision, not bolted on with fences and firewalls. An oil company executive noted:

> "The security program has made great strides in establishing security as a competitive issue. Security officers routinely take part in discussions involving issues such as political risk, country risk and strategic reserves. The capabilities of our security program give us a competitive advantage. We operate in countries that our competitors cannot."

Or as a financial services executive remarked: "Security is the support structure for the relationship we have with our customers."

More innovative and enterprisewide security solutions can yield bottom line results, both as a productivity-enabler and potentially a profit center. Insight into workflow efficiencies, reduced losses from fraud or waste, and savings on insurance premiums can create competitive benefits that still remain largely uncalculated in many companies.

In the chemical sector, firms report that new access control systems can reduce loss (from pilferage) and that better time and attendance monitoring—including better monitoring of contractor hours—increase productivity. One utility combines automated meter reading with a service call system that targets outage locations and reports repair times back to customers.

A study by Stanford University, the National Association of Manufacturers and IBM found that a funny thing happens on the way to supply chain security. Companies discovered increased efficiency, better inventory management, and reduced cycle and shipping times.

Some companies are taking advantage of the technologies and capabilities developed for security to create whole new business lines. In the financial services sector, a few firms actively market security-related products and processes to peers. One company in the chemical sector is marketing an open-source software system designed to integrate safety, health and security-related information. At Waste Management, an integrated security center has not only streamlined costs, it is becoming a profit center for the company. (See "Innovation at Waste Management" on following page.)

Innovation at Waste Management: Business Benefits from Security

After 9/11 and a break-in a few months later at a landfill in Cut and Shoot, Texas, that destroyed half a million dollars in heavy equipment, Waste Management began to investigate the benefits of a state-of-the-art security operations center. It found that its own security was inconsistent across its 2,000 facilities. Some facilities lacked alarms altogether, and other alarms were broken or not in use. So, the company created the Life Safety Control Center (LSCC) and deployed smart video and alarm technologies to monitor intrusions into secured areas, as well as to monitor for fire or workplace violence.

The LSCC is creating benefits for the company that go well beyond protection.

- It serves as an emergency operations and communications hub during natural disasters or other crises, really proving its value during hurricanes Katrina and Rita.
- The Center monitors business transactions to reduce vulnerability to theft and fraud.
- The LSCC's video systems allows Waste Management to analyze work-process efficiency and safety operations—analyses that employees can conduct from anywhere within Waste Management's network, saving considerable time and travel costs.
- Video monitoring also is used in Waste Management's growing business of "witnessed and certified" product destruction. There are thousands of products destroyed daily, all under contract to manufacturers who want to prevent defective materials from entering the market through gray-market channels.
- LSCC provides GPS monitoring that can alert Waste Management if certain trucks leave designated routes. From a national security point of view, the LSCC represents a step forward in meeting the national mission to secure sensitive materials in transit and to strengthen disaster resilience.

And from a competitiveness point of view, Waste Management is demonstrating that good security can become a bottom-line benefit. Waste Management now actively markets these capabilities to other small- and medium-sized companies that would rather outsource these costs effectively than make the capital investments in their own monitoring centers. Despite the considerable capital costs, LSCC's year-over-year productivity and financial return has increased—from $490,000 in 2004 to more than $5 million in 2006.

For some of the leading organizations, the added confidence in the brand, shareholder value, customer satisfaction and employee confidence, though less easy to quantify, also are significant aspects of the value proposition from security. Chart 3 on the following page lays out a framework of the prospective business benefits from security.

Why Companies May Not Recognize the Business Benefits of Security

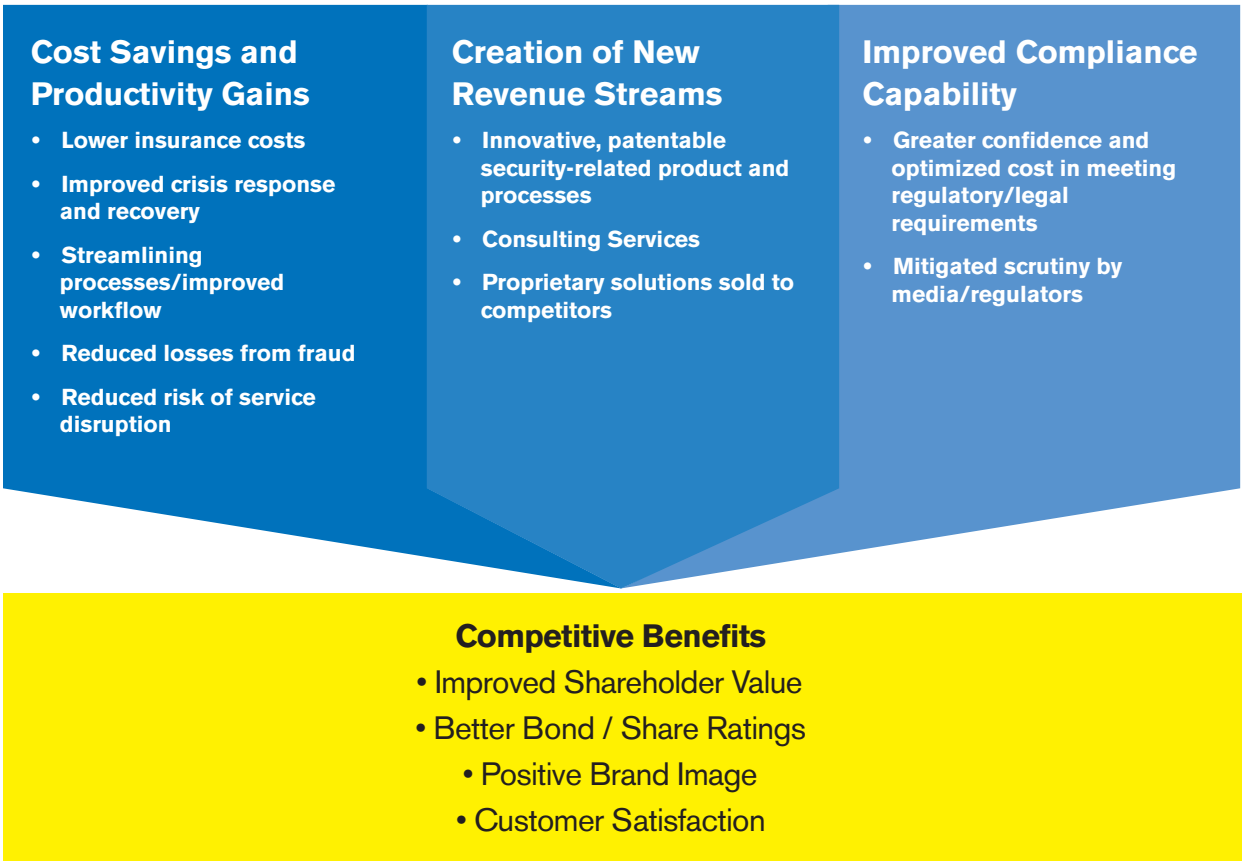
Despite the prospective bottom-line benefits from security, most companies have not moved creatively to capture them. Many continue to see security as a necessary function, but not a core business value. Organizationally, the security function is often disconnected from business continuity and business drivers. Few companies have developed consistent metrics to quantify cost, benefits or performance.

The five sector studies highlighted that the barriers to the business case are often organizational and cultural—a product of the way in which companies have historically positioned security. Looking across the sectors, there are common patterns that capture some of these critical barriers.

- **Security Is Not Linked to Strategic Planning and Risk Management**
  Security in many of the sectors was not aligned with business strategy and not integrated into strategic planning, product development, engineering risk management or supply chain management. Indeed, the security function often does not report at the same level as other senior managers, resulting in what one executive called "security by obscurity".
- **MIA: Metrics for Success**
  In most companies, metrics to capture the value of the security function to the enterprise are unavailable, anecdotal or inconsistent. The lack of a framework to demonstrate efficiency gains, reduced theft or fraud, new business opportunities or new markets is a critical barrier. The inability to measure value reinforces the conventional perception that security is an overhead cost rather than a core business enabler. And, it impedes the ability to develop market-based standards by which ratings agencies or the insurance companies could assess different types of security risks.
- **Security Functions Are Stovepiped**
  In a number of companies, different aspects of security are siloed by function: physical and employee security; supply chain security; IT security; and IP security. The practical consequences of security silos is that companies within a sector find it difficult to agree on cross-cutting best practices. Between sectors, the existence of different organizational silos bogs down efforts to reduce the risks that stem from infrastructure interdependencies. Lack of a common lingo makes it harder to partner effectively with each other or with federal, state, and local governments—or even to demonstrate to Congress and the American public that companies are exercising due diligence.
- **Security Executives: Company Cops or Global Risk Managers?**
  Unlike most other C-Suite positions, the roles and responsibilities of chief security officers are not well defined. They can range from company cop (viewed with suspicion) to global risk manager (where no business decision is made without a security sign-off). Reporting often goes through the Office of the General Counsel (where the focus is on compliance) or through Human Relations (where the focus is on guards with guns).
- **Culture Wars: Linking Security to the Language of Risk and Reward**
  Many chief security executives come out of law enforcement, often with distinguished 30-year careers. That makes them exceedingly well equipped to catch crooks, but often less conversant with how to demonstrate the value of security to the overall enterprise. And they need to be

3. Business Benefits of Security

Source: Council on Competitiveness



able to speak the language of risk and reward when they're competing for investment capital. By the same token, business executives do not typically speak the language of security.

- **Lack of Worker Training as the First Line of Defense**
  Integrating security across the enterprise requires a culture that includes workers as a first line of defense. But few of the companies in the studies had taken steps to engage workers in securing the enterprise. Incidents were not always formally reported. In some cases, it took days before security executives were even aware that an incident had occurred. Given advances in IT and software, automated tracking systems are relatively simple to institute, create a valuable learning tool and could be a key component in developing the quantitative models to measure security risk and performance. Similarly, many companies lack the training programs to achieve a cultural transformation. In leader organizations, training is detailed, role-specific, automated and required at regular intervals. But this is the exception rather than the rule.
- **Learning to Change: Education and Research**
  Professional curricula largely ignore security as part of risk management and resilience. Business schools do not include security as part of the standard CEO education. Although engineering schools have embraced the principles of designing for quality, safety and more recently sustainability, they often lack a "design for security" focus.

4. Summary of Council on Competitiveness Study Observations

Source: Council on Competitiveness

	Financial Services	Oil	Chemical	Electric Power	Pharmaceutical
Management recognizes security as a key driver of shareholder value.	Yes	Yes	No	No	No
Security function is tied to risk management, business, continuity and strategic planning.	Yes	Yes	No	Yes	No
Security includes people, property, processes, information, intellectual property and supply chain.	Yes	Yes	Yes	Yes	Yes
Accountability and lines of authority are clear with a security executive at or near the C suite.	Yes	Yes	Yes	No	Yes
Metrics are in place to quantify risk, losses, performance, and opportunities.	Yes	No	No	No	No
Security training begins at hire with annual risk-appropriate certification for employees and contractor labor.	Yes	No	No	No	Yes
Track and trend information management systems are in place as crisis management and planning tools.	Yes	Yes	No	Yes	No
Government regulations and requirements create incentives for enterprise-wide risk management.	Yes	No	No	No	No
Government regulations and requirements are consistent with common reporting standards.	No	No	Yes	No	No
Federal, state, and local homeland security regulations are clear and consistent and incent investments in security.	No	No	No	No	No

In the same way, academic research centers study many aspects of many industry sectors—from organization and management to supply chain and product design—but only a handful embed concepts of security or risk management into the research agenda. They represent a large—and largely untapped—potential to create the intellectual content (and metrics) that will drive a paradigm shift toward resilience.

Looking Ahead

Challenge for Companies

The challenge for companies is to overcome a historical perspective that views security as static defenses—whether fences or firewalls—and security executives as company cops. To the contrary, security must be integrated into the risk management continuum, not only for loss avoidance, but also for value creation. (see "Transforming Security into a Strategy for Resilience" below)

Transforming Security into a Strategy for Resilience

Old Think

- Passive Private Sector/Wait for Regulation
- Security = Static Defences (fences and firewalls)
- Security = Compliance-driven
- Security = Sunk Cost

New Think

- Dynamic Leadership Vision
- Security = Agility/Adaptability
- Security = Core Business Value
- Security = Strategic Opportunity

Challenge for Government

The dilemma for public policy is that the "security" in homeland security does not necessarily match up to the corporate security function. Arguably, homeland security missions are as much about economic resilience as they are about protection. And the functional equivalents to the economic resilience mission in the private sector are business continuity, disaster management and risk management functions, not just security.

Yet, the focus of much of the government's efforts has been to create public-private partnerships that reach out principally to security executives. From a resilience perspective, this may not be the logical partnership focus. Moreover, government attempts to create a regulatory structure to assure private sector preparedness may actually reinforce risk silos, rather than strengthen private sector risk management and response capabilities.

Warning: Turbulence Ahead

The risk environment has changed dramatically for countries and companies alike. Added to the threat of global terrorism are new technical, operational and strategic risks: extended supply chains; technological interdependencies; IT vulnerabilities; mutating viruses; even weather phenomena. These combine to create the potential for disruptions that propagate quickly across technological networks and geographic borders.

In fact, many of these emerging trends not only create new homeland security challenges, they exacerbate operational risks for companies as well—risks that not all companies are well-prepared to meet. What the sector studies highlight is that the silos in security are characteristic of many aspects of operational risk management. Just as security functions (physical and employee, IT, supply chain security) are siloed, so too are business continuity; safety, environment and health; disaster management.

Within these risk specialties, there are, to be sure, very sophisticated management processes. The problem is that risks do not respect silos. An IT data breach is not just a problem for the IT security executive; it can rapidly evolve into a reputation risk, a litigation risk and a financial risk that can engage the entire company.[7]

Given some of the turbulence ahead, the lack of an integrated approach to risk management is itself becoming a potential risk factor. Some of the trends that change the risk that companies face include:

- The Emergence of Global Enterprises
- New Technology and Infrastructure Risks
- Evolving Legal and Regulatory Risks
- Over the Horizon Risks: Energy Volatility and Pandemics

"The world is becoming turbulent faster than organizations are becoming resilient. The evidence is all around us. Big companies are failing more frequently. Of the 20 largest U.S. bankruptcies in the past two decades, 10 occurred in the last two years. Corporate earnings are more erratic. Over the past four decades, year-to-year volatility in the earning growth rate of the S&P 500 companies has increased by nearly 50 percent, despite vigorous efforts to manage earnings.

Technological discontinuities, regulatory upheavals, geopolitical shocks, industry deverticalization and disintermediation, abrupt shifts in consumer tastes and hordes of nontraditional competitors—these are just a few of the forces undermining the advantages of incumbency."[6]

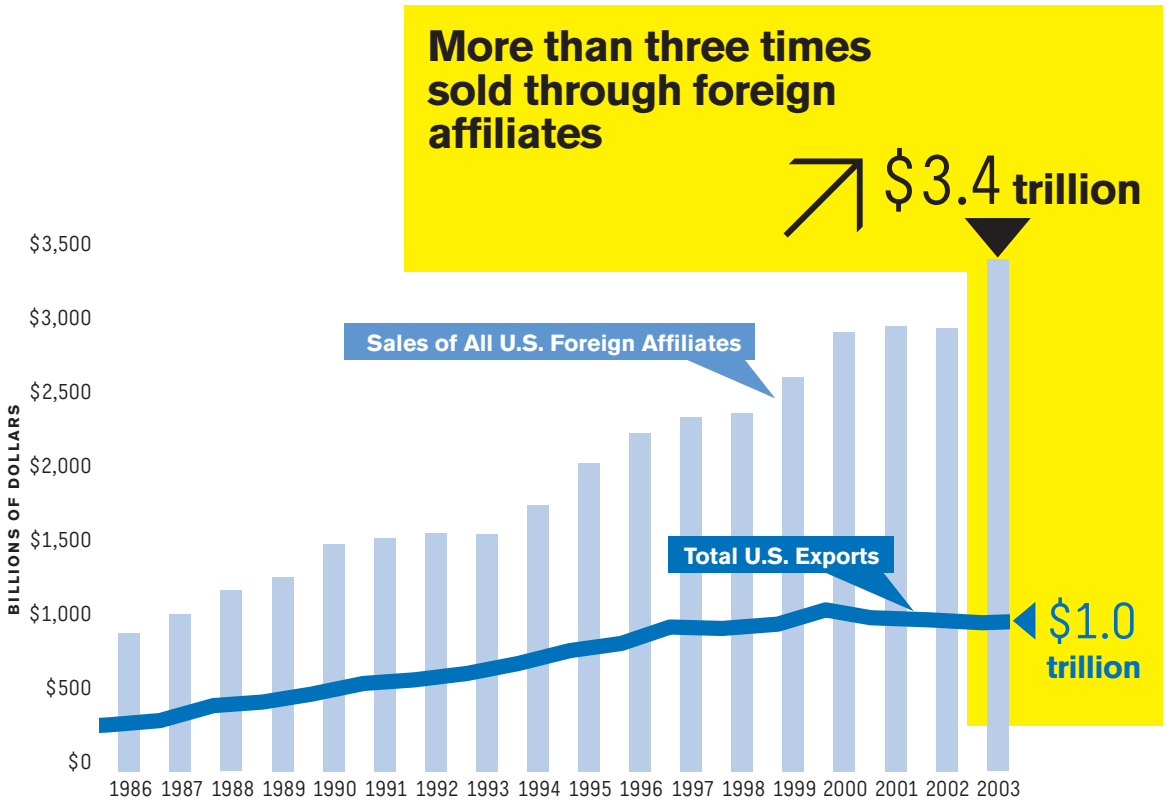
Gary Hamel and Liisa Valikangas. "The Quest for Resilience." Harvard Business Review. September 2003.

Emergence of Global Enterprises

Global enterprises of the 21st century are very dif-

5. U.S. Multinationals Sell Three Times More Through Foreign Affiliates Than Through Exports

Source: U.S. Bureau of Economic Analysis



ferent from the multinationals of the last century. Where multinational companies typically transplanted themselves as self-contained businesses on foreign shores, global enterprises disperse pieces of their business operations across different geographies, which are networked to each other through voice and data IT systems and supply chains.

The Council's *Competitiveness Index: Where America Stands* highlights just how fast the U.S. companies are shifting from multinational firms to global enterprises. Sales of U.S. foreign subsidiaries dwarf those of their U.S.-based parents—three times higher than U.S. exports and even 50 percent higher than the trade deficit. (See Chart 5 above)

From a corporate risk perspective, globalization of companies cuts two ways. On one hand, companies are able to leverage geography to disperse risk. Indeed, rather than creating static backup sites (that often gather dust until a disruption occurs), some of the leading companies are rolling out plans to automatically shift operations among global hubs, should one site go down. They are creating shadow seats in each of their locations and cross-training employees in different geographies to assure business continuity for critical functions in case of an emergency.

On the other hand, the diffusion of interconnected operations also increases a company's exposure: to infrastructure disruptions—in transportation, communications, information—that enable the enterprise to operate seamlessly across different geographies, to the rapid spread of contagious diseases among

employees who are traveling between sites, and to geo-political instabilities and terrorism.

New Technology and Infrastructure Risks

Infrastructure risks continue to mount as disruptions across networks and catastrophic losses escalates.

Electric power outages and power quality problems already cost the private sector and the nation about $80 billion every year in lost productivity and downtime. But when an outage cascaded across multiple transmission systems in the August blackout of 2003, the losses escalated to between $6–10 billion for a single incident.[8]

The Internet is creating an entirely new set of vulnerabilities and risks that many companies have not mastered. A recent study indicated that almost seven out of 10 companies were losing sensitive data or having it stolen out from under them as many as six times a year. It turns out that losing data is expensive. Companies that publicly reported a data loss or breach had an average of 8 percent loss of revenue.[9]

The recent Internet attack in Estonia ushered in a new kind of threat. The attackers used a giant network of bots—perhaps as many as one million computers in places as far away as the United States and Vietnam—to amplify the impact of their assault.[10] One cybersecurity expert noted:

"Everything you have seen in hacking up until now has been a Beta Test of what is possible. This was a multi-pronged attack against several asset classes and financial institutions. What was not widely reported were the digital ripples globally: shutdowns of central banks; processing centers; parts of the U.S. and EU Treasuries; and other financial elements."[11]

Even without data breaches or cyber-attacks, the cost of computer systems going down is enormous. The last published analysis of the cost of these kinds of events appears to have been conducted seven years ago. In 2000, it was estimated that the cost of an hour of downtime for e-Bay was $225,000, for Amazon.com $180,000, and for brokerage companies $6,450,000. (These numbers are not only dated, they do not include the cost of lost productivity.)[12]

The chart below estimates loss per hour by sector.

INDUSTRY SECTOR	(Millions)
Energy	$2.8
Telecommunications	$2.0
Manufacturing	$1.6
Financial Institutions	$1.4
Information Technology	$1.3
Insurance	$1.2
Retail	$1.1
Pharmaceuticals	$1.0
Banking	$0.996

Meta Group. "It Performance Engineering & Measurement Strategies: Quantifying Performance Loss." Rome: Meta Group, October 2000. http://www.creativedata.net/index.cfm?webid=207

Evolving Legal and Regulatory Risks

America's legal and regulatory environment affects companies' risk calculus in two ways. First, the patchwork quilt of laws and regulations and inconsistent application in the court system raises their cost structure. The "direct" cost of liability litigation—including damage awards, plaintiff attorneys' fees, defense costs, administrative costs and deadweight costs from torts such as product liability cases, medical malpractice litigation and class action lawsuits—is as much as 2 percent of GDP. Indeed, the cost of tort litigation has outpaced GDP growth by 2.4 percent, on average over the last five decades. (See "Growth in Tort Costs," next page.)

The combination of uncertainty, costs of insurance, and liability litigation is having a chilling effect on companies' willingness to take sound business risks;

GROWTH IN TORT COSTS

	Growth in Tort Costs Percent Average Annual Increase	Growth in GDP Percent Average Annual Increase
1951–60	11.6	6
1961–1970	9.8	7
1971–1980	11.9	10.4
1981–1990	11.8	7.6
1991–2000	3.2	5.4
2001	14.7	3.2
2002	13.4	3.4
2003	5.5	4.7
2004	5.7	6.9
2005	0.5	6.3
55 Year Average:	**9.5**	**7.1**

Tillinghast. "2006 Update on U.S. Tort Cost Trends." New York: Towers Perrin, 2006.

to invest in R&D and to deploy new technologies, products, and processes.[13] No one argues that victims of incompetence, negligence or malfeasance are not entitled to compensation. Phillip Howard notes: "What has replaced risk is not a culture of caution, but one of blame."[14]

On the regulatory front, new governance controls, such as Sarbanes-Oxley, also are having an impact on how companies manage risk. Former SEC Chairman Ralph Ferraro noted that companies with cash on their balance sheets are increasingly cautious about investing, even in their own futures. There are a number of potentially worrisome trends that are not fully understood: **1** the growing number of companies delisting from public stock exchanges; **2** the loss of U.S. share of global Initial Public Offerings (IPOs); **3** the increase in the cost of directors' liability insurance and new limits on coverage, and **4** and the growing number of companies which no longer provide earnings guidance to investors.[15]

Over the Horizon Risks: Energy Volatility and Pandemics

Energy could become a significant risk factor. The rapid growth in demand from developing economies, such as China and India, is putting pressure on both prices and supply. Indeed, the recent volatility in oil, natural gas and electric power has shaved a percentage point off U.S. GDP growth, increased the costs of energy for U.S. companies, and reduced discretionary income for most Americans.[16]

Daniel Yergin, chairman of the Cambridge Energy Research Associates, notes that the twin energy challenges—the need for energy to drive growth and the need to manage the consequences of energy use—will be dominant challenges in the decades ahead.

On the demand side, the magnitude is daunting. Every day, the global economy requires 86 million barrels of oil, and that is only 40 percent of the total daily world energy consumption.[17] The supply side risks are growing as well. Investments in low carbon alternatives by major financial institutions, energy companies and technology developers could be put at risk if governments around the world fail to agree on an equitable framework for allocating carbon emissions.[18]

Similarly, public health officials have been warning that a future pandemic is not a matter of "if" but "when". The risk of an avian flu outbreak is growing, according to the Congressional Budget Office assessment, because of the way the virus is evolving.

- It is entrenched among the domestic ducks in rural areas of Asia—a permanent ecological niche.
- It is more robust than a weaker 1997 strain; able to survive longer under a broader range of environmental conditions.
- It has increased the range of species it can infect, including cats and captive tigers.
- It has become resistant to one of the two classes of antiflu drugs.[19]

Estimates of the cost of such a pandemic run into the trillions of dollars—costs that could be mitigated by advance planning. Yet a recent survey by Deloitte highlighted that although 73 percent of businesses are aware of the pandemic flu threat and 68 percent are very concerned about the avian flu, only half believe that they have adequately planned to protect themselves from an event—and less than half feel confident about the plan.[4]

Managing Risk on an Enterprise Basis

Enterprise Risk Management appears to be more popular on paper than in practice. Consider that:

- Only 25 percent of directors of non-financial companies report that the board considers all major risks to the company versus 55 percent of financial industry directors.[21]
- Most companies give themselves high marks in financial risk management, but only 29 percent describe their ability to track non-financial performance as excellent or good, and more than a third describe it as fair or poor.[22]
- During the past 12 months, one in five companies surveyed had suffered significant damage from a failure to manage risk and more than half had experienced at least one near miss. As many as 10 percent reported three near misses during the past year.[23]

One of the missing links in moving toward an enterprise view of risk is the lack of a disciplined approach to operational risk. Notes Joe Sabatini, JP Morgan Chase Managing Director and Head of Corporate Operational Risk: "The industry loses money every day in credit and market risk. We're not bothered by that when we take those risks and incur those losses on an informed basis. The key is to create the same disciplined approach to operational risk."[24]

In fact, the lack of a disciplined approach to operational risk increases the potential for what Harvard Business School professors Max Bazerman and Michael Watkins call "predictable surprise—the disasters you should have seen coming."[25] One example might be in the energy area. Most executives recognize that energy is becoming a risk factor, but few companies appear to have integrated energy planning into risk management. A recent survey from Hill & Knowlton found that, although 82 percent of senior technology leaders from around the globe said they "closely monitor" global warming news, only 35 percent have a concrete energy strategy to deal with it.[26] Similarly, in each of the five sectors studied, senior executives clearly understood that the risk dynamic in their industry was changing, but few had integrated that knowledge into the company's risk management operations. (see "The Changing Landscape of Risk" on page 29)

Why The Markets Are Not Driving Enterprise Risk Management

Given the evidence that integrated risk management is a shareholder value and bottom-line issue, as well as an asset protection strategy, why aren't the markets creating new standards and best practices that capture management attention though lower risk premiums or stronger market valuations? One barrier might be the lack of a common set of priorities among the key stakeholders or any commonly accepted metrics.

WHOSE RISK? Top 10 Risk Priorities

Corporate Executives	Insurance Executives	Hometown Security
Reputation	Hurricane	Chemical Threats
Business Interruption	Flood	Biological Threats
Third Party Liability	Oil Spill	Crime
Supply Chain Failure	Terrorism	Fire
Market Environment	Blackout	Cyber-attack
Regulation/Legislation	Wildfires	Tornado
Talent	Industrial Accident	Nuclear Threats
Market Risk	Cyber-attack	Earthquake
Physical Damage	Pandemic	Hurricane
Merger & Acquisition	Earthquake	Flooding

Executive Risk Rankings: Aon, 2007 Global Risk Management Survey

Insurance Risk Rankings: Risk and Insurance, Top 10 Risks, April 15, 2007

Mayors' Risk Rankings: Key survey findings, conducted by the U.S. Conference of Mayors and DuPont through their Cities United for Science Progress partnership

"Whose Risk?" at right dramatically highlights widely divergent views of risk between corporate CEOs and insurance executives. Corporate risk managers are most concerned about risks to reputation or continuity that are often uninsurable, while insurance executives are primarily concerned with physical damage and losses. This could make communication about managing risk relatively more difficult.

But the lack of metrics impedes the creation of even a baseline for discussion about transformational approaches to risk and resilience. The lack of risk metrics, particularly operational risk metrics, is a show stopper. Insurance companies accept and price risk based on actuarial data. But for many types of operational risk, there are no actuarial data. Similarly, although Wall Street ratings analysts are increasingly homing in on risk management capabilities, they are struggling to come up with appropriate metrics and methodologies to assess risk management systems or to value resilience. For its part, while the government has a vested interest in creating more robust risk management capabilities in the private sector, homeland security generally views risk through the lens of catastrophic events and not as part of a risk continuum.

The increasing turbulence of the business environment is partially at fault for the slowness of response to mounting risks. When a ceaseless array of day-to-day pressures and unexpected crisis bombard executives, it is difficult to step back and develop an integrated strategy. In a simpler time, companies were able to achieve operating efficiency by establishing stable business models with repeatable, uniform processes. Today, stability is elusive, and companies must learn new skills—agility, adaptability, and resilience—in order to deliver consistently high performance and shareholder value.

The Changing Landscape of Risk: Lessons from the Sector Studies

In every sector studied, industry trends—market, financial and technological—during the past decade have rendered companies more vulnerable to a variety of disruptions, supply chain problems, product counterfeiting or diversion, and theft or fraud, irrespective of the events of 9/11 and the threat of global terrorism.

Electric Power Deregulation resulted in major restructuring and vertical segregation in the industry, which in turn increased the number of technical interfaces between the utilities and the transmission companies and more potential failure nodes. Reduced profit margins from greater competition, along with regulatory uncertainty (created largely by restructuring trends), has the ability to upgrade aging infrastructure. New technologies, such as automated control systems, which enable remote access and control efficiencies, are creating new IT dependencies and vulnerabilities. More generally, advances in technology have increased the interdependencies between the energy, information, communications and transportation sectors. Embedded IT control systems across the economy have increased reliance on secure and continuous electric power, while the electric power utilities themselves increased reliance on natural gas supplies. Emerging technologies, like VoIP, make communications more critically dependent on electric power.

Financial Services The focus on industry security in the financial services sector is driven by a set of stringent regulations and guidelines that is more comprehensive than in virtually any other sector. But technology continues to create new security risks. Fraud, software vulnerabilities, patch management and the proliferation of viruses and botnets are among some of the new challenges that the industry faces. Similarly, strong interdependencies with other critical infrastructures—communications, energy and transportation—complicate the industry's own business continuity and crisis management planning.

Oil Industry The geographic concentration of industry assets in politically unstable—and more recently, climatologically unstable—regions continues to make security a key component of supply assurance. As oil companies continue to search for new supply, the risks in upstream exploration and development are increasing, both geopolitically and technically. The slowing pace of downstream investment in the United States—a combination of low refinery margins and environment regulations—has increased the criticality of existing refineries. Additionally, the increasing penetration of IT and the internet through the business operation—and the difficulties of securing legacy systems—creates new avenues for attack and disruption.

Pharmaceutical Rising costs of development combined with downward pressure on prices means that pharmaceutical companies are imposing more stringent cost-benefit criteria on every investment dollar. For the industry, cost pressures are impacting production and supply chain resilience by reducing the redundancies, resulting in a potentially decreased capacity to respond to emergencies ranging from pandemics to biological attacks. On the other side, customers' demand for low prices is altering the balance between safety/efficacy and price, potentially opening the door to importation of drugs that, at a minimum, may not have been fully vetted, or may be counterfeit. As with other industries, the shift to digitalization of intellectual property and manufacturing control systems creates new layers of IT vulnerability. And the globalization of the production network creates dependency on continuous operation of global supply chains.

Ratcheting Up Resilience: Best Practices Among the Leaders

The challenges are mounting, but so too is the amount of ingenuity being applied to meet them. Innovative organizations are fielding new ideas and deploying new solutions that increase both their risk intelligence and capacity for resilience. DuPont is building a new framework for integrated risk management that brings with it a leadership vision to walk the talk. Georgetown University serves as a model for academic institutions in terms of reaping rewards from effective risk management. FM Global's systems approach provides a model for meeting emerging types of risks, while NASDAQ has embraced reliability as a cultural goal. Companies like Wal-Mart, Waste Management, AEP, Educational Testing Service and Limited Brands are paving the way with success stories and best practices that serve both competitiveness and homeland security goals.

1. Best Practice: Walk the Talk at the Top

Enterprise risk management requires an enterprisewide approach, and that means that the impetus for change has to come from the top. The first steps are to connect the organizational silos and embed risk management in day-to-day business operations, to engage the entire workforce, and to create cultural change.

Case in Point: Risk Management Done Right at DuPont

The growing complexity of risk has triggered a transformation restructuring of risk management at DuPont. Ten, even 20 years ago, addressing one risk at a time worked pretty well. Today, risks that weren't even on the radar screen a decade ago—global warming and carbon caps, Sarbanes-Oxley, to name a few—have a profound impact on business performance. The world has gotten too complicated to take one risk at a time. They have to be rolled up into a risk portfolio. So, DuPont is creating a new work process and leadership structure that integrates risk management across the entire enterprise. Principles guiding the transformation include:

Traditional Risk Management	Enterprise Risk Management
Risk as individual hazards	Risk in context of business strategy
Risk identification and assessment	Risk portfolio development
Focus on all risks	Focus on critical risks
Risk mitigation	Risk optimization
Risk limits	Risk strategy
Qualitative risk assessment	Monitoring and measurement
Risk is not my responsibility	Risk is everyone's responsibility

Understanding the big picture on risk enables the company to prioritize which to accept, which to transfer, which to manage—and which to eliminate.

In this more complex world of interdependent risks, gut instinct and managerial experience are no longer sufficient. New risk structures demand fully integrated business teams that bring every perspective to the table in strategic decision-making. In addition, knowledge management systems have become critical to capture and share information and insights within the company about risks and risk management processes.

Understanding the bigger picture is its own reward. It enables DuPont to capitalize on strategic opportunities with a more complete understanding of all the potential risks. That process requires clarity of goals and transparent processes to achieve them—increasingly a critical factor in relations with shareholders, customers, communities and employees. And the integrated approach to risk creates insight into workflow and supply chain efficiency, ultimately resulting in better business performance.

2. Best Practice: Treat Risk as a Continuum

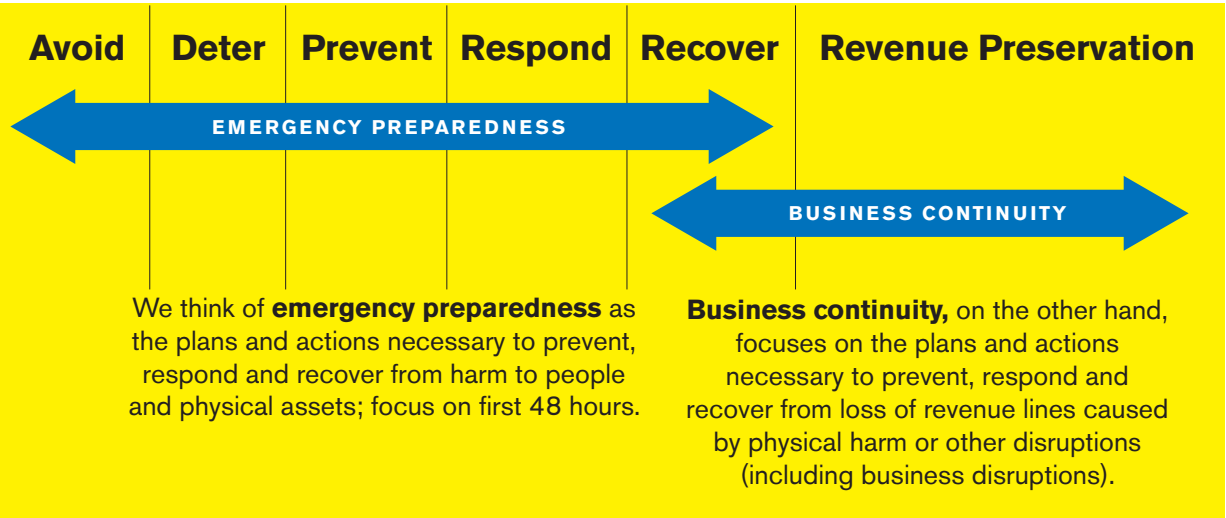
One of the limitations of most organizations is that risks are managed in silos, not strategically. Emergency preparedness is handled separately from business continuity, which in turn is not always part of strategic risk management. This fragmented approach impedes a clear understanding of the tradeoffs between different risk management strategies (avoid, accept, mitigate, transfer) and the different kinds of investments that can be made to implement those strategies.

Case in Point: Georgetown University—Managing Risk Strategically

Georgetown realized that traditional risk approaches had become too limiting. Consider, for example, a specific operating risk—say a facility fire. Under a traditional framework, facilities management, safety, and insurance could each be independently making investment decisions to protect against risk. This piecemeal approach could result in over-investment, under-investment and almost certainly, inefficient investment.

6. The Risk Continuum

Source: Spiros Dimolitsas, Georgetown University



Georgetown re-organized its risk management processes as a continuum.

The integrated framework enables the university to capture the business returns on effective risk management. Georgetown University began by mapping its core missions and revenue streams and working backward to understand what key risks could disrupt them.

Take, for example, education and the associated tuition, which provides one of the University's main sources of operating revenue. In this context, student housing is a critical function. If it isn't available, neither is the revenue stream. Georgetown undertook a project to improve residence hall safety standards that exceeded code—installing sprinklers and other equipment—resulting in a significant decrease in its insurance premiums. The University then took these savings and increased its business interruption insurance fivefold (well before Katrina). That turned out to be a positive factor in determining the University's cost of capital in a recent bond issue.

This kind of dynamic business model doesn't happen by accident. It requires a risk management approach that is:

- Integrative: Creating a single framework to address the continuum of risks and responses at the strategic level
- Quantitative: Applying performance metrics to understand the impacts of different types of responses, and the ability to meet rare but high impact contingencies
- Systematic: Taking a systems engineering approach to address multiple interacting risks and focus on solutions that combine business payback with risk reduction.

And, it creates one key advantage. In adopting a capabilities-based approach rather than a scenario-based, threat model, Georgetown is evolving its focus on how it approaches business continuity—reinforcing the most critical assets and functions needed to deliver the revenue stream—rather than what-if contingencies. The university may not be able to anticipate every scenario, but it is trying to create response capabilities that will be resilient no matter what the cause of disruption.

3. Best Practice: Taking a Systems Approach

Business continuity requires a systems approach that identifies potential weak links and how disruption might unfold throughout the organization. Sometimes, the ability to map business continuity not only helps to understand the modes of failure, but it clarifies business processes in ways that enhance efficiency or streamline costs.

Case in Point: FM Global—Managing Risk and Minimizing Loss

Terrorists and black-hat hackers may evoke powerful concerns among corporate risk managers, but one-third of U.S. GDP is directly affected by weather. Indirect effects, like downed phone or power lines, can throw a wrench into a company's operations and business continuity.

Business property insurance giant, FM Global, believes that it is better to prevent a loss than to try to recover from one. Its motto: Hurricanes cannot be stopped…but losses can. The insurance provider has adopted a systems engineering approach to risk management that minimizes physical damage and downtime.

The company built a $78 million research campus that specializes in destruction by such things as fire, explosion, high winds and golf-ball sized hail. Roofing tiles are slammed by ice balls exceeding 70 miles an hour. A giant fan creates hurricane-force winds with speeds of up to 160 miles an hour. A debris cannon shoots two-by-fours up to 90 miles an hour at walls, windows and doors to see what happens when debris is tossed around in a storm.

The campus also features a dust explosion bunker used to demonstrate how quickly airborne particles can ignite and create an explosion, and an electrical hazards lab to test explosion-proof and flame-proof products.

Nearly one third of its workforce consists of loss prevention engineers. As an insurer of one in three FORTUNE 1000 companies, FM Global believes that an engineering-based loss prevention strategy works better than an actuarial approach. In fact, locations that implemented the company's engineering recommendations during the 2004 and 2005 hurricane season sustained approximately eight times less damage than those that did not.

Its advice to Ocean Spray provides a useful example. Calculating that a major hurricane could potentially create a $75 million to $100 million loss, Ocean Spray sought help in securing its Florida-based, grapefruit-processing operation. Ocean Spray invested in securing the sections of buildings most vulnerable to high winds and purchasing back-up generators for use in the event of a power outage. During the wild 2004 hurricane season when the plant took direct hits from two of the four major hurricanes that struck the Florida coastline, the total systems approach paid off. The facilities sustained only superficial damage during two major storms and the generators prevented spoilage of the grapefruit inventory.

The Message

Insurance alone is not enough to make your company whole when disaster strikes. You can insure your assets against physical loss, but insurance won't bring back lost opportunities or market share.

4. Best Practice: Manage with Metrics

It is often said that you manage what you can measure. A resilient enterprise needs to adopt a common definition of resilience and measurement framework that supports the operational and cultural values of the organization. An enterprise must quantify just how resilient it is before adopting strategies to improve or leverage resilience.

Case in Point: Educational Testing Service—Measuring Resiliency

Many organizations are actively searching for metrics to assess their operational risk exposure and resilience. The Educational Testing Service (ETS)—an organization that administers and scores more than 50 million tests annually in more than 180 countries—is already implementing them. As a nonprofit institution with a core competency in measuring performance, ETS has established a framework not only to understand how resilient the enterprise is, but to leverage its resiliency when assessing new ventures and opportunities.

For ETS, the roadmap to enterprise resilience runs through three phases:

Phase 1: Establish a resiliency baseline

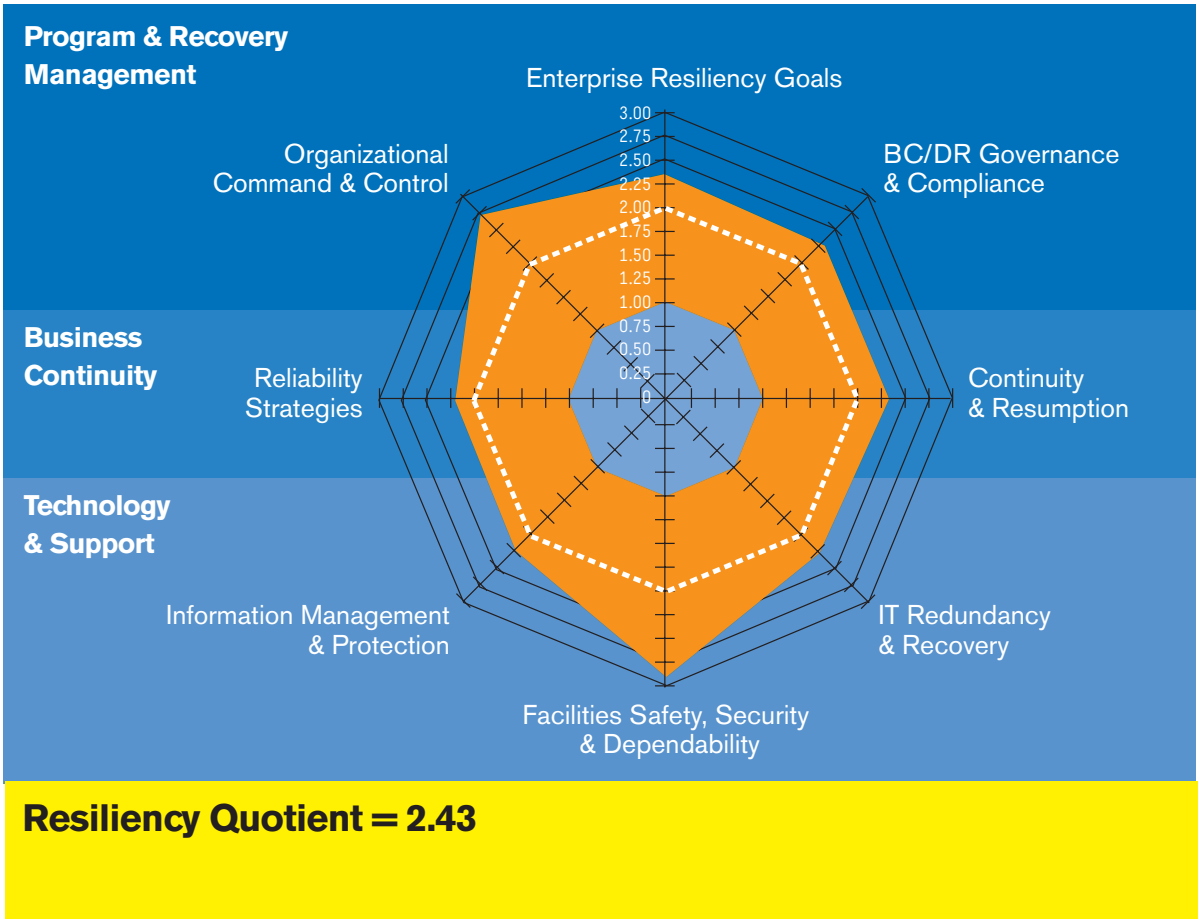
Conduct a detailed assessment of specific resiliency elements and observations across eight dimensions:

- Resiliency Goals
- Governance and Compliance
- Organizational Command and Control
- Reliability Strategies
- Continuity and Resumption
- Information Management and Protection
- Technology Redundancy and Recovery
- Facilities Safety, Security and Dependability

Compare the results to a "straw man" position of where management thought the organization was and where it needed to be. Score the results to determine a baseline resiliency quotient or rating. In and of itself, this rating is not very meaningful. However, it establishes a starting point, or baseline, where activities and resources can be prioritized and

7. Summary of Resilience Elements

Source: Educational Testing Services



progress measured. An example resilience assessment is shown in Chart 7, above.

Phase 2: Improve Operational Resiliency

Identify gaps and adopt solutions to address them. Implement policy, procedural and organizational changes, and prioritize resources to address high-leverage areas where the greatest improvements can be made. Consider solutions based on their specific contribution to improving overall enterprise resiliency. Measure annual objectives as the bar is raised.

Phase 3: Capture strategic opportunities and competitive advantages from a comprehensive enterprise resiliency program

New business Significant new contracts have been won by demonstrating a commitment to enterprise resiliency. The competitiveness of ETS bids and proposals has been enhanced by offering operational resilience as a feature of its products and services.

Supply chain A chain is only as strong as its weakest link. Having strong and resilient partners and suppliers improves overall enterprise resiliency. New vendors and suppliers can be assessed against the internal enterprise resiliency quotient. Their rating becomes a key criterion for negotiation and ultimate selection.

Acquisition Just as a CARFAX or bond rating can assist with the value of and decision to buy an automobile or a junk-bond, a resiliency rating can identify and illuminate areas of strength or concern of a potential acquisition or business partner. During the diligence phase, the resiliency assessment can compare elements of the target on an "apples-to-apples" basis and determine the incremental effect to the overall enterprise resiliency of the combined organization, product or service.

The Message

Enterprise resiliency, when institutionalized into the operations and culture of an organization, can provide strategic competitive advantage and confidence to pursue new opportunities.

5. Best Practice: Harness Technology to Reinforce Resilience

Technology creates new vulnerabilities, but strategic applications of technology also can reinforce a company's ability to anticipate problems, weather turbulence and respond to crises. Nowhere is this more evident than in the IT arena. Organizations that focus on protecting the keys to the kingdom (increasingly their data and IT systems)—and use that capability to monitor their operations—do better across a variety of measures: security, business continuity, efficiency and customer confidence.

Case in Point: Resilience NASDAQ style

Resilience requirements do not get much more complicated than those at NASDAQ. Launched in 1971, the world's first electronic stock exchange now provides data to more than 400,000 terminals and workstations, connecting thousands of traders across North America. It processes more than 230 million transactions daily at a rate of 64,000 transactions per second, each with a 1 millisecond response time. In the time it takes to read this sentence, NASDAQ will process nearly 200,000 transactions.

Resilience wasn't always a NASDAQ byword. In fact, one of the earliest challenges was the local squirrel population. In 1984, a squirrel knocked out a power line and the battery-powered backup system failed to kick in, causing a 30-minute trading disruption. Again, in 1987, a squirrel triggered a power surge in a transformer, which brought down the network for 82 minutes—and the losses mount into the millions by the minute, not the hour or the trading day.

Today, NASDAQ operates at what they call the "4 nines of uptime"—99.998 percent or about as close to zero room for error as anyone can get. Twenty years of engineering its IT systems, emergency operations and contingency planning came to a head on 9/11.

Despite the shock of a front row seat to the tragedy unfolding at the World Trade Center, the NASDAQ exchange remained open and operational throughout the day. The problem: Many of its customers' systems, that had to connect to NASDAQ electronically, were down. In fact, during the week of 9/11, the NASDAQ system operated continuously so that customer firms could test their connectivity in preparation for the resumption in trading.

The Message

The big lesson from 9/11 was that operational readiness has to exist in a practical sense—not just on paper or in emergency operations centers that are essentially gathering dust—and it has to engage the entire industry, not just the NASDAQ exchange. More frequent and more inclusive testing is now a big part of their resilience planning. Quarterly testing of backup sites turned into monthly tests involving select market participants. Disaster recovery tests are now conducted multiple times in a year with NASDAQ's customers and key service providers.

The 2003 August blackout created another key learning opportunity. In a quarter century of NASDAQ operations, the blackout represented the first time that both northeast utilities failed. Although a

diesel powered backup generator in Connecticut kept the exchange operational, the implications for resilience were not lost—that is, the desire to achieve increased operational efficiency through consolidation of data centers has to be balanced against the need for geographic diversity to manage infrastructure risks.

Wall Street has clearly learned some valuable lessons during the past few years. One of the most important: There is an extremely tight correlation between money, profits and resilience.

6. Best Practice: Put Plans in Place that Anticipate

With so many different permutations of things that can go wrong, it is impossible to plan for every contingency. The leader companies are putting plans in place to manage outcomes, rather than specific scenarios. They are creating a capabilities-based approach.

Case in Point: Protecting Supply Channels: Resilience at the Limited Brands

No industry sector is more challenged by rapid change and unpredictability than the global apparel industry. At Limited Brands, which operates Victoria's Secret, Bath & Body Works, and a number of other well-known retail chains, resilience is ingrained into the culture.

Limited Logistics Services (LLS) is a division of the company that provides integrated management of global supply chain operations for all of the brands. Since the 9/11 crisis, resilience has become standard operating procedure for LLS. They rely on a number of key strengths—continuous vigilance, contingency planning, cross-functional teamwork, frequent communication, and an adaptive, problem-solving approach. These strengths were evident during the September, 2002 port shutdown on the West Coast, which disrupted the supply chain operations of many U.S. companies. Recognizing the potential for a disruption, LLS began to work with the various Limited Brands businesses on risk avoidance tactics to identify new and alternative distribution channels.

The port shutdown was a prolonged test of Limited Brands' resilience; a dynamic, ever-changing situation requiring daily assessments and decision-making. As a result of this experience, LLS gained credibility for their expertise in crisis management, and they are now a key player in Limited Brands' efforts to further strengthen its emergency preparedness and enterprise risk management capabilities.

The capacity to "sense and respond" across the supply chain continues to be reinforced as a standard operating procedure. LLS avoids getting locked into a single scenario of how things should be. Instead, they confront uncertainties and constantly question their assumptions. Individuals are encouraged to think holistically, not just focus on narrow cost or efficiency criteria. According to Rick Jackson, the vice president that oversaw the 2002 crisis: "Resilience goes beyond conventional business continuity and security—it is an intuitive mindset that pervades our organization."[27]

Case in Point: Resilience at American Electric Power—A Leader in Emergency Response

When the electricity doesn't work, it is not just the lights that go out. Information, communications, transportation, water and sewer networks all depend on the availability of electric power at some point in their production or delivery process. Virtually all service providers and every retail cash register in the country depend on electricity.

The electric power industry has become best in class in recovering from localized, usually weather-related, disruptions that affect every region in the country—and none better than American Electric Power (AEP). AEP is a recognized leader in the field of emergency response, often helping companies outside of its own service areas.

AEP's resilience was tested on January 12, 2007, when a severe ice storm struck several communities in the territory served by Public Service Company of Oklahoma (PSO), an AEP operating company based in Tulsa. The storm came in three successive waves during a period of several days, depositing up to two inches of ice. Ultimately, the storm interrupted electrical service for close to 250,000 customers, with some customers losing power for more than 10 days.

To respond to such disruptions, AEP has evolved an elaborate, company-wide system, governed by a detailed Service Restoration Plan that is updated continually. Additionally, it is common for AEP and other utilities to provide emergency support to each other, coordinated through "mutual assistance networks" involving dozens of regional utility companies. During the Oklahoma event, PSO requested assistance and was able to promptly mobilize more than 2,000 emergency workers. After such an event, the affected utilities reimburse those that provide restoration service.

The coordination required to manage and support these emergency resources is an enormously complex task. Outside contractors are often utilized; AEP contracts with forestry companies to clear branches for line crews and with logistics companies to supply tents, trailers, food, and laundry services. AEP has adopted advanced technologies, such as handheld data entry and communication devices, to help dispatch crews quickly to the areas of greatest need. Satellite positioning devices are being installed on line repair trucks so that resources can be monitored centrally and deployed in real time.

The Service Restoration Plan lays out a detailed organizational structure, with different levels of responsibility. Voluntary participation—all hands on deck—is part of the AEP culture. During an emergency, it is not unusual for more than 75 percent of employees in the affected operating company to be engaged. Each person receives an alternative "storm" assignment. For example, Hazard Standby Associates are assigned to guard broken wires in order to prevent residents from being injured. AEP provides standardized training and materials so that different operating companies can collaborate effectively.

According to AEP Chief Risk Officer Laura Thomas, the company's emphasis on reliable service delivery is essential to assuring customer satisfaction, since "AEP is part of the business continuity plan for every company we serve." AEP Emergency Restoration Planning Manager Jim Nowak adds: "Restoring power is not just a responsibility, it's a moral imperative."

7. Best Practice: Create Cutting Edge Research Centers

It is tempting to believe that 9/11 was a watershed event that changed America's economic, homeland and national security. But the reality is that many threads have converged to create a new landscape of global risk. U.S. competitiveness, as well as security, depends on being able to understand and manage these risks. Our universities will play a critical role in developing the framework for understanding resilience and training a new generation of Americans to deal with an inherently riskier future.

Case in Point: Resilience at Ohio State

Known as a Big Ten sports powerhouse, The Ohio State University (OSU) campus in Columbus, Ohio, also is the first university in the nation to launch a Center for Resilience (CfR), dedicated to strengthening the resilience of enterprise systems and the environments in which they operate.

The university saw a growing gap between the real-world challenges of enterprise management and the analytical tools available for understanding complex, adaptive systems. Companies that use traditional methods of risk analysis and decision-making often find themselves in a continuous crisis mode, unable to cope with a rapidly changing business environ-

ment. The multidisciplinary center is focusing on introducing new analytic tools and methodologies, for example:

- A web-based supply chain resilience assessment protocol, developed with Limited Brands, which enables companies to identify supply chain vulnerabilities and enhance their capabilities.
- A decision model for design of industrial networks incorporating innovative technologies that enable conversion of waste materials and energy into profitable byproduct streams.
- An approach for building resilient organizations that can make effective decisions under pressure, such as when confronted with tradeoffs between safety and performance.
- A comprehensive life cycle analysis tool that captures the linkages between industrial and ecological systems, such as the hidden dependence of fuel production on ecosystem services.

A key step in the formation of the Center was the recruitment of an industrial advisory board, with senior representatives from companies such as American Electric Power, Chevron, Dow Chemical, General Motors, and Limited Brands, as well as government agencies and non-profits.

Center Co-Director Joseph Fiksel points out that short-term business continuity and long-term sustainability are two ends of the resilience spectrum. According to Fiksel, there are several ways that companies can improve their resilience, including re-engineering their physical assets, improving their human-centered business processes, and strengthening their position with respect to the "competitive context"—the social and environmental assets that provide employee talent, market demand, and a reliable supply of materials and energy.

Addressing resilience in an integrated manner will require breaking down a large number of functional silos and creating new management tools. But universities can be key partners in providing the research and new curricula to make this happen.

Much more can be done to capture best practices and the measurement systems that demonstrate their effectiveness.

Policy Priorities

When it comes to homeland security, there are some jobs that only the government can do, such as intelligence and border control. But there also is a critical aspect of the homeland security challenge that is less about security and more about economic resilience: the capacity to minimize disruption and recover quickly. The distinction is critical.

Making a case for businesses to invest large amounts in static defenses against low-probability events is never an easy sell to shareholders. But making the business case for investment in business continuity and risk management doesn't require much heavy lifting. The following vignettes highlight just how far investments by some of the nation's leading companies in supply chain agility, physical security, information security, business continuity, risk management and risk measurement capabilities—investments that were made to serve their own business needs and bottom-lines—actually go toward meeting national objectives.

Government policies can reinforce resilience in some key ways: incentivizing investments in resilience through the power of government procurement contracts; identifying resilience as a desired criteria in research and development funding; strengthening market mechanisms to reward companies with stronger risk management capabilities; investing in new computational models, that is, analytic tools that improve risk assessment capabilities; encouraging regional information-sharing networks that support disaster-resistant communities; leveraging public-private partnerships to reduce the cost and risks of deploying new security technologies; and funding new programs to embed resilience in America's research agenda and educational curricula.

Lead by Incentive

Leverage the government's buying clout to embed resilience criteria into procurement processes and supply chains

The government should never underestimate its ability to influence the private sector through the procurement system, which spends about $400 billion annually on goods and services. The government could leverage that buying power to create resilience requirements for its contractors.

In fact, private sector entities are already developing model contract language for use with their own vendors and through their own supply chains. The Internet Security Alliance and the American National Standards Institute have proposed language that incorporates globally recognized IT security management practices into contract-based business operations. Similarly, the SCADA Procurement Project, a joint effort between the public and private sectors, is focused on developing common procurement language to help ensure that best in class security standards are integrated into the computer systems that control critical infrastructures and plant operat-

ing systems. The chemical industry is developing standards to require industry security and responsible conduct codes for use in its own supply chains. If the private sector can embed resilience into its supply chains, the public sector should do no less.

Leverage the government's investments in technology to embed resilience criteria into the evaluation and selection of emerging technologies.

In each of the five industry sectors, senior business executives could imagine future technologies that would make their operations inherently more resilient and robust. Some of these technologies are already in the research and development pipeline of federal agencies, but none were evaluated on the basis of their contribution to the nation's critical infrastructure resiliency.

Among the most promising future technologies for both competitiveness and resilience identified by private sector leaders were: self-optimizing grids; advanced pipeline technologies; smart refineries; small, just-in-time chemical processing; and renewable raw materials.

- **Self-Optimizing Grids**

  Self-optimizing transmission grids have the ability to self-diagnose and "heal" the system in real-time. They make use of advances in grid technology to detect and locate damage in the transmission network, incorporating autonomic system reconfiguration in response to disruptions and fluctuations in supply and demand. This increases the efficiency of the entire power system and lowers the cost of delivery, maintenance and repair, as well as the cost of blackouts for suppliers and consumers.

- **Advanced Pipeline Technologies**

  Recent developments in pipelines maintenance and security technology facilitate faster recovery from attacks while enabling cost-effective and efficient pipeline maintenance procedures. These technologies incorporate the ability to detect precisely the location and the severity of pipeline damage as soon as a security event occurs, essentially reducing repair and maintenance costs while increasing reliability.

- **Smart Refineries**

  Smart refineries would combine the latest developments in computer and communications technologies to capture comprehensive and frequent measurements of operating conditions. These real-time measurements—collected from motors and valves that provide data on temperature, flux, run-times, pressure, and sensors with photographic, audiometric near infra-red (INR) and nuclear magnetic resonance (NMR) imaging—are analyzed and compared to previously collected data and outputs of sophisticated forecasting models to realize the differences between the actual and expected states. The technology not only increases efficiency and creates a capacity for predictive maintenance models, but can monitor attacks, accidents or disruption in real time and potentially reduce the scope of damage.

- **Small, Just-In-Time Chemical Processing**

  One promising technology option is process intensification, which combines different processes into smaller, compact and efficient units that can also be co-located at the manufacturing site. The pay-off is not only in streamlined processes, but in a much smaller environmental footprint and the potential to transport non-hazardous materials to a co-located facilities where it can be processed on site in a just-in-time mode. From a homeland security perspective, this keeps the toxic products off the road and co-located at the manufacturing facility.

- **Renewable Raw Materials**

  Replacing oil-based raw materials with locally available renewable agricultural feedstocks cre-

ates another long-term vision for future resilience. Such a capability would create a reduction in the cost-of-goods while eliminating a major source of security risk, in addition to providing clear environmental and sustainability benefits.

Leverage Market Incentives More Creatively

- **Expand guidance on disclosure of non-financial material risks in SEC filings**

The year is 1998 and Y2K concerns are taking hold. SEC chairman Arthur Levitt sends a letter to executives at more than 9,000 publicly traded companies that states:

"At midnight on December 31, 1999, the vast majority of computer systems may not be able to distinguish the year 2000 from the year 1900. Many experts fear that this programming flaw could debilitate computer systems world wide…Time is short…Because the lack of information regarding your preparations for the year 2000 could seriously undermine the confidence investors place in your company, it is imperative that you provide thorough, meaningful disclosure on this topic."[28]

In the Y2K case, the SEC did not ask companies to expose their vulnerabilities, but rather to disclose their readiness to deal with the risk. Today, the capabilities to protect against disruption as well as rebound from it are becoming increasingly relevant to shareholder value and future earnings.

There are some clear parallels between the Y2K example and the rise in operational risks. Companies may not be able to project a specific probability of risk, but they can certainly disclose more about whether risk management processes are enterprisewide, anticipatory across a spectrum of contingencies and based on performance metrics. Understanding a company's risk readiness is likely to become far more material to investors as a predictor of future earnings.

Create More Effective Partnerships: Reduce Risk and Cost

- **Fund additional research to apply computational modeling and simulation capabilities to assessments of operational risk**

One of America's technological advantages is its strong leadership in computational modeling and high performance computers. These computational capabilities, resident today in America's universities and national laboratories, could be applied to creating more sophisticated operational risk management tools.

The financial side of risk management already employs high performance computers and sophisticated algorithms to assess risk exposure. But there is no comparable computational capability for operational risk, which is, in fact, a far more complex challenge. Operational risk is sometimes defined by what it does not include (e.g. market risk, credit risk, and liquidity risk). But it does include almost everything else, with some key risk areas being: system, supply chain, technology or infrastructure breakdowns; employee fraud or misconduct; security breaches; natural disasters; industrial accidents; and worker safety.

With better modeling capabilities, the interrelationship between different types of operational risk, their potential failure paths, and the company's exposure to loss can be modeled and quantified —data which might motivate CEOs and boards to action. Such models have been developed for complex engineering challenges, but could be equally relevant in modeling multiple interacting operational risks.

This is one area in which leveraging investment that the federal government has supported for the past four decades could have a huge impact on the private sector's ability to deploy more sophisticated risk management processes, while serving both competitiveness as well as homeland security goals.

- **Create regional networks to exchange information on infrastructure or system risk management, crisis planning and preparedness, non-proprietary best practices and intelligence-sharing between the public and private sectors**

Governor Tom Ridge famously noted that homeland security is based on hometown security. Community risk management really comes together at the grassroots, where companies come together with infrastructure providers, universities research centers and training programs, emergency responders, and government executives. It is at the grassroots where the fusion of interests and responsibilities creates the potential for fruitful exchanges of information and best practices.

Although fusion centers were originally proposed as vehicles for information and intelligence sharing among federal, state and local officials, the value of regional networks goes far beyond the original concept.

Collaborative regional centers could provide needed exchanges of information between companies and their infrastructure providers on redundancies in the service and interdependencies between the networks; create regular communications paths between first responders and local businesses (who also have a vested interest in quick recovery and business continuity); provide a venue for sharing ideas and best practices on a non-proprietary basis; explore new crisis management options; and serve as a test bed for exercising current crisis plans.

The focus on terrorism and criminal activity of the original fusion centers is simply too narrow. These centers could serve as a focal point for creating disaster-resistant communities and the bridge between the public and private sectors to meet a spectrum of risks and contingencies.

- **Expand the program of technology test beds, such as the DOE SCADA test bed, that help companies test innovative security solutions and their interface with current operating systems**

The Department of Energy understood that the country and companies alike faced a critical threat in the Internet-accessible systems that controlled the production, generation and transmission of the nation's energy resources.

Unfortunately, the threats were not theoretical. In 1997, a teenager hacked in and remotely disabled part of a public switching network, disrupting phone service to local residents and causing a malfunction at a nearby airport. In 2001, a former employee of a software developer hacked into a sewage plant in Australia, triggering a large sewage discharge. In 2003, the Slammer Worm infiltrated the operations network of a nuclear power plant via a high speed connection from an unsecured contractor's network. Migrating from the business to the operations network, the worm disabled a panel used to monitor the plant's most crucial safety indicators for about 5 hours and caused the plant's process computer to fail.

Rather than regulate a security standard, the DOE created a win-win solution that encouraged market-based solutions. Through its SCADA testbed, DOE created an opportunity for companies to test any glitches between their security software and operating systems in a simulated environment, before actually deploying the software. The ultimate effect of the test bed is to reduce the costs and risks of deploying new, more secure SCADA systems. (See "Government Collaboration Boosts the Nation's Resiliency," next page.)

Education and Training: Change the Culture

- **Establish a Resilience Curriculum Fund under which universities and other education/training providers could apply for competitively**

Government Collaboration Boosts the Nation's Resiliency

Since the mid-1990's, security experts have become increasingly concerned about the threat of malicious cyber-attacks on the vital supervisory control and data acquisition (SCADA) systems used to monitor and manage our energy systems (electricity, oil and natural gas). Most SCADA system designs did not anticipate the security threats posed by today's reliance on common software and operating systems, public telecommunication networks and the Internet. Left unsecured, these energy control systems may be vulnerable to extortionists, hackers, disgruntled employees, and even terrorists. The risks are not just theoretical. The U.S. Government Accountability Office has reported that such attacks could be mounted with a high degree of anonymity and without even setting foot in the country.

Adequately addressing this risk requires the combined efforts of private energy asset owners and operators, commercial control system vendors, and government intelligence and cybersecurity experts. How might such a collaborative effort be launched? Enter the U.S. Department of Energy (DOE). In 2003, the DOE created the National SCADA Test Bed—a national capability to help secure communications and control systems within the energy sector. NSTB's cybersecurity experts at the national laboratories forged agreements with major vendors of control system equipment and set up their systems on a realistic but safe network. They then used the latest cyber-attack tools to aggressively probe the vulnerability of their systems. Based on the results, NSTB provided each vendor with a confidential assessment and mitigation roadmap. While the DOE did not require the vendors to implement the recommendations, all vendors have chosen to act on the NSTB advice for improving system security. The test bed experts followed up by testing each "security fix" to make sure all problems were solved.

Four years later, more than 80 percent of the vendors of control systems in the oil, natural gas, and power industries have taken advantage of the opportunity to secure their systems. Vendors have developed next-generation systems, and utilities are deploying these "hardened" systems in their operations. Every system that goes through the test bed increases security at multiple sites. Each system represents a class of more secure SCADA technology, creating a powerful multiplier effect on energy resilience nationwide.

awarded grants to develop resilience courses and training programs—either stand-alone or embedded in existing curricula

Universities can play a pivotal role in creating new undergraduate and professional education curricula that ensures tomorrow's leaders will be well grounded in the principles of resilience and risk management.

Today, the cross-disciplinary understanding required for resilience is absent from most of the curricula. Business school programs do not emphasize the link between operational risk (often thought of as an engineering problem) and revenues. Engineering schools have embraced the principles of design for quality or safety, but they often lack a design for resilience focus. Security executives typically don't speak the language of finance. Enterprisewide risk management and resilience should be part of the graduate school curricula, and must become a core concept within graduate school curricula in business, engineering and public policy.

- **Stimulate cross-disciplinary synthesis of resilience research.**

The concept of resilience in complex and dynamic systems cuts across multiple disciplines, including many of the sciences, economics, ecology, psychology, sociology and network theory. It is cutting edge to understand how to deal with challenge and change in many types of systems; it is an emerging field that transcends traditional disciplines in the universities. Research programs that model resilience can be responsive to the more practical needs of industry and government, because they create linkages among security, complex interdependencies, crisis management and risk management options. But the same tools can be used to study resilience, robustness and adaptability in other complex systems and environmental ecosystems.

Notes

1 Chad Holliday and Jared Cohon, co-chairs Council on Competitiveness Steering Committee on Competitiveness and Security. First Security and Competitiveness Symposium, October, 2002.

2 Definition adopted from Center for Resilience, The Ohio State University.

3 Deloitte Research. "Disarming the Value Killers." Deloitte, February 2006

4 K.B. Hendricks & V. R. Singhal. "An Empirical Analysis of the Effect of Supply-Chain Disruptions on Long-Run Stock Price Performance and Risk of the Firm." Productions and Operations Management. 14 (2005) 35-52. In FM Global, "The New Supply Chain Challenge: Risk Management in a Global Economy." (April, 2006)

5 Economist Intelligence Unit. "Business Resilience: Ensuring Continuity in a Volatile Environment." The Economist. 2007. Citing a U.S. National Archives study.

6 Gary Hamel and Liisa Valikangas. "The Quest For Resilience." Harvard Business Review. September 2003.

7 Deloitte Research. "The Risk Intelligent Chief Audit Executive." Risk Intelligence Series. Issue No. 5. Deloitte, May 2007.

8 Lawrence Berkley National Laboratory: Kristina Hamachi-LaCommare and Joe Eto. "Understanding the Cost of Power Interruptions to U.S. Electricity Consumers." Berkley: U.S. Department of Energy's Office of Electric Transmission and Distribution.

9 Lisa Vasas. "Some Companies Lose Data Six Times a Year." EWeek. March 7 2007. June 6, 1995. http://www.eweek.com/article2/0,1895,2101683,00.asp

10 Landler and John Markoff. "After Computer Siege in Estonia, War Turns to Cyberspace." New York Times. May 29, 2007, Final, Technology. June 5, 2007. http://www.nytimes.com/2007/05/29/technology/29estonia.html

11 Stephen Spoonamore. Cybrinth:CEO. May 29, 2007.

12 David A. Patterson. "A Simple Way to Estimate the Cost of Downtime." The Proceedings of LISA 2002: Sixteenth Systems Administration Conference. Berkley: Berkley USENIX Association, 2002. Pp. 185-188

13 Peter W. Huber and Robert Litan. The Liability Maze: The Impact of Law on Safety and Innovation. Washington D.C.: Brookings Institution Press, 1991.

14 Philip K. Howard. "Danger!" Chicago: Mckinsey and Company, 2004. June 5, 2007. http://www.mckinsey.com/ideas/wef2004/riskcontrol/PDF/mckinsey_risk_howard.pdf

15 Council on Competitiveness. "Innovate America" Washington D.C.: Council on Competitiveness, 2004.

16 Council on Competitiveness. "Energy Security, Innovation and Sustainability Initiative" Washington D.C.: Council on Competitiveness, May 2007.

17 Daniel Yergin. "Energy's Challenges." Forbes.com. April 23, 2007. June 5, 2007. http://www.forbes.com/opinions/2007/04/23/solutions-energy-yergin-opinion-cx_lm_0423yergin.html

18 CERA Insights. "Carbon Markets: Globally Warming." CERA, April 2007.

19 Congressional Budget Office. "A Potential Influenza Pandemic: Possible Macroeconomic Effects and Policy Issues." Washington D.C.: U.S. Congress, July 2006

20 Deloitte Research. "Year Two Pandemic Preparedness Survey Results." Deloitte, December 2006.

21 Conference Board. CEO Challenge, 2006.

22 Deloitte Research. "In the Dark II" Deloitte, 2007.

23 Lloyd's, In Association with the Economic Intelligence Unit. "Taking Risk On Board." London: Lloyd's, 2006.

24 Neil Davey. "Operational Risk: A Disciplined Approach." First Services Technology. June 5, 2007.

25 Max. H. Bazerman and Michael D. Watkins. Predictable Surprises: The Disasters You Should Have Seen Coming, and How to Prevent Them. Cambridge: Harvard Business School Press, 2004.

26 Hill and Knowlton. "Return on Environment" New York: Hill and Knowlton, April, 2007. June 5, 2007 http://www.greenbiz.com/news/news_third. cfm?NewsID=35038

27 Limited Brands is a sponsor of The Center for Resilience at The Ohio State University, where this case study was developed.

28 http://www.sec.gov/news/extra/y2k/y2klettr.htm

Competitiveness and Security Steering Committee

CO-CHAIRS:

Charles O. Holliday, Jr.
Chairman and CEO
DuPont

Jared Cohon
President
Carnegie Mellon University

DISTINGUISHED FELLOW

Thomas Ridge
Former Secretary U.S. Department of Homeland Security

MEMBERS:

Morton Bahr
Former President
Communications Workers of America

John T. Casteen III
President
University of Virginia

Ruth David
President and CEO
Analytic Services Inc.

John Menzer
Vice Chairman
Wal-Mart Stores, Inc.

John A. Edwardson
Chairman and CEO
CDW Corporation

Shirley Ann Jackson
President
Rensselaer Polytechnic Institute

Douglas McCarron
General President
United Brotherhood of Carpenters & Joiners of America

John Morgridge
Chairman
Cisco Systems, Inc.

Clayton Daniel Mote, Jr.
President
University of Maryland

Kenan Sahin
President and Founder
TIAX, LLC

Andrew L. Stern
President
Service Employees International Union

Paul Yarossi
President
HNTB Companies

William D. Zollars
Chairman, President & CEO
Yellow Roadway Corporation

Competitiveness and Security Advisory Committee

ADVISORY COMMITTEE CO-CHAIRS:

Catherine Allen
Former CEO
BITS Financial Services Roundtable

Robert Moore
Executive Director, Global Security Group
Merck & Co., Inc.

MEMBERS:

Don Anthony
President
Council for Chemical Research

David Barron
AVP, Federal Relations and National Security
BellSouth

Roger Bowers
Vice President, Government Affairs
HNTB Companies

Ed Casey
Director, Corporate Security
Procter and Gamble

Cheryl Charles
Senior Vice President
BITS Financial Services Roundtable

Jerry Cox
Chairman and CEO
Potomac Energy Associates

Alex de Alvarez
Director, Office of Energy Security and Assurance
U.S. Department of Energy

Steven Flynn
Senior Fellow, National Security Studies
Council on Foreign Relations

Mildred Hastbacka
Director
TIAX, LLC

Christopher Heinz
Political and Legislative Director
Brotherhood of Carpenters & Joiners

Michael Hickey
Vice President for Homeland Security
Verizon

Connie Hughes
Commissioner
New Jersey Board of Public Utilities

Mike Kelley
Vice President, Government Affairs
Yellow Roadway Corporation

Henry Kenchington
Program Manager
U.S. Department of Energy

Ben Levitan
President and CEO
EnvoyWorldWide

Timothy McNulty
Special Assistant for Strategic Technology Initiatives
Carnegie Mellon University

Mark P. Mills
Chairman, CTO
ICx Technologies

James B. Porter, Jr.
Vice President, Engineering and Operations
DuPont

Rob Quartel
CEO and Chairman
Freight Desk Technologies

Harvey Rubin
Professor of Medicine, Division of Infectious Diseases
University of Pennsylvania

John Ryan
Director of Corporate Security
Constellation Energy

John Sullivan
Vice President, British Petroleum Group Security
British Petroleum, Plc.

Denise Swink
Formerly Director, Office of Energy Assurance
U.S. Department of Energy

Robert Weber
Director
TIAX, LLC

Margaret Welsh
Senior Vice President
Energetics

Chelsea White, III
IsyE Chair, Transportation and Logistics
Georgia Institute of Technology

Martin Wilhelm
President
M.C. Wilhelm Associates, LLC

About the Committee Leaders

STEERING COMMITTEE CO-CHAIRS

Jared L. Cohon, Ph.D., President, Carnegie Mellon University

Jared L. Cohon became the eighth president of Carnegie Mellon University in July 1997.

During his presidency, Carnegie Mellon has continued along its trajectory of innovation and growth, developing and implementing new and successful efforts in undergraduate education; information technology; biotechnology; the environment; the fine arts and humanities; diversity; and international education. Under Cohon, the university has continued to play a vital role in the economic development of southwest Pennsylvania. In 2001, Cohon shared Pittsburgh Magazine's "Pittsburgher of the Year" honors with Mark Nordenberg, chancellor of the University of Pittsburgh.

Cohon came to Carnegie Mellon from Yale University, where he was dean of the School of Forestry and Environmental Studies and professor of environmental systems analysis from 1992 to 1997. He started his teaching and research career in 1973 at Johns Hopkins, where he was a faculty member in the Department of Geography and Environmental Engineering for 19 years. He also served as Assistant and Associate Dean of Engineering and Vice Provost for Research at Johns Hopkins. Cohon earned a B.S. degree in civil engineering from the University of Pennsylvania in 1969, and a Ph.D. in civil engineering from the Massachusetts Institute of Technology in 1973.

A national authority on environmental and water resource systems analysis, Cohon authored "Multiobjective Programming and Planning," published by Academic Press (1978) and reissued as a "Classic of Operations Research" by Dover Press in 2004. In addition, he has authored, co-authored and edited more than 80 professional publications focusing on this interdisciplinary field that combines engineering, economics and applied mathematics. He has worked on water resource problems in the United States, South America and Asia, and on energy facility siting, including nuclear waste shipping and storage. In addition to his academic experience, he served in 1977 and 1978 as legislative assistant for energy and the environment to Daniel Patrick Moynihan, former U.S. Senator from New York.

President Bill Clinton appointed Cohon to the Nuclear Waste Technical Review Board in 1995 and appointed him as chairman in 1997. His term on the board ended in 2002. President George W. Bush appointed Cohon in 2002 to his Homeland Security Advisory Council. He also was appointed as Chairman of the Council's Senior Advisory Committee on Academia and Policy Research.

Dr. Cohon is a member of the board of directors of Mellon Financial Corporation and American Standard, Inc. He also serves on the boards of several national and local non-profit organizations, including the Health Effects Institute, the Council on Competitiveness, the Carnegie Museums of Pittsburgh, the Pittsburgh Cultural Trust, Pittsburgh Life Sciences Greenhouse, the Technology Collaborative and the Allegheny Conference on Community Development.

Charles O. Holliday, Jr., Chairman and CEO, DuPont

Chad Holliday, Jr., 59, is the chairman of the board and chief executive officer of DuPont. Holliday is the 18th executive to lead the company in more than 200 years of DuPont history. He became CEO on February 1, 1998, and chairman on January 1, 1999.

Holliday has been with DuPont for more than 30 years. He started at DuPont in the summer of 1970 at DuPont's Old Hickory site after receiving a B.S. in Industrial Engineering from the University of Tennessee. He is a licensed professional engineer.

In 2004, he was elected a member of the National Academy of Engineering. He became chairman of the Business Roundtable's Task Force for Environment, Technology and Economy the same year. Holliday also is past chairman of the World Business Council for Sustainable Development (WBCSD), The Business Council and the Society of Chemical Industry—American Section. While chairman of the WBCSD, Holliday co-authored a book "Walking the Talk" which details the business case for sustainable development and corporate responsibility.

Holliday also serves on the board of directors of HCA and is chair of the board of directors of Catalyst. In addition, he is chairman of the U.S. Council on Competitiveness and is a founding member of the International Business Council.

Under Holliday's direction, DuPont established the mission to achieve sustainable growth—increasing shareholder and societal value while decreasing the company's environmental footprint

About our Advisory Committee Leaders

Thomas J. Ridge

Thomas J. Ridge became the nation's first cecretary of the Department of Homeland Security, where he served from January 24, 2003, until February 1, 2005. The creation of the country's 15th Cabinet Department marked the largest reorganization of government since the Truman administration, combining 22 federal agencies with more than 180,000 employees.

Prior to being secretary of homeland security, Ridge served as the first assistant to the president for homeland security from October 8, 2001. Following the tragic events of 9/11, President Bush established the Office of Homeland Security and the Homeland Security Council. The president charged Ridge to develop and coordinate a comprehensive national strategy to strengthen protections against terrorist threats and attacks in the United States.

Before the events of 9/11, Ridge was twice elected governor of Pennsylvania, where he served from 1995 to 2001. Keeping his promise to make Pennsylvania "a leader among states and a competitor among nations," Ridge's aggressive technology strategy helped fuel the state's advances in economic development, education, health care and the environment.

Born and raised in Erie, PA, Ridge graduated from Harvard University in 1967 with honors. After his first year at The Dickinson School of Law, he was drafted into the U.S. Army, where he served as an infantry staff sergeant in Vietnam, earning the Bronze Star for Valor, the Combat Infantry Badge and the Vietnamese Cross of Gallantry. After returning to Pennsylvania, he earned his law degree and was in private practice before becoming assistant district attorney in Erie County.

Ridge was elected to Congress in 1982 as the first enlisted Vietnam combat veteran elected to the U.S. House and was overwhelmingly re-elected five times.

After more than 25 years in public service, Ridge now consults on a range of issues, including security, international relations, economic development, civil institution building, technology, education and other matters that encompass his diverse portfolio. Throughout his public and private sector career, Ridge has received numerous honors, awards and honorary degrees.

Ridge and his wife, Michele, the former executive director of the Erie County Library system, reside in Washington, D.C., and have two children, Lesley and Tommy.

Catherine A. Allen, Chairman and CEO, The Santa Fe Group

For more than 30 years, Catherine A. Allen has been an outstanding leader in technology strategy and financial services, and a luminary in business innovation. Allen has won accolades from industry, government, academia, business groups and the press for her success in fostering innovation, promoting new technologies, and bringing stakeholders together to address common challenges.

Today, Allen is chairman and CEO of The Santa Fe Group, a strategic consulting company based in Santa Fe, NM. Allen established The Santa Fe Group in 1996, which specializes in briefings to C-level executives and boards of directors at financial institutions and other critical infrastructure companies.

As the former and founding CEO of financial services industry consortium BITS, Allen led the organization to its current status as a key industry forum for cutting-edge issues in financial service. During her tenure, Allen worked closely with CEOs, CIOs and executives at the nation's largest financial institutions on critical risk management strategy issues.

Earlier in her career, Allen served in several senior executive positions at Citicorp in the retail, bankcards, and corporate technology divisions. She represented Citibank as founding chair and president of the multi-industry Smart Card Forum.

Allen is a sought-after expert on a range of issues. She sits on the boards of Giesecke & Devrient, Stewart Title Guaranty Company, NBS Technologies, Liquid Machines, LLC, and Hudson Ventures, and is chair of the advisory council for the National Foundation for Credit Counseling.

In May 2005, Allen received an Honorary Doctorate of Humane Letters from the University of Missouri, recognizing her professional achievements in financial services and technology. She is a member of the advisory board of the Belizean Grove, an influential group of women CEOs across the United States.

Robert Moore, Executive Director, Corporate Security, Merck & Co. Inc.

Robert D. (Bob) Moore was appointed Merck's executive director of global security on March 1, 1999. Moore has led the restructuring and development of Merck's worldwide security organization since joining the company. A key element of this restructuring has been the development of the company's anti-counterfeiting strategy to address the increasing risks/threats from these activities.

Prior to employment with Merck, Moore worked with Amoco's Corporate Security Group from 1980–1999. He joined Amoco Corporation (later acquired by BP) following four years in the Cincinnati Division of the Federal Bureau of Investigation (FBI), where he began working after graduating from the University of South Carolina in 1976.

Moore has a Bachelor of Arts in Interdisciplinary Studies from the University of South Carolina (1976, with honors) and has completed course work toward a Master's Degree in public administration. His undergraduate studies focused on criminology, business and the French language.

About the Case Study Leaders

Cheryl Charles, Ph.D.
Cheryl Charles, Senior Vice President at BITS, has been a member of the BITS staff since its founding in 1997. She served as co-lead of the Council's financial services study with Catherine Allen, Founding CEO of BITS. Charles served for four years as chief operating officer of The Santa Fe Group. Prior to her service with both BITS and The Santa Fe Group, she served for 20 years as national director of the two most widely used environment education programs in North America for K-12 educators, Project Learning Tree and Project WILD. Among her many civic contributions, she has served on a variety of non-profit boards. She is author, editor and designer of many publications including books, articles, educational materials, and monographs, and has received numerous awards for her leadership. Her most recent book, co-authored with her husband Bob Samples, is titled "Coming Home: Community, Creativity and Consciousness" (Personhood Press, April 2004). She has been listed for many years in the Marquis Who's Who in America and Who's Who in the West. Charles holds a B.A. from the University of Arizona, an M.A. from Arizona State, and a Ph.D. from the University of Washington.

John Glover, Ph.D.
John D. Glover, D.P.A., is the lead interviewer on the pharmaceutical case study. Glover currently serves as a consultant to the U.S. pharmaceutical industry and certain corporate entities. Glover formerly served as the executive assistant director for administration in the FBI, one of three direct reports to the director of the FBI. Immediately upon retiring from the FBI, Glover assumed the position of vice president of corporate security for the Bristol-Myers Squibb Company, where he refocused the security function and aligned it with the overall corporate objectives. He also was instrumental in creating the Pharmaceutical Security Institute, and industry wide, anti-counterfeiting body, and also has served as co-chairman of the U.S. State Department's Overseas Security Advisory Council.

Mildred Hastbacka, Ph.D.
Mildred Hastbacka, Ph.D., a director with TIAX, LLC, is a member of the TIAX team leading the chemical sector case study. She has more than 20 years of commercial industrial experience in business management, business planning, marketing, commercial development, manufacturing technical support, and product and process research and development at corporate and divisional levels. Her area of technical expertise includes physical chemistry, physical biochemistry, analytical chemistry, rubber and plastics compounding, and polymer rheology. At TIAX, she has led or been a significant contributor to cases involving specialty and commodity chemicals, advanced materials, and polymer process, product, and formulation technologies, as well as new commercial applications of proprietary technologies. TIAX, LLC, is a premier product development and technology based consulting firm operating at the intersection of business and technology. Formerly Arthur D. Little's Technology & Innovation business, TIAX builds upon a rich, century-old heritage of breakthrough innovation.

Martin C. Wilhelm
Martin Wilhelm is managing partner of M.C.Wilhelm Associates in Chicago. M.C.Wilhelm Associates is conducting the Council's electric power, oil, and natural gas case studies. Wilhelm advises senior management at electric utility, banking, and energy exchange clients in North American and European energy markets, focusing on strategy, organization design, risk policy and risk management, financial engineering, energy trading, and electric transmission management. Before co-founding the firm, he worked as an assistant to the chairman of the German Council of Economic Advisors, a research fellow at the MIT Energy Laboratory and Cologne Institute of Energy Economics in Germany. Wilhelm has completed an M.S. in economics at Cologne University in Germany, Ph.D. studies in management science and electrical engineering at MIT and Cologne University, as well as an international management degree at Ecole des Hautes Etudes Commerciales, Paris. He is the author of two books on regulatory economics and power generation and numerous articles and working papers on energy industry issues. Wilhelm is a member of IEEE, the International Association of Energy Economists, the Chicago Committee of the Chicago Council on Foreign Relations and the German Society on Foreign Relations.

CASE STUDY ADVISORS

Donald B. Anthony, Sc.D.
Donald B. Anthony, Sc.D., became president and executive director of the Council for Chemical Research in January 2004 and is providing support for the chemical study. Prior to that, he served as president and CEO of NineSigma, Inc., president of Bailey Controls and ABB Process Automation, vice president of Technology for Bechtel Petroleum and Chemicals, and vice president of R&D for BP America and Standard Oil of Ohio. He also was assistant professor and director of MIT's School of Chemical Engineering Practice. Anthony earned his Sc.D. and S.M. in chemical engineering from MIT. He received his B.S. in chemical engineering from the University of Toledo.

Alan Erera, Ph.D.
Dr. Alan Erera is an assistant professor in the School of Industrial and Systems Engineering at the Georgia Institute of Technology. He received his B.S. Eng. from Princeton University, and his Ph.D. from the University of California, Berkeley, under a Berkeley Fellowship and an Eisenhower Fellowship. Erera has a large, active research program with diverse funding sources, and he currently serves as the associate director of the USDOT-funded Transportation Research Center for Freight, Trade, Security, and Economic Strength. He conducts research on transportation and logistics systems planning and control, with a focus both on innovative modeling and solution methodologies, and on challenging application areas including dynamic and stochastic vehicle routing and scheduling, robust asset management, integrating security and efficiency in logistics systems, and logistics and highway traffic network design. Erera was awarded the 2001 First Prize in the Transportation Science Dissertation Award competition from the Institute for Operations Research and Management Science.

Denise Swink
Denise Swink retired from federal service (2004) after 35 years experience spanning a variety of programs at the U.S. Geological Survey, the U.S. Environmental Protection Agency and the U. S. Department of Energy, and is currently serving as a consultant to private sector and non-profit organizations. At the Department of Energy, Swink held positions as director, Office of Planning and Environment, Office of Fossil Energy; deputy assistant secretary, Office of Industrial Technologies, Office of Energy Efficiency and Renewable Energy; and deputy director and acting director, Office of Energy Assurance. For the last two decades, Swink held management/supervisory positions, and the last decade she was a member of the Senior Executive Service. Swink has worked at the highest levels of government, both nationally and internationally, on topics including: fossil energy technology advancement for extraction, transport and utilization of resources; manufacturing productivity and efficiency with emphasis on technology advancement and adoption; electricity infrastructure development; and safety and reliability of the entire energy infrastructure. To enhance the efficiency and competitiveness of industry, Swink created and led extensive public/private partnerships with state and academic entities to develop strategies promoting innovation, fund and implement plans, and monitor results and effectiveness. As the energy infrastructure is the bedrock infrastructure for the reliability of all other critical infrastructures, Swink has substantial knowledge of interdependencies among infrastructures, such as banking and finance, telecommunications, water systems, agriculture and manufacturing operations. She holds an undergraduate degree in mathematics and Masters Degree in environmental sciences. Swink has been recognized in her career by several industry sponsored awards, the Department of Energy Gold Medal, the U.S Environmental Protection Agency Bronze Award, and the Senior Executive Presidential Rank Award. Swink also is currently senior advisor to the Council on Competitiveness, focusing on building the Business Case for Resilience, much as was done for quality and safety during the past decades.

Chelsea (Chip) C. White III, PhD
Co-leading the study on transportation and logistics, professor Chelsea C. White III is a chaired professor in transportation and logistics in the School of ISyE, Georgia Tech. White is editor-in-chief of the ITS Journal and editor of the IEEE Transactions on Systems, Man and Cybernetics, Part A. He is past president of the IEEE Systems, Man, and Cybernetics Society, president-elect of the ITS Michigan Board of Directors, a member of the ITS World Congress Board of Directors, and a member of the ITS America Coordinating Council. He is a fellow of the IEEE, director of the ITS Research Center, co-director of the Sloan Trucking Project, and director of the EECS ITS Laboratory.

Council Membership

COUNCIL ON COMPETITIVENESS BOARD

Chairman
Charles O. Holliday, Jr.
DuPont

Industry Vice Chairman
John B. Menzer
Wal-Mart Stores, Inc.

University Vice Chairman
G. Wayne Clough
Georgia Institute of Technology

Labor Vice Chairman
Douglas J. McCarron
United Brotherhood of Carpenters and Joiners of America

Chairman Emeritus
F. Duane Ackerman
BellSouth Corporation

President
Deborah L. Wince-Smith

EXECUTIVE COMMITTEE

William R. Brody
Johns Hopkins University

Jean-Lou A. Chameau
California Institute of Technology

Richard T. Clark
Merck & Co. Inc.

Jared L. Cohon
Carnegie Mellon University

John J. DeGioia
Georgetown University

Robert C. Dynes
University of California

John M. Engler
National Association of Manufacturers

Marye Anne Fox
University of California, San Diego

William D. Green
Accenture

James Hagedorn
The Scotts Miracle-Gro Company

Sheryl Handler
Ab Initio

John L. Hennessy
Stanford University

John A. Hillerich IV
Hillerich & Bradsby Co.

Susan Hockfield
Massachusetts Institute of Technology

Shirley Ann Jackson
Rensselaer Polytechnic Institute

D. Michael Langford
Utility Workers of America

Edward J. McElroy
American Federation of Teachers

John P. Morgridge
Cisco Systems, Inc.

Samuel J. Palmisano
IBM Corporation

James M. Phillips
Luminetx Corporation

Michael E. Porter
Harvard University

Luis M. Proenza
The University of Akron

James H. Quigley
Deloitte Touche Tohmatsu

Ian C. Read
Pfizer Inc

Robert L. Reynolds
Fidelity Investments

Patricia F. Russo
Alcatel-Lucent

Kenan Sahin
TIAX LLC

David E. Shaw
D. E. Shaw & Co., Inc.

William L. Walton
Allied Capital Corporation

Lawrence Weber
W2 Group Inc.

Robert J. Zimmer
The University of Chicago

Council Membership

GENERAL MEMBERSHIP

Norman Abrams
University of California, Los Angeles

Michael F. Adams
The University of Georgia

Anthony J. Alexander
FirstEnergy Corp.

Richard A. Anthes
University Corporation for Atmospheric Research

Richard E. Anthony
Synovus Financial Corporation

William F. Ballhaus, Jr.
Aerospace Corporation

Steven A. Ballmer
Microsoft Corporation

Brian M. Barefoot
Babson College

Craig R. Barrett
Intel Corporation

Robert J. Birgeneau
University of California, Berkeley

Lee C. Bollinger
Columbia University

David L. Boren
The University of Oklahoma

Erskine Bowles
The University of North Carolina

Richard H. Brodhead
Duke University

Amber M. Brookman
Brookwood Companies Incorporated

Michael J. Burns
Dana Corporation

George Campbell, Jr.
The Cooper Union for the Advancement of Science and Art

Judith Cardenas
Lansing Community College

Curtis R. Carlson
SRI International

John T. Casteen, III
University of Virginia

Jeff Chapman
Harbinger Technologies Group, Inc.

Roy A. Church
Lorain County Community College

Mary Sue Coleman
University of Michigan

France A. Córdova
University of California, Riverside

Michael M. Crow
Arizona State University

Ruth A. David
Analytic Services, Inc. (ANSER)

Ernest J. Dianastasis
Computer Aid, Inc.

Michael V. Drake
University of California, Irvine

Roger A. Enrico
DreamWorks Animation SKG Inc.

Alice P. Gast
Lehigh University

E. Gordon Gee
Vanderbilt University

Thomas F. George
University of Missouri, St. Louis

James W. Griffith
The Timken Company

Amy Gutmann
University of Pennsylvania

Peter Halpin
World Resources Company

David C. Hardesty, Jr.
West Virginia University

Jack Harding
eSilicon Corporation

Robert Hemenway
The University of Kansas

Adam W. Herbert
Indiana University

Richard Herman
University of Illinois, Urbana Champaign

Karen A. Holbrook
The Ohio State University

Jerry MacArthur Hultin
Polytechnic University

Mark V. Hurd
Hewlett-Packard Company

Jeffrey R. Immelt
General Electric Company

Irwin M. Jacobs
QUALCOMM, Inc.

John I. Jenkins
University of Notre Dame

Martin C. Jischke
Purdue University

Doane Kelly
KLG Consulting

Terri Kelly
W. L. Gore & Associates

Carl F. Kohrt
Battelle Memorial Institute

Raymond R. Kwong
SCRAM Technologies, Inc.

A. G. Lafley
The Procter & Gamble Company

Robert W. Lane
Deere & Company

Lester A. Lefton
Kent State University

Richard I. McCormick
Rutgers, The State University of New Jersey

William A. McDonough
William McDonough + Partners

Richard K. Miller
Franklin W. Olin College of Engineering

James B. Milliken
University of Nebraska

Clayton Daniel Mote, Jr.
University of Maryland

Mark A. Nordenberg
University of Pittsburgh

Edward E. Nusbaum
Grant Thornton LLP

Peter O'Donnell, Jr.
O'Donnell Foundation

James L. Oblinger
North Carolina State University

Thomas F. O'Neill
Sandler O'Neill Partners

James W. Owens
Caterpillar, Inc.

Constantine Papadakis
Drexel University

Antonio M. Perez
Eastman Kodak Company

Krista Peternostro
Pittsburgh Technology Council

Peter G. Peterson
Blackstone Group

Judith Ramaley
Winona State University

John W. Rowe
Exelon Corporation

Michael C. Ruettgers
EMC Corporation

Stephen B. Sample
University of Southern California

Carl J. Schramm
Ewing Marion Kauffman Foundation

Ivan G. Seidenberg
Verizon Communications

Joel Seligman
University of Rochester

Robert N. Shelton
The University of Arizona

Sanford C. Shugart
Valencia Community College

Ruth J. Simmons
Brown University

Lou Anna K. Simon
Michigan State University

Albert J. Simone
Rochester Institute of Technology

John B. Simpson
State University of New York at Buffalo

David J. Skorton
Cornell University

Christine J. Sobek
Waubonsee Community College

Andrew A. Sorenson
University of South Carolina

Graham B. Spanier
The Pennsylvania State University

Susan S. Stautberg
Partner Com Corporation

Charles W. Steger
Virginia Polytechnic Institute and State University

Randall L. Stephenson
AT&T

John D. Stobo
University of Texas Medical Branch

Lydia Waters Thomas
Noblis, Inc.

Lee T. Todd, Jr.
University of Kentucky

Stephen J. Trachtenberg
The George Washington University

Steven L. VanAusdle
Walla Walla Community College

Larry N. Vanderhoef
University of California, Davis

G. Richard Wagoner, Jr.
General Motors

Edie Weiner
Weiner, Edrich, Brown, Inc.

William C. Weldon
Johnson & Johnson

William Weyand
MSC.Software Corporation

Sharon P. Whiteley
ThirdAge Inc.

Jack M. Wilson
The University of Massachusetts

James Wright
Dartmouth College

Mark S. Wrighton
Washington University

Henry T. Yang
University of California, Santa Barbara

Paul A. Yarossi
HNTB Corporation

Nancy L. Zimpher
University of Cincinnati

Steven G. Zylstra
Technomic Growth Strategies

National Affiliates and Council Staff

NATIONAL AFFILIATES

Alliance for Excellent Education

American Association for the Advancement of Science

American Institute for Medical and Biological Engineering Inc.

American Mathematical Society

American Petroleum Institute

American Society for Engineering Education

American Society for Quality

ASME International

Association of American Colleges and Universities

Association of American Universities

Association of University Related Research Parks

AVETeC, Inc.

BITS Financial Services Roundtable

The Conference Board, Inc.

The Consortium for Entrepreneurship Education

Council on Governmental Relations

Delaware Technology Park, Inc.

General Aviation Manufacturers Association

IEEE-USA

Innovation Philadelphia

Innovation Works

Iowa Business Council

JumpStart, Inc

National Association of Manufacturers

National Association of Seed and Venture Funds, Inc.

National Center for Manufacturing Sciences

National Center for Women & Information Technology

NorTech

Nuclear Energy Institute

Oak Ridge Associated Universities

Rothman Institute for Entrepreneurial Studies

SMC3

Technology CEO Council

United Negro College Fund, Inc.

U.S. Council for International Business

University Economic Development Association

COUNCIL STAFF

Deborah L. Wince-Smith
President

C. William Booher, Jr.
Chief Operating Officer

Debra S. van Opstal
Senior Vice President, Programs & Policy

William C. Bates
Vice President, Government Affairs

Chad Evans
Vice President, Strategic Initiatives

Randall T. Kempner
Vice President, Regional Innovation

Mohamed N. Khan
Vice President, Information Technology

Michael J. Meneer
Vice President, Communications

Susan P. Rochford
Vice President, Sustainability Initiatives

Betsy Thurston
Vice President, Strategic Development

Suzanne P. Tichenor
Vice President, High Productivity Computing

Jennifer J. Mateik
Controller

David A. Attis
Senior Director of Policy Studies

Samuel Leiken
Senior Director of Policy Studies

Amanda B. Welch
Program Manager

Mary B. Marchal
Senior Research Associate

Lars-eric Rödén
Senior Research Associate

Marco V. Rodriguez Tapia
Senior Research Associate

Lee Dachi
Membership Manager

Marcy S. Jones
Executive Assistant to the President

Blythe D. Chorn
Research Associate

Kristy L. Hawley
Research Associate

Jennifer Carr
Communications Coordinator

Jorge Lima
International Fellow

COUNCIL FELLOWS

Erich Bloch
Distinguished Fellow

Daniel S. Goldin
Distinguished Fellow

Alan P. Larson
Distinguished Fellow

Thomas J. Ridge
Distinguished Fellow

Ed Donnelly
Senior Fellow

Lisa Guillermin Gable
Senior Fellow

COUNCIL ADVISORS

Jennifer S. Bond
Senior Advisor

Robert B. Graybill
Senior Advisor

COUNCIL INTERNS

Patrick Barry

Lindsay Gund

Kara Jones

Melanie Lum

Brian McNamara

Maura Mondelli

Zachary Rynar

April Volke

About the Council on Competitiveness

WHO WE ARE

The Council's mission is to set an action agenda to drive U.S. competitiveness, productivity and leadership in world markets to raise the standard of living of all Americans.

The Council on Competitiveness is the only group of corporate CEOs, university presidents and labor leaders committed to the future prosperity of all Americans and enhanced U.S. competitiveness in the global economy through the creation of high-value economic activity in the United States.

Council on Competitiveness
1500 K Street, NW
Suite 850
Washington, D.C. 20005
T 202 682 4292
Compete.org

HOW WE OPERATE

The key to U.S. prosperity in a global economy is to develop the most innovative workforce, educational system, and businesses that will maintain the United States' position as the global economic leader.

The Council achieves its mission by:

- Identifying and understanding emerging challenges to competitiveness
- Generating new policy ideas and concepts to shape the competitiveness debate
- Forging public and private partnerships to drive consensus
- Galvanizing action to translate policy into action and change

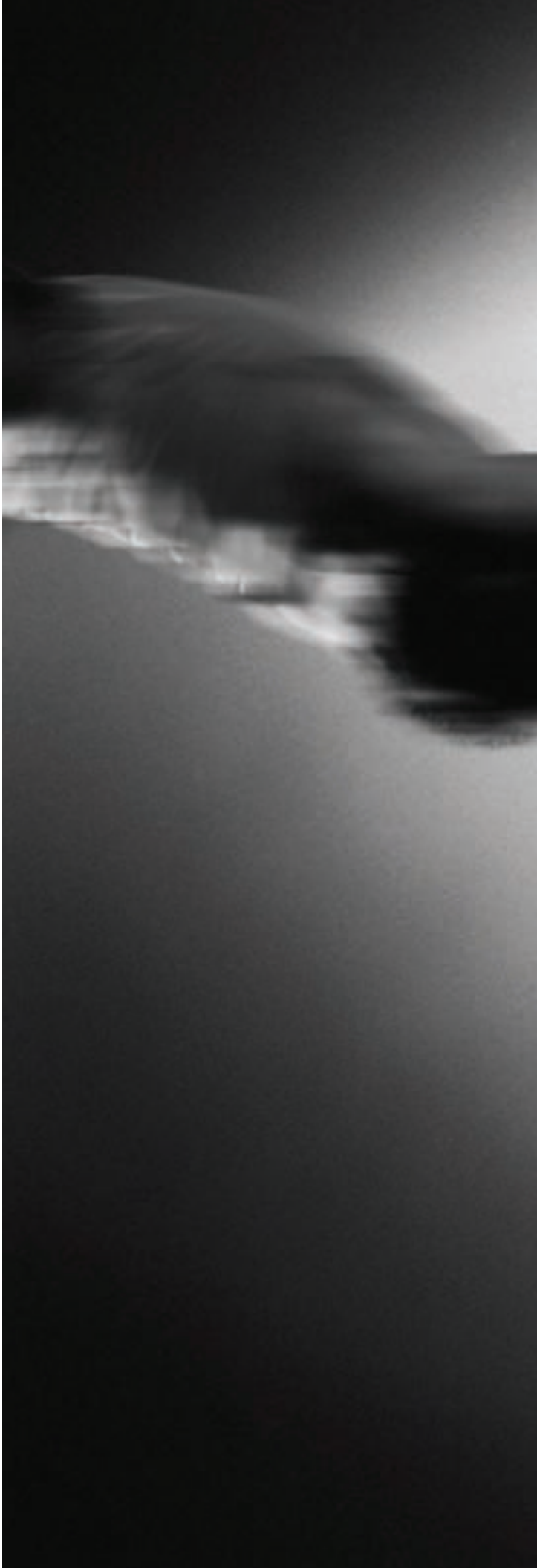
The Council on Competitivness is a non-partisan, non-governmental action tank located in Washington, D.C.

Program Leadership

Deborah L. Wince-Smith is president of the Council on Competitiveness. An internationally recognized expert on science and technology policy, innovation strategy and global competition, Wince-Smith was most recently appointed as a member of the board of directors of the NASDAQ Stock Market and as chairman of the Secretary of Commerce's Strengthening America's Communities Initiative Secretarial Advisory Committee. A senior fellow at the Council since 1993, Wince-Smith served as the first assistant secretary for technology policy in the Department of Commerce Technology Administration from 1989 to 1993.

Debra van Opstal is senior vice president for policy and programs at the Council on Competitiveness and project director of the Enterprise Resilience Initiative. Van Opstal joined the Council as a vice president in 1998 to manage its ongoing work on innovation policy and national competitiveness. She edited *Going Global: The New Shape of American Innovation* and co-authored with Michael Porter of the Harvard Business School the Council's 2001 *Competitiveness Index.* Her most recent article, "Moving Beyond Security: The Resilience Imperative" appeared the May 2006 edition of the Cutter IT Journal.

Mary Marchal is the senior research associate on Enterprise Resilience at the Council on Competitiveness. Before joining the Council she conducted research at the Center for Public Policy and Private Enterprise at the University of Maryland on public-private partnerships and security studies. She holds a master's in public policy from the University of Maryland with a specialization in international security and economic policy and received a B.A. with honors in political science and mathematics from Villanova University.



Council on Competitiveness
1500 K Street NW, Suite 850, Washington, D.C. 20005 T 202 682 4292
Compete.org

Compete.

Council on Competitiveness